Contents

1 MD-100: Windows 10

- **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 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

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.

1.5.2 Windows 10

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

2 Content Directory

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

2.1 Labs

{% assign labs = site.pages | where_exp:"page", "page.url contains '/Instructions/Labs'" %} | Module | Lab | | --- | --- | {% for activity in labs %}| {{ activity.lab.module }} | [{{ activity.lab.title }}{% if activity.lab.type %} - {{ activity.lab.type }}{% endif %}](/home/ll/Azure_clone/Azure_new/MD-100T00-Windows10/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

{% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/MD-100T00-Windows10/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

3 MD-100: Windows 10

3.1 Lab Change Log

This log will be updated whenever updates are made to the lab steps in MD-100. Note that this log only contains changes to the labs. The change log for course content is still located in the Learning Download Center.

3.1.1 Apr 16 2012

- 0601 Corrected step to expand correct partition
- 0301 Path to Labfiles corrected, corrected missing angle bracket in Ex3-Task2
- 1202 Added step to select local download

3.1.2 Feb 12 2021

- All labs have been refreshed
  - New Lab VM Set
  - New VM names (now SEA, instead of LON)
  - See Trainer Prep Guide for details and lab list.
- Clients now using Windows 10 20H2, Servers now on 2019
- MD-100 now has an M365 tenant

3.1.3 Jul 17 2020

- Minor formatting corrections.

3.1.4 May 15 2020

- Minor formatting corrections.

3.1.5 Dec 02 2019

- Minor formatting corrections.

3.1.6 Nov 08 2019

- Minor updates related to compliance and accessibility.

3.1.7 Nov 04 2019

- Initial Release.

4 Practice Lab: Deploying Windows using Windows ADK tools

4.1 Summary

In this lab, you will identify the tools included in the Windows ADK, create bootable Windows PE media, prepare a Windows 10 computer to be imaged, capture a reference Windows 10 image, and deploy a captured Windows 10 image.

4.1.1 Scenario

As part of the Desktop Administration team at Contoso, you have been tasked with creating and testing a Windows 10 image to be used for a future Windows 10 desktop deployment project. You have already used Hyper-V to create a virtual machine named GoldImage1 and installed Windows 10 to be used as the reference image. You now need to capture GoldImage1 and validate that the image can be deployed to a new computer.

4.1.2 Task 1: Identify the Windows ADK tools

1. Sign in to SEA-SVR2 as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Start** and then select **Control Panel**.
3. Select **Programs**, and then select **Programs and Features**. Notice that the **Windows Assessment and Deployment Kit - Windows 10** and the **Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10** programs are installed.
4. Select **Windows Assessment and Deployment Kit - Windows 10** and then select **Change**.
5. On the **Maintain your Windows Assessment and Deployment Kit - Windows 10 features** page, ensure that **Change** is selected and then select **Next**.
6. Notice the features that have been installed on SEA-SVR2. Features include:
   - Deployment Tools
   - Imaging and Configuration Designer (ICD)
   - Configuration Designer
   - User State Migration Tool (USMT)
   - Microsoft User Experience Virtualization (UE-V) Template
7. Select **Cancel** to close the wizard. Select **Yes** and then select **Close**.
8. Close the **Programs and Features** window.

4.1.3 Task 2: Create bootable Windows PE media

1. On SEA-SVR2, select **Start**, expand **Windows Kits**, and then select **Deployment and Imaging Tools Environment**.

2. At the command prompt type `copype amd64 E:\WinPE`. The Windows PE working files are installed to the target location.

3. Open **File Explorer** and then browse to **E:\WinPE**.

4. In the **WinPE** folder, select the **media** folder and then select the **sources** folder. Notice the **boot.wim** file located in this folder. This is the boot image that is used for a default configuration of Windows PE.

5. Close **File Explorer**.

6. At the command prompt type the following command to create the Windows PE media in ISO format:

```
MakeWinPEMedia /ISO E:\WinPE E:\WinPE\WindowsPE_amd64.iso
```

7. Open **File Explorer** and then browse to **E:\WinPE**. Notice the **WindowsPE__amd64.iso** file located in this folder. This ISO file will be used to boot an Windows 10 installation to be captured as a gold image.
8. Close **File Explorer**.

4.1.4 Task 3: Prepare a Windows 10 computer to be imaged

1. On SEA-SVR2, on the taskbar, select **Hyper-V Manager**.
2. In Hyper-V Manager, select **SEA-SVR2** and then under **Virtual Machines** select **GoldImage1**.
3. From the **Action** menu, select **Checkpoint**. A checkpoint is created as shown in the **Checkpoints** pane.
4. From the **Action** menu, select **Connect**, and then select **Start**. After the virtual machine starts, maximize the **GoldImage1 on SEA-SVR2 - Virtual Machine Connection** window.
5. Sign in to **GoldImage1** as **Admin** with the password of **Pa55w.rd**.
6. Select the **Start** button, type **command**, and then select **Run as administrator**. At the User Account Control, select **Yes** to open the command prompt with administrative credentials.
7. At the command prompt, ensure that you are at **C:\Windows\System32**, and then type the following command and then press Enter:

```
cd sysprep
```

8. At the **C:\Windows\System32\Sysprep** prompt, type the following command and then press Enter:

```
sysprep
```

9. At the **System Preparation Tool 3.1.4** dialog box, ensure that **System Cleanup Action** shows **Enter System Out-of-Box Experience (OOBE)** and then select the check box next to **Generalize**.
10. Under **Shutdown Options**, select **Shutdown**.
11. Select **OK**. Sysprep generalizes the virtual machine and then shuts down the operating system. This will take a few minutes to complete.

4.1.5 Task 4: Capture a reference Windows 10 image

1. If necessary, restore the **GoldImage1 on SEA-SVR2 - Virtual Machine Connection** window.
2. From the **GoldImage1 on SEA-SVR2 - Virtual Machine Connection** window, select **Media**, point to **DVD Drive** and then select **Insert Disk**.
3. Browse to **E:\WinPE**, select **WindowsPE__amd64.iso**, and then select **Open**. You have attached the Windows PE boot disk to the virtual machine.
4. In the GoldImage1 window, from the **Action** menu, select **Start**.
5. As the computer starts, click in the GoldImage1 window and continually press the spacebar to boot from the CD. After the virtual machine starts, maximize the **GoldImage1 on SEA-SVR2 - Virtual Machine Connection** window. Note: If you miss the option to boot from the CD, revert GoldImage1 and redo Task 3.
6. At the command prompt type the following command to configure IP settings for Windows PE:

   ```
   netsh int ipv4 set address "Ethernet" static 10.10.0.11 255.255.255.0
   ```

7. At the command prompt type the following command to map a network location for the image:

   ```
   net use z: \\10.10.0.10\Captures /user:Contoso\Administrator Pa55w.rd
   ```

   The Z drive maps to the Captures shared folder on SEA-SVR2.

8. At the command prompt type the following command to capture the image of the GoldImage1 reference computer:

   ```
   dism /Capture-Image /ImageFile:z:\GoldImage.wim /CaptureDir:d:\ /name:"GoldImage"
   ```

It will take approximately 15 minutes for the image capture to complete. Continue with the next task while the image capture progresses.

4.1.6 Task 5: Deploy a captured Windows 10 image

1. In Hyper-V Manager, select **SEA-SVR2** and then in the Actions pane, select **New** and then select **Virtual Machine**.
2. On the **Before you Begin** page, select **Next**.
3. On the **Specify Name and Location** page, in the **Name** box type **Computer1**.
4. Select the check box next to **Store the virtual machine in a different location** and then next to **Location** type **E:\Labfiles\VirtualMachines**. Select **Next**.
5. On the **Specify Generation** page, ensure that **Generation 1** is selected and then select **Next**.
6. On the **Assign Memory** page, next to **Startup memory** type **8192** and then select **Next**.
7. On the **Configure Networking** page, next to **Connection**, select **Internal Network** and then select **Next**.
8. On the **Connect Virtual Hard Disk** page, select **Create a virtual hard disk** and enter the following and then click **Next**:
   - Name: Computer1.vhdx
   - Location: E:\Labfiles\VirtualMachines
   - Size: 60 GB
9. On the Installation Options page, select **Install an operating system from a bootable CD/DVD-ROM** and configure the following:
   - Image file (.iso): E:\WinPE\WindowsPE_amd64.iso
10. Select **Next** and then **Finish**.
11. Restore the GoldImage1 window and verify that the image capture task is complete. When it is complete, close the GoldImage1 window.
12. In Hyper-V Manager, select **SEA-SVR2** and then under **Virtual Machines** select **GoldImage1**.
13. From the **Action** menu, select **Revert** and then in the message box, select **Revert**. GoldImage1 is reverted back to its state prior to performing sysprep.
14. In Hyper-V Manager, select **SEA-SVR2** and then under **Virtual Machines** select **Computer1**.
15. From the **Action** menu, select **Connect** and then in the Computer1 window, from the **Action** menu, select **Start**. Maximize the Computer1 window.
16. At the command prompt type the following command to configure IP settings for Windows PE:

    ```
    netsh int ipv4 set address "Ethernet" static 10.10.0.11 255.255.255.0
    ```

17. At the command prompt type the following command to map a network location for the image:

    ```
    net use z: \\10.10.0.10\Captures /user:Contoso\Administrator Pa55w.rd
    ```

    The Z drive maps to the Captures share on SEA-SVR2.

18. At the command prompt type the following commands in order to configure the hard disk on Computer1:

    ```
    Diskpart

    List disk

    Select disk 0

    Clean

    Create partition primary size=100

    Select partition

    Format fs=ntfs quick label=system

    Assign letter=f
    ```

```
Active

Create partition primary

Select partition 2

Format fs=ntfs quick label=windows

Assign letter=g

Exit
```

19. At the command prompt type the following command to apply the gold image to Computer1:

    ```
    Dism /apply-image /imagefile:Z:\GoldImage.wim /index:1 /ApplyDir:G:\
    ```

20. At the command prompt type the following commands to apply the boot record to the system partition:

    ```
    F:

    bcdboot G:\Windows
    ```

21. Restore the Computer1 window and then from the **Acton** menu, select **Reset**. In the message box, select **Reset**. Computer1 restarts. It will take several minutes for the computer to initialize, and will restart.

22. After Computer1 initializes, complete the following setup tasks:

    - Region: United States
    - Keyboard layout: US
    - Second keyboard: Skip
    - Connect to a network: I don't have internet
    - Connect to the internet: Continue with limited setup
    - License Agreement: Accept

23. On the **Who's going to use this PC**, enter **LocalAdmin** and then select **Next**.

24. On the password and confirm password pages, enter **Pa55w.rd** and then select **Next**.

25. On the security questions page, select and provide answers to three security questions.

26. On the privacy settings page, select **Accept**.

27. On the **Do more across devices with activity history** page, select **Yes**.

28. On the Cortana page, select **Not now**.

29. After the computer signs in, select **Start** and then enter **Control Panel**. Select **Control Panel**.

30. In the Control Panel, select **View network status and tasks**.

31. Select **Change adapter settings** and then configure the Ethernet adapter TCP/IPv4 settings as follows:

    - IP address: 10.10.0.12
    - Subnet mask: 255.255.255.0

32. Right-click the **Start** button and then select **System**.

33. In the **About** page, select **Rename this PC**.

34. In the **Rename this PC** dialog box, enter **Computer1** and then select **Next**.

35. Select **Restart later**.

36. Shut down Computer1.

37. On SEA-SVR2, leave Hyper-V Manager open for the next practice lab.

Results: After finishing this lab, you will have successfully prepared and captured a Windows 10 reference computer and deployed a Windows 10 image.

END OF LAB

5 Practice Lab: Migrating user state using USMT

5.1 Summary

In this lab you will learn how to migrate user state from one computer to another using the User State Migration Tool (USMT).

5.1.1 Scenario

You have deployed a new Windows 10 computer named Computer1. You need to migrate the user state from a source computer named Win81Source to Computer1. The best way to do so is using the User State Migration Tool (USMT). The USMT install files are located at \\SEA-SVR2\Labfiles\Install\USMT. A location to store migration data has been provided at \\SEA-SVR2\Labfiles\Install\MigrationStore. For this lab, you will use the IP address 10.10.0.10 to reference SEA-SVR2.

5.1.2 Task 1: Prepare the source computer

1. Sign in to SEA-SVR2 as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On SEA-SVR2, on the taskbar, select **Hyper-V Manager**.
3. In Hyper-V Manager, select **SEA-SVR2** and then under **Virtual Machines** select **Win81Source**.
4. From the **Action** menu, select **Connect**, and then select **Start**. After the virtual machine starts, maximize the **Win81Source on SEA-SVR2 - Virtual Machine Connection** window.
5. Sign in to **Win81Source** as **Admin** with the password of **Pa55w.rd**.
6. Right-click the **desktop**, hover over the **New** menu item, and then select **Text Document**. Type **Demofile** and press **Enter**.
7. Double-click **Demofile.txt** and type some random text and then save the file. There should be several items on the desktop including DemoFile.txt and various desktop icons.
8. On the desktop, right-click **This PC** and then select **Manage**.
9. Expand **Local Users and Groups**, and then select **Users**. Notice the local accounts including Admin, LocalUser1 and LocalUser2.
10. Close **Computer Management**.
11. Right-click **Start** and then select **Command Prompt (Admin)** . In the **User Account Control** window select **Yes**.
12. At the command prompt, type the following command, and then press **Enter**:

```
Net Use F: \\10.10.0.10\Labfiles\Install\USMT /user:Contoso\Administrator Pa55w.rd
```

6. At the command prompt, type **F:**, and then press **Enter**.

7. At the command prompt, type the following, and then press **Enter**:

```
Scanstate \\10.10.0.10\Labfiles\Install\MigrationStore\Win81 /i:migapp.xml /i:miguser.xml /o
```

***Note**: This will take several minutes to complete.*

8. Close all open windows and then shut down Win81Source.

5.1.3 Task 2: Complete the migration

1. On SEA-SVR2, on the taskbar, select **Hyper-V Manager**.

2. In Hyper-V Manager, select **SEA-SVR2** and then under **Virtual Machines** select **Computer1**.

3. From the **Action** menu, select **Connect**, and then select **Start**. After the virtual machine starts, maximize the **Computer1 on SEA-SVR2 - Virtual Machine Connection** window.

4. Sign in to **Computer1** as **Admin** with the password of **Pa55w.rd**.

   Notice that the desktop icons are not visible and there is no Demofile.txt file on the desktop.

5. Right-click **Start** and then select **Computer Management**.

6. Expand Local Users and Groups, and then select Users.

   Notice that LocalUser1 and LocalUser2 are not listed.

7. Select **Start** and type **cmd**. Select **Run as administrator**. In the **User Account Control** window select **Yes**.

8. At the command prompt, type the following command, and then press **Enter**:

```
Net Use F: \\10.10.0.10\Labfiles\Install\USMT /user:Contoso\Administrator Pa55w.rd
```

9. At the command prompt, type **F:**, and then press **Enter**.
10. At the command prompt, type the following, and then press **Enter**:

```
Loadstate \\10.10.0.10\Labfiles\Install\MigrationStore\Win81 /i:migapp.xml /i:miguser.xml /lac:Pa55w.rd
```

11. Type **exit** to close the command prompt.
12. Restore **Computer Management** and refresh the **Users** folder. Notice that LocalUser1 and LocalUser2 are both available.
13. At the Protected Content Migration notice, select **Cancel**.

    Notice the desktop icons and the DemoFile.txt file migrated from the old computer.

14. Shut down Computer1.
15. On SEA-SVR2, close Hyper-V Manager.

END OF LAB

6 Practice Lab: Managing Local User and Microsoft Account Authentication

6.1 Summary

In this lab you will configure and manage local accounts and assign a Microsoft account to a Windows 10 device.

6.1.1 Scenario

You need to create two new local user accounts on SEA-WS1. User1 will be a local administrator and User2 will be a standard user. User1 will also assign a Microsoft account to SEA-WS1 and configure Windows Hello with a PIN.

Note: To complete Task 2, you need to have a Microsoft account to add to SEA-WS1. You can create a free Microsoft account at https://outlook.live.com. Your instructor can guide you on how to create an account if required.

6.1.2 Task 1: Configure and manage local accounts

1. Sign in to **SEA-WS1** as **Admin** with the password **Pa55w.rd**.
2. Select **Start**, and then select **Settings**.
3. In the **Windows Settings** page, select **Accounts**.
4. In the Navigation pane, select **Family & other users**.
5. In the **Other users** section, select **Add someone else to this PC**.
6. On the **Microsoft account** dialog box, select **I don't have this person's sign-in information**.
7. On the **Create account** dialog box, select **Add a user without a Microsoft account**.
8. On the **Create a user for this PC** page, in the **User name** box, enter **User1**.
9. In the **Enter password** and **Re-enter password** boxes, enter **Pa55w.rd**.
10. Select three security questions, provide appropriate answers and then select **Next**. The User1 local account is created and listed under **Other users**.
11. Select **User1** and then select **Change account type**.
12. In the **Change account type** dialog box, select the drop-down menu and then select **Administrator**.
13. Select **OK** to return to the **Family & other users** page. Notice that User1 is now listed as an Administrator.
14. Right-click the **Start** button and select **Computer Management**.
15. Under **System Tools**, expand **Local Users and Groups**.
16. Select the **Users** node. Notice that User1 is listed along with other local accounts. Accounts with an arrow pointing downwards are disabled accounts.
17. Right-click **User1**. Notice the **Set Password** command, used to set a new password for the account.
18. Select **Properties**.
19. Select the **Member Of** tab and take note of the default group memberships. Notice that User1 is a member of the **Administrators** group as configured previously.
20. Select **OK** to close the **User1 Properties**.

21. Right-click the **Users** node and then select **New User**.
22. In the **New User** dialog box, enter the following and then select **Create**:
    - User name: User2
    - Password: Pa55w.rd
    - User must change password at next logon: not selected
23. Select **Close** to close the **New User** dialog box. Notice that User2 is now included in the list of users.
24. Sign out of SEA-WS1.
25. Sign in to SEA-WS1 as **User1** with the password of **Pa55w.rd**. Notice that it takes several minutes for the user profile to be created.
26. At the **Choose privacy settings for your device** page, select **Accept**. The Windows 10 desktop displays.
27. On the taskbar, select **File Explorer**.
28. In **File Explorer**, browse to **C:\Users**. Take note of the user profiles that have been created on this device.
29. Double-click **User1** to display the profile content and folders.
30. Close **File Explorer**.

6.1.3 Task 2: Configure a Microsoft Account on Windows 10

1. Verify that you are signed in to SEA-WS1 as **User1** with the password of **Pa55w.rd**.
2. Select **Start** and then select **Settings**.
3. In the **Windows Settings** page, select **Accounts**.
4. On the **Accounts** page, select **Your info**. Notice that User1 is currently signed in as a Local Account.
5. Select the link that states **Sign in with a Microsoft account instead**.
6. In the **Microsoft account Sign in** page, enter your Microsoft account email address and then select **Next**.
7. On the **Enter password** page, enter your Microsoft account password and then select **Sign in**.
8. If a **Help us protect your account** dialog box appears, select **Skip for now**.
9. In the **Sign into this computer using your Microsoft account** page, enter **Pa55w.rd** and then select **Next**.
10. On the **Create a PIN** page, select **Next**.
11. In the **Set up a PIN** dialog box, enter **1029** in both the **New PIN** and **Confirm PIN** boxes. Select **OK**. Notice that your Microsoft account is now listed on the Your info page.
12. Sign out of SEA-WS1.
13. From the Sign-in page, select your Microsoft account and enter **1029** for the PIN. Your account signs in to the desktop.

6.1.4 Task 3: Remove a Microsoft Account on Windows 10

1. Verify that you are signed in to SEA-WS1 with your Microsoft account.
2. Select **Start** and then select **Settings**.
3. In the **Windows Settings** page, select **Accounts**.
4. On the **Accounts** page, select **Your info**. Notice that User1 is currently signed in with your Microsoft account.
5. Select the link that states **Sign in with a local account instead**.
6. In the **Are you sure you want to switch to a local account** page, select **Next**.
7. On Windows Security page, enter **1029** for your PIN.
8. In the Enter your local account info page, configure the following and then select **Next**:
    - User Name: User1
    - New password: Pa55w.rd
    - Confirm password: Pa55w.rd
    - Password hint: default
9. Select **Sign out and finish**.

Results: After completing this exercise you have successfully configured and managed local accounts and assigned a Microsoft account to a Windows 10 device.

END OF LAB

7 Practice Lab: Managing Domain Authentication

7.1 Summary

In this lab you will join a device to a Windows Active Directory domain.

7.1.1 Scenario

You need to join SEA-WS1 to the Contoso.com domain. This will enable central management of the device and enable users to sign in using their domain credentials.

7.1.2 Task 1: Join a device to an Active Directory domain

1. Sign in to SEA-WS1 as **Admin** with the password **Pa55w.rd**.
2. Select **Start**, and then select the **Settings** icon.
3. In **Settings**, select **Accounts**.
4. Select **Access work or school**.
5. On the **Access work or school** page, select **Connect**.
6. Select **Join this device to a local Active Directory domain**.
7. On the **Join a domain** prompt, type **Contoso** and select **Next**.
8. Type as User name **Contoso\Administrator**, type as Password **Pa55w.rd**, and then select **OK**.
9. In the **Add an account** dialog box, under User account, enter **Ben**.
10. Under **Account type**, ensure that **Standard User** is selected and then select **Next**.
11. Select **Restart now**.

7.1.3 Task 2: Verify that the device is joined properly

1. Sign in to **SEA-WS1** as **Contoso\Ben** with the password **Pa55w.rd**. It will take several minutes for the profile to be provisioned on SEA-WS1.
2. Select **Start**, and then select the **Settings** icon.
3. In **Settings**, select **Accounts**.
4. Select **Access work or school**. Notice that the device is connected to Contoso AD domain.
5. From the taskbar, open **File Explorer**.
6. Right-click This PC and then select **Properties**.
7. On the **System** page, take note of the **Computer name, domain, and workgroup settings**. The Domain shows Contoso.com.
8. Close the System and File Explorer windows.
9. Right-click the **Start** button and then select **Computer Management**.
10. Expand **Local Users and Groups**, and then select **Users**. Notice that Ben is not added to the local users list because Ben is a domain account.
11. Select the **Groups** node.
12. Double-click the **Users** group. Notice the Contoso\Ben is added to the local Users group. This allows Ben to sign in to the device. Select **Cancel**.
13. Double-click the **Administrators** group. Notice that Ben is not a local administrator. However, the Contoso\Domain Admins Active Directory group is added as a local administrator. Any user that is a member of the Contoso\Domain Admins group will be a local administrator on this device. Select **Cancel**.
14. Sign out of SEA-WS1.

Results: After completing this exercise you have successfully joined a device to a Windows Active Directory domain.

END OF LAB

8 Practice Lab: Managing password and account options

8.1 Summary

In this lab you will learn how to create and manage domain password policies, account options, and User Account Control.

8.2 Exercise 1: Managing Domain Password Policies

8.2.1 Scenario

You have been delegated the task to configure the domain password policy for Contoso.com. Part of your task is to implement a new security requirement that specifies a longer password and a 20 minute account lockout if a user incorrectly enters their password more than twice in succession.

Note: You will use SEA-SVR1 which includes all Windows Administrative Tools for remotely managing SEA-DC1 and to perform Active Directory management tasks.

8.2.2 Task 1: Configure password and account options

1. Sign in in to SEA-SVR1 as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Click **Start** and then select **Server Manager**.
3. Select **Tools** and then select **Group Policy Management.**
4. In the Group Policy Management console, expand **Forest:Contoso.com\Domains\Contoso.com**, and then select the **Group Policy Objects** node.
5. In the **Group Policy Objects in Contoso.com** window, right-click the **Default Domain Policy** policy, and then select **Edit**.
6. In the Group Policy Management Editor, expand the **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies** node, and then select **Password Policy.**
7. In the list of policies, double-click the **Minimum password length** policy.
8. On the **Minimum password length Properties** page, set the **Password must be at least** value to **12** characters, and then select **OK**.
9. In the console tree, select the **Account Lockout Policy** node.
10. Double-click the **Account lockout duration** policy.
11. In the **Account Lockout Duration Properties** dialog box, select **Define this policy setting**, and then set the **Account is locked out for** value to **20** minutes. Select **OK**.
12. In the **Suggested Value Changes** dialog box, select **OK**.
13. Double-click the **Account lockout threshold** policy.
14. In the **Account lockout threshold Properties** dialog box, set the **Account will lock out after** setting to **2** invalid logon attempts, and then select **OK**.
15. Close the Group Policy Management Editor.
16. Close the Group Policy Management console.
17. In Server Manager, in the **Tools** list, select **Active Directory Users and Computers**.
18. Expand the **Contoso.com** node, and then select the **IT** OU.
19. Right-click the **Jane Dow** user account, and then select **Properties**.
20. In the **Jane Dow Properties** dialog box, select the **Account** tab.
21. In the list of **Account Options**, clear the **Password never expires** check box, and then select the **User must change password at next logon** check box. select **OK**.

8.2.3 Task 2: Refresh GPOs

1. On LON-DC1, right-click **Start**, and then select **Windows PowerShell (Admin)**.
2. In the Administrator: Windows PowerShell window, type the following command, and then press **Enter**:

```
Invoke-Gpupdate -force
```

3. Close the **Active Directory Users and Computers** and the **Windows PowerShell** window.

Results: After completing this exercise you created a password policy that will affect the password settings for all domain users.

8.3 Exercise 2: Testing Password Policy Settings

8.3.1 Scenario

After configuring a more strict set of password policies you will then ask Jane Dow to test the policy settings.

8.3.2 Task 1: Verify password settings

1. Switch to **SEA-CL1** and sign in as **Contoso\Jane** with the password **Pa55w.rd**.

2. When the message appears that indicates the user's password must be changed before signing in, select **OK**.
3. In the New password box and the Confirm password box, type **Pa55w.rd12**, and then press **Enter**.
4. When the message displays that indicates that the new password does not meet the length, complexity, or history requirements of the domain, select **OK**. Type the old password, **Pa55w.rd**.
5. In the New password box and the Confirm password box, type **Pa55w.rd1234**, and then press **Enter**.
6. When a message displays that indicates that the password has been changed, select **OK**.
7. Sign out of **SEA-CL1**.

8.3.3 Task 2: Attempt repeated sign-ins

1. Attempt to sign in to **SEA-CL1** as **Contoso\Jane** with the incorrect password **password1**.
2. When a message displays that indicates that the password is incorrect, select **OK**.
3. Attempt again to sign in to **SEA-CL1** as **Contoso\Jane** with the incorrect password **password1**.
4. When a message displays that indicates that the password is incorrect, select **OK**.
5. Attempt again to sign in to **SEA-CL1** as **Contoso\Jane** with the incorrect password **password1**.
6. When the message displays that indicates that the referenced account is locked out, select **OK**.

8.3.4 Task 3: Unlock a locked account

1. Sign in in to SEA-SVR1 as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Click **Start** and then select **Server Manager**.
3. In Server Manager, in the **Tools** list, select **Active Directory Users and Computers**.
4. Expand the **Contoso.com** node, and then select the **IT** OU.
5. Right-click the **Jane Dow** user account, and then select **Properties**.
6. In the **Jane Dow Properties** dialog box, select the **Account** tab.
7. Select the check box next to **Unlock account**. **This account is currently locked out on this Active Directory Domain Controller**.
8. Select **OK** to close the **Jane Dow Properties** box.
9. Close **Active Directory Users and Computers**.

Results: After completing this exercise you verified that the password policy works as expected.

8.4 Exercise 3: Configuring UAC

8.4.1 Scenario

You need to configure UAC so that when the UAC dialog box prompts a standard user, he or she can enter the credentials of an administrator account to gain elevated privileges. You also need to restrict the execution of unsigned applications.

8.4.2 Task 1: Modify UAC prompts

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. In the **Type here to search** box on the taskbar, type **gpedit.msc**, and then press Enter.
3. In the Local Group Policy Editor, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then select **Security Options**.
4. In the results pane, double-click **User Account Control: Behavior of the elevation prompt for standard users**.
5. In the **User Account Control: Behavior of the elevation prompt for standard users** dialog box, select the **Prompt for credentials** drop down list, select **Prompt for credentials on the secure desktop**, and then select **OK**.
6. In the results pane, double-click **User Account Control: Only elevate executables that are signed and validated**.

7. In the **User Account Control: Only elevate executables that are signed and validated** dialog box, select **Enabled**, and then select **OK**.
8. In the results pane, double-click **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**.
9. In the **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** dialog box, select the **Prompt for consent for non-Windows binaries** drop down list, select **Prompt for consent on the secure desktop**, and then select **OK**.
10. Close the Local Group Policy Editor.
11. Sign out of **SEA-CL1**.

8.4.3 Task 2: Test the UAC prompts as a standard user

1. Sign in to **SEA-CL1** as **Contoso\Jon** with the password **Pa55w.rd**.
2. Right-click **Start**, and then select **Windows PowerShell (Admin)**.

   Note: *The Windows operating system displays the User Account Control prompt.*
3. In the **User name** box, type **Administrator**, and in the **Password** box, type **Pa55w.rd**, and then select **Yes**.
4. Close the Windows PowerShell prompt.
5. Sign out of **SEA-CL1**.

8.4.4 Task 3: Verify the UAC notifications as an administrator

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. In the **Type here to search** box on the taskbar, type **Control Panel**, and then press Enter.
3. In Control Panel, select **System and Security**.
4. In **System and Maintenance**, select **Change User Account Control settings**.
5. Verify that the slider is configured for **Always notify**.
6. Select **Cancel**.
7. Close all open windows and sign out of SEA-CL1.

Results: After completing this exercise you have configured the prompt behavior of UAC.

END OF LAB

9 Practice Lab: Managing Azure AD Authentication

9.1 Summary

In this lab you will create a new user and then join a Windows 10 device to an Azure AD tenant.

9.1.1 Scenario

You have a new Windows 10 device that you would like to join to your Azure AD tenant. You will create a new Azure AD user account for User2 and then join SEA-WS3 to Azure AD.

Note: To complete this lab, you need to use the Azure AD tenant information as provide by your instructor. You will also need to use a mobile phone for receiving a text message to finish the Azure AD join procedures as listed in Task 2.

9.1.2 Task 1: Create a new user account in Azure AD

1. Sign in to SEA-CL1 as **Contoso\Administrator** with the password **Pa55w.rd**.
2. On the taskbar, select **Microsoft Edge**.
3. In the address bar, enter http://portal.azure.com.
4. In the **Sign in** dialog box, enter your admin email address as provided by your instructor. It should be in the form of admin@M365xXXXXXX.onmicrosoft.com and then select **Next**.

5. At the **Enter password** dialog box, enter the password as provided by your instructor. When prompted to save the password, select **Yes**.
6. When prompted to **Stay signed in**, select **Yes**.
7. If you receive a recommendations prompt, close the window.
8. On the **Welcome to Azure** page, under **Manage Azure Active Directory**, select **View**.
9. In the navigation pane, under **Manage**, select **Users**.
10. On the **All users** page, select **New user**.
11. On the **New user** page, ensure that **Create user** is selected and then enter the following:
    - User name: User2
    - Name: User2
    - Password: Select Let me create the password and then enter **Pa55w.rd**.
12. Select **Create**.
13. Verify that User2 is listed as a member of the Azure AD tenant.

9.1.3 Task 2: Join a Windows 10 device to an Azure AD tenant

1. Switch to SEA-WS3.
2. Sign in to **SEA-WS3** as **Admin** with the password **Pa55w.rd**.
3. Select **Start**, and then select the **Settings** icon.
4. In **Settings**, select **Accounts**.
5. Select **Access work or school** and then select **Connect**.
6. In the **Set up a work or school account** page, under **Alternate actions** select **Join this device to Azure Active Directory**.
7. On the **Sign in** page, enter User2@M365xXXXXXX.onmicrosoft.com (where the email address represents your tenant reference).
8. On the **Enter password** page, enter **Pa55w.rd** and then select **Sign in**.
9. On the **Update your password** page enter the following and then select **Sign in**:
    - Current password: Pa55w.rd
    - New password: Pa55w.rd1234
    - Confirm password: Pa55w.rd1234
10. On the **Make sure this is your organization** page, verify the tenant name and user name and then select **Join**.
11. On the **You're all set** page, select **Done**.
12. Sign out of SEA-WS3.
13. Sign in to SEA-WS3 as User2@M365xXXXXXX.onmicrosoft.com (where the email address represents your tenant reference) with the password of **Pa55w.rd1234**. A new profile is created for User2.
14. At the **Use Windows Hello with your account** page, select **OK**.
15. At the **More information required** page, select **Next**.
16. On the **Keep your account secure** page, select **I want to set up a different method**.
17. On the **Choose a different method** page, select **Phone** and then select **Confirm**.
18. On the **Keep your account secure** page, enter your mobile phone number and then select **Next**.
19. On the **Phone** page, enter the six digit verification code that is sent to your mobile phone and then select **Next**.
20. On the **Phone verification** page, select **Next**.
21. On the **Success** page, select **Done**.
22. On the **Windows Security** page, in the **New PIN** and **Confirm PIN** boxes, enter **102938** and then select **OK**.
23. On the **All set** page, select **OK**.

9.1.4 Task 3: Verify the device is joined to Azure AD

1. On **SEA-WS3**, select **Start**, and then select the **Settings** icon.
2. In **Settings**, select **Accounts**.
3. Select **Access work or school** and then notice the **Connected to Contoso's Azure AD** object.
4. Right-click the **Start** button and then select **Computer Management**.
5. Expand **Local Users and Groups** and then select **Groups**.
6. Double-click the **Administrators** group. Notice that **AzureAD\User2** is listed as a local administrator. Note: The other two SID references refer to the Azure AD global administrator role and the Azure AD device administrator role.
7. Select **Cancel** and then close **Computer Management**.
8. Switch to SEA-CL1.

9. In the Microsoft Azure portal, at the top of the page, select **Contoso**.
10. On the **Contoso** page, under **Manage**, select **Devices**. Notice that SEA-WS3 is listed with a join type of **Azure AD joined**.
11. Close Microsoft Edge and then sign out of SEA-CL1.

9.1.5 Task 4: Remove the device from Azure AD

1. On **SEA-WS3**, select **Start**, and then select the **Settings** icon.
2. In **Settings**, select **Accounts**.
3. Select **Access work or school** and then notice the **Connected to Contoso's Azure AD** object.
4. Select the the **Connected to Contoso's Azure AD** object and then select **Disconnect**.
5. Select **Yes** to confirm and then in the **Disconnect from the organization** box, select **Disconnect**.
6. On the **Windows Security** page, enter **Admin** with the password of **Pa55w.rd**. Select **OK**.
7. Select **Restart now** to restart SEA-WS3.

Results: After completing this exercise you have successfully created a new user and joined a Windows 10 device to an Azure AD tenant.

END OF LAB

10 Practice Lab: Managing Windows 10 Settings

10.1 Summary

In this lab you will learn how to configure computer settings using Windows Settings, the Control Panel, and Windows PowerShell. You also learn how to customize and deploy a custom Windows 10 Start page layout.

10.2 Exercise 1: Configuring Settings Using Windows Settings and Control Panel

10.2.1 Scenario

You need to use Windows Settings to validate protection settings, device specifications, and Windows specifications. You also need to determine which applications are slowing down the startup process for Windows 10. Finally, you need to create a new power plan that minimizes power usage, but does not impact multimedia presentations while the device is running on battery.

### Task 1: Using Windows Settings

1. Sign in to SEA-CL1 as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start,** and then select the **Settings** icon.
3. In **Windows Settings**, select **System**, and then select **About**. Take note of the protection settings, Device specifications, and Windows specifications.
4. Select **Storage**. Take note of the storage information including how storage is used on the device.
5. Select **Multitasking**. In the Multitasking page, under **Timeline** disable the **Show suggestions in your timeline** option.
6. Select **Home**.
7. In **Windows Settings**, select **Apps**, and then select **Apps & features**. Take note of the Apps & features installed on the device.
8. Select **Startup**. Take note of the apps that are configured to start when you sign in to the device. Notice that Microsoft OneDrive has a high impact to the startup of the device.
9. In the **Startup** page, disable the **Microsoft OneDrive** option. This will prevent OneDrive from starting automatically.
10. Select **Home**.
11. Close **Windows Settings**.

10.2.2 Task 2: Using Control Panel

1. Select **Start** and type **Control Panel**. Press **Enter**.
2. In the Control Panel window, select **Hardware and Sound** and then select **Power Options**.
3. Select **Create a power plan.**
4. In the **Plan name** box, enter **Power Save - Presentation** and select **Next**.
5. Select **Create**.
6. Under **Preferred plans**, next to **Power Save - Presentation**, select **Change plan settings**.
7. Select **Change advanced power settings**.

8. Expand **Hard disk** and then expand **Turn off hard disk after**. Change the setting to **60** minutes.
9. Scroll down and expand the **Multimedia settings** option.
10. Expand the **When playing video** option and change the setting to **Balanced**.
11. Select **OK** to close the **Power Options** dialog box.
12. Close all open windows.

Results: After finishing this exercise you will have configured computer settings using Windows Settings and the Control Panel.

10.3 Exercise 2: Using PowerShell to Configure Windows

10.3.1 Scenario

You need to use Windows PowerShell to test the scripting environment. To become familiar with PowerShell you will run several commands and the use PowerShell ISE to create a script to list all running services on the device.

10.3.2 Task 1: Use Windows PowerShell to configure a device

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd.**
2. Select **Start** and type **PowerShell**. Select **Run as Administrator**.
3. At the PowerShell window, type the following and then press **Enter**:

```
Get-ExecutionPolicy
```

4. Confirm the current setting of the PowerShell execution policy is set to **Restricted.**
5. If the execution policy is set to **Restricted**, change it to **Unrestricted** by running the following command at the PowerShell window:

```
Set-ExecutionPolicy Unrestricted
```

6. Confirm that the execution policy is now **Unrestricted**.
7. At the PowerShell window, launch Notepad by typing the following command and then press **Enter**:

```
Start-Process Notepad
```

8. At the PowerShell window, type the following command and then press **Enter**:

```
Get-Process
```

9. Review the list of all running processes. Identify that Notepad is running and note the Process ID.
10. At the PowerShell window, type the following command and then press **Enter**. Replace [ID] with the Process ID identified in step 9.

```
Stop-Process -Id [ID]
```

11. Verify that the Notepad window is no longer open.
12. At the PowerShell window, list the application log entries by typing the following command and then press **Enter**:

```
Get-EventLog -LogName "Application"
```

12. Select **Start** and type **Telnet**. Select **Turn Windows features on and off**.
13. In the **Windows Features** window, verify that **Telnet Client** is not selected.
14. At the PowerShell Window, type the following command, and then press **Enter**:

```
Enable-WindowsOptionalFeature -Online -FeatureName "TelnetClient"
```

Note: This will install the Telnet Client windows feature.

15. Select **Start** and type **Telnet**. Select **Open**.
16. Close all open windows.

10.3.3 Task 2: Use a Windows PowerShell Script

1. In the **Type here to search** box, type **\\SEA-DC1\Labfiles** and then press Enter.
2. In the content pane, double-click the **Configure** folder.
3. Copy the **Services.ps1** file into the **E:\Labfiles** folder on SEA-CL1.
4. Select **Start** and type **Powershell ISE**. Press **Enter**.
5. In the Windows PowerShell ISE, open the script file **E:\Labfiles\Services.ps1**.
6. Read the script, and then note what the script is doing, according to the following note.
   - *Note:*
   - *Comments are green.*
   - *Variables are red.*
   - *Cmdlets are bright blue.*
   - *Text in quotation marks is dark red.*
7. Select line 3 in the script, and then select **Run selection (F8)**.

   Note: Only the command in line 3 will be executed.
8. Select **Run script (F5)**, and then read the output.

   Note: The output does not have multiple colors.
9. At the end of line 14, type –**ForegroundColor $color**
10. On the toolbar, select **Run script (F5)** in the Windows PowerShell ISE window. Select **OK** to save the file, and then read the output.

    Note: Running services are green, and services that are not running are red.
11. On line 16, type **Write-Host ”A total of” $services.count ”services were evaluated”**
12. Select **Run script (F5)**, and in the Windows PowerShell ISE window select **OK**.
13. Select **Show Command Add-on** in the PowerShell ISE toolbar.
14. In the **Commands** pane, select the **Write-Host** cmdlet and then configure the following options:
    - BackgroundColor: **Gray**
    - ForegroundColor: **Black**
    - Object: **”Script execution is complete”**
15. Select **Copy** and paste the command to line 17 of the script.
16. Select **Run script (F5)**, and in the Windows PowerShell ISE window select **OK**.
17. Select **Start** and type **PowerShell**. Press **Enter**.
18. At the PowerShell window, type the following command and then press **Enter**:

```
Set-Location E:\Labfiles
```

13. At the PowerShell window, type the following and then press **Enter**:

```
.\Services.ps1
```

14. Close all open windows and sign out of SEA-CL1.

Results: After completing the exercise you have learned how to manage Windows 10 using PowerShell and PowerShell scripts.

10.4 Exercise 3: Customizing the Start Layout in Windows 10

10.4.1 Scenario

You need to ensure that all Windows 10 devices contain the Contoso utilities apps on the Start menu. To do this, you decide to create and export a custom Start layout that only locks down the specified groups in the XML file. Users will still be able to customize other areas of the Start menu as needed.

10.4.2 Task 1: Customize the Start screen

1. Sign in to **SEA-CL1** as **.\Admin** with the password **Pa55w.rd.** This signs in as the local administrator on the device.
2. Select **Start**, and right-click each tile and then select **Unpin from Start**.
3. From the Start menu, right-click each of the following apps and then select **Pin to Start:**
   - Snip & Sketch
   - Sticky Notes
   - Voice Recorder
   - Calculator
   - Alarms & Clock
   - Maps
4. In the Start screen, just above the tiles, click and select **Name group** and then replace the text with **Contoso Utilities**.
5. Close the Start menu.

10.4.3 Task 2: Export the Start layout

1. On SEA-CL1, right-click the Start menu and then select **Windows PowerShell (Admin)**. Select **Yes** at the User Account Control.

2. At the PowerShell window, type the following command and then press **Enter**:

```
Export-StartLayout -UseDesktopApplicationID -Path E:\Labfiles\ContosoLayout.xml
```

3. Open **File Explorer** and then browse to **E:\Labfiles**.
4. Right-click **ContosoLayout.xml**, point to **Open with** and then select **Notepad**.
5. At the first instance of **<DefaultLayoutOverride>**, type the following:

```
<DefaultLayoutOverride LayoutCustomizationRestrictionType="OnlySpecifiedGroups">
```

6. Save the **ContosoLayout.xml** file and then close Notepad.
7. Close all open windows and sign out of SEA-CL1.

10.4.4 Task 3: Deploy the Start layout using Group Policy

1. Sign in to SEA-CL1 as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. Open **File Explorer** and then browse to **E:\Labfiles**.
3. Right-click **ContosoLayout.xml**, and then Copy the file.
4. In the Address bar, browse to **\\SEA-DC1\Netlogon**.
5. Paste **ContosoLayout.xml** into the **Netlogon** folder and then close File Explorer.
6. Sign out of SEA-CL1.
7. Switch to SEA-SVR1.
8. If necessary, sign in to SEA-SVR1 as **Contoso\Administrator** with the password of **Pa55w.rd**.
9. Select **Start** and then select **Server Manager**.
10. Select **Tools** and then select **Group Policy Management**.
11. Maximize the Group Policy window. In the console tree, expand **Forest:Contoso.com**, expand **Domains**, and then expand **Contoso.com**. Select the **Group Policy Objects** node.
12. Right-click the **Group Policy Objects** node, and then select **New**.
13. In the **New GPO** dialog box, in the **Name** box, type **Win10StartLayout**, and then select **OK**.
14. In the details pane, right-click **Win10StartLayout**, and then select **Edit**. Maximize the Group Policy Management Editor window.
15. In the console tree, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then select **Start Menu and Taskbar**.
16. Double-click **Start Layout**.
17. In the **Start Layout** box, select **Enabled** and then under **Start Layout File** enter **\\SEA-DC1\Netlogon\ContosoLayout.xml**. Click **OK** and then close the **Group Policy Management Editor**.
18. In the Group Policy Management console, right-click **Sales** and then select **Link an Existing GPO**.
19. From the **Select GPO** box, select **Win10StartLayout** and then select **OK**.
20. Close the Group Policy Management console.

10.4.5 Task 4: Verify the Windows 10 Start layout

1. Switch to SEA-CL1.

2. Sign in to SEA-CL1 as **Contoso\Reda** with the password of **Pa55w.rd**.
3. Select **Start** and then take note of the Start page. The **Contoso Utilities** group displays a lock icon that specifies that the group cannot be modified.
4. In the Start menu, right-click **Word** and then select **Pin to Start**. Notice that you can still customize other sections of the Start page.
5. Sign out of SEA-CL1.

Results: After completing the exercise you have learned how to customize and deploy a custom Windows 10 Start layout.

END OF LAB

11 Practice Lab: Synchronizing settings between devices

11.1 Summary

In this lab you will learn how to synchronize settings to support users working on multiple devices.

11.1.1 Scenario

You frequently use two devices, SEA-WS1 and SEA-WS2, and would like to ensure that Windows settings and Microsoft Edge favorites are synchronized between the two devices. You need to add your Microsoft account to both devices and configure synchronization settings between the devices.

Note: To complete this lab, you need to have a Microsoft account. You can obtain a free Microsoft account which can be created at https://outlook.live.com. Your instructor can guide you on how to create an account if required.

11.1.2 Task 1: Connect your Microsoft account to SEA-WS1 and SEA-WS2

1. Sign in to **SEA-WS1** as **Student** with the password **Pa55w.rd**.
2. Select **Start** and then select **Settings**.
3. In the **Windows Settings** page, select **Accounts**.
4. On the **Accounts** page, select **Your info**.
5. Select the link that states **Sign in with a Microsoft account instead**.
6. In the **Microsoft account Sign in** page, enter your Microsoft account email address and then select **Next**.
7. On the **Enter password** page, enter your Microsoft account password and then select **Sign in**.
8. If a **Help us protect your account** dialog box appears, select **Skip for now**.
9. In the **Sign into this computer using your Microsoft account** page, enter **Pa55w.rd** and then select **Next**.
10. On the **Create a PIN** page, select **Next**.
11. In the **Set up a PIN** dialog box, enter **1029** in both the **New PIN** and **Confirm PIN** boxes. Select **OK**. Notice that your Microsoft account is now listed on the Your info page.
12. Under your Microsoft account name, select **Verify**.
13. On the Verify your identity, select the method that you set up with you configured your Microsoft account and verify your account. This is required for synchronization between devices.
14. Sign out of SEA-WS1.
15. Repeat steps 1-14 on SEA-WS2.

11.1.3 Task 2: Configure synchronization on SEA-WS1

1. On SEA-WS1, sign in with your Microsoft account using the PIN **1029**.
2. Select **Start**, then **Settings**, then select **Accounts**.
3. Select **Sync your settings** on the left. Verify that **Sync settings** and all the options under **Individual sync settings** are all enabled.
4. Select **Home**.
5. Select **System** and then select **Clipboard**.
6. Under **Clipboard history**, enable the option button.
7. Under **Sync across devices**, enable the option button and ensure that **Automatically sync text that I copy** is selected.
8. Close **Settings**.
9. On the taskbar, select **Microsoft Edge**.

10. At the **Sync your profile** prompt, select **Sync**.
11. On the **Personalize ads, search, and news**, select **Allow**.
12. Navigate to http://www.microsoft.com/learn.
13. In the address bar, select the **Add this page to favorites** button to save as a favorite.
14. Ensure that the **Folder options** shows **Favorites bar**, and then select **Done**.
15. Select the **Favorites** button, select **More options**, and then select **Show favorites bar**.
16. Select **Always** and then select **Done**.
17. Close **Microsoft Edge**.
18. Sign out of SEA-WS1.

11.1.4 Task 3: Configure synchronization on SEA-WS2

1. Sign in to **SEA-WS2** with your Microsoft account using the PIN **1029**.
2. Select **Start**, then **Settings**, then select **Accounts**.
3. Select **Sync your settings** on the left. Verify that **Sync settings** and all the options under **Individual sync settings** are all enabled.
4. Select **Home**.
5. Select **System** and then select **Clipboard**.
6. Under **Clipboard history**, enable the option button.
7. Under **Sync across devices**, enable the option button and ensure that **Automatically sync text that I copy** is selected.
8. Close **Settings**.
9. On the taskbar, select **Microsoft Edge**.
10. At the **Sync your profile** prompt, select **Sync**. Notice that the Favorites bar and the saved favorite is available in the browser on SEA-WS2.
11. In the Microsoft Edge browser, select **Settings and more**, and then select **Settings**.
12. Select **Sync** and then validate the sync settings for Microsoft Edge.
13. In the address bar, enter https://docs.microsoft.com and press Enter.
14. In the address bar, select the **Add this page to favorites** button to save as a favorite.
15. Ensure that the **Folder options** shows **Favorites bar**, and then select **Done**.
16. In the address bar. select the **Collections** button and then in the Collections pane, select **Next** to complete the introduction.
17. Under **New collection**, select **Add current page**.
18. In the **Favorites** bar, select **Microsoft Learn**, and then in the **New collection** pane, select **Add current page** to add this second page to the collection.
19. Close **Microsoft Edge**.
20. Sign out of SEA-WS2.

11.1.5 Task 4: Validate synchronization

1. On SEA-WS1, sign in with your Microsoft account using the PIN **1029**.
2. On the taskbar, select **Microsoft Edge**.
3. Verify that there are two favorites attached to the Favorites bar.
4. Select the **Collections** button.
5. Select **New collection** and verify that the two pages that you added in the previous task are available in the collection.
6. Close **Microsoft Edge**.
7. Sign out of SEA-WS1.

Results: After finishing this exercise, you will have added your Microsoft account to multiple devices and configure synchronization settings between the devices.

END OF LAB

12 Practice Lab: Managing local and network printers

12.1 Summary

In this exercise, you will perform basic printer configuration. You will add a local printer by using Devices and Printers. You then will configure printer security, and use the Print Management tool to add a printer on a remote computer. You also will connect to a remote printer, and then manage a print job.

12.1.1 Scenario

The Contoso Marketing department has purchased a new printer that uses a Microsoft PCL6 Class Driver that's attached to SEA-SVR1. Marketing wants to share the printer but restrict use to just the Managers group. There is a another printer attached to SEA-SVR2 that uses the Microsoft PS Class Driver, which is also to be shared with access for everyone to print. You need to configure these printers as requested. After you configure the printers you will have a user named Terry test that she can only print to the printer on SEA-SVR2, and that print jobs initiated from SEA-SVR2 can be seen in the queue on SEA-SVR1.

12.1.2 Task 1: Add and share a local printer

1. Sign in to SEA-SVR1 as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start** and then select **Control Panel**.
3. In Control Panel, select **View devices and printers**.
4. In Devices and Printers, select **Add a printer**.
5. In the **Add a device** dialog box, select **The printer that I want isn't listed**.
6. On the **Find a printer by other options** page, select the **Add a local printer or network printer with manual settings** option, and then select **Next**.
7. On the **Choose a printer port** page, verify that **Use an existing port** is selected, and then select **Next**.
8. On the **Install the printer driver** page, in the **Manufacturer** list, select **Microsoft**. In the **Printers** list, select **Microsoft PCL6 Class Driver**, and then select **Next**.
9. On the **Type a printer name** page, in the **Printer name** field, type **Managers Printer**, and then select **Next**.
10. On the **Printer Sharing** page, select **Next**, and then select **Finish**.

12.1.3 Task 2: Configure printer security

1. On SEA-SVR1, in Devices and Printers, right-click **Managers Printer**, select **Printer properties**, and then select the **Security** tab.
2. In the **Managers Printer Properties** dialog box, verify that **Everyone** is selected, and then select **Remove**.
3. Select **Add**, in the **Enter the object names to select (examples)** box, type **Managers**, and then select **OK**. In the **Permissions for Managers** section, verify that **Print** check box is selected in the **Allow** column, and then select **OK**.
4. Close the Devices and Printers window.

12.1.4 Task 3: Use Print Management to manage a remote printer

1. On SEA-SVR1, select **Start**, type **print**, and then select **Print Management**.
2. In Print Management, in the navigation pane, expand **Print Servers**, and then verify that SEA-SVR1 is the only print server listed.
3. Right-click **Print Servers**, and then select **Add/Remove Servers**.
4. In the **Add/Remove Servers** dialog box, in the **Add Servers** field, type **SEA-SVR2**, and then select **Add to List**.
5. Select **OK**, and then verify that the navigation pane lists two print servers.
6. Right-click **SEA-SVR2**, and then select **Add Printer**.
7. On the **Printer Installation** page, select **Add a new printer using an existing port**, and then select **Next**.
8. On the **Printer Driver** page, verify that the **Install a new driver** option is selected, and then select **Next**.
9. On the **Printer Installation** page, in the **Manufacturer** list, select **Microsoft**. In the **Printers** list, select **Microsoft PS Class Driver**, and then select **Next**.
10. On the **Printer Name and Sharing Settings** page, in the **Printer Name** box, type **PostScript Printer**, then in the **Share Name** box, type **PostScript Printer**, select **Next** twice, and then select **Finish**.
11. Under the **SEA-SVR2** node, select **Printers** and verify that **PostScript Printer** is installed and ready.

12.1.5 Task 4: Connect to a remote printer

1. Switch to SEA-CL1, and sign in as **Contoso\Terry** with the password **Pa55w.rd**.

   Note: Terry is member of the IT group, but she is not a member of the Managers group.

2. In the taskbar, in the **Type here to search** text box, type **control**, and then select **Control Panel**.
3. In Control Panel, select **View devices and printers**.
4. Select **Add a printer**.
5. In the **Add a device** dialog box, select **The printer that I want isn't listed**.
6. On the **Find a printer by other options** page, select **Select a shared printer by name**, type **\\SEA-SVR1\Managers Printer** in the box, and then select **Next**.
7. In the **Connect to SEA-SVR1** dialog box, select **Cancel**.
8. In the box, type **\\SEA-SVR2\PostScript Printer**, select **Next** twice, and then select **Finish**.

   Note: Because Terry is not a member of the Managers group, and she does not have permissions to \\SEA-SVR1\Managers Printer, you were asked to type credentials that have the appropriate permissions.

9. In Devices and Printers, verify that **PostScript Printer on SEA-SVR2** was added.
10. Right-click **PostScript Printer on SEA-SVR2**, and then select **Set as default printer**. In the **Printers** dialog box, select **OK**.
11. Verify that the printer has a green check mark next to it, which indicates that it is the default printer.

12.1.6 Task 5: Print a document, and manage a print job

1. On SEA-CL1, on the taskbar, in the **Type here to search** text box, type **notepad**, and then press Enter.
2. In Notepad, type your name, select the **File** menu, and then select **Print**.
3. In the **Print** dialog box, select **PostScript Printer on SEA-SVR2**, and then select **Print**.
4. Switch to SEA-SVR1.
5. On SEA-SVR1, in Print Management, in the navigation pane, select **Printers With Jobs**. In the details pane, view that **PostScript Printer** is listed and that it has one job in the queue.
6. Switch to SEA-CL1.
7. On SEA-CL1, in the notification area, select **Show hidden icons**, right-click the printer icon, and then select **PostScript Printer on SEA-SVR2**.
8. In the **PostScript Printer on SEA-SVR2** window, verify that you can see a single document called **Untitled – Notepad**. Right-click **Untitled – Notepad**, review its properties, and then select **OK**.
9. Right-click **Untitled-Notepad**, select **Cancel**, and then select **Yes**.

   Note: You now have canceled Terry's print job.

10. Sign out from SEA-CL1.
11. Switch to SEA-SVR1.
12. On SEA-SVR1, in Print Management, verify that there are no longer any printers listed under the **Printers With Jobs** node.
13. Close all open windows.
14. Sign out of SEA-SVR1.

Results: After completing this exercises you will have performed basic printer configuration like adding and sharing a printer, configuring printer security, managing and connecting a remote printer and managing a print job.

END OF LAB

13 Practice Lab: Managing Windows Update Settings

13.1 Summary

In this lab you will learn how to manage Windows Update settings for a single device and how to manage feature and quality updates for multiple devices using Windows Update for Business Group Policy settings.

13.2 Exercise 1: Configuring Windows Update for a Single Device

13.2.1 Scenario

You need to validate the Windows Update settings for SEA-WS3. You have also been asked to ensure that the following Windows update settings are applied to the device:

- Updates for other Microsoft products should be enabled.
- A notification must be shown when the PC requires a restart to finish updating.
- Delivery optimization must be configured to allow downloads from the local network and PCs from the Internet.
- Active hours should be changed to match the recommended daily activity notification.

13.2.2 Task 1: Configure Windows Update

1. Sign in to **SEA-WS3** as **Admin** with the Password of **Pa55w.rd**

2. Right-click **Start**, and then select **Windows PowerShell (Admin)**. At the User Account Control dialog box, select **Yes**.

3. In the Administrator: Windows PowerShell window, type the following command, and then press Enter:

```
Set-Service wuauserv -StartupType Manual
```

Note: For the lab setup, the Windows Update service is disabled. The above command is not necessary to run in typical Windows 10 scenarios.

4. Close Windows PowerShell.
5. Select **Start**, and then select the **Settings** icon.
6. In **Settings**, select **Update & Security**.
7. Under **Update & Security**, select **Windows Update**.
8. On the **Windows Update** tab, select **Advanced options**.
9. On the **Advanced options** page, under **Update options**, enable the **Receive updates for other Microsoft products when you update Windows** option.
10. On the **Advanced options** page, scroll down under **Update notifications** enable the **Show a notification when your PC requires a restart to finish updating** option.
11. Scroll down and then select **Delivery Optimization**.
12. On the Delivery Optimization page, verify that the **Allow downloads from other PCs** option is enabled.
13. Select **PCs on my local network, and PCs on the Internet**.
14. Scroll down and then select **Activity monitor**. Take note of the Download Statistics and Upload Statistics and then select **Back**.
15. In the navigation pane, select **Windows Update**.

13.2.3 Task 2: Change active hours and review applied updates

1. On the **Windows Update** page, select **Change active hours**.
2. On the Change active hours page, verify that the current active hours are from 8:00AM to 5:00PM. Also notice that a message displays suggesting a change to the active hours. Select **Change**.
3. On the Active hours window, change the Start time to 7:00AM and the End time to 8:00PM.
4. Select **Save** and then select **Back**.
5. On the **Windows Update** page, select **View update history**.
6. Review the updates listed, and then select **Uninstall updates**.
7. Review the updates listed in **Installed Updates**. Close **Installed Updates**.
8. On the **View Update history** page, select **Back**.
9. Close the **Settings** page.
10. Sign out of SEA-WS3.

Results: After completing this exercise, you will have successfully configured and/or confirmed Windows Update settings.

13.3 Exercise 2: Managing Feature and Quality Updates with Windows Update for Business

13.3.1 Scenario

You have been delegated the task to create Group Policy Objects to configure Windows Update for Business. Your first task is to determine how many deployment rings you will need and the associated Windows update settings based upon business requirements. You then need to configure a Group Policy object for each deployment ring. The Group Policy Objects will then be applied to organizational units by the Active Directory administrators at a later time.

13.3.2 Task 1: Identify Windows Update for Business Requirements

Contoso currently configures each Windows 10 device to apply Windows updates based upon manual operating system settings. However a number of issues have come up that requires you to revisit and propose a new solution:

- Updates are not fully tested before they are installed on the all the computers in the organization. This is especially troublesome for when a new feature update is released.
- Some users have been pausing updates for an extended period of time.
- Some users have been enrolling into the Windows Insider Program, which has caused compatibility issues for some of the devices.
- As more Windows 10 computers are added to the network, it is difficult to maintain and manage the update settings using the current manual process.

You have been asked to address these issues by:

- Ensuring that updates are tested at least 10 days before being deployed to everyone in the organization.
- Restricting standard users from configuring Windows Update settings.
- Implementing Windows Update for Business.

You need to develop a plan to implement Windows Update for Business. Consider the following questions to help you with your solution:

1. How will you ensure that an update has been tested properly before being deployed throughout the entire organization? *Answer: Create Active Directory Group Policy Objects that align with deployment rings. One possible solution is to create a pilot deployment ring that does not defer quality or feature updates. This will allow any device that has this policy to immediately obtain a released update and start its testing process. A second Broad deployment ring can be created that has a deferral for 10 days for both quality and feature updates. This second object would be applied to the rest of the organization and will not receive released updates until 10 days have passed.*
2. How will you ensure that standard users are restricted from configuring Windows Updates? *Answer: Using Group Policy settings will provide the ability to restrict various settings such as pausing updates and enrolling into the Windows Insiders Program.*
3. How will you manage and maintain Windows Updates for your organization? *Answer: Windows Update for Business uses Active Directory Group Policy. For more granular control and management, Microsoft Intune or Microsoft Endpoint Configuration Manager can also be used.*

13.3.3 Task 2: Use Group Policy to configure Windows Update for Business

1. Sign in to SEA-SVR1 as **Contoso\Administrator** with the password of **Pa55w.rd**.
2. Select **Start**, and then select **Server Manager**.
3. Select **Tools** and then select **Group Policy Management**.
4. Maximize the Group Policy Management window. In the console tree, expand **Forest:Contoso.com**, expand **Domains**, and then expand **Contoso.com**. Select the **Group Policy Objects** node.
5. Right-click the **Group Policy Objects** node, and then select **New**.
6. In the **New GPO** dialog box, in the **Name** box, type **Pilot Release - Ring 1**, and then select **OK**.
7. In the details pane, right-click **Pilot Release - Ring 1**, and then select **Edit**. Maximize the Group Policy Management Editor window.
8. In the console tree, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then select **Windows Update**.

9. In the details pane, double-click Configure Automatic Updates.
10. In the **Automatic Updates** window, configure the following and then select **OK**:
    - Enabled: **Selected**
    - Configure automatic updating: **4 - Auto download and schedule the install**
    - Install updates for other Microsoft products: **Selected**
11. In the details pane, double-click **Windows Update for Business**.
12. In the details pane, double-click **Manage preview builds**.
13. In the **Manage preview builds** window, configure the following and then select **OK**:
    - Enabled: **Selected**
    - Set the behavior for receiving preview builds: **Disable preview builds**
14. In the details pane, double-click **Select when Preview Builds and Feature Updates are received**.
15. In the **Select when Preview Builds and Feature Updates are received** window, configure the following:
    - Enabled: **Selected**
    - Select the Windows readiness level for the updates you want to receive: **Semi-Annual Channel**
16. Verify that the **After a Preview Build or a Feature Update is released, defer receiving it for this many days** is set to **0**. The Pilot Release - Ring 1 configuration will not have any updates deferred.
17. Select **OK** to close the **Select when Preview Builds and Feature Updates are received** window.
18. In the details pane, double-click **Select when Quality Updates are received**.
19. In the **Select when Quality Updates are received** window, configure the following and then select **OK**:
    - Enabled: **Selected**
    - After a quality update is released, defer receiving it for this many days: 0

13.3.4 Task 3: Use Group Policy to configure Windows Update experience for users

1. On SEA-SVR1, ensure that you are still in the Group Policy Management Editor for the **Pilot Release - Ring 1** policy.
2. In the console tree, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then select **Windows Update**.
3. In the details pane, double-click **Remove access to "Pause updates" feature**.
4. In the **Remove access to "Pause updates" feature** window, select **Enabled** and then select **OK**.
5. In the details pane, double-click **Specify deadline before auto-restart for update installation**.
6. In the **Specify deadline before auto-restart for update installation** window, configure the following and then select **OK**:
    - Enabled: **Selected**
    - Specify the number of days before a pending restart will automatically be executed outside of active hours: Quality Updates (days): **3**; Feature Updates (days): **3**
7. Close the Group Policy Management Editor.

13.3.5 Task 4: Use Group Policy to configure the Broad Release update ring

1. On SEA-SVR1, ensure that you are still in the Group Policy Management console.
2. Maximize the Group Policy Management window. In the console tree, expand **Forest:Contoso.com**, expand **Domains**, and then expand **Contoso.com**. Select the **Group Policy Objects** node.
3. In the details pane, right-click **Pilot Release - Ring 1**, and then select **Copy**.
4. Right-click the **Group Policy Objects** node and then select **Paste**.
5. In the **Copy GPO** dialog box, ensure that **Use the default permissions for new GPOs** is selected and then select **OK**.
6. At the **Copy** dialog box, select **OK**.
7. In the details pane, select **Copy of Pilot Release - Ring 1** and then select **Rename**. Rename the object to **Broad Release - Ring 2**.
8. Right-click **Broad Release - Ring 2** and then select **Edit**.
9. In the console tree, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then select **Windows Update**.
10. In the details pane, double-click **Windows Update for Business**.
11. In the details pane, double-click **Select when Preview Builds and Feature Updates are received**.
12. In the **Select when Preview Builds and Feature Updates are received** window, configure the following:
    - Enabled: **Selected**
    - Select the Windows readiness level for the updates you want to receive: **Semi-Annual Channel**

13. Next to **After a Preview Build or a Feature Update is released, defer receiving it for this many days**, set the value to **10** and then select **OK**.
14. In the details pane, double-click **Select when Quality Updates are received**.
15. In the **Select when Quality Updates are received** window, configure the following and then select **OK**:
    - Enabled: **Selected**
    - After a quality update is released, defer receiving it for this many days: **10**
16. Close the Group Policy Management Editor.

Results: After completing this exercise, you will have successfully configured Group Policy Objects to be later assigned to organizational units to manage Windows Update for Business settings.

END OF LAB

14 Practice Lab: Configuring Network Connectivity

14.1 Summary

In this lab, you will identify IPv4 settings and validate connectivity on a Windows 10 device. You will also configure a Windows 10 device to automatically obtain IPv4 settings from a DHCP service.

14.2 Exercise 1: Verifying and Testing IPv4 Settings

14.2.1 Scenario

You need to identify the current static IPv4 settings on SEA-CL1. You also need to test connectivity from SEA-CL1 to SEA-DC1.

14.2.2 Task 1: Verify IPv4 settings from Settings and the Network and Sharing Center

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

2. Select the **Network** icon in the notification area, and then select **Network & Internet settings**.

3. In the **Settings** window, on the **Status** page, select **Properties**.

4. Scroll down and identify the **IP settings** and **Properties** for the network adapter. The following information should be available:

    - IPv4 address
    - IPv4 subnet prefix length
    - IPv4 DNS servers
    - IPv4 gateway

    Also take note that the IP assignment is set to Manual, which indicates that this is a static IP address assignment.

5. Under **IP settings**, select **Edit**. Notice that you can modify the IPv4 and IPv6 settings.

6. Select **Cancel** to close the **Edit IP settings** window.

7. Select the **Back** button and then select **Status**.

8. In the Status details pane, scroll down and then select **Network and Sharing Center**. Notice the domain and connection information.

9. In **Network and Sharing Center**, to the right of the Contoso.com Domain network, select **Ethernet**.

10. In the **Ethernet Status** dialog box, select **Details**. This window displays the same configuration information for this adapter as the Settings status page.

11. In the **Network Connection Details** window, select **Close**.

12. In the **Ethernet Status** dialog box, select **Properties**. You can configure protocols in this window.

13. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then select **Properties**.

    Note: You can configure the IP address, subnet mask, default gateway, and Domain Name System (DNS) servers in this window.

14. Select **Cancel** and then close all open windows without modifying any settings.

14.2.3 Task 2: Verify IPv4 settings from the command line

1. On SEA-CL1, right-click **Start**, and then select **Windows PowerShell (Admin)**.
2. At the Windows PowerShell command prompt, type following command, and then press **Enter**.

```
Get-NetIPAddress
```

Note: The IPv4 address from the Ethernet interface should match what you identified earlier.

3. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
netsh interface ipv4 show config
```

Note: The current IPv4 configuration is displayed and should match what you identified earlier.

4. At the Windows PowerShell command prompt, type the following command, and then press Enter.

```
ipconfig /all
```

Note: Again, the information should match what you identified earlier.
5. Leave the **Administrator: Windows PowerShell** window open.

14.2.4 Task 3: Test connectivity

1. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
Test-Connection SEA-DC1
```

2. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
Ping SEA-DC1
```

3. At the Windows PowerShell command prompt, type type the following command, and then press **Enter**.

```
PathPing SEA-DC1
```

4. Observe and describe the differences between the three connectivity tests performed.

   Note: Test-Connection and Ping provides information on time and success of connectivity directly to a target host. PathPing provides statistics on how many connections it takes to route to a target host.

5. Close the Windows PowerShell window.

Results: After completing this exercise you have verified the IPv4 settings of a windows device and used various tools to test connectivity.

14.3 Exercise 2: Configuring Automatic IPv4 Settings

14.3.1 Scenario

Your network administrative team has configured DNS and DHCP services located on SEA-DC1. You need to reconfigure SEA-CL1 to obtain its IPv4 settings using the DHCP service. You will then test and verify the connectivity between SEA-CL1 and SEA-DC1 using the newly obtained IPv4 address settings.

14.3.2 Task 1: Reconfigure the IPv4 settings

1. On **SEA-CL1**, select the **Network** icon in the notification area, and then select **Network & Internet settings**.
2. Select **Network and Sharing Center**.
3. In **Network and Sharing Center**, to the right of the Contoso.com Domain network, select **Ethernet**.
4. In the **Ethernet Status** dialog box, select **Properties**.
5. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then select **Properties**.
6. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Obtain an IP address automatically**.
7. Select **Obtain DNS server address automatically**.

8. Select **OK** to save the changes.
9. In the **Ethernet Properties** dialog box, select **Close**.
10. In the **Ethernet Status** dialog box, select **Details**. Notice that DHCP is enabled, and that the IP address of the DHCP server displays.
11. On SEA-CL1, right-click **Start**, and then select **Windows PowerShell (Admin)**.
12. At the Windows PowerShell command prompt type the following command, and then press **Enter**.

    ```
    ipconfig /all
    ```

13. Verify that the IPv4 address is obtained from DHCP.

14.3.3 Task 2: Test connectivity

1. At the Windows PowerShell command prompt, type type the following command, and then press **Enter**.

    ```
    Test-Connection SEA-DC1
    ```

Note: You should receive four replies from SEA-DC1.
2. Close all open windows. 3. Sign out of SEA-CL1.

14.3.4 Task 3: View the impact on the DHCP server

1. Switch to **SEA-SVR1**.
2. Sign in to SEA-SVR1 as **Contoso\Administrator** with the password **Pa55w.rd**.
3. Select **Start** and then select **Server Manager**.
4. In **Server Manager**, select **All Servers**, right-click **SEA-DC1**, and then select **DHCP Manger**.
5. In **DHCP**, expand **SEA-DC1.Contoso.com**, expand **IPv4**, expand **Scope [172.16.0.0] Contoso**, and then select **Address Leases**.
6. In the details pane, you should see the address lease for the SEA-CL1 Windows 10 client.
7. Close the DHCP window.
8. Sign out of SEA-SVR1.

Results: After completing this exercise you have configured a Windows device to automatically obtain IPv4 settings from a DHCP service.

END OF LAB

15 Practice Lab: Configuring and Testing Name Resolution

15.1 Summary

In this lab, you will verify and manage name resolution for a Windows 10 network client. You will also test and troubleshoot name resolution by using command line tools, DNS, and a hosts file entry.

15.2 Exercise 1: Verify and Manage Name Resolution

15.2.1 Scenario

You need to check and verify current DNS settings on SEA-CL1. You will also test out command line tools used to view and clear the DNS client cache.

15.2.2 Task 1: Verify current DNS settings

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Right-click **Start**, and then select **Windows PowerShell (Admin)**.
3. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

    ```
    ipconfig /all
    ```

Note: DHCP should be enabled from the previous lab. Take note of the IP address of the DHCP server and the IP address of the DNS server.

4. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
Get-NetIPConfiguration
```

Note: The PowerShell command also provides IP address information.

15.2.3 Task 2: View and clear the DNS resolver cache

1. At the Windows PowerShell command prompt, type the following command, and then press **Enter**. This will resolve SEA-SVR1.contoso.com to an IP address and store the results in the DNS resolver cache.

```
ping SEA-SVR1.contoso.com
```

2. At the Windows PowerShell command prompt, type the following command, and then press **Enter**. This will resolve SEA-DC1.contoso.com to an IP address and store the results in the DNS resolver cache.

```
Test-Connection SEA-DC1.contoso.com
```

3. At the Windows PowerShell command prompt, type the following command, and then press **Enter**. This displays the current DNS resolver cache.

```
ipconfig /displaydns
```

4. At the Windows PowerShell command prompt, type the following command, and then press **Enter**. This displays the current DNS resolver cache using a PowerShell command.

```
Get-DnsClientCache
```

5. At the Windows PowerShell command prompt, type the following command, and then press **Enter**. This flushes the current DNS resolver cache.

```
ipconfig /flushdns
```

6. At the Windows PowerShell command prompt, type the following command, and then press **Enter**. This flushes the current DNS resolver cache using a PowerShell command.

```
Clear-DnsClientCache
```

Note: It is not necessary to run this in addition to the preceding command.

7. At the Windows PowerShell command prompt, type the following command, and then press **Enter**. This verifies that you have no entries in the cache.

```
ipconfig /displaydns
```

Results: After completing this exercise you have verified current DNS settings on SEA-CL1 and used command line tools to view and clear the DNS client cache.

15.3 Exercise 2: Testing Name Resolution

15.3.1 Scenario

A user reports that SEA-CL1 cannot connect to www.Contoso.com or intranet.Contoso.com. To address the issue, you decide to add www to the hosts file along with the SEA-SVR1.contoso.com IP address. You will also add an alias DNS record for intranet.Contoso.com that resolves to SEA-SVR1.contoso.com. Finally you will verify name resolution and connectivity.

15.3.2 Task 1: Create and test a hosts file entry

1. On SEA-CL1, at the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
ping www
```

2. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
ping intranet
```

Note: Neither name is reachable because www and intranet cannot be resolved to a valid IP address.

3. At the Windows PowerShell command prompt, type the following command, and then press Enter.

```
notepad C:\windows\system32\drivers\etc\hosts
```

4. Scroll to the end of the file, type the following, and then press **Enter**.

```
172.16.0.11 www
```

5. Select **File**, and then select **Save**.
6. Close Notepad.
7. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
Test-Connection www
```

8. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
Get-DnsClientCache | Format-List
```

9. View the www record in the cache.
10. Leave PowerShell open.

15.3.3 Task 2: Add a DNS record

1. Sign in to **SEA-SVR1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start** and then select **Server Manager**.
3. In Server Manager, select **All Servers**.
4. Right-click SEA-DC1, and then select **DNS Manager**.
5. Expand the **Forward Lookup Zones** folder and select **Contoso.com**.
6. Select **Action** in the top menu, then select **New Alias (CNAME)**.
7. In the **Alias Name** field, type **intranet**.
8. In the Fully Qualified domain name (FQDN) field, type **SEA-SVR1.Contoso.com** and select **OK.**
9. Sign out of SEA-SVR1.
10. Switch to **SEA-CL1**.
11. In the PowerShell window, type the following command, and press **Enter**.

```
ping intranet.Contoso.com
```

10. Verify that intranet.Contoso.com is resolving to SEA-SVR1.contoso.com and IP Address 172.16.0.11.

15.3.4 Task 3: Troubleshoot name resolution

1. On SEA-CL1, at the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
nslookup www
```

Note: nslookup does not find the entry as it's only a hosts entry on the local computer.

2. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
nslookup intranet
```

3. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
Resolve-Dnsname SEA-SVR1 | Format-List
```

4. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
nslookup -debug intranet > file.txt
```

5. At the Windows PowerShell command prompt, type the following command, and then press **Enter**.

```
notepad file.txt
```

6. Review the information. Note that you might have to scroll to the section starting with **Got answer**.
7. What was the question that was asked of the DNS server?
   - QUESTIONS: intranet.Contoso.com, type = A, class = IN
8. What was the response?
   - ANSWERS: intranet.Contoso.com
   - canonical name = SEA-SVR1.Contoso.com
   - ttl = 3600 (1 hour)
   - SEA-SVR1.Contoso.com
   - internet address = 172.16.0.11

- ttl = 1200 (20 mins)

9. How long will the intranet.Contoso.com record be cached?
   - 1 hour
10. Close all open windows.
11. Sign out of SEA-CL1.

Results: After completing this exercise you have added a hosts file entry, created a DNS record, and tested name resolution.

END OF LAB

16 Practice Lab: Administering Windows 10 Using Remote Management

16.1 Summary

In this lab you will learn how to perform remote Windows administration using Remote PowerShell, Remote Desktop, and Windows Admin Center.

16.2 Exercise 1: Administering Windows using Remote PowerShell and Remote Desktop

16.2.1 Scenario

Your company is planning to open a new branch office. To manage the devices in the new branch office you need to use Remote PowerShell and Remote Desktop. You need to test remote administration by running remote PowerShell commands on SEA-SVR2 and you need to enable Remote Desktop on SEA-CL1.

16.2.2 Task 1: Perform remote management using Windows PowerShell

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password: **Pa55w.rd**.
2. Right-click **Start**, and then select **Windows PowerShell**.
3. To view all of the services that are stopped on SEA-SVR2, in the Windows PowerShell window, type the following command, and then press **Enter**:

   ```
   Get-Service -ComputerName SEA-SVR2 | Where-Object {$_.Status -eq "Stopped"}
   ```

4. To view the the content of the C:\Program Files folder on SEA-SVR2, in the Windows PowerShell window, type the following command, and then press **Enter**:

   ```
   Invoke-Command -ComputerName SEA-SVR2 -ScriptBlock {Get-ChildItem "C:\Program Files"}
   ```

5. To view the the System event log on SEA-SVR2, in the Windows PowerShell window, type the following command, and then press **Enter**:

   ```
   Invoke-Command -ComputerName SEA-SVR2 -ScriptBlock {Get-EventLog -log system}
   ```

6. To determine if the WinRM service is running on SEA-SVR2, in the Windows PowerShell window, type the following command, and then press **Enter**:

   ```
   Test-WsMan SEA-SVR2
   ```

   Note: The output on SEA-SVR2 validates that the WinRM service is running and it is ready to receive WS-Management requests. If it was not configure, you would have needed to run ***Winrm quickconfig*** *on SEA-SVR2.*

7. In the Windows PowerShell window, type the following commands, and then press **Enter** after each one:

   ```
   Enter-PSSession SEA-SVR2
   Get-command
   Add-Content Remote.txt "Adding text to file on SEA-SVR2"
   Exit-PSSession
   ```

16.2.3 Task 2: Enable Remote Desktop

1. On **SEA-CL1**, select **Start**, and then select the **Settings** icon.
2. In **Settings**, select **System**.
3. On the **System** tab, select **Remote Desktop**.
4. Switch **Enable Remote Desktop** on.
5. In the Remote Desktop Settings window select **Confirm**.
6. On the Remote Desktop page, select **Advanced settings**.
7. Verify that Require computers to use Network Level Authentication to connect is selected. Also take note of the Current Remote Desktop Port, which is set to 3389.
8. Close the Settings page and close Windows PowerShell.

Results: After completing this exercise, you will have enabled and tested remote PowerShell and Remote Desktop.

16.3 Exercise 2: Administering Windows using Windows Admin Center

16.3.1 Scenario

You need to test remote administration capabilities of the Windows Admin Center. For this scenario, you will install Windows Admin Center on SEA-CL1 and then perform remote administration tasks on SEA-SVR1.

16.3.2 Task 1: Install Windows Admin Center

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password: **Pa55w.rd**.
2. On the taskbar, select **File Explorer**.
3. In File Explorer, browse to **E:\Labfiles\Tools**, and then double-click **WindowsAdminCenter2009.msi**. Windows Installer begins the installation process.
4. On the **Windows Admin Center Setup** license page, select the check box next to **I accept these terms**, and then select **Next**.
5. Select **I don't want to use Microsoft Update**, and then select **Next**.
6. On the **Configure Gateway Endpoint** page, select **Next**.
7. On the **Installing Windows Admin Center** page, configure the following and then select **Install**:
   - Select a port for the Windows Admin Center site: **6516**
   - Allow Windows Admin Center to modify this machine's trusted hosts settings: **Selected**
   - Create a desktop shortcut to launch Windows Admin Center: **Selected**.
8. On the **One more thing** page, take note of the message and then select **Finish**.
9. Close File Explorer.

16.3.3 Task 2: Add connections to Windows Admin Center

1. On **SEA-CL1**, on the desktop, double-click the **Windows Admin Center** icon.
2. In the **Select a certificate for authentication** window, select **OK**.
3. On the **All connections** page, select **Add**.
4. On the **Add or create resources** page, in the **Servers** pane, select **Add**.
5. On the **Add one** tab, under **Server name**, type **SEA-SVR1**. Windows Admin Center queries Active Directory and then displays the server.
6. Select **Add** to add SEA-SVR1.Contoso.com to the All connections page.

16.3.4 Task 3: Perform Remote Administration using Windows Admin Center

1. In the **Windows Admin Center**, select **SEA-SVR1.Contoso.com**.
2. On the **Overview** page, take note of the server information and performance statistics.
3. On the **Tools** pane, select **Events**.
4. On the **Events** pane, take note of the event logs that are available from SEA-SVR1 and then under **Windows Logs** select **System**.
5. Review the System log events and then select the **Clear** button.
6. On the **Clear** prompt, select **Clear log**.
7. On the **Tools** pane, select **Files & file sharing**.
8. In the details pane, on the **File explorer** tab, take note of the file structure from SEA-SVR1.
9. In the details pane, select the **File share** tab. Take note of the current shared folders.
10. On the **Tools** pane, select **Local users & groups**. Take note of the Users and Groups tabs where you can manage local users and groups on SEA-SVR1.

11. On the **Tools** pane, select **PowerShell**. A remote PowerShell session is established to SEA-SVR1.
12. In the PowerShell pane, type `Get-Service` and then press Enter. SEA-SVR1 services are displayed.
13. On the **Tools** pane, select **Remote Desktop**. On the **Navigating away closes PowerShell** box, select **Continue**.
14. On the **Remote Desktop** page, read the message and then select **Go to settings**.
15. On the **Settings** page, select **Remote Desktop** and then under **Remote Desktop** select **Allow remote connections to this computer**. Select **Save**.
16. On the **Tools** pane, select **Remote Desktop**.
17. On the **Do you want to connect using the certificate presented by sea-svr1.contoso.com** prompt, select **Connect**.
18. On the **Enter credentials for the Remote Desktop connection**, type Username **Contoso\Administrator** with the Password of **Pa55w.rd**. Select **Connect**. The SEA-SVR1 desktop displays in the Remote Desktop pane.
19. Select **Disconnect**.
20. On the **Tools** pane, select **Roles & features**. Notice that you can remotely install or uninstall server roles and features on SEA-SVR1.
21. Close Windows Admin center and then sign out of SEA-CL1.

Results: After completing this exercise, you will have installed Windows Admin Center on SEA-CL1 and then performed remote administration tasks on SEA-SVR1.

END OF LAB

17 Practice Lab: Managing Storage

17.1 Summary

In this lab you will learn how to manage local disk storage using Disk Management and PowerShell.

17.2 Exercise 1: Creating and Managing a Simple Volume

17.2.1 Scenario

You need to add storage to SEA-WS2. Additional disks have been installed and you now have to create two new partitions to store data.

17.2.2 Task 1: Use Disk Management to initialize a disk

1. Sign in to SEA-WS2 as **Admin** with the password **Pa55w.rd**.

2. Right-click Start and select **Disk Management**.

3. In the **Initialize Disk** window, remove the check marks next to **Disk 2** and **Disk 3**, and then select **OK**. Disk 1 now has a status of Online.

17.2.3 Task 2: Create a simple volume using Disk Management

1. Right-click the Unallocated space on Disk 1, and then select **New Simple Volume**.

2. In the New Simple Volume Wizard window, select **Next**.

3. On the Specify Volume Size page, next to Simple volume size in MB, type **5120**, and then select **Next**.

4. On the Assign Drive Letter or Path page, make sure that **Assign the following drive letter: E** is selected, and then select **Next**.

5. On the Format partition page, in the Volume Label text box, type **Data**.

6. Ensure that the check box is selected next to **Perform a quick format**, and then select **Next**.

7. On the Completing the New Simple Volume Wizard page, select **Finish**. If you receive the error message Location is not available, then select OK.

   Note: If prompted to format drive E:, select Cancel.

8. From the taskbar, select **File Explorer**. Verify that you have a new E drive named Data.

9. Close the **File Explorer** window.

17.2.4 Task 3: Create a simple volume using PowerShell

1. Right-click Start and then select **Windows PowerShell (Admin)**.
2. At the command prompt, type the following and then press Enter:

```
New-Partition -DiskNumber 1 -Size 5gb -AssignDriveLetter
```

3. At the Microsoft Windows prompt, select **Format disk**.
4. In the Format Local Disk (F:) dialog box, select **Start** and then **OK**.
5. Select **OK** to close the Format Complete message.
6. In the Format Local Disk (F:) dialog box, select **Close**.
7. In **File Explorer**, verify that you have a new F drive named Local Disk.
8. Close the **File Explorer** window. If a Microsoft Windows prompt is visible select **Cancel**.
9. Switch to Disk Management and verify that Drive F shows 5GB in size.

17.2.5 Task 4: Extend a simple volume

1. In Disk Management, right-click **Data (F:)**, and then select **Extend Volume**.
2. In the Extend Volume Wizard window, select **Next**.
3. On the Select Disks page, next to Select the amount of space in MB, type **8192**, and then select **Next**.
4. On the Completing the Extend Volume Wizard page, select **Finish**. Notice that Drive F is now 13 GB in size.

17.2.6 Task 5: Shrink a simple volume

1. In Disk Management, right-click **(F:)**, and then select **Shrink Volume**.
2. On the Shrink F: page, next to Select the amount of space to shrink in MB, type **2048**, and then select **Shrink**. Notice that Drive F is now 11 GB in size.
3. Close all open windows and sign out of SEA-WS2.

Results: After completing this exercise, you will have managed local disk storage using Disk Management and Windows PowerShell.

END OF LAB

18 Practice Lab: Creating a Storage Space

18.1 Summary

In this lab you will configure a storage space that will combine multiple disk drives to one large single disk.

18.1.1 Scenario

The sales department requires a new file share on SEA-WS2 that requires a mirror for resiliency. You have added three new disk drives to SEA-WS2, and have decided to configure a storage space. You will remove the partition from Disk 1 first and then use Disk 1, Disk 2, and Disk 3 to create a two-way mirror storage pool inside a newly created storage space.

18.1.2 Task 1: Initialize the required disks

1. Sign in to **SEA-WS2** as **Admin** with the password **Pa55w.rd**.
2. Right-click **Start**, and then select **Windows PowerShell (Admin)**. At the User Account Control, select **Yes**.
3. To remove all data from Disk 1, at the PowerShell Window type the following command and confirm with ”Yes”:

```
Clear-Disk -Number 1 -RemoveData
```

4. To initialize Disk 1, Disk 2, and Disk 3, at the PowerShell Window type the following command:

```
Get-Disk | Where partitionstyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
```

5. Close Windows PowerShell.

18.1.3 Task 2: Create a mirrored storage pool

1. Select **Start**, and then type **Storage**. Select **Manage Storage Spaces** in the list.
2. Select **Create a new pool and storage space**. In the User Account Control, select **Yes**.
3. In the **Create a storage pool** window notice that Disk 1, Disk 2, and Disk 3 are selected. Select **Create pool**.
4. In the **Drive letter** dropdown field select **E:**
5. Notice that a Two-way mirror resiliency type is selected.
6. Click **Create storage space**. This will automatically open the File Explorer window.

18.1.4 Task 3: Verify the storage space

1. In File Explorer, right-click **Storage Space (E:)**, and then select **Properties**.
2. Notice that the capacity is approximately 187 gigabytes (GB).
3. Close all open windows.
4. Select **Start**, and then type **Storage**. Select **Manage Storage Spaces** in the list.
5. In the Storage Spaces dialog box expand the **Storage spaces** and the **Physical drives** sections.
6. Close the Storage Spaces window.
7. Sign out of SEA-WS2.

Results: After completing this exercise, you will have created and verified a two-way mirror storage space.

END OF LAB

19 Practice Lab: Configuring and Managing Permissions and Shares

19.1 Summary

In this lab you will learn how to create folders and manage local and share permissions.

19.1.1 Scenario

You need to create file shares for the Marketing and IT department to enable users to store their shared files. You have to ensure that only people from the specific departments have access to the files. You decide to create both shares on SEA-CL1 in the E:\Data folder. The IT department requires that the share and local folder is only accessible to members of the IT group. You advise Bruce Keever and Briana Hernandez to test the file shares and local access to the files.

19.1.2 Task 1: Create a folder structure

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select the **File Explorer** icon on the taskbar.
3. In File Explorer, in the navigation pane, expand **This PC**, and then select **Allfiles (E:)**. In the details pane, right-click the **empty space**, select **New**, select **Folder**, and then type **Data** for the new folder's name.
4. In File Explorer, in the navigation pane, expand **Allfiles (E:),** and select **Data**. In the details pane, right-click the empty space, select **New**, select **Folder**, and then type **Marketing** for the new folder's name.
5. In File Explorer, in the details pane, right-click the **empty space**, select **New**, select **Folder**, and then type **IT** for the new folder's name.

19.1.3 Task 2: Review default permissions

1. Right-click the **IT** folder, and then select **Properties**.
2. In the IT Properties window, select the **Security tab**, and then select **Edit**.
3. In the Permissions for IT dialog box, verify that Authenticated Users is selected in the Group or user names section, and then select **Remove**. Read the text in the Windows Security dialog box that appears, which explains why you cannot remove an Authenticated Users. select **OK**, and then select **Cancel**.

4. In the IT Properties window, on the Security tab, select **Advanced**.
5. In the Advanced Security Settings for IT dialog box, verify that all permissions entries are inherited from E:\. Also, verify that Users (SEA-CL1\Users) have Read & execute access, while Authenticated Users have Modify access. Select **OK** twice.

19.1.4 Task 3: Configure permissions for the IT and Marketing folders

1. On SEA-CL1, in File Explorer, right-click the **IT** folder, select **Give access to**, and then select **Specific people**.
2. In the Type a name and then select Add, or select the arrow to find someone text box, type **IT**, and then select **Add**.
3. Verify that IT is added and selected. In the Permission Level column, select **Read/Write**, select **Share**, and then select **Done**.
4. Right-click **Marketing**, and then select **Properties**.
5. In the Marketing Properties dialog box, select the **Sharing tab**. In the Network File and Folder Sharing section, verify that Marketing is not shared.
6. In the Advanced Sharing section, Select **Advanced Sharing**.
7. In the Advanced Sharing dialog box, select the **Share this folder** check box. Verify that the share name is Marketing (the same as the folder name), and that Limit the number of simultaneous users to is set to 20.
8. Select **Permissions**.
9. In the Permissions for Marketing dialog box, select the **Everyone** group and select **Remove**.
10. Select **Add**, in the Enter the object names to select (examples) box, type **Marketing**, and then select **OK**. In the Permissions for Marketing section, select the **Change** check box in the Allow column, and then select **OK** twice.
11. In the Marketing Properties dialog box, in the Network File and Folder Sharing section, verify that Marketing is now shared as \\LON-CL1\Marketing, and then select **Close**.
12. Select **Start**, type **cmd** and then select **Command Prompt**.
13. At the command prompt, type the following command, and then press **Enter**.

    ```
    net view \\sea-cl1
    ```

    Note: *This will show you all shares created on SEA-CL1*
14. Close the command prompt.
15. Right-click **Start**, and then select **Computer Management**.
16. In Computer Management, in the navigation pane, expand **Shared Folders**, and then select **Shares**. In the details pane, verify that you see IT and Marketing shares, and the default Windows 10 administrative shares.
17. Close Computer Management.

19.1.5 Task 4: Review configured permissions

1. On SEA-CL1, in File Explorer, right-click **IT**, and then select **Properties**.
2. In the IT Properties window, select the **Security** tab, and then select **Advanced**.
3. In the Advanced Security Settings for IT dialog box, verify that all the permissions entries are set explicitly at this level, because their permission inheritance is set to None.
4. Verify that only the Administrator, Administrators (SEA-CL1\Administrators) group, SYSTEM and IT (Contoso\IT) group have access to the IT folder. These settings match the permissions that you configured in the File Sharing dialog box.
5. In the Advanced Security Settings for IT dialog box, select **OK**.

6. In the IT Properties dialog box, select the **Sharing** tab, in the Network File and Folder Sharing section, verify that IT now is shared as \\Sea-cl1\it, and then select **Advanced Sharing**.

7. In the Advanced Sharing dialog box, select **Permissions**. In the Permissions for IT dialog box, verify that the Everyone and Administrators groups have Full Control permissions to the share, select **OK** twice, and then select **Close**.

   Note: *If you share a folder by using the File Sharing dialog box, you will modify the local file permissions to match your configuration, while the Everyone and Administrators groups will have the Full Control share permission.*

8. In File Explorer, right-click **Marketing**, and then select **Properties**.

9. In the Marketing Properties window, select the **Security tab**, and then select **Advanced**.

10. In the Advanced Security Settings for Marketing dialog box, verify that all of the permissions entries are inherited from E:\. Also verify that Users (SEA-CL1\Users) have Read & execute access, while Authenticated Users have Modify access, which are the same file permissions as before you shared the Marketing folder. Select **OK** twice.

    Note: *If you share a folder by using the Advanced Sharing feature, this does not modify local file permissions. You only modify share permissions if you use Advanced Sharing.*

11. Sign out of **SEA-CL1**.

19.1.6 Task 5: Test local file permissions

1. Sign in to **SEA-CL1** as **Contoso\Bruce** with the password **Pa55w.rd**.

   Note: *Bruce is a member of the Marketing group, but is not a member of the IT group.*

2. Select the **File Explorer** icon on the taskbar.

3. In File Explorer, in the navigation pane, expand **This PC**, expand **AllFiles (E:)**, expand **Data**, and then select **Marketing**.

4. In the details pane, right-click the empty space, select **New**, select **Text Document**, and then type **File10** as the name of the file.

   Note: *Bruce has local file permissions to create a new file in the Marketing folder, because permissions were configured by using the Advanced Sharing feature. This modified only the share permissions, while the default local file permissions were not modified. By default, Authenticated Users have the Modify permission.*

5. In File Explorer, in the navigation pane, select **IT**, and then select **Cancel**.

   Note: *You will get an error, because Bruce does not have local file permissions to the IT folder. Permissions were configured by File Sharing,and only members of the IT group have local file permissions to the folder.*

6. Sign out of **SEA-CL1**.

7. Sign in to **SEA-CL1** as **Contoso\Briana** with the password **Pa55w.rd**.

   Note: *Briana is member of the IT group, and she is not member of the Marketing group.*

8. Select the **File Explorer** icon on the taskbar.

9. In File Explorer, in the navigation pane, expand **This PC**, expand **AllFiles (E:)**, expand **Data**, and then select **Marketing**.

10. In the details pane, verify that you can see File10 that was created by Bruce.

11. Right-click the empty space, select **New**, select **Text Document**, and then type **File20** as the name of the file.

    Note: *Briana has local file permissions to create a new file in the Marketing folder because you configured permissions by using the Advanced Sharing feature. This modified only the share permissions, while the default local file permissions were not modified. By default, Authenticated Users have the Modify permission.*

12. In File Explorer, in the navigation pane, select **IT**. In the details pane, right-click the empty space, select **New**, select **Text Document**, and then type **File21** as the name of the file.

    Note: *Briana is able to create a file, because you configured permissions by using File Sharing. Members of the IT group have local file permissions to the IT folder.*

    Note: *Be aware that Network File and Folder Sharing modifies file permissions and share permissions. However, the Advanced Sharing feature does not modify file permissions, and only sets share permissions.*

13. Sign out of **SEA-CL1**.

19.1.7 Task 6: Test share permissions

1. Switch to **SEA-CL2**.
2. Sign in to **SEA-CL2** as **Contoso\Bruce** with the password **Pa55w.rd**.

   Note: *Bruce is a member of the Marketing group, but he is not a member of the IT group.*

3. Select the **File Explorer** icon on the taskbar.
4. In File Explorer, type **\\SEA-CL1** in the Address bar, and then press **Enter**.
5. Verify that you can see the IT and Marketing shares in the details pane.
6. Double-click **Marketing**. Verify that you can see the files that Bruce and Briana created locally.
7. In the details pane, right-click the empty space, select **New**, select **Text Document**, and then type **File30** as the name of the file. Bruce has permissions to create a new file in the Marketing share because he is a member of the Marketing group.
8. In File Explorer, select **SEA-CL1** in the address bar. In the details pane, double-click **IT**. Read the text in the Network Error dialog box, and then select **Close**.

   Note: *Bruce is not a member of the IT group, so he does not have permissions to the IT share.*

9. Sign out of **SEA-CL2**.
10. Sign in to **SEA-CL2** as **Contoso\Briana** with the password **Pa55w.rd**.

    Note: *Briana is a member of the IT group, but she is not a member of the Marketing group.*

11. Select the **File Explorer** icon on the taskbar.
12. In File Explorer, type **\\SEA-CL1** in the Address bar, and then press **Enter**.
13. Verify that you can see the IT and Marketing shares in the details pane.
14. Double-click **Marketing**.
15. Read the text in the Network Error dialog box.

    Note: *Briana is not a member of the Marketing group, so she does not have permissions to the Marketing share.*

16. Select **Close**.
17. In the details pane, double-click **IT**. Right-click the empty space in the details pane, select **New**, select **Text Document**, and then type **File40** as the name of the file.

    Note: *Briana has permissions to create a new file in the IT share because she is a member of the IT group. Users can connect only to shares that were shared for groups in which they are members, regardless of whether they were shared by File Sharing or Advanced Sharing.*

18. Sign out of **SEA-CL2**.

Results: After completing this exercise, you will have created a folder structure for the Marketing and information technology (IT) departments, shared their folders, and tested local and share permissions.

END OF LAB

20 Practice Lab: Using Conditions to Control Access and Effective Permissions

20.1 Summary

In this lab you will learn how to use conditions to dynamically control access to files based on specific criteria.

20.1.1 Scenario

Members of the IT, Marketing, and Research departments all require access to file shares located on SEA-CL1, but require different permissions for the data they use. You've been instructed to create a new shared folder in E:\Data named Research. The Research shared folder should only be accessible by users in the Research Department. The IT shared folder should only by accessible by employees located in the United States who are members of the IT Department. The Active Directory administrator has already configured Dynamic Access Control to allow for you to assign Department and Country based Claim Types to permissions on shared folders.

20.1.2 Task 1: Configure conditions to control access

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select the **File Explorer** icon on the taskbar.
3. In File Explorer, in the navigation pane, expand **AllFiles (E:)**, and then select **Data**. In the details pane, right-click the empty space, select **New**, select **Folder**, and type **Research** as the new folder name.
4. Right-click **Research**, select **Properties**, select the **Sharing** tab, and then select **Advanced Sharing**.
5. In the Advanced Sharing dialog box, select the **Share this folder** check box, and then select **Permissions**.
6. In the Permissions for Research dialog box, in the Permissions for Everyone section, select the **Change** check box in the Allow column, and then select **OK** twice.
7. In the Research Properties dialog box, select the **Security** tab, select **Advanced**, and then verify that all permissions entries are inherited from E:\.
8. In the Advanced Security Settings for Research dialog box, select **Users (SEA-CL1\Users)**, and then select **Remove**. Read the text in the Windows Security dialog box that appears, select **OK**
9. Select **Disable inheritance**.
10. In the Block Inheritance dialog box, select **Convert inherited permissions into explicit permissions on this object**, and then verify that all permissions entries are set explicitly at this level because their permission inheritance is set to **None**.
11. In the Advanced Security Settings for Research dialog box, select **Users (SEA-CL1\Users)**, and then select **Remove**.

    Note: *The entry for Users is now removed from the Permission entries because it was explicitly set at this level.*

12. Verify that **Authenticated Users** is selected, and then select **Edit**.
13. In the Permission Entry for Research dialog box, select **Add a condition**, and compose the following expression: **User Department Equals Value Research**. You will need to type research manually in the last box. Select **OK** twice, then select **Close**.

    Note: *A claim type for the department attribute was preconfigured for the purpose of this lab.*

14. In File Explorer, in the navigation pane, select **Data**, right-click **IT**, select **Properties**, select the **Security** tab, and then select **Advanced**.
15. In the Advanced Security Settings for IT dialog box, select **IT (Contoso\it)**, and then select **Edit**.
16. In the Permission Entry for IT dialog box, select **Add a condition**, and compose the following expression: **User Country Equals Value US**. You will need to type US manually in the last field. select **OK** three times.

    Note: *A claim type for the c (country) attribute was preconfigured for the purpose of this lab.*

17. Select **OK** twice, then select **Close** to close the IT Properties window.

18. Sign out of SEA-CL1.

20.1.3 Task 2: Test conditions to control access

1. Sign in to **SEA-CL1** as **Contoso\Briana** with the password **Pa55w.rd**.
2. Select the **File Explorer** icon on the taskbar.
3. In File Explorer, type \\SEA-CL1 in the Address bar, and then press **Enter**.
4. In the details pane, double-click **Research**. Read the text in the Network Error dialog box, and then select **Close**.
5. Select **Start**, type **cmd** and then select **Command Prompt**.
6. At the command prompt, type the command, `whoami /claims` and then press **Enter**. Review the output, and then **close** the command prompt.

   Note: *This will show the current claims for the user. Briana has a department claim value of IT and so she cannot connect to the Research share.*
7. In the details pane, double-click **IT**.
8. In the details pane, right-click the empty space, select **New**, select **Text Document**, and then type **File50** as the name of the file.

   Note: *Briana has permissions to create a new file in the IT share because she is a member of the IT group and her Country claim has a value of US.*
9. Sign out of **SEA-CL1**.
10. Sign in to **SEA-CL2** as **Contoso\Mike** with the password **Pa55w.rd**.

    Note: *Mike is a member of the IT group.*
11. Select the **File Explorer** icon on the taskbar.
12. In File Explorer, type \\SEA-CL1 in the Address bar, and then press **Enter**.
13. In the details pane, double-click **IT**.

    Note: *Mike is a member of the IT group, but he cannot connect to the IT share.*
14. Select **Close**.
15. Select **Start**, type **cmd** and then select **Command Prompt**
16. At the command prompt, type the following command, and then press **Enter** `whoami /claims`. Review the output, and then **close** the command prompt.

    Note: *Mike has a Country claim with the value of GB, so he cannot connect to the IT share, even though he is a member of the IT group.*
17. Sign out of **SEA-CL2**.
18. Sign in to **SEA-CL2** as **Contoso\Davy** with the password **Pa55w.rd**.
19. Select **Start**, type **cmd** and then select **Command Prompt**.
20. At the command prompt, type the following command, `whoami /claims`, and then press **Enter**.
21. Review the output, and then close the command prompt.

    Note: *Davy is in the Research department, and his department claim has the value of Research.*
22. Select the **File Explorer** icon on the taskbar.
23. In File Explorer, type \\SEA-CL1 in the Address bar, and then press **Enter**.
24. In the details pane, double-click **Research**, and then verify that Davy can view the contents of the Research folder.
25. In the details pane, right-click the **empty space**, select **New**, select **Text Document**, and then type **File60** as the name of the file.

__Note:__ Davy has permissions to create a new file in the Research share because his department claim has a value of Research.

26. Sign out of **SEA-CL2**.

20.1.4 Task 3: View effective permissions

1. Switch to **SEA-CL1**.
2. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
3. Select the **File Explorer** icon on the taskbar.
4. In File Explorer, browse to **E:\Data**.
5. In File Explorer, right-click **Marketing**, select **Properties**, select the **Security tab**, select **Advanced**, and then select the **Effective Access** tab.
6. In the Advanced Security Settings for Marketing dialog box, select **Select a user**, in the Enter the object name to select (examples) box, type **Anders**, select **OK**, and then select **View effective access**. View the effective permissions, and then select **OK** twice.

   __Note:__ As Authenticated Users have the Modify permission to the Marketing folder, you can see that Anders has the most permissions allowed.

7. In File Explorer, right-click **Research**, select **Properties**, select the **Security** tab, select **Advanced**, and then select the **Effective Access** tab.
8. In the Advanced Security Settings for Research dialog box, select **Select a user**, in the Enter the object name to select (examples) text box, type **Brian**, select **OK**, and then select **View effective access**.

   __Note:__ Brian is a member of Development group. Only users with the department claim with a value of Research have permissions to the folder, you can see that Brian has no permissions allowed.

9. In the Advanced Security Settings for Research dialog box, select **Include a user claim**, select **department** in the drop-down list, type **Research** in the Enter value here text box, and then select **View effective access**.

   __Note:__ You can see that if Brian had the department user claim with the value of Research, he would have most permissions allowed.

10. In the Advanced Security Settings for Research dialog box, select **Select a user**, in the Enter the object name to select (examples) box, type **Aaron**, select **OK**, and then select **View effective access**. Review the effective permissions, and then select **OK** twice.

    __Note:__ If Aaron had the user claim of department with the value of Research, he would have the most permissions allowed.

11. Sign out of **SEA-CL1**.

Results: After completing this exercise, you will have configured and tested conditions to control access to file shares. You will have also viewed effective permissions.

END OF LAB

21 Practice Lab: Work Folders

21.1 Summary

In this lab you will learn how to configure Work Folders as a method of synchronizing files to provide access from multiple devices.

21.1.1 Scenario

Members of the Marketing group often use multiple devices for their work. To help manage file access you decide to implement Work Folders. This allows for files to be stored in a central location and synchronized to each device automatically. To implement this solution, first you will install and configure the Work Folders server role on SEA-SVR1 and store the content in a shared folder named C:\syncshare1. To enable the Work Folders for all marketing users, you configure a Group Policy Object to point to https://SEA-SVR1.Contoso.com. You have asked Bruce Keever to test the solution on a domain-joined device named SEA-CL1 and a stand-alone device named SEA-WS3. Bruce will validate synchronization and identify how synchronization conflicts are handled.

21.1.2 Task 1: Install and Configure Work Folders

1. Sign in to **SEA-SVR1** as **Contoso\Administrator** with the password **Pa55w.rd.**
2. Right-click **Start**, and then select **Windows PowerShell (Admin)**.
3. In Windows PowerShell, type the following cmdlet, and then press **Enter**:

   ```
   Install-WindowsFeature FS-SyncShareService
   ```

   Note: *After the feature installs, you might see a warning display, because Windows automatic updating is not enabled. For the purposes of this lab, ignore the warning.*
4. In Windows PowerShell, type the following cmdlet, and then press **Enter**:

   ```
   Start-Service SyncShareSvc
   ```
5. Close the **Windows PowerShell** window.
6. Select **Start**, and then select **Server Manager**.
7. In Server Manager, in the navigation pane, select **File and Storage Services**, and then select **Work Folders**.
8. In the **WORK FOLDERS** section, select **TASKS**, and then select **New Sync Share**.
9. In the **New Sync Share Wizard**, on the **Before you begin** page, select **Next**.
10. On the **Select the server and path** page, in the **Enter a local path** text box, type **C:\syncshare1**, select **Next**.

    Important: *If **SEA-SVR1** is not listed in the **Server** section, select **Cancel**. In Server Manager, select **Refresh**, and then repeat this task, beginning with step 6 and completing the remaining steps. This may take a few minutes for SEA-SVR1 to show.*
11. In the New Sync Share Wizard dialog select **OK**.
12. On the **Specify the structure for user folders** page, verify that **User alias** is selected, and then select **Next**.
13. On the **Enter the sync share name** page, select **Next** to accept the default sync share name.
14. On the **Grant sync access to groups** page, select **Add**, and in the **Enter the object name to select** text box, type **Marketing**. select **OK**, and then select **Next**.
15. On the **Specify security policies for PCs** page, verify the two available options. Clear the **Automatically lock screen, and require a password** check box, and then select **Next**.
16. On the **Confirm selections** page, select **Create**.
17. On the **View Results** page, select **Close**.
18. In Server Manager, in the **WORK FOLDERS** section, verify that **syncshare1** is listed, and that in the **USERS** section, the user **Bruce Keever** is listed.
19. On **SEA-SVR1**, in Server Manager, select **Tools**, and then select **Internet Information Services (IIS) Manager**.
20. In the Microsoft Internet Information Services (IIS) Manager, in the navigation pane, expand **SEA-SVR1 (Contoso\Administrator)**. Expand **Sites**, right-click **Default Web Site**, and then select **Edit Bindings**.
21. In the **Site Bindings** dialog box, select **Add**.
22. In the **Add Site Binding** dialog box, in the **Type** box, select **https**. In the **SSL certificate** box, select **Work Folders Cert**, select **OK**, and then select **Close**.
23. Close the IIS Manager.

21.1.3 Task 2: Create a GPO to deploy the Work Folders

1. On **SEA-SVR1**, in Server Manager, select **Tools,** and then select **Group Policy Management**.
2. In the Group Policy Management console, in the navigation pane, expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**, and then select the **Marketing** organizational unit (OU).
3. Right-click **Marketing**, and then select **Create a GPO in this domain, and Link it here**. In the **Name** text box, type **Deploy Work Folders**, and then select **OK**.
4. Right-click **Deploy Work Folders**, and then select **Edit**.
5. In the Group Policy Management Editor, in the navigation pane expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then select **Work Folders**.
6. In the details pane, right-click **Specify Work Folder settings**, and then select **Edit**.
7. In the **Specify Work Folder settings** dialog box, select **Enabled**. In the **Work Folders URL** text box, type https://SEA-SVR1.Contoso.com, select the **Force automatic setup** check box, and then select **OK**.
8. Close the Group Policy Management Editor and the Group Policy Management console.
9. Close Server Manager.

21.1.4 Task 3: Test the work folders

1. Switch to **SEA-CL1**.

2. Sign in to **SEA-CL1** as **Contoso\Bruce** with the password **Pa55w.rd**.

3. Select the **File Explorer** icon on the taskbar.

4. In the navigation pane, select **Work Folders**.

5. In the details pane right-click the empty space, select **New**, select **Text Document**, and then name the file **On SEA-CL1**.

6. Select **Start**, type **Work folders** and select **Manage Work Folders**.

7. On the Manage Work Folders page, check the option **Sync files over metered connections**.

   Note: *This is only needed due to the hosted lab environment configuration.*

8. Close the **Manage Work Folders** window.

9. Switch to **SEA-WS3**.

10. Sign in to **SEA-WS3** as **SEA-WS3\Admin** with the password **Pa55w.rd**.

11. On **SEA-WS3** select **Start**, type **\\SEA-DC1\certenroll**, and then press **Enter**.

12. In the **Enter Network credentials** dialog box, enter the user name as **Contoso\Administrator** and the password as **Pa55w.rd**. Select **OK**.

13. In the **certenroll** window, double-click **SEA-DC1.Contoso.com_ContosoCA.crt.**

14. On the **Certificate** dialog box, select **Install Certificate**.

15. On the **Certificate Import Wizard**, select **Local Machine** and select **Next**.

16. On the **User Account Control** dialog box, select **Yes**.

17. On the **Certificate Store** page, select **Place all certificates in the following store**, and then select **Browse**.

18. On the **Select Certificate Store** page, select **Trusted Root Certification Authorities** and select **OK**.

19. On the **Certificate Store** page, select **Next**.

20. On the **Certificate Import Wizard** page, select **Finish**.

21. In the **Certificate Import Wizard** dialog select **OK**, and then in the **Certificate** window, select **OK**.

22. Restart **SEA-WS3**.

23. Sign in to **SEA-WS3** as **SEA-WS3\Admin** with the password **Pa55w.rd**.

24. On **SEA-WS3**, select **Start**, type **Control Panel**, and then press Enter.

25. In Control Panel, select **System and Security,** and then select **Work Folders**.

26. On the **Manage Work Folders** page, select **Set up Work Folders**.
27. On the **Enter your work email address** page, select **Enter a Work Folders URL instead**.
28. On the **Enter a Work Folders URL** page, in the **Work Folders URL** text box, type https://SEA-SVR1.Contoso.com, and then select **Next**.
29. In the **Windows Security** dialog box, in the **User name** text box, type **Contoso\Bruce**, and in the **Password** text box, type **Pa55w.rd**, and then select **OK**.
30. On the **Introducing Work Folders** page, review the local Work Folders location, and then select **Next**.
31. On the **Security policies** page, select the **I accept these policies on my PC** check box, and then select **Set up Work Folders**.
32. On the **Work Folders has started syncing with this PC** page, select **Close**.
33. Switch to the Manage Work Folders window.
34. On the Manage Work Folders window, check the option **Sync files over metered connections**.

    Note: *This is only needed due to the hosted lab environment configuration.*
35. Switch to the Work Folders File Explorer window.
36. Verify that the **On SEA-CL1.txt** file displays.
37. Right-click in the details pane, select **New**, select **Text Document**, and then in the **Name** text box, type **On SEA-WS3**, and then press **Enter**.

21.1.5 Task 4: Test conflict handling

1. Switch to **SEA-CL1**.
2. On **SEA-CL1**, in **Work Folders**, verify that that both files, **On SEA-CL1** and **On SEA-WS3**, display.
3. In the notification area, right-click the connection icon, and then select **Open Network & Internet settings**.
4. Select the Ethernet page, and then select **Change adapter options**.
5. Right-click **Ethernet**, and then select **Disable**. In the **User Account Control** dialog box, in the **User name** text box, type **Administrator**. In the **Password** text box, type **Pa55w.rd**, and then select **Yes**.
6. In **Work Folders**, double-click the **On SEA-CL1** file.
7. In Notepad, type **Modified offline**, press Ctrl+S, and then close Notepad .
8. In **Work Folders**, right-click in the details pane, select **New**, select **Text Document**, and then name the file **Offline SEA-CL1**.
9. Switch to **SEA-WS3.**
10. On **SEA-WS3**, in **Work Folders**, double-click the **On SEA-CL1.txt** file.
11. In Notepad, type **Online modification,** press Ctrl+S, and then close Notepad.
12. Switch to **SEA-CL1.**
13. On **SEA-CL1**, in the **Network Connections** window, right-click **Ethernet**, and then select **Enable**.
14. In the **User Account Control** dialog box, in the **User name** text box, type **Administrator**, and in the **Password** text box, type **Pa55w.rd**, and then select **Yes**.
15. Switch to **Work Folders**, and then verify that files display in the details pane, including **On SEA-CL1** and **On SEA-CL1-SEA-CL1**.

    Note: Because you modified the file at two locations, a conflict occurred, and one of the copies was renamed.
16. Sign out from **SEA-CL1** and **SEA-WS3**.

Results: After finishing this lab you have installed and configured Work Folders.

21.1.6 Lab cleanup

1. Sign in to **SEA-SVR1** as **Contoso\Administrator** with the password **Pa55w.rd.**
2. Right-click **Start**, and then select **Windows PowerShell (Admin)**.
3. In Windows PowerShell, type the following cmdlet, and then press **Enter**:

   ```
   Remove-WindowsFeature FS-SyncShareService
   ```

   Note: *The feature will be removed and requires a restart of the server.*
4. In Windows PowerShell, type the following cmdlet, and then press **Enter**:

   ```
   Restart-Computer
   ```

END OF LAB

22 Practice Lab: Synchronizing files with OneDrive

22.1 Summary

In this lab you will learn how to synchronize content between devices using OneDrive.

22.1.1 Scenario

Your organization would like to leverage OneDrive as a method for accessing user files from any device. You test this solution by signing in with your Microsoft account and creating a file on SEA-WS2 and verifying that the file automatically synchronizes to SEA-WS1.

Note: To complete this lab, you need to have a Microsoft account. You can use the Microsoft Account that you configured previously in the Module 3: Synchronizing settings between devices lab. If needed please refer to Module 3 for adding your Microsoft account to SEA-WS1 and SEA-WS2.

22.1.2 Task 1: Enable OneDrive sync on SEA-WS2

1. Sign in to **SEA-WS2** with your Microsoft account and the PIN **1029**.
2. On the task bar, select **File Explorer**, and then select the **OneDrive** node.

Note: *The OneDrive node in File Explorer might take several minutes to appear. Please wait for it to appear before proceeding. If it takes longer than 15 minutes, sign out, and then sign back in by using your Microsoft account.*

3. In the File Explorer console tree, expand **OneDrive**, and then select the **Documents** folder.

   If the Documents folder is not visible, wait approximately 5 minutes for it to appear.
4. Right-click the empty space in the **Details pane**, select **New**, and then select **Text Document**.
5. Type **File from SEA-WS2** in the **Name** box, and then press Enter.
6. Double-click the document, and when Notepad opens, type **I was here on SEA-WS2**. Press **Ctrl+S**, and then close Notepad.
7. Wait until OneDrive has synchronized the changes indicated by a green check mark symbol in the **Status** row.

Note: *If OneDrive indicates it is paused, right-click on the OneDrive status icon, select Resume Syncing.*

22.1.3 Task 2: Sign in to SEA-WS1 with your Microsoft account, and update the synchronized document

1. Switch to **SEA-WS1**.
2. Sign in to **SEA-WS1** with your Microsoft account with the PIN **1029**.
3. On the task bar, select **File Explorer**, and then select the **OneDrive** node.

4. In the **File Explorer** console tree, expand **OneDrive**, and then select the **Documents** folder. After a few minutes, the **File from SEA-WS2** document should appear (it can take up to five minutes).

   ***Note**: By default OneDrive has the Files On-Demand feature enabled that will download files only on the first use on a device. Such cloud files that have been created Online or on another device are indicated by a cloud symbol in Status.*

5. Double-click the **File from SEA-WS2** document.

   ***Note**: The file will now be downloaded to your device before it will open. If OneDrive indicates it is paused, right-click on the OneDrive status icon, select Resume Syncing.*

6. In the **Notepad** window, directly under the **I was here on SEA-WS2** line, type **Now I'm here on SEA-WS1**, and then press **Enter**.
7. Press **Ctrl+S**, and then close Notepad.
8. Make a note of the date and time of the **File from SEA-WS2** file.
9. Switch to **SEA-WS2**.
10. Check the date and time of the **File from SEA-WS2** document. When it changes to the date and time you noted on **SEA-WS1**, double-click the file (it takes up to five minutes to change).

```
_**Note**: You should now see the two lines in Notepad._
```

11. Close Notepad.
12. Right-click the **File from SEA-WS2** document, and select **Always keep on this device.**

    ***Note**: The check mark symbol in Status will now change to a white check mark in a green circle indicating that this file is always available on your device.*

13. Right-click the **File from SEA-WS2** document, and select **Free up space.**

    ***Note**: This will convert the file back to an online document indicated by the cloud symbol that needs to be downloaded on the first use. This is intended to free up space on your local hard disk.*

14. Sign out of **SEA-WS1** and **SEA-WS2**.

Results: During this lab you have synchronized files between different devices using OneDrive.

END OF LAB

23 Practice Lab: Installing Apps in Windows 10

23.1 Summary

In this lab you will learn how install and update Microsoft Store Apps and how to install Microsoft 365 Apps for enterprise from Microsoft 365.

Dependency Note: To complete this lab, you need to have a Microsoft account. You can use the Microsoft Account that you configured previously in the Module 3 lab: Synchronizing settings between devices lab. You will also use the User2 Microsoft 365 user account, which was created in Module 2 lab: Managing Azure AD Authentication.

23.2 Exercise 1: Installing and updating Windows Store apps

23.2.1 Scenario

You need to test the download and update functionality of the Microsoft App Store. You will download and install an app named the **Microsoft To Do: Lists, Tasks & Reminders**. You also need to validate how Microsoft Store apps are updated and uninstalled.

23.2.2 Lab preparation

Note: In some situations, the Windows Update service may be disabled. Use the following steps to validate and enable the Windows update service if needed. Not that this is not necessary to run in typical Windows 10 scenarios.

1. Sign in to **SEA-WS1** as **Admin** with the password of **Pa55w.rd**.

2. Right-click **Start**, and then select **Windows PowerShell (Admin)**.
3. In the **User Account Control** dialog box, select **Yes**.
4. In the **Administrator: Windows PowerShell** window, type **the following command** and then press **Enter**.

```
Set-Service wuauserv -Startuptype Manual
```

5. Sign out of SEA-WS1.

23.2.3 Task 1: Install a Windows Store app

1. Sign in to **SEA-WS1** with your Microsoft account and the PIN **1029**.
2. In the taskbar, select the **Microsoft Store** icon.
3. In the Microsoft Store app, select **Search**, type **Microsoft To Do**, and then select **Microsoft To Do: Lists, Tasks & Reminders**.
4. Select **Get**.

   Note: If prompted by the Your account is missing some key info dialog box, complete the information regarding Birthdate and Country/Region and select ***Next****.*

5. If a **Try again later** dialog box appears, select **Close**.
6. Wait for the download and installation to finish and then then select **Launch**.
7. In the message dialog box, select **No** and then close **Microsoft To Do**.
8. Select **Start** and verify that Microsoft To Do is added to the Start menu.

23.2.4 Task 2: Configure app updates

1. In the **Microsoft Store** app, select the the **See more** ellipsis symbol on the menu bar, and then select **Settings**.
2. In **Settings**, under **App updates**, verify that **Update apps automatically** is set is enabled.
3. In the **Microsoft Store** app, select the **See more** icon on the menu bar, and then select **Downloads and updates**. Notice that there are several apps waiting to be updated.
4. Select **Update all**.
5. After the updates start, select **Pause all**.
6. Select **Start**, right-click **Feedback Hub**, and then select **Uninstall**.
7. In the **This app and its related info will be uninstalled** dialog box, select **Uninstall**.
8. Sign out of SEA-WS1.

Results: After completing this exercise, you will have installed a Microsoft Store app, managed Microsoft Store app updates, and uninstalled an app.

23.3 Exercise 2: Install Microsoft 365 Apps for Enterprise from Microsoft 365

23.3.1 Scenario

You have been asked to configure the deployment of the Office 365 apps included in your subscription. You will first assign an Office 365 E5 license to User2 and configure Office installation options. Finally User2 will validate that Office 365 can be downloaded and installed from the Microsoft 365 portal.

23.3.2 Task 1: Assign a Microsoft 365 license

1. Sign in to **SEA-WS1** with your Microsoft account and the PIN **1029**.
2. In the taskbar, select the **Microsoft Edge **icon.
3. In the address bar, enter http://portal.office.com.
4. In the **Sign in** dialog box, enter your admin email address as provided by your instructor. It should be in the form of admin@M365xXXXXXX.onmicrosoft.com and then select **Next**.

5. At the **Enter password** dialog box, enter the password as provided by your instructor. When prompted to save the password, select **Save**.
6. When prompted to **Stay signed in**, select **Yes**.
7. From the App Launcher, select **Admin**.
8. In the Microsoft 365 admin center, in the Navigation menu, expand **Users**, and then select **Active users**.
9. In the User list, select **User2**. This user should have been created earlier in module 2. If you do not have this user, refer to the Module 2 lab: Managing Azure AD Authentication.
10. In the User2 properties, select the **Licenses and apps** tab.
11. In the Licenses list, select **Office 365 E5**, and then select **Save changes**.
12. Close the User2 properties page.

23.3.3 Task 2: Configure Office installation options

1. In the Microsoft 365 admin center, in the Navigation menu, expand **Settings**, and then select **Org settings **.
2. In the **Org settings** page, on the **Services** page, select **Office installation options**.
3. On the Office installation options page, under Feature updates, select **Once a month (Monthly Enterprise Channel)**.
4. Under Office apps that users can install, remove the check box next to **Skype for Business (Standalone)**, and then select **Save**.
5. Close the Office installation options page.
6. In the top-right corner, select the Account manager button and then select **Sign out**.
7. Close Microsoft Edge.

23.3.4 Task 3: Install Microsoft 365 Apps for Enterprise

1. On SEA-WS1, in the taskbar, select the **Microsoft Edge **icon.
2. In the address bar, enter http://portal.office.com.
3. On the Pick an account prompt, select **Use another account**.
4. In the **Sign in** dialog box, enter User2@M365xXXXXXX.onmicrosoft.com and then select **Next**.
5. At the **Enter password** dialog box, enter **Pa55w.rd1234** and then select **Sign in**. When prompted to save the password, select **Save**.
6. Close all welcome and introduction pages.
7. On the Office 365 page, select **Got it!** close the Office 365 apps prompt.
8. Select **Install Office** and then select **Other install options**.
9. On the My account page, in the navigation pane, select **Apps & devices**. Notice the option to install Office. Also notice that Skype for Business has been turned off.
10. On the Apps & devices page, select **Install Office**.
11. At the bottom of the Edge window, under OfficeSetup.exe, select **Open file**.
12. At the User Account Control, select **Yes**.
13. Office downloads and installs on the local computer. In the notification area, you can select the Office icon to monitor the process as needed. It will take approximately five minutes to complete.
14. After the install completes, select Close to close the Office prompts.
15. On SEA-WS1, select the Start menu and verify that the Office apps display. For example, you should see Word, PowerPoint, and Excel in addition to the other apps included in this subscription.
16. Close Microsoft Edge and sign out of SEA-WS1.

Results: After completing this exercise, you will have configured the deployment of the Office 365 apps included in Microsoft 365 and validated an installation of the apps.

END OF LAB

24 Practice Lab: Configuring Microsoft Edge to support Internet Explorer Enterprise Mode

24.1 Summary

In this lab you will learn how to configure the Internet Explorer Enterprise Mode to provide compatibility for Microsoft Edge to open legacy web sites.

24.1.1 Scenario

Contoso uses a web site located at intranet.contoso.com. This site currently only works properly using older Internet Explorer versions. As you recently upgraded all devices to Windows 10 and Microsoft Edge Chromium, you must ensure that this web site still opens and works with compatibility mode.

Dependency Notice: This lab requires that a DNS CNAME entry for intranet.Contoso.com be added which resolves to SEA-SVR1.Contoso.com, as instructed in the Module 5: Configuration and Testing Name Resolution lab. If you did not complete the module 5 lab, complete Exercise 2: Task 2 from that lab before continuing. Also note that Microsoft Edge .admx templates have already been installed to allow for the creation of Microsoft Edge Chromium group policy settings.

24.1.2 Task 1: Verify the site is not displayed in Enterprise Mode

1. Sign in to **SEA-CL1** as **Contoso\Cari** with the password **Pa55w.rd**.
2. On the task bar, select **Microsoft Edge**.
3. In the Microsoft Edge window, select **Complete setup**, select **Focused**, and then select **Confirm**.
4. Select **Continue without signing in**.
5. In the Internet Explorer Address bar, type **edge://compat/enterprise**, and then press **Enter**. Notice that the Enterprise Mode Site List does not contain any entries.
6. Sign out of **SEA-CL1**.

24.1.3 Task 2: Create a Site list for Internet Explorer Enterprise Mode

1. Switch to **SEA-SVR1**.
2. Sign in to **SEA-SVR1** as **Contoso\Administrator** with the password **Pa55w.rd**.
3. Select the **File Explorer** icon on the taskbar.
4. In File Explorer, browse to **\\SEA-DC1\Labfiles\Apps**.
5. Double-click the **EMIESiteListManager.msi** file.
6. In the Enterprise Mode Site List Manager Setup window, select **Next**.
7. On the End-User License Agreement page, select the check box for **I accept the terms in the License Agreement**, and then select **Next**.
8. On the Destination Folder page, select **Next**.
9. On the Ready to install Enterprise Mode Site List Manager page, select **Install**.
10. On the Completed the Enterprise Mode Site List Manager Setup Wizard page, select **Finish**.
11. Close File Explorer.
12. Select the **Start** button, type **Enterprise**, right-click **Enterprise Mode Site List Manager** and select **Run as administrator**.
13. In the Enterprise Mode Site List Manager for v.2 schema window, select **Add**.
14. In the Add new website window, in the URL text box, type **intranet.contoso.com**. In the Compat Mode drop-down list box, select **IE9 Document Mode**, and then select **Save**.
15. Select the **File** menu, and then select **Save to XML**.
16. In the Save as… dialog box, navigate to **C:\inetpub\wwwroot**. In the File name text box, type **ContosoEnterpriseMode**, and then select **Save**.
17. Close Enterprise Mode Site List Manager.
18. On the task bar, select **Internet Explorer**.
19. In the Internet Explorer window, in the Address bar, type **http://Intranet.Contoso.com/ContosoEnterpriseMode** and then press **Enter**.
20. Verify that the XML file opens correctly.
21. Close Internet Explorer.

24.1.4 Task 3: Create a policy to enable Internet Explorer Enterprise Mode

1. On SEA-SVR1, switch to **Server Manager**, select **Tools**, and then select **Group Policy Management**.

2. In the Group Policy Management window, expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**, and select **Group Policy Objects**.

3. Right-click **Group Policy Objects**, and then select **New**.

4. In the New GPO dialog box, in the Name box, type **Internet Explorer Enterprise Mode Policy**, and then select **OK**.

5. Right-click **Internet Explorer Enterprise Mode Policy**, and then select **Edit**.

6. In the Group Policy Management Editor window, in the left pane, expand **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, and then select **Microsoft Edge**.
7. In the content pane, double-click **Configure Internet Explorer integration**.
8. Select **Enabled**, and then from the **Configure Internet Explorer integration** drop down menu, select **Internet Explorer mode** and then select **OK**.
9. In the content pane, double-click **Configure the Enterprise Mode Site List**.
10. Select **Enabled**, in the **Configure the Enterprise Mode Site List** text box, type **http://Intranet.Contoso.com/C** and then select **OK**.
11. Close the Group Policy Management Editor window.
12. In the Group Policy Management window, right-click the **Contoso.com** domain, and then select **Link an existing GPO**.
13. In the Select GPO window, select **Internet Explorer Enterprise Mode Policy**, and select **OK**.
14. Close the Group Policy Management window.

24.1.5 Task 4: Verify the site is now in enterprise mode

1. Switch to **SEA-CL1** and sign in as **Contoso\Cari** with the password of **Pa55w.rd**.
2. Select **Start** and type **cmd**. Press **Enter**.
3. At the command prompt, type the following command, and then press Enter.

   ```
   gpupdate /force
   ```

4. On the task bar, select **Microsoft Edge**.
5. In the Internet Explorer Address bar, type **edge://compat/enterprise**, and then press **Enter**. Notice that the Enterprise Mode Site List contains http://intranet.contoso.com/ContosoEnterpriseMode.xml.
6. In the Internet Explorer Address bar, type **http://intranet.Contoso.com**, and then press **Enter**.
7. Verify that the website displays correctly, and that the Internet Explorer mode icon appears in the address bar. Select the Internet Explorer mode icon to view information about how this site opens.
8. Sign out of **SEA-CL1**.

Results: After completing this exercise, you should have successfully configured the Internet Explorer Enterprise Mode for Microsoft Edge.

END OF LAB

25 Practice Lab: Configuring Microsoft Defender Antivirus and Windows Security

25.1 Summary

In this exercise you will learn how to configure Microsoft Defender Antivirus and Windows Security settings.

25.2 Exercise 1: Detecting threats using Microsoft Defender Antivirus

25.2.1 Scenario

You've been asked to configure and test Microsoft Defender Antivirus on SEA-CL1. You need to configure protection settings to enable controlled folder access and to exclude E:\Labfiles\Tools from scanning. You've decided to simulate a virus using a test file, sample.txt, located at C:\Files, to validate successful threat detection.

25.2.2 Task 1: Configure Microsoft Defender Antivirus

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start**, and then select the **Settings** icon.

3. In the Settings window, select **Update & Security**, and then select the **Windows Security** tab. Take note of the Protection areas listed under Windows Security.
4. Select **Open Windows Security**.
5. In Windows Security, select **Virus & threat protection**.
6. On the Virus & threat protection page, under Virus & threat protection settings, select **Manage settings**.
7. Under Controlled folder access, select **Manage Controlled folder access**.
8. On the Ransomware protection page, enable **Controlled folder access**.
9. Under Controlled folder access, select **Protected folders** to view the default folders that are protected from unauthorized changes.
10. Click **Back** to return to the Ransomware protection page.
11. Click **Back** to return to the Virus & threat protection settings page.
12. Under the Exclusions section, select **Add or remove exclusions**.
13. On the Exclusions page, select **Add an exclusion** and then from the drop-down list select **Folder**.
14. In the **Select Folder** dialog box, browse to and select **E:\Labfiles\Tools** and then click **Select Folder**.
15. Click **Back** to return to the Virus & threat protection settings page.
16. Click **Back** to return to the Virus & threat protection page.

25.2.3 Task 2: Perform a scan

1. On the Virus & threat protection page, select **Scan options**.
2. Take note of the options available to configure and then select **Quick scan** and then select **Scan now**.
3. The quick scan begins and provides information on the number of files scanned and estimated time remaining. The final result should state **No current threats**.
4. In the Scan options window, select the **Back** button to return to the Virus & threat protection page.
5. Close the Windows Security window.

25.2.4 Task 3: Introduce suspicious software

1. In the Settings window, select the Home button.

2. Select **System** and then select **Notifications & actions**.

3. Under Notifications, enable the **Get notifications from apps and other senders**. This option enables notifications from Microsoft Defender and other apps.

4. Close Settings.

5. On the task bar, select the **File Explorer** icon.

6. In **File Explorer** browse to **C:\Files**.

7. In the Files folder, double-click **sample.txt**.

   Note: *The sample.txt file contains a text string to test malware detection.*

8. In the sample.txt file, **delete both instances of <remove>,** including the brackets and any extra lines or blank spaces.

9. Select **Save** and close Notepad.

   Note: *Microsoft Defender will immediately detect a potential threat and remove the file. It may take a minute for the file to automatically be removed.*

25.2.5 Task 4: View the quarantined file

1. In the notification area, select the **Notifications** icon, and then in the Action Center, select the notification that states that **Threats found**.

Note: *This will open the* ***Virus & threat protection*** *page in Windows security. The file is quarantined now.*

2. Under Current threats, select **Protection history**.

3. Take note of and select the **Threat quarantined** item.

4. Read the information about the threat and then select the **Actions** button and then select **Remove**.

5. Close all open windows.

Results: After completing this exercise, you will have configured and tested Microsoft Defender Antivirus.

25.3 Exercise 2: Configuring Windows Security Settings

25.3.1 Scenario

You need to verify that Microsoft Defender SmartScreen has been enabled and is configured on SEA-CL1. You also need to verify that Exploit Protection settings are On by default.

25.3.2 Task 1: Configure Windows Security

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Select **Start**, and then select the **Settings** icon.
3. In the Settings window, select **Update & Security**, and then select the **Windows Security** tab. Take note of the Protection areas listed under Windows Security.
4. Select **Open Windows Security**.
5. In Windows Security, select **App & browser control**.
6. On the App & browser control page, under Reputation-based protection, select **Reputation-based protection settings**.
7. Verify that Microsoft Defender SmartScreen has been enabled for apps, files, Microsoft Edge, and Microsoft Store apps.
8. Under Potentially unwanted app blocking, select the check box to enable **Block downloads**.
9. Click **Back** to return to the App & browser control page.
10. Under Exploit protection, select **Exploit protection settings**.
11. Verify that System settings are all configured to Use default (On).
12. Close the Windows Security window.
13. Sign out of SEA-CL1.

Results: After completing this exercise, you will have verified settings related to Microsoft Defender SmartScreen and Exploit protection.

END OF LAB

26 Practice Lab: Configuring Firewall and Connection Security

26.1 Summary

In this exercise you will learn how to create and configure firewall rules to block and allow specific service connections to a device. In this exercise you will learn how to create and configure connection security rules to encrypt network traffic between Windows devices.

26.2 Exercise 1: Creating and Testing Inbound Firewall Rules

26.2.1 Scenario

Users that work on SEA-CL2 are not allowed to remote desktop into SEA-CL1. You need to verify that remote desktop currently is allowed and then configure a firewall rule on SEA-CL1 that will block remote desktop connections. You will leave the Remote desktop service enabled to allow for other device connections to be configured at a later time.

26.2.2 Task 1: Validate existing functionality

1. Sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Right-click Start and then select **System**.
3. In the System navigation pane, select **Remote Desktop**.
4. On the Remote Desktop page, verify that **Enable Remote Desktop** is enabled. If it is not, then enable Remote Desktop.
5. Close the **Settings** window.
6. Switch to **SEA-CL2**.
7. Sign in to **SEA-CL2** as **Contoso\Administrator** with the password **Pa55w.rd**.
8. Select **Start**, type **mstsc.exe**, and then press **Enter**.
9. In the Computer box, type **SEA-CL1**, and then select **Connect**. The Windows Security dialog box displays asking for credentials to connect to SEA-CL1. This indicates successful connectivity to SEA-CL1.
10. In the Windows Security dialog, select **Cancel**.

26.2.3 Task 2: Create an inbound rule

1. Switch to **SEA-CL1**.
2. On SEA-CL1, select **Start**, and type **Windows Firewall**.
3. In the results pane, select **Windows Defender Firewall**.
4. In Windows Defender Firewall, in the left pane, select **Advanced settings**, select **Inbound Rules**, and then select **New Rule**.
5. In the New Inbound Rule Wizard window, select **Predefined**, select the **drop-down list**, select **Remote Desktop**, and then select **Next**.
6. On the Predefined Rules page, select the check box next to all available rules, and then select **Next**.
7. On the Action page, select **Block the connection**, and then select **Finish**.
8. Minimize the Windows Defender Firewall with Advanced Security window.

26.2.4 Task 3: Test the rule

1. Switch to **SEA-CL2**.
2. If necessary, select **Start**, type **mstsc.exe**, and then press **Enter**.
3. In the Computer box, type **SEA-CL1**, and then select **Connect**. Notice that the connection attempt fails and displays a Remote Desktop Connection error message.
4. In the Remote Desktop error message window, select **OK**.
5. Close all open windows.

Results: After completing this exercise, you should have created and verified inbound firewall rules.

26.3 Exercise 2: Creating and Testing Outbound Firewall Rules

26.3.1 Scenario

SEA-SVR1 also needs to be configured to allow remote desktop connections, however SEA-CL1's firewall configuration should not allow any user to use a remote desktop connection to SEA-SVR1 from SEA-CL1. You will configure an outbound firewall rule on SEA-CL1 to prevent remote desktop connections to the server.

26.3.2 Task 1: Test existing functionality

1. Switch to **SEA-SVR1** and sign in as **Contoso\Administrator** with the password **Pa55w.rd**
2. Select **Start**, type **control**, and then select **Control Panel**.
3. In the Control Panel, select **System and Security**, and then select **System**.
4. On the System dialog box, select Remote settings.
5. On the **Remote** tab, under **Remote Desktop**, select **Allow remote connections to this computer** and select **OK**.
6. Select **OK** to close the **System Properties** window and then close the Control Panel.
7. Switch to **SEA-CL1**.
8. Select **Start**, type **mstsc.exe**, and then press **Enter**.
9. In the Computer box, type **SEA-SVR1**, and then press **Enter**. The Windows Security dialog box displays asking for credentials to connect to SEA-SVR1. This indicates successful connectivity to SEA-SVR1.
10. In the Windows Security dialog, select **Cancel**.
11. Close Remote Desktop Connection.

26.3.3 Task 2: Create an outbound rule

1. On **SEA-CL1**, on the taskbar, select the **Windows Firewall with Advanced Security** window, and then select **Outbound Rules**.
2. In the Actions pane, select **New Rule**.
3. On the Rule Type page, verify that you are creating a **Program** rule, and then select **Next**.
4. On the Program page, browse and select **C:\Windows\System32\mstsc.exe**, select **Open**, and then select **Next**.

5. On the Action page, verify that the action is **Block the Connection**, and then select **Next**.
6. On the Profile page, verify that **all profiles are checked**, and then select **Next**.
7. On the Name page, type **Block Outbound RDP to SEA-SVR1** in the Name box, and then select **Finish**.
8. In the Windows Defender Firewall with Advanced Security window, select the **Block Outbound RDP to SEA-SVR1** rule, and then in the Actions pane, select **Properties**.
9. Select the **Scope tab**, and then under the **Remote IP address heading**, select the **These IP addresses** option.
10. Under the Remote IP address heading, select **Add**, in the This IP address or subnet box, type **172.16.0.11**, and then select **OK**.
11. In the Block Outbound RDP to SEA-SVR1 Properties dialog box, select **OK**.

26.3.4 Task 3: Test the rule

1. On SEA-CL1, select **Start**, type **mstsc.exe**, and then press **Enter**.
2. In the Computer box, type **SEA-SVR1**, and then press **Enter**. Notice that the connection attempt fails and displays a Remote Desktop Connection error message.
3. In the Remote Desktop Connection dialog box, select **OK**.
4. **Close** all open windows.

Results: After completing this exercise, you should have created and tested outbound firewall rules.

26.4 Exercise 3: Creating Connection Security Rules

26.4.1 Scenario

Your manager wants you to ensure that all network traffic between SEA-CL1 and SEA-CL2 is encrypted. You need to configure a connection security rule with the setting ”Require authentication for inbound connections and request authentication for outbound connections” enabled on both devices.

26.4.2 Task 1: Verify that communications are not secure

1. Sign in to **SEA-CL2** as **Contoso\Administrator** with the password **Pa55w.rd**.
2. Right-click **Start**, and then select **Windows PowerShell**.
3. In the Windows PowerShell window, type the following command and then press **Enter**

   ```
   ping SEA-CL1
   ```

4. Verify that the ping generated four Reply messages.
5. Select **Start**, type **firewall** and select **Windows Defender Firewall**.
6. In the left pane, select **Advanced settings**.
7. In the left pane, expand **Monitoring,** and then expand **Security Associations**.
8. Select **Main Mode**, and then examine the information in the center pane.

   Note: *No information should be present.*

9. Select **Quick Mode**, and then examine the information in the center pane.

   Note: *No information should be present.*

10. Switch to **SEA-CL1**. If necessary, sign in to **SEA-CL1** as **Contoso\Administrator** with the password **Pa55w.rd**.
11. Right-click **Start**, and then select **Windows PowerShell (Admin)**.
12. To examine the Main Mode Security Associations (SAs), at the Windows PowerShell prompt, type the following cmdlet, and then press **Enter**:

    ```
    Get-NetIPsecMainModeSA
    ```

13. To examine the Quick Mode SAs, at the Windows PowerShell prompt, type the following cmdlet, and then press **Enter**:

    ```
    Get-NetIPsecQuickModeSA
    ```

    Note: *Running each command should produce no result.*

26.4.3 Task 2: Create the Connection Security Rule

1. On **SEA-CL1** select **Start**, type **firewall** and select **Windows Defender Firewall**.
2. In the left pane, select **Advanced settings**, and then select **Connection Security Rules**.
3. In the Actions pane, select **New Rule**.
4. On the Rule Type page, verify that **Isolation** is selected, and then select **Next**.
5. On the Requirements page, select **Require authentication for inbound connections and request authentication for outbound connections**, and then select **Next**.
6. On the Authentication Method page, select **Computer and user (Kerberos V5)**, and then select **Next**.
7. On the Profile page, select **Next**.
8. On the Name page, in the Name text box, type **Authenticate all inbound connections**, and then select **Finish**.
9. Close the Windows Defender Firewall with Advanced Security window.
10. Switch to **SEA-CL2**.
11. In the Windows Defender Firewall with Advanced Security window, in the left pane select **Connection Security Rules**.
12. In the Actions pane, select **New Rule**.
13. On the Rule Type page, verify that **Isolation is selected**, and then select **Next**.
14. On the Requirements page, select **Require authentication for inbound connections and request authentication for outbound connections**, and then select **Next**.
15. On the Authentication Method page, select **Computer and user (Kerberos V5)**, and then select **Next**.
16. On the Profile page, select **Next**.
17. On the Name page, in the Name text box, type **Authenticate all inbound connections**, and then select **Finish**.

26.4.4 Task 3: Verify the rule, and monitor the connection

1. On SEA-CL2, in the Windows PowerShell window, type the following command and then press **Enter**

    ```
    ping SEA-CL1
    ```

2. Verify that the ping generated four reply messages.
3. In the Windows Defender Firewall with Advanced Security window, in the left pane expand **Monitoring,** and then expand **Security Associations**.
4. Select **Main Mode**, and then examine the information in the center pane.
5. Select **Quick Mode**, and then examine the information in the center pane.
6. **Close** all open windows.
7. Switch to **SEA-CL1.**
8. To examine the Main Mode Security Associations (SAs), at the Windows PowerShell command prompt, type the following cmdlet, and then press **Enter**:

```
Get-NetIPsecMainModeSA
```

9. Review the result.
10. To examine the Quick Mode SAs, at the command prompt, type the following cmdlet, and then press **Enter**:

    Get-NetIPsecQuickModeSA
    ```

11. Review the result and then close all open windows.

12. Sign out of SEA-CL1 and SEA-CL2.

**Results**: After completing this exercise, you should have created and tested connection security rul

**END OF LAB**
# Practice Lab: Configuring BitLocker

## Summary

In this exercise you will learn how to encrypt a local disk drive using BitLocker.

### Scenario

You have a Windows 10 computer that has sensitive data stored on the E drive. You decide to configure a

### Task 1: Configure GPO settings

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

2.  Select the Start menu, type **gpedit.msc**, and then press Enter.

3.  In the Local Group Policy Editor, under **Computer Configuration** node, expand **Administrative Te

4.  Select **Operating System Drives**, and then double-click **Require additional authentication at st

5.  In the **Require additional authentication at startup** dialog box, select **Enabled**, and then se

6. Close the Local Group Policy Editor.

   *Note: This configuration change is made to enable BitLocker without a TPM. This is a necessary step

### Task 2: Enable BitLocker

1.  On the taskbar, select the **File Explorer** icon.

2.  In File Explorer, in the navigation pane, expand **This PC**.

3.  In the navigation pane, right-click **Allfiles (E:)**, and then select **Turn on BitLocker**.

4.  In the **BitLocker Drive Encryption (E:)** dialog box, select **Use a password to unlock the drive*

5.  In the **Enter your password** and **Reenter your password** boxes, type **Pa55w.rd**, and then sel

6.  On the **How do you want to back up your recovery key?** page, select **Save to a file**.

7.  In the **Save BitLocker recovery key as** dialog box, select **Local Disk (C:)**.

8.  Select **New folder**, type **BitLocker**, and then press Enter.

9.  In the **Save BitLocker recovery key as** dialog box, select **Open**, and then select **Save**,

10. On the **How do you want to back up your recovery key?** page, select **Next**.

11. On the **Choose how much of your drive to encrypt** page, ensure that **Encrypt used disk space onl

12. On the **Choose which encryption mode to use** page, ensure that **New encryption mode (best for fi
    ```

13. On the **BitLocker Drive Encryption (E:)** page, select **Start encrypting**, and then select **Clo

15. Restart SEA-CL1.

### Task 3: Verify BitLocker

1. Sign in to **SEA-CL1** as **Contoso\\Administrator** with the password **Pa55w.rd**.
2. Select the **File Explorer** icon on the taskbar.
3. In File Explorer in the navigation pane expand **This PC**, and select **Local Disk (E:)**. Notice
4. In the BitLocker (E:) window, enter the password **Pa55w.rd**, press Enter to unlock the drive, and
5. Right-click **Allfiles (E:)** and then select **Manage BitLocker**. Take note of the options availa
6. Select **Turn off BitLocker**.
7. In the BitLocker Drive Encryption dialog box, select **Turn off BitLocker**.
8. Close the BitLocker Drive Encryption window.
9. In File Explorer, notice that that lock icon is no longer visible next to Allfiles (E:).
10. Close all open windows and sign out of SEA-CL1.

Results: After completing this exercise, you will have configured BitLocker to encrypt a local disk

END OF LAB
# Practice Lab: Monitoring Events

## Summary

In this lab, you will learn how to manage Windows 10 event logs and configure Event log subscriptions.

## Exercise 1: Manage Windows 10 Event Logs

### Scenario

You need to perform maintenance tasks on the Event logs for SEA-CL1. You will first review the event lo

### Task 1: Review Event Log entries

1. Sign in to **SEA-CL1** as **Contoso\\Administrator** with the password: **Pa55w.rd**.
2. Select **Start**, and then type **Event Viewer**.
3. In the search results, select the **Event Viewer** app. The Event Viewer opens.
4. Maximize the Event Viewer window.
5. Under Event Viewer (Local), expand **Windows Logs**.
6. Under Windows Logs, select **Application** and then scroll through the reported events. Take note of
7. Under Windows Logs, select **Security** and then scroll through the reported events. Take note of th
8. Under Windows Logs, select **System** and then scroll through the reported events. Take note of the
9. With the System log selected, in the Actions pane select **Filter Current Log**.
10. In the Filter Current Log dialog box, on the Filter tab, next to Event level, select the check box
11. Select **OK** to return to the System log events. Notice that only Warning and Error events are now
12. In the Actions pane, select **Clear Filter**. All System events are now displayed.
13. In the navigation pane, expand **Applications and Services Logs**. These logs relate to specific se
14. Under Applications and Services Logs, expand **Microsoft**, and then expand **Windows**. Notice the
15. Under the Windows node, expand **GroupPolicy** and then select the **Operational** log. Take note o
16. In the navigation pane, close the **Applications and Services Logs** branch.

### Task 2: Configure Event Log Properties

1. Under Windows Logs, select **Application** and then in the Actions pane, select **Properties**.
2. In the Log Properties - Application dialog box, on the General tab, change the **Maximum log size (
3. On the General tab, select **Clear log** and then in the Event Viewer prompt select **Clear**.
4. Select **OK** to close the Log Properties - Application dialog box.
5. Under Windows Logs, select **Security** and then in the Actions pane, select **Properties**.
6. In the Log Properties - Security dialog box, on the General tab, change the **Maximum log size (KB)

7. Under When maximum event log size is reached, select **Archive the log when full, do not overwrite
8. Select **OK** to close the Log Properties - Security dialog box.
9. Close the Event Viewer.

Results: After completing this exercise, you will have successfully reviewed event log entries and

## Exercise 2: Configure and Manage Event Subscriptions

### Scenario

SEA-CL2 is a critical workstation that needs to be monitored and maintained on a regular basis. To effi

### Task 1: Configure Event Log Subscriptions
1. Sign in to **SEA-CL2** as **Contoso\\Administrator** with the password **Pa55w.rd**.

2. Right-click **Start**, and then select **Windows PowerShell (Admin)**.

3. At the PowerShell command prompt, type the following command, and then press **Enter**:
    ```
    winrm quickconfig
    ```

4. At the PowerShell command type **Y** when prompted. You will be prompted to configure the WinRM ser

5. Close Windows PowerShell.

6. Right-click **Start**, and then select **Computer Management**.

7. Expand **System Tools**, expand **Local Users and Groups**, and then select **Groups**.

8. In the results pane, double-click **Event Log Readers**.

9. In the **Event Log Readers Properties** dialog box, select **Add**, and then in the **Select Users,

10. In the **Object Types** dialog box, select the **Computers** check box, and then select **OK**.

11. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the obje

12. In the **Event Log Readers Properties** dialog box, select **OK**.

13. Close the **Computer Management** window.

14. Switch to **SEA-CL1** and sign in as **Contoso\\Administrator** with the password **Pa55w.rd**.

15. Right-click **Start**, and then select **Windows PowerShell (Admin)**.

16. At the PowerShell command prompt, type the following command, and then press **Enter**:
    ```
    wecutil qc
    ```

17. When prompted, type **Y**, and then press **Enter**.

18. Close the Windows PowerShell window.

### Task 2: View and filter events

1. On **SEA-CL1**, right-click **Start**, and then select **Event Viewer**. Maximize the Event Viewer

2. In **Event Viewer**, in the navigation pane, select **Subscriptions**.

3. Right-click **Subscriptions**, and then select **Create Subscription**.

4. In the **Subscription Properties** dialog box, in the **Subscription name** box, type **SEA-CL2 Eve

5. Select **Collector Initiated**, and then select **Select Computers**.

6. In the **Computers** dialog box, select **Add Domain Computers**.

7. In the **Select Computer** dialog box, in the **Enter the object name to select (examples)** box, t

8. In the **Computers** dialog box, select **OK**.

9. In the **Subscription Properties - SEA-CL2 Events** dialog box, select **Select Events**.

10. In the **Query Filter** dialog box, select the **Critical**, **Warning**, **Information**, **Verbos

11. In the **Logged** dropdown list, select **Last 30 days**.

12. In the **Event logs** dropdown list, select **Windows Logs**, and then select **OK**.

13. In the **Subscription Properties - SEA-CL2 Events** dialog box, select **OK**. A subscription entry

14. In **Event Viewer**, in the navigation pane, expand **Windows Logs**.

15. Select **Forwarded Events**.

16. Right-click **Forwarded Events**, and then select **Create Custom View**.

17. In the **Create Custom View** dialog box, select the **Critical** and **Error** check boxes, and th

18. In the **Save Filter to Custom View** dialog box, in the **Name** box, type **SEA-CL2 errors**, and

19. Examine any listed events. The list may be empty.

20. Close all open windows and then sign out of SEA-CL1.

Results: After completing this exercise, you will have successfully configured Event subscriptions

END OF LAB
# Practice Lab: Monitoring Reliability and Performance

## Summary

In this lab, you will learn how to use Task Manager and Reliability Monitor to review Windows 10 reliab

## Exercise 1: Review Windows 10 performance using Task Manager and Reliability Monitor

### Scenario

A user reports performance and speed issues with a client workstation named SEA-CL1. You first step is

### Task 1: Use Task Manager to review performance

1. Sign in to **SEA-CL1** as **Contoso\\Administrator** with the password: **Pa55w.rd**.
2. Right-click the taskbar and then select **Task Manager**.
3. In the Task Manager window, select **More details**.
4. In the Task Manager window, on the Processes tab, review the running processes.
5. On the taskbar, select **Start**, and then on the Start menu select **Word**.
6. Minimize the **Word** window and then switch to the **Task Manager**. Take note of the **Microsoft
7. In the Task Manager, select the **Performance** tab. Take note of the real-time performance of the

8. In the Task Manager, select the **App history** tab. Take note of the resource usage and then selec
9. In the Task Manager, select the **Startup** tab. Take note of the apps that start up when Windows s
10. In the Task Manager, select the **Details** tab. Take note of the specific executables running on
11. In the Task Manager, select the **Services** tab. Take note of the services that are running and s
12. In the Task Manager, select the **Processes** tab.
13. Under Apps, right-click **Microsoft Word (32-bit)** and then select **End task**. This will end th
14. Close Task Manager.

### Task 2: Review reliability history using Reliability Monitor ###

1. On SEA-CL1, on the taskbar, select **Start**, type **reliability**, and then select **View reliabili
2. In the Reliability Monitor window, select any date that contains an information or warning notificat
3. In the Reliability details section, next to a Warning or Informational event, select **View technica
4. Review the details and then select **OK**.
5. Close the Reliability Monitor.
6. Sign out of SEA-CL1.

Results: After completing this exercise, you will have successfully reviewed performance and reliab

## Exercise 2: Monitor Windows 10 using Performance Monitor

### Scenario

You need to use Performance Monitory to identify performance bottlenecks on the Windows 10 workstation

### Task 1: Use Performance Monitor to gather a baseline
1. Sign in to **SEA-CL1** as **Contoso\\Administrator** with the password: **Pa55w.rd**.

2. Select **Start**, type **performance**, and then select **Performance Monitor**.

3. In **Performance Monitor**, in the navigation pane, expand **Data Collector Sets**.

4. Select **User Defined**, right-click **User Defined**, point to **New**, and then select **Data Coll

5. In the **Create new Data Collector Set** wizard, on the **How would you like to create this new data

6. Select **Create manually (Advanced)**, and then select **Next**.

7. On the **What type of data do you want to include?** page, select the **Performance counter** check

8. On the **Which performance counters would you like to log?** page, in the **Sample interval** field,

9. In the **Available counters** list, expand **Network Interface**, select **Packets/sec**, and then s

10. In the **Available counters** list, expand **PhysicalDisk**, select **% Disk Time**, and then selec

11. Under **PhysicalDisk**, select **Avg. Disk Queue Length**, and then select **Add**.

12. In the **Available counters** list, expand **Processor**, select **% Processor Time**, and then sel

13. In the **Available counters** list, expand **System**, select **Processor Queue Length**, select **

14. On the **Which performance counters would you like to log?** page, select **Next**.

15. On the **Where would you like the data to be saved?** page, select **Next**.

16. On the **Create the data collector set?** page, select **Finish**.

17. In **Performance Monitor**, in the details pane, right-click **Contoso Baseline**, and then select

18. Select **Start**, and then select **Word**.

19. Select **Start**, and then select **Excel**.

20. Select **Start**, and then select **PowerPoint**.

21. Close all open Microsoft Office apps, and then switch to **Performance Monitor**.

22. In the navigation pane, right-click **Contoso Baseline**, and then select **Stop**.

23. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, ex

24. View the chart. On the menu bar, select the drop-down arrow, and then select **Report**.

25. Record the following values:

    - Network Interface Packets per second

    - PhysicalDisk % Disk Time

    - PhysicalDisk Avg. Disk Queue Length

    - Processor % Processor Time

    - System Processor Queue Length

### Task 2: Simulate load using the load generator script ###
1. On SEA-CL1, open File Explorer, and browse to **\\\\SEA-DC1\\labfiles\\Support\\**.

2. In the content pane, double-click **CopyMonitor.bat** to copy lab files to the local client.

3. Click Start, type **cmd**. Right-click on **Command Prompt** and select **Run as administrator**.

_**Note**: The following step initiates a script which generates a resource load. Be sure to continue o

4. In the Command Prompt Window, type each of the following commands and press **Enter**:
    ```
    cd\Monitor
    MonitorScenario.vbs
    ```

### Task 3: Use Performance Monitor to identify possible bottlenecks ###

1. On SEA-CL1, switch to **Performance Monitor**.

2. Under **Data Collector Sets**, select **User Defined**.

3. Right-click **Contoso Baseline**, and then select **Start**.

4. On the taskbar, in the **Type here to search** type **perfmon /res**, and then press **Enter**.

5. In **Resource Monitor**, which components are under strain?

    _**Note**: Answers will vary depending upon the usage scenario and host configuration, although cen

6. After a few minutes, in the **Windows Script Host** prompt, select **OK**.

    **Note**: Check the taskbar to see if this dialog may be hidden.

7. Wait for the instance of the Command Prompt windows launched by the script to close.

8. Switch to **Performance Monitor**.

9. In the navigation pane, right-click **Contoso Baseline**, and then select **Stop**.

10. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, ex

11. View the chart.

12. On the menu bar, select the drop-down arrow, and then select **Report**.

13. Record the component details:
-   Network Interface Packets per second
-   PhysicalDisk % Disk Time
-   PhysicalDisk Avg. Disk Queue Length
-   Processor % Processor Time
-   System Processor Queue Length

14. In your opinion, which components is the script affecting the most?

    **Note**: The script is affecting the CPU and network, but it is also affecting all counters.

15. Close all open windows and sign out of SEA-CL1.

Results: After completing this exercise, you will have successfully use Performance Monitor to dete

END OF LAB
# Practice Lab: Using File History to Recover Files

## Summary
In this exercise you will learn how configure File History and use it to restore previous versions of a

## Exercise 1: Configure File History

### Scenario

You need to ensure that users can recover deleted files stored in the Documents library on their local

### Task 1: Create a shared folder for File History

1. Sign in to **SEA-SVR1** as **Contoso\\Administrator** with the password **Pa55w.rd**.
2. Select the **File Explorer** icon on the taskbar and in the navigation pane, select **Local Disk (C
3. In File Explorer, in the details pane, right-click an empty space, point to **New**, and then selec
4. Right-click the **FileHistory** folder, and then select **Properties**.
5. In the **FileHistory Properties** dialog box, on the **Security** tab, select **Edit**. Select **Ad
6. Select **Domain Users**, and then select **OK**.
7. In the **Permissions for Domain Users** section, in the Allow column, select the **Full control** c
8. On the **Sharing** tab, select **Advanced Sharing**.
9. Select the **Share this folder** check box, and then select **Permissions**. In the **Permissions f
10. In the **FileHistory Properties** dialog box, select **Close**.
11. Close File Explorer.
12. Sign out of SEA-SVR1.

### Task 2: Configure and test File History

1. Switch to **SEA-CL2** and sign in as **Contoso\\Administrator**, with the password **Pa55w.rd**.
2. On **SEA-CL2**, on the taskbar, select the **File Explorer** icon.
3. In File Explorer, in the navigation pane, expand **This PC**, and then select **Documents**. In the
4. Double-click **Report.txt**, and in Notepad, type **This is a report**. Close the Notepad file, and
5. Select Start, type **file history**, and then select **Restore your files with File History**.
6. In the **Home - File History** window, select **Configure File History settings**.

7. In the **File History** window, in the navigation pane, select **Select drive**.
8. In the **Select Drive** dialog box, select **Add network location**.
9. In the **Folder** box, type **\\\\SEA-SVR1\\FileHistory**, select **Select Folder**, and then selec
10. In the **File History** window, in the details pane, select **Turn on**.
11. In the navigation pane, select **Advanced settings**, review the default values for how often to s
12. In File Explorer, in the navigation pane, select **Documents**, right-click **Report.txt**, and th
13. In File Explorer, select the **Home** tab, and then select **History**.
14. In the Documents - File History window, right-click **Report.txt**, and select **Preview**. Confir
15. File Explorer opens. Verify that Report.txt has been recovered to the original location. Double-cl
16. In the Report.txt - File History window, on the left of the address box, select the upward-pointin
17. Review the folders and libraries that File History is protecting, and confirm that the a folder na
18. Close the Home - File History window.

Results: After completing this exercise, you will have successfully configured File History and val

## Exercise 2: Protect Additional Data

### Scenario

An additional request has been made to protect specific files being added to SEA-CL2. A script has been

### Task 1: Run the CopyUserData script

1. On **SEA-CL2**, in File Explorer, browse to **\\\\SEA-DC1\\labfiles\\Support\\**.

2. In the content pane, double-click **CopyUserData** to copy lab files to the local client.

3. In File Explorer, in the navigation pane, expand **Local Disk (C:)**, and then select **Data**. In

### Task 2: Configure Additional Folders

1. In the navigation pane, right-click **Data**, select **Include in library**, and then select **Docu

2. In File Explorer, in the navigation pane, select **Reports**. In the details pane, right-click **Re

3. On the taskbar, in the **Type here to search** box, enter **file history**, and then select **Backu

4. In the **Settings** window, in the **Back up using File History** section, select **More options**.

5. On the **Backup options** page, in the **Back up these folders** section, select **Add a folder**,

6. In the **File History** window**,** in the **File History is on** section, select **Run now**.

7. In File Explorer, in the details pane, right-click **Report.txt**, select **Properties**, select th

8. In the navigation pane, right-click **Data**, select **Properties**, select the **Previous Versions

9. Select the arrow near the **Restore** button, and then verify that you can restore the previous ver

10. In the **Data Properties** dialog box, select the arrow near the **Open** button, and then select *

11. In the Data - File History window, on the left of the address box, select the upward-pointing arrow

12. In the C:\\ - File History window, select the upward-pointing arrow again to view all folders and l

13. Close the Home - File History window, in the **Data Properties** dialog box, select **OK**.

14. Close all open windows and sign out of SEA-CL2.

Results: After completing this exercise, you will have successfully added additional files to be pr

END OF LAB
# Practice Lab: Using Advanced Startup and Windows RE to recover from Boot Failures

## Summary

During this lab you will learn how to work with the Windows RE, manipulate the BCD from the Command Pro

### Scenario

You need to test and validate the features available for when you need to recover from boot failures on

### Lab Preparation

To complete this lab you need to attach **Win10_20H2_Eval.iso** to SEA-CL2. Consult with your instructo

### Task 1: Use Windows RE

1. Restart SEA-CL2.
2. When prompted to **Press any key to boot from CD or DVD**, select the spacebar. The computer starts
3. In Windows Setup, select **Next**.
4. On the **Install now** page, select **Repair your computer**.
5. On the **Choose an option** page, select **Troubleshoot**.
6. On the **Advanced options** page, notice the five tools that are available.
7. Select **Command Prompt**.
8. At the command prompt, enter **diskpart**, and then select Enter.
9. At the command prompt, enter **list disk**, and then select Enter.
10. At the command prompt, enter **list volume**, and then select Enter.
11. At the command prompt, enter **exit**, and then select Enter.
12. At the command prompt, enter **d:**, and then select Enter.
13. At the command prompt, enter **dir**, and then select Enter. This is the system drive.
14. At the command prompt, enter **cd\\windows\\system32**, and then select Enter.
15. At the command prompt, enter **net start**, and then select Enter. A list of running services is re
16. At the command prompt, enter **sc query**, and then select Enter. A list of services and their curr
17. At the command prompt, enter **regedit**, and then select Enter. The Registry Editor opens.
18. Close the Registry Editor.
19. At the command prompt, enter **exit**, and then select Enter.
20. On the Choose an option page, select **Troubleshoot**.
21. On the Advanced options page, select **Startup Repair**.
22. On the Startup Repair page, select **Windows 10**. Automatic startup repair begins.
23. On the Startup Repair page, notice the log file (D:\\Windows\\System32\\Logfiles\\Srt\\SrtTrail.txt
24. Select **Advanced options**.
25. On the Choose an option page, select **Continue**.
26. Sign in as **Contoso\\Administrator** by using the password **Pa55w.rd**.
27. On the taskbar, select the **File Explorer** icon.
28. In File Explorer, navigate to **C:\\Windows\\System32\\Logfiles\\Srt**.
29. In the Srt folder, open **SrtTrail.txt**.
30. Examine the file for any errors. There should be none.
31. Close the file, and then close File Explorer.

### Task 2: Work with BCD

1. On SEA-CL2, select **Start**, and then select **Settings**.
2. In Settings, select **Update & Security**.
3. Select **Recovery**.
4. In the results pane, under **Advanced startup**, select **Restart now**.
5. On the Choose an option page, select **Troubleshoot**.
6. On the Troubleshoot page, select **Advanced options**.
7. On the Advanced options page, select **Command Prompt**. SEA-CL2 restarts into the Command Prompt m
8. On the Command Prompt page, select **Admin**. This is the local administrator account.
9. In the Password box, enter **Pa55w.rd**, and then select **Continue**.

10. At the command prompt, enter **bcdedit /enum**, and then select Enter. This lists the available bo
11. At the command prompt, enter **bootrec /scanos**, and then select Enter. This command scans the pa
12. At the command prompt, enter **bootrec /rebuildbcd**, and then select Enter. This command rebuilds
13. At the command prompt, enter **exit**, and then select Enter.
14. On the Choose an option page, select **Continue**.
15. Sign in as **Contoso\\Administrator** by using the password **Pa55w.rd**.

### Task 3: Access Advanced Startup options

1. On SEA-CL2, in the **Type here to search** box, enter **msconfig.exe**, and then select Enter. The
2. In the System Configuration dialog box, select the **Boot** tab.
3. On the Boot tab, select the **Safe boot** check box, and then select **OK**.
4. In the System Configuration dialog box, select **Restart**.
5. When the computer restarts, sign in as **Contoso\\Administrator** by using the password **Pa55w.rd*
6. Right-click **Start** or activate its context menu, and then select **Run**.
7. In the Run box, enter **msconfig.exe**, and then select Enter.
8. In the System Configuration dialog box, on the General tab, select **Normal startup**, and then sel
9. In the System Configuration dialog box, select **Restart**.
10. When the computer restarts, sign in as **Contoso\\Administrator** by using the password **Pa55w.rd*
11. On SEA-CL2, select **Start**, and then select **Settings**.
12. In Settings, select **Update & Security**.
13. Select **Recovery**.
14. In the results pane, under Advanced startup, select **Restart now**.
15. On the Choose an option page, select **Troubleshoot**.
16. On the Troubleshoot page, select **Advanced options**.
17. On the Advanced options page, select **Startup Settings**.
18. On the Startup Settings page, select **Restart**.
19. When the computer restarts, on the Startup Settings page, select Enter to start normally.

Results: After completing this exercise, you should have started Windows RE, manipulated the BCD fr

END OF LAB

# Practice Lab: Recovering Windows using Reset This PC

## Summary

During this lab you will learn how to recover a Windows 10 device using Reset This PC.

### Scenario

You discover that SEA-CL2 is having intermittent issues. Repeated attempts have been made to correct th

### Task 1: Use the Reset this PC option

1. Sign in to **SEA-CL2** as **Contoso\\Administrator** with the password of **Pa55w.rd**.
2. On **SEA-CL2**, right-click the desktop, point to **New**, select **Text Document**, type **Report*
3. Right-click the **Start** icon, select **Windows PowerShell**.
4. In the **Windows PowerShell** prompt, type **ipconfig /all** and then press **Enter.**
5. Verify that the Ethernet connection is not Dynamic Host Configuration Protocol-enabled (DHCP-enable
6. In the Windows PowerShell prompt, type `sysdm.cpl` and then press **Enter**.
7. Verify that the device name is **SEA-CL2** and that it is in the **Contoso.com** domain.
8. Select **Start**, select **Settings**, and then select **Update & Security**.
9. In the **Update & Security** navigation pane, select **Recovery**.
10. On the Recovery page, under **Reset this PC**, select **Get started**.
11. On the Reset this PC dialog box, select **Keep my files**.
12. When prompted to select where to reinstall Windows from, select **Local reinstall**.
13. On the Ready to reset this PC page, select **View apps that will be removed**. Take note of the ap
14. On the Ready to reset this PC page, select **Reset**.
15. Wait for the reset to complete. It will take a while to complete.

### Task 2: Verify that Reset this PC was successful

1. Sign in to **SEA-CL2** as **Contoso\\Administrator** with the password of **Pa55w.rd**.
2. Verify that the file Report.txt is still available on the desktop.
3. On the desktop, double-click the **Removed Apps** report and verify the apps that have been removed
4. Close Microsoft Edge.
5. Right-click the **Start** icon, select **Windows PowerShell**.
6. At the **Windows PowerShell** prompt, type `ipconfig /all` and then press **Enter**.
7. Verify that the Ethernet connection is now Dynamic Host Configuration Protocol-enabled (DHCP-enable
8. In the Windows PowerShell prompt, type `sysdm.cpl` and then press **Enter**.
9. Verify that the device name is SEA-CL2 and that it is in the Contoso.com domain.
10. Close all open windows.

Results: After completing this exercise, you will have successfully recovered SEA-CL2 by using Rese

END OF LAB
# Practice Lab: Recovering Windows by using a Restore Point

## Summary

During this lab, you will learn how to recover a Windows 10 device by using a Restore Point.

### Scenario

One your colleagues reports that after installing a hardware driver that his device is no longer respon

### Lab Preparation

To complete this lab you need to attach **Win10_20H2_Eval.iso** to SEA-CL1. Consult with your instructo

### Task 1: Configure System Protection and Create a System Restore Point

1. Sign in to **SEA-CL1** as **Contoso\\Administrator** with the password of **Pa55w.rd**.

2. On the taskbar, select **File Explorer**.

3. In File Explorer, in the navigation pane, right-click **This PC**, and then select **Properties**.

4. On the About page, scroll down and then select **System protection**.

5. In the **System Properties** dialog box, in the **Protection Settings** section, select **Local Disk

6. Right-click **Start** and select **Windows PowerShell (Admin).**

7. In the Administrator: PowerShell window type the following command and press **Enter**:

Checkpoint-Computer -Description ”Lab Start”

8. When complete, close the PowerShell Window.

### Task 2: Simulate the Problem

1. On SEA-CL1, in File Explorer, browse to **E:\\Labfiles\Mod13**.
2. In the Mod13 folder, double-click **scenario1.vbs**. SEA-CL1 will restart.
3. After the computer restarts, a blue screen displays that states that the device ran into a problem.

### Task 3: Perform a System Restore

1. Restart SEA-CL1.
2. When prompted to **Press any key to boot from CD or DVD**, select the spacebar. The computer starts
3. In Windows Setup, select **Next**.

4. On the **Install now** page, select **Repair your computer**.
5. On the **Choose an option** page, select **Troubleshoot**.
6. On the **Advanced options** page, notice the five tools that are available.
7. On the Advanced options page, highlight **System Restore** and press **Enter**.
8. On the Choose a target operating system page, select **Windows 10**.
9. On the Restore system files and settings page, select **Next**.
10. On the System Restore window, select the **Lab Start** line and select **Scan for affected program
11. Note that no programs will be affected. Select **Close**.
12. Select **Next**, then **Finish**, and then **Yes**.
13. After the restore is complete, select **Restart**. You may be asked to restart twice to complete t
14. Sign in to **SEA-CL1** as **Contoso\\Administrator** with the password of **Pa55w.rd**.
15. In the System Restore window select **Close**.
16. Sign out of SEA-CL1.

Results: After completing this exercise, you should have successfully recovered a Windows 10 device

END OF LAB
# Practice Lab: Troubleshooting Hardware by Using Windows Memory Diagnostics

## Summary

In this lab, you will learn how to use the Windows Memory Diagnostics Tool to check for memory problems

### Scenario

SEA-CL1 is still having issues with blue screen and performance symptoms. You decide to check for memor

### Task 1: Use the Windows Memory Diagnostic Tool

1. Sign in to **SEA-CL1** as **Contoso\\Administrator** with the password of **Pa55w.rd**.
2. Select the **Start** icon, and then type **Windows memory Diagnostic**.
3. In the results, select **Windows Memory Diagnostic**.
4. In the Windows Memory Diagnostic dialog box, select **Restart now and check for problems**. SEA-CL1
5. Press **F1** to open the **Options** screen.
6. Press **TAB** to move to the **Pass Count** section and change the Pass Count to **1**.
7. Press **TAB** to move to the **Test Mix** section, and change the Test Mix to **Basic**.
8. Press **F10** to apply the change. It will take some time to complete the scan.
9. After the computer restarts, sign in to **SEA-CL1** as **Contoso\\Administrator** with the password
10. Sign out of SEA-CL1.

Results: After completing this exercise, you will have used the Windows Memory Diagnostics Tool to

END OF LAB