Contents

...

1 Lab: Configuring Windows 10

1.1 Exercise 1: Using the Settings App

1.1.1 Task 1: Use the Settings app to configure a device

1. On **LON-CL1** login as **ADATUM\Administrator** with password: **Pa55w.rd**
2. Click the **Start** menu, then Settings.
3. Maximize the Settings page, and click the **Update & Security** item.
4. In the console tree, click the **Windows Defender** item, and then in the details pane, click **Open Windows Defender Security Center**.
5. In the Windows Defender Security Center app, click the **Expand icon (triple bar),** and then click **Virus & threat protection**.
6. On the Virus & threat protection page, click **Virus and threat protection settings**.
7. On the Virus & threat protection settings page, under Exclusions, click **Add or remove exclusions**.
8. On the Exclusions page, click the **plus sign (+)**, and then in the list, click **Folder**.
9. In the Select Folder window, navigate to **E:\Labfiles,** and then click **Select folder**.

10. Close the Windows Defender Security Center.
11. At the upper left of the screen, click the back arrow. This will return you to the main Settings page.
12. On the **Settings page**, click the **Devices** item.
13. Click the **Add a printer or scanner** plus sign.

- *Note: The Settings app scans for printers or scanners, but finds none.*

14. Scroll down and select the **Devices and printers** hyperlink.

- *Note that in the Control Panel, Devices and Printers appears. Note that some Settings-level configurations still use the Control Panel.*

15. Click **Add a printer**.
16. Click **The printer that I want isn't listed**, select **Add a local printer or network printer with manual settings**, and then click **Next**.
17. On the **Choose a printer port** page, click **Next**.
18. On the **Install the printer driver page**, under the Manufacturer column, select **HP**, and in the Printers column, scroll down and choose **HP Photosmart 7520 series Class Driver**, and then click Next.
19. On the **Printer Sharing** page, make sure sharing the printer is enabled, and set the Share name to **HP Photosmart 7520**. Click Next.
20. On the You've successfully added HP Photosmart 7520 page, click **Finish**.
21. Close the Control Panel, Devices and Printers.
22. This will return to the **Printers & scanners page** of the Settings app. Click the **HP Photosmart 7520 icon**. Note the Remove device option that appears. Without selecting it, close the Settings app.

    Results: After completing this exercise, you should have successfully used the Settings app to configure a device.

1.2 Exercise 2: Using Control Panel

1.2.1 Task 1: Use the Control Panel to configure a device

1. On **LON-CL1**, click the **Start** , and type **control**. Click **Control Panel** in the menu.
2. In the Control Panel, in the Hardware and Sound category, click the **View devices and printers** hyperlink.
3. You should see the printer named **HP Photosmart 7520**. Double-click it.
4. In the HP Photosmart 7520 window, click the **Printer menu**, and then select **Printing Preferences**.
5. In the HP Photosmart 7520 Printing Preferences window, note that Print on Both Sides is not found. Click Cancel, and then close the HP Photosmart 7520 window.
6. Right-click HP Photosmart 7520, and then click **Printer Properties**. In the HP Photosmart 7520 Properties sheet, select the **Device Settings** tab.
7. Note the installable options. To the right of Automatic Duplexing Unit:, click **Not installed**, change the drop-down selection to **Installed**, and then click **OK**.
8. Double-click the **HP Photosmart 7520** item.
9. In the HP Photosmart 7520 window, click the **Printer** menu, and then select **Printer Preferences**.
10. In the HP Photosmart 7520 Printing Preferences window, in the Print on both sides drop-down list, select **Flip on Long Edge**, and then click **OK**.
11. Close the HP Photosmart 7520 Control Panel window.
12. Close Devices and Printers.

    Results: After completing this exercise, you should have successfully used the Control Panel to configure a device.

1.3 Exercise 3: Using Windows PowerShell

1.3.1 Task 1: Use Windows PowerShell to configure a device

1. On the taskbar, in the Ask me anything text box, type **PowerShell**, right-click **Windows PowerShell**, and then select **Run as administrator**.
2. At the Windows PowerShell command prompt, type **Get-ExecutionPolicy**, and then press Enter. Confirm that the current execution policy is Unrestricted. If the execution policy is Unrestricted, skip steps 3 and 4, and proceed to step 5.
3. If set to Restricted, then in the Windows PowerShell command prompt, type **Set-ExecutionPolicy Unrestricted**, and then press **Enter**.
4. Select Yes to All [A] by typing an **A**, and then press **Enter**. Leave the Windows PowerShell command prompt open.
5. Click the **Start** Menu icon, and then in the Start menu, select **Settings**.
6. On the Settings page, click **Devices**.
7. Ensure that Printers & Scanners is selected in the console tree, and then select the **HP Photosmart 7520 series Class Driver**. Click **Manage**.
8. In the HP Photosmart 7520 series Class Driver window, click **Printing Preferences**.
9. In the HP Photosmart 7520 Printing Preferences window, note that the Print on Both Sides drop-down box is available, and then click **Cancel**.
10. Return to the Windows PowerShell command prompt.
11. At the Windows PowerShell command prompt, type the following, and then press Enter:

```
Get-PrinterProperty -PrinterName "HP Photosmart 7520"
```

- *Note:* The property named Config:DuplexUnit is set to TRUE.

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

```
Set-PrinterProperty -PrinterName "HP Photosmart 7520" -PropertyName "Config:DuplexUnit"
-Value FALSE
```

- *Note:* You must use all caps for the TRUE or FALSE values.

  Note: Note that in Windows PowerShell, each cmdlet parameter name is preceded immediately by a dash symbol, such as the –Value parameter, which you used above. However, the word wrap feature may separate the dash from the parameter when you copy and paste from a file. Therefore, you need to ensure that you inspect all pasted cmdlets and parameters to ensure they follow Windows PowerShell syntax requirements.

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

```
Get-PrinterProperty -PrinterName "HP Photosmart 7520"
```

- *Note: The property named Config:DuplexUnit is now FALSE.*

14. In the HP Photosmart 7520 window, select **Printing Preferences**.

- *Note: In the HP Photosmart 7520 Printing Preferences window, note that the Print on Both Sides drop-down list box is gone.*

15. Click **Cancel**, and then close all open windows.
16. In the Ask me anything text box, type **PowerShell ISE**, and then press **Enter**.
17. In Windows PowerShell ISE, on the tool bar, click the **open icon**, navigate to **E:\Labfiles\Mod03\Services.ps1**, and then **read the script**.

- *Note the following:*
  - *Comments are green.*
  - *Variables are red.*
  - *Cmdlets are bright blue.*
  - *Text in quotation marks is dark red.*

18. **Select line 3** in the script, and then **run the selection**. You can run the selection by **right-clicking the line** and selecting the **Run** selection option or by selecting the line and pressing **F8**.
19. Run the script by clicking the **green arrow** on the ribbon, and then read the output. Notice that it does not have multiple colors.
20. At the end of line 14, type –**ForegroundColor $color.**
21. Run the script by clicking the **green arrow** on the ribbon, and then read the output. Click **OK** in the Windows PowerShell ISE window if prompted to save the script.

    Note: Running services are green and services that are not running are red.
22. On line 16, type **Write-Host "A total of " $services.count "services were evaluated."**
23. **Run the script**. Click **OK** in the Windows PowerShell ISE window if prompted to save the script.
24. In the Commands pane, build a Write-Host cmdlet on line 17 with the following options:

- -BackgroundColor Gray
- -ForegroundColor Black
- -Object "Script execution is complete"

25. Run the script. Click OK in the Windows PowerShell ISE window if prompted to save the script.
26. Save the script by pressing **Ctrl+S** on the keyboard.
27. Open the **Windows PowerShell command prompt**.
28. At the command prompt, type **Set-Location E:\Labfiles\Mod03**, and then press **Enter**.
29. Type **.\Services.ps1**, and then press **Enter**. Close all open windows.

    Results: After completing this exercise, you should have successfully configured the device with Windows PowerShell.

2 Lab: Installing Windows 10

2.1 Exercise 1: Upgrading Windows 7 to Windows 10

2.1.1 Task 1: Verify that the computer meets the minimum requirements

1. Login to LON-CL3 as **Adatum\Administrator** with the password **Pa55w.rd**
2. If a Microsoft Windows dialog box opens, click **Restart Later**.
3. If a Windows Activation dialog box opens, click **Ask me later**. Click **OK**.
4. On the taskbar, click **Start**. Right-click **Computer**, and then click **Properties**.
5. Write down the settings for:

- Processor: _____
- Installed memory (RAM):_____

6. **Close** the System window.
7. Right-click **the desktop**, and then click **Screen Resolution**.
8. Write down the screen resolution:_____
9. On the taskbar, click the **Windows Explorer** icon.
10. Click **Computer**.

- Write down the available disk space for drive C: _____
- Do the noted values match the minimum requirements? _____

2.1.2 Task 2: Perform an in-place upgrade from local media

1. Login to LON-CL3 as **Adatum\Administrator** with the password **Pa55w.rd**
2. If a Microsoft Windows dialog box opens, click **Restart Later**.
3. If a Windows Activation dialog box opens, click **Ask me later**. Click **OK**.
4. On the taskbar, click the **Windows Explorer** icon.
5. In Windows Explorer, click the **DVD drive**.
6. In the contents pane, double-click the **setup.exe** file.
7. On the Get important updates page, click **Not right now**, and then click **Next**.
8. On the License terms page, click **Accept**.
9. On the Choose what to keep page, click **Nothing**. Click **Next**, and then click **Yes**.
10. Click **Install**. The setup program will now upgrade your Windows 7 installation to Windows 10. This will take approximately 30 minutes.
11. On the Hi there page, click **Next**.
12. On the Get going fast page, click **Use Express settings**.
13. On the Choose how you'll connect, select **Join a local Active Directory domain**, then **Next**.
14. On the Create an account for this PC page, provide the following, and then click Next:
    - Username: L**ocalAdmin**
    - Password: **Pa55w.rd**
    - Hint: **Standard password**
15. On the Meet Cortana page, click **Not now.**
16. After the setup finishes, you should be at the desktop of the new installation.

2.1.3 Task 3: Verify that the upgrade was successful

1. Click **Start** and type **winver**. Press **Enter**.
2. Make sure that the version number is 1607(OS Build 14393.0).

   Results: After completing this exercise, you will have upgraded your Windows 7–based computer to Windows 10.

2.2 Exercise 2: Migrating User Settings

2.2.1 Task 1: Prepare the source computer

1. Start and then sign in to **LON-CL3** as the Local **Admin** with the password of **Pa55w.rd**
2. Click **Start**, and type **Connect**. Select **Connect to work or school**.
3. On the Connect to work or school page, click the **+Connect**.
4. Select **Join this device to a local Active Directory domain**.
5. On the Join a domain prompt, type **ADATUM** and click **Next**.
6. Enter the credentials with Username: **adatum\administrator**, Password: **Pa55w.rd**
7. In the Add account dialog, change the Account type to **Administrator** and click **Next**.
8. **Restart** the PC.
9. Start and then sign in to LON-CL3 as **ADATUM\administrator**, Password: **Pa55w.rd**
10. Right-click the **desktop**, hover over the **New** menu item, and then click **Text Document**. Type **Demofile** and press **Enter**.
11. Double-click **Demofile.txt** and type some random text. Press **Alt+F4**, and then click the **Save** button.

12. Right-click **Start** and select **Command Prompt (Admin)**.
13. At the command prompt, type the following command, and then press **Enter**:

```
Net Use F: \\\\LON-DC1\\USMT
```

14. At the command prompt, type **F:**, and then press **Enter**.
15. At the command prompt, type the following, and then press **Enter**:

```
Scanstate \\\\LON-DC1\\MigrationStore\\LON-CL3\\ /i:migapp.xml /i:miguser.xml /o
```

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

2.2.2 Task 2: Complete the migration

1. **Switch to the LON-CL2** on Host computer Virtual Machine Connection window.
2. Sign in to LON-CL2 as **Adatum\Administrator** with the password **Pa55w.rd**

- *Notice that there is no Demofile.txt on the desktop and no Internet Explorer or Windows Media Player icon in the taskbar.*

4. Click **Start**, type **cmd**, and then press **Enter**.
5. At the command prompt, type the following command, and then press **Enter**:

```
Net Use F: \\\\LON-DC1\\USMT
```

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

```
Loadstate \\\\LON-DC1\\MigrationStore\\Lon-CL3\\ /i:migapp.xml /i:miguser.xml /lac:Pa55w.rd
/lae
```

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

8. Type **exit** to close the command prompt.

- *Notice that the demofile.txt is now on the desktop and the Internet Explorer and Windows Media Player icons are visible on the taskbar.*

Results: After completing this exercise, you will have migrated your settings from your Windows 7–based computer to a new Windows 10–based computer.

3 Lab: Updating Windows 10

3.1 Exercise 1: Configuring Updates for a Single Device

3.1.1 Task 1: Configure update settings for a single device

Switch to **LON-CL1**.

2. Login with the username ADATUM\Administrator, Password: Pa55w.rd
3. Right-click **Start**, and then select **Windows PowerShell (Admin)**.
4. 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.*

5. Click **Start**, and then click the **Settings** icon.
6. In **Settings**, click **Update & security**.
7. On the **Windows Update** tab, click **Advanced options**.
8. On the Advanced options page, in the **Semi-Annual Channel (Targeted)** drop-down list, select **Semi-Annual Channel**.
9. Click **Delivery Optimization**.

10. On the Delivery Optimization page, enable the **Allow downloads from other PCs** option.
11. Select **PCs on my local network, and PCs on the Internet**, and then click **Back** twice.
12. In the navigation pane, click **Windows Insider Program**. Notice that the **Get Started** option is available.
13. In the navigation pane, click **Windows Update**.

3.1.2 Task 2: Review applied updates

1. On the **Windows Update** page, click **View installed update history**.
2. Review the updates listed, and then click **Uninstall updates**.
3. Review the updates listed in **Installed Updates**. Close **Installed Updates**.
4. On the **Update history** page, click **Back**.

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

3.2 Exercise 2: Configuring Updates with GPOs

3.2.1 Task 1: Configure update settings by using GPOs

1. In the **Ask me anything** box, type **gpedit.msc**, and then press Enter.
2. In **Local Group Policy Editor**, navigate to **Computer Configuration/Administrative Templates /Windows Components/Data Collection and Preview Builds**.
3. In the right pane, double-click **Toggle user control over Insider builds**.
4. In the **Toggle user control over Insider builds** dialog box, click **Disabled**, and then click **OK**.
5. In **Local Group Policy Editor**, navigate to **Computer Configuration/Administrative Templates /Windows Components/Windows Update/Windows Update for Business**.
6. In the right pane, double-click **Select when Preview Builds and Feature Updates are received.**
7. In the Select when Preview Builds and Feature Updates are received dialog box, click **Enabled**.
8. In the **Select Windows Readiness level** for the updates you want to receive drop-down list, **select Semi-Annual Channel (Targeted)**, and then click OK.
9. In the navigation pane, click **Windows Update**.
10. In the right pane, double-click **Do not connect to any Windows Update Internet locations**.
11. In the **Do not connect to any Windows Update Internet locations** dialog box, click **Enabled**, and then click **OK**.
12. Close **Local Group Policy Editor**.

3.2.2 Task 2: Verify that the device's update settings are managed centrally

1. Click **Start**, type **cmd**. Right-click on **Command Prompt** and click **Run as Administrator**.
2. In the command prompt, type **gpupdate /force**, and then press Enter.
3. Switch to **Settings**.
4. In the navigation pane, click **Windows Insider Program**.
5. On the **Windows Insider Program** tab, notice that the option to **Get started with Insider builds** is unavailable.
6. Close all open apps and windows.

   Results: After completing this exercise, you will have successfully configured Group Policy Objects (GPOs) to configure Windows Update settings.

4 Lab: Managing Storage

4.1 Exercise 1: Adding a Disk

4.1.1 Task 1: Use Disk Management to initialize a disk

1. On **LON-CL2,** login as **Adatum\Administrator with** the password **Pa55w.rd**
2. Click Start and type **diskmgmt.msc.** Click diskmgmt.msc in the list.
3. In the Initialize Disk window, **clear the Disk 2 and Disk 3** check boxes, and then click **OK**. You can see that Disk 1 now has a status of Online.

   Results: After completing this exercise, you will have initialized one hard disk.

4.2 Exercise 2: Creating a Simple Volume

4.2.1 Task 1: Create a simple volume

1. Right-click the right side of Disk 1, and then click **New Simple Volume**.
2. In the New Simple Volume Wizard window, click **Next**.
3. On the Specify Volume Size page, **type 5120**, and then click **Next**.
4. On the Assign Drive Letter or Path page, make sure that **drive E** is selected, and then click **Next**.
5. On the Format partition page, in the Volume Label text box, **type Data**, and then click **Next**.
6. On the Completing the New Simple Volume Wizard page, click **Finish**. If you receive the error message Location is not available, then click OK.

   Note: If prompted whether to format drive E:, click Cancel.
7. **Close File Explorer** window.

4.2.2 Task 2: Extend the simple volume

1. Click Start, and then **type PowerShell**, then select **PowerShell** in the list.
2. In Windows PowerShell, **type the following two commands**:

```
$MaxSize = (Get-PartitionSupportedSize -DriveLetter e).sizeMax

Resize-Partition -DriveLetter e -Size \$MaxSize
```

3. **Switch to the Disk Management window**, and then verify that the E volume now occupies the entire Disk 1.

   Note: If the change is not visible, press F5 to refresh the view in Disk Management.
4. **Close** all Windows.

   Results: After completing this exercise, you will have created a simple volume and then extended the volume.

4.3 Exercise 3: Compressing a Folder

4.3.1 Task 1: Verify current folder size

1. Click the File Explorer icon on the taskbar.
2. Navigate to the **C:\Users folder**. Right-click the **Admin folder**, and then click **Properties**.
3. On the General tab, note the Size on Disk in megabytes (MB):_____

4.3.2 Task 2: Configure compression on the folder

1. On the General tab, click **Advanced**.
2. Click **Compress contents to save disk space**, and then click **OK**.

3. Click **Apply**, and then in the Confirm Attribute Changes window, click **OK**.

   Note: If the Access Denied window appears, click Continue. If the Error Applying Attributes window appears, click Ignore All.

4.3.3 Task 3: Verify the storage consumed by the compressed folder

1. After the compression finishes, on the General tab, note the Size on Disk in MB: _____, and then click **OK**.
2. Notice that the Admin folder is now represented as a compressed folder icon.

   Results: After completing this exercise, you will have compressed a folder with files.

5 Lab: Configuring and Managing Permissions and Shares

5.1 Exercise 1: Creating, Managing, and Sharing a Folder

5.1.1 Task 1: Create a folder structure

1. On **LON-CL1**, sign in as **Adatum\Administrator** with the password **Pa55w.rd**
2. On the taskbar, click **File Explorer.**
3. In File Explorer, in the navigation pane, expand This PC, and then click **Local Disk (C:)**. 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 Local Disk (C:),** click **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.

5.1.2 Task 2: Review default permissions

1. On LON-CL1, in File Explorer, in the navigation pane, double-click **Data** below Local Disk (C:), right-click **IT**, and then select **Properties**.
2. In the IT Properties window, click the **Security tab**, and then click **Edit**.
3. In the Permissions for IT dialog box, verify that Authenticated Users is selected in the Group or user names section, and then click Remove. Read the text in the Windows Security dialog box that appears, which explains why you cannot remove an authenticated user. Click **OK**, and then click **Cancel**.
4. In the IT Properties window, on the Security tab, click **Advanced**.
5. In the Advanced Security Settings for IT dialog box, verify that all permissions entries are inherited from C:\. Also, verify that Users (LON-CL1\Users) have Read & execute Access, while Authenticated Users have Modify Access. Click OK twice.

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

1. On LON-CL1, in File Explorer, in the navigation pane, right-click the **IT folder**, select **Give access to**, and then select **Specific people**.
2. In the File Sharing dialog box, verify that Administrator is selected, click **Read/Write** in the Permission Level column, and then select **Remove**.
3. In the Type a name and then click **Add,** or click the arrow to find someone text box, **type IT**, and then click **Add**.
4. Verify that IT is added and selected. Click **Read** in the Permission Level column, select **Read/Write**, click **Share**, and then click **Done**.
5. In File Explorer, in the navigation pane, right-click **Marketing**, and then select **Properties**.

6. In the Marketing Properties dialog box, select the **Sharing tab**. In the Network File and Folder Sharing section, verify that Marketing is not shared, and then in the Advanced Sharing section, click **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. Click **Permissions**.
8. In the Permissions for Marketing dialog box, select the **Everyone** group and click **Remove**. Click **Add**, in the Enter the object names to select (examples) box, type **Marketing**, and then click **OK**. In the Permissions for Marketing section, select the **Change check box** in the Allow column, and then click **OK** twice.
9. 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 click **Close**.
10. Click the **Start** icon, type **cmd** and then select **Command Prompt**.
11. At the command prompt, view shares created on LON-CL1 by typing **net view \\lon-cl1**, and then pressing Enter. **Close** the command prompt.
12. Right-click the **Start** icon, and then select **Computer Management.**
13. In Computer Management, in the navigation pane, expand **Shared Folders**, and then click **Shares**. In the details pane, verify that you see IT and Marketing shares, and the default Windows 10 shares. **Close** Computer Management.

5.1.4 Task 4: Review configured permissions

1. On LON-CL1, in File Explorer, in the navigation pane, right-click **IT**, and then select **Properties**.
2. In the IT Properties window, click the **Security tab**, and then click **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 an Administrator, Administrators [LON-CL1\Administrators group, SYSTEM and IT (ADATUM\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, click **OK**. 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 \\Lon-cl1\it, and then click **Advanced Sharing**.
6. In the Advanced Sharing dialog box, click **Permissions**. In the Permissions for IT dialog box, verify that the Everyone and Administrators groups have Full Control permissions to the share, click **OK** twice, and then click **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.
7. In File Explorer, in the navigation pane, right-click **Marketing**, and then select **Properties**.
8. In the Marketing Properties window, click the **Security tab**, and then click **Advanced**.
9. In the Advanced Security Settings for Marketing dialog box, verify that all of the permissions entries are inherited from C:\. Also verify that Users (LON-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. Click **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.
10. Click the **Start** icon, select the **user icon**, and then select **Sign out**.

5.1.5 Task 5: Test local file permissions

1. On LON-CL1, sign in as **Adatum\Bill** with the password **Pa55w.rd**

   Bill is a member of the Marketing group, but is not a member of the IT group.

2. On the taskbar, click **File Explorer**. In File Explorer, in the navigation pane, expand **This PC**, expand **Local Disk (C:)**, expand **Data**, and then select **Marketing**.
3. 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: Adam 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.
4. In File Explorer, in the navigation pane, select **IT**, and then click **Cancel**.

   Note: You will get an error, because Adam 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.
5. Click the **Start** icon, select the **user icon**, and then select **Sign out**.
6. On LON-CL1, sign in as **Adatum\Beth** with the password **Pa55w.rd**

   April is member of the IT group, and she is not member of the Marketing group.
7. On the taskbar, click **File Explorer.** In File Explorer, in the navigation pane, expand **This PC**, expand **Local Disk (C:)**, expand **Data**, and then select **Marketing**.
8. In the details pane, verify that you can see File10 that was created by Bill. Right-click the **empty space**, select **New**, select **Text Document**, and then type **File20** as the name of the file.

   Note: April 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.
9. 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: April 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.
10. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.

5.1.6 Task 6: Test share permissions

1. **Switch to LON-CL2**, sign in as **Adatum\Bill** with the password **Pa55w.rd**

   Bill is a member of the Marketing group, but he is not a member of the IT group.
2. On the taskbar, click **File Explorer**. In File Explorer, click the **arrow** in the Address bar, type **\\LON-CL1**, and then press **Enter**.
3. Verify that you can see the IT and Marketing shares in the details pane. Double-click **Marketing**. Verify that you can see the files that Bill and Beth created locally.
4. In the details pane, right-click the **empty space**, select **New**, select **Text Document**, and then type **File30** as the name of the file. Bill has permissions to create a new file in the Marketing share because he is a member of the Marketing group.
5. In File Explorer, click **LON-CL1** in the address bar. In the details pane, double-click **IT**. Read the text in the Network Error dialog box, and then click **Close**.

   Note: Bill is not a member of the IT group, so he does not have permissions to the IT share.
6. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.
7. Sign in as **Adatum\Beth** with the password **Pa55w.rd**

   Beth is a member of the IT group, but she is not a member of the Marketing group.

8. On the taskbar, click **File Explorer**. In File Explorer, click the **arrow** in the Address bar, type **\\LON-CL1**, and then press **Enter**.
9. Verify that you can see the IT and Marketing shares in the details pane. Double-click **Marketing**.
10. Read the text in the Network Error dialog box. Beth is not a member of the Marketing group, so she does not have permissions to the Marketing share. Click **Close**.
11. 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. Beth has permissions to create a new file in the IT share because she is a member of the IT group.

    Note: 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.

    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.

5.2 Exercise 2: Using Conditions to Control Access and Effective Permissions

5.2.1 Task 1: Configure conditions to control access

1. On **LON-CL1**, sign in as **Adatum\Administrator** with the password **Pa55w.rd**
2. On the taskbar, click **File Explorer**.
3. In File Explorer, in the navigation pane, expand **Local Disk (C:)**, and then click **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 click **Advanced Sharing**.
5. In the Advanced Sharing dialog box, select the **Share this folder check box**, and then click **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 click **OK** twice.
7. In the Research Properties dialog box, select the **Security tab**, click **Advanced**, and then verify that all permissions entries are inherited from C:\.
8. In the Advanced Security Settings for Research dialog box, select **Users (LON-CL1\Users)**, and then click **Remove**. Read the text in the Windows Security dialog box that appears, click **OK**, and then click **Disable inheritance**.
9. In the Block Inheritance dialog box, click **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.
10. In the Advanced Security Settings for Research dialog box, select **Users (LON-CL1\Users)**, and then click **Remove**. Entry for Users is removed from the Permission entries because it was explicitly set at this level.
11. Verify that **Authenticated Users** is selected, and then click **Edit**.
12. In the Permission Entry for Research dialog box, click **Add a condition**, and compose the following expression: **User department Equals Value research**. You will need to type research manually in the last box. Click **OK** twice, and then click **Close**.
13. In File Explorer, in the navigation pane, expand **Data**, right-click **IT**, select **Properties**, select the **Security tab**, and then click **Advanced**.
14. In the Advanced Security Settings for IT dialog box, select **IT (ADATUM\it)**, and then click **Edit**.
15. In the Permission Entry for IT dialog box, click **Add a condition**, and compose the following expression: **User Country Equals Value US**. You will need to type US manually in the last field. Click **OK** three times.

5.2.2 Task 2: Test conditions to control access

1. **Switch to LON-CL2**, where you are signed in as **Adatum\Beth**, in File Explorer, in the address bar, click **LON-CL1**. In the details pane, double-click **Research**. Read the text in the Network Error dialog box, and then click **Close**.
2. Click the **Start** icon, type **cmd** and then select **Command Prompt** in the list.
3. At the command prompt, view user claims by typing **whoami /claims**, and then press **Enter**. Review the output, and then **close** the command prompt.

   Note: Beth has a department claim value of IT and she cannot connect to the Research share.
4. In File Explorer, in the address bar, click **LON-CL1**. In the details pane, double-click **IT**.
5. 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: Beth 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.
6. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.
7. Sign in as **Adatum\Nestor** with the password **Pa55w.rd**

   Nestor is a member of the IT group.
8. On the taskbar, click **File Explorer**. In File Explorer, click the **arrow** in the Address bar, type **\\LON-CL1**, and then press **Enter**.
9. In the details pane, double-click **IT**. Jesper is a member of the IT group, but he cannot connect to the IT share. Click **Close**.
10. Click the **Start** icon, type **cmd** and then select **Command Prompt** in the list.
11. At the command prompt, view user claims by typing **whoami /claims**, and then press **Enter**. Review the output, and then **close** the command prompt.

    Note: Jesper 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.
12. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.
13. Sign in as **Adatum\Max** with the password **Pa55w.rd**
14. Click the **Start** icon, type **cmd** and then select **Command Prompt** in the list.
15. At the command prompt, view user claims by typing **whoami /claims**, and then pressing **Enter**. Review the output, and then **close** the command prompt.

    Note: Max is in the Research department, and his department claim has the value of Research.
16. On the taskbar, click **File Explorer**. In File Explorer, click the **arrow** in the Address bar, type **\\LON-CL1**, and then press **Enter**.
17. In the details pane, double-click **Research**, and then verify that Max can view the contents of the Research folder.
18. 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: Max has permissions to create a new file in the Research share because his department claim has a value of Research.

5.2.3 Task 3: View effective permissions

1. **Switch to LON-CL1**, in File Explorer, in the navigation pane, right-click **Marketing**, select **Properties**, select the **Security tab**, click **Advanced**, and then select the **Effective Access tab**.
2. In the Advanced Security Settings for Marketing dialog box, click **Select a user**, in the Enter the object name to select (examples) box, **type Ernie**, click **OK**, and then click **View effective access**. View the effective permissions, and then click **OK** twice.

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

3. In File Explorer, in the navigation pane, right-click **Research**, select **Properties**, select the **Security tab**, click **Advanced**, and then select the **Effective Access tab**.
4. In the Advanced Security Settings for Research dialog box, click **Select a user**, in the Enter the object name to select (examples) text box, type **Bruno**, click **OK**, and then click **View effective access**. Bruno is a member of Development group.

   Note: Only users with the department claim with a value of Research have permissions to the folder, you can see that Bruno has no permissions allowed.
5. In the Advanced Security Settings for Research dialog box, click **Include a user claim**, select **department** in the drop-down list, **type Research** in the Enter value here text box, and then click **View effective access**.

   Note: You can see that if Bruno had the department user claim with the value of Research, he would have most permissions allowed.
6. In the Advanced Security Settings for Research dialog box, click **Select a user**, in the Enter the object name to select (examples) box, type **Arturs**, click **OK**, and then click **View effective access**. Review the effective permissions, and then click **OK** twice.

   Note: If Arturs had the user claim of department with the value of Research, he would have the most permissions allowed.
7. Sign out of LON-CL1.

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

6 Lab: Managing Network Security

6.1 Exercise 1: Creating and Testing Inbound Rules

6.1.1 Task 1: Test existing functionality

1. Sign in to **LON-CL2** as **Adatum\Administrator** with the password **Pa55w.rd**
2. Right-click **Start**, click **Run**, **type mstsc.exe**, and then press **Enter**.
3. In the Computer box, **type LON-CL1**, and then press **Enter**.
4. In Remote Desktop Connection, sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**
5. Open the **Start** menu on **LON-CL1**, click **Administrator**, and then click **Sign out**.

6.1.2 Task 2: Create an inbound rule

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa55w.rd**
2. Click **Start**, and type **control**, then click **Control Panel** in the list.
3. Click **System and Security**, and then click **Windows Defender Firewall**.
4. In the left pane, click **Advanced settings**, click **Inbound Rules**, and then click **New Rule**.
5. In the New Inbound Rule Wizard window, select **Predefined**, click the **drop-down list**, click **Remote Desktop**, and then click **Next**.
6. On the Predefined Rules page, **check all available rules**, and then click **Next**.
7. On the Action page, select **Block the connection**, and then click **Finish**.
8. **Minimize** the Windows Firewall with Advanced Security window.

6.1.3 Task 3: Test the rule

1. **Switch to LON-CL2**.
2. Click **Start**, type **mstsc.exe**, and then press **Enter**.
3. In the Computer box, **type LON-CL1**, and then press **Enter**.
4. In the Remote Desktop Connection window, click **OK**.
5. Verify that the connection attempt fails.

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

6.2 Exercise 2: Creating and Testing Outbound Rules

6.2.1 Task 1: Test existing functionality

1. **Switch to LON-CL1**.
2. Right-click **Start**, click **Run**, type **mstsc.exe**, and then press **Enter**.
3. In the Computer box, type **LON-DC1**, and then press **Enter**.
4. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa55w.rd**
5. Open the Start screen on **LON-DC1**, click **Administrator**, and then click **Sign out**.

6.2.2 Task 2: Create an outbound rule

1. On **LON-CL1**, on the taskbar, click the **Windows Firewall with Advanced Security** window, and then click **Outbound Rules**.
2. In the Actions pane, click **New Rule**.
3. On the Rule Type page, verify that you are creating a **Program rule**, and then click **Next**.
4. On the Program page, browse and select **C:\Windows\System32\mstsc.exe**, click **Open**, and then click **Next**.
5. On the Action page, verify that the action is **Block the Connection**, and then click **Next**.
6. On the Profile page, verify that **all profiles are checked**, and then click **Next**.
7. On the Name page, type **Block Outbound RDP to LON-DC1** in the Name box, and then click **Finish**.
8. In the Windows Firewall with Advanced Security window, click the **Block Outbound RDP to LON-DC1** rule, and then in the Actions pane, click **Properties**.
9. Click the **Scope tab**, and then under the **Remote IP address heading**, select the **These IP addresses** option.
10. Under the Remote IP address heading, click **Add**, in the This IP address or subnet box, type **172.16.0.10**, and then click **OK**.
11. In the Block Outbound RDP to LON-DC1 Properties dialog box, click **OK**.

6.2.3 Task 3: Test the rule

1. Right-click Start, click Run, **type mstsc.exe**, and then press **Enter**.
2. In the Computer box, **type LON-DC1**, and then press **Enter**.
3. In the Remote Desktop Connection dialog box, click **OK**.
4. **Close** all open windows.

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

6.3 Exercise 3: Creating and Testing Connection Security Rules

6.3.1 Task 1: Verify that communications are not secure

1. Sign in to **LON-CL2** as **Adatum\Administrator**.
2. In the search box on the taskbar, type **PowerShell**, and then click **Windows PowerShell**.
3. In the Administrator: Windows PowerShell window, type **ping LON-CL1**, and then press **Enter**.
4. Verify that the ping generated four "Reply from 172.16.0.40: bytes=32 time=$x$ms TTL=128" messages. Please note, the times that the message lists may vary from the example.
5. Click **Start**, type **control** and click **Control Panel** in the list.
6. Click **System and Security**, and then click **Windows Defender Firewall**.
7. In the left pane, click **Advanced settings**.
8. In the left pane, expand **Monitoring,** and then expand **Security Associations**.
9. Click **Main Mode**, and then examine the information in the center pane. No information should be present.
10. Click **Quick Mode**, and then examine the information in the center pane. No information should be present.
11. **Switch to LON-CL1**.
12. In the search box on the taskbar, type **PowerShell**, and then click **Windows PowerShell**.
13. To examine the Main Mode Security Associations (SAs), at the Windows PowerShell prompt, type the following cmdlet, and then press Enter:

```
Get-NetIPsecMainModeSA
```

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

```
` Get-NetIPsecQuickModeSA`
```

15. Running each command should produce no result.

6.3.2 Task 2: Create the Connection Security Rule

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

16. On the Rule Type page, verify that **Isolation is selected**, and then click **Next**.
17. On the Requirements page, select **Require authentication for inbound connections and request authentication for outbound connections**, and then click Next.
18. On the Authentication Method page, select **Computer and user (Kerberos V5)**, and then click **Next**.
19. On the Profile page, click **Next**.
20. On the Name page, in the Name text box, type **Authenticate all inbound connections**, and then click **Finish**.
21. Close the **Windows Firewall with Advanced Security** window.

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

1. On **LON-CL2**, in the Administrator: Windows PowerShell window, type **ping LON-CL1**, and then press **Enter**.
2. Verify that the ping generated four "Reply from 172.16.0.40: bytes=32 time=$x$ms TTL=128" messages. Please note, the times that the message lists may vary from the example.
3. Click **Start**, type **Windows Defender**, then click **Windows Defender Firewall**.
4. In the left pane, click **Advanced settings**.
5. In the left pane, expand **Monitoring**, and then expand **Security Associations**.
6. Click **Main Mode**, and then examine the information in the center pane.
7. Click **Quick Mode**, and then examine the information in the center pane.
8. **Close** all open windows.
9. **Switch to LON-CL1.**
10. To examine the Main Mode Security Associations (SAs), at the Windows PowerShell command prompt, type the following cmdlet, and then press Enter:

```
Get-NetIPsecMainModeSA
```

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

```
` Get-NetIPsecQuickModeSA`
```

13. Review the result.

Results: After completing this exercise, you should have created and tested connection security rules.

6.4 Exercise 4: Configuring Windows Defender

6.4.1 Task 1: Perform a quick scan

1. On **LON-CL1** click **Start**, and then select **Settings**.
2. In the Settings app, open **Update & Security**, and then open the **Windows Defender tab**.
3. Click **Open Windows Defender Security Center**.
4. In Windows Defender Security Center, select **Virus & threat protection**.
5. On the Virus & threat protection page, select **Quick scan**.
6. **Close** Windows Defender Security Center .

6.4.2 Task 2: Introduce suspicious software

1. Open **File Explorer**, and then browse to **E:\Labfiles\Mod10**.
2. In the Mod10 folder, open **sample.txt** in Notepad. The sample.txt file contains a text string to test malware detection.

3. In the sample.txt file, **delete both instances of <remove>,** including the brackets and any extra lines or blank spaces.
4. **Save and close** the file. Immediately, Windows Defender detects a potential threat.

6.4.3 Task 3: View the quarantined file

1. In the notification area, click **Notifications**, and then in the Action Center, select the notification that states that **Windows Defender Antivirus found a threat**.
2. Windows Defender Security Center opens on the Scan history page.
3. Select the **down arrow** next to Virus:DOS/EICAR_Test_File, and then select **Remove**.
4. Notice the sample.txt file is now gone from the Mod10 folder.
5. **Close** all open windows.

   Results: After completing this exercise, you should have configured and tested Windows Defender.

7 Lab: Monitoring Windows 10

7.1 Exercise 1: Monitoring Events

7.1.1 Task 1: Configure Event Viewer to collect data from multiple devices

1. On **LON-DC1**, sign in as **adatum\Administrator** with the password: **Pa55w.rd**
2. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
3. At the command prompt, type the following command, and then press **Enter**:

   ```
   winrm quickconfig
   ```

   Note: This is just a check, as the remote management feature is probably enabled.
4. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
5. In **Active Directory Users and Computers**, in the navigation pane, expand **Adatum.com**, and then click **Builtin**.
6. In the results pane, double-click **Event Log Readers**.
7. In the **Event Log Readers Properties** dialog box, click the **Members** tab.
8. Click **Add**, and then in the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
9. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
10. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** box, type **LON-CL1**, and then click **OK**.
11. In the **Event Log Readers Properties** dialog box, click **OK**.
12. Switch to **LON-CL1**.
13. Right-click **Start**, and then click **Command Prompt (Admin)**.
14. At the command prompt, type the following command, and then press **Enter**:

    ```
    Wecutil qc
    ```
15. When prompted, type **Y**, and then press Enter.

7.1.2 Task 2: View and filter events

1. On **LON-CL1**, right-click **Start**, and then click **Event Viewer**.
2. In **Event Viewer**, in the navigation pane, click **Subscriptions**.
3. Right-click **Subscriptions**, and then click **Create Subscription**.
4. In the **Subscription Properties** dialog box, in the **Subscription name** box, type **LON-DC1 Events**.

5. Click **Collector Initiated**, and then click **Select Computers**.
6. In the **Computers** dialog box, click **Add Domain Computers**.
7. In the **Select Computer** dialog box, in the **Enter the object name to select (examples)** box, type **LON-DC1**, and then click **OK**.
8. In the **Computers** dialog box, click **OK**.
9. In the **Subscription Properties – LON-DC1 Events** dialog box, click **Select Events**.
10. In the **Query Filter** dialog box, select the **Critical**, **Warning**, **Information**, **Verbose**, and **Error** check boxes.
11. In the **Logged** dropdown list, click **Last 30 days**.
12. In the **Event logs** dropdown list, select **Windows Logs**. Click in the **Query Filter** dialog box, and then click **OK**.
13. In the **Subscription Properties – LON-DC1 Events** dialog box, click **OK**.
14. In **Event Viewer**, in the navigation pane, expand **Windows Logs**.
15. Click **Forwarded Events**.
16. Right-click **Forwarded Events**, and then click **Create Custom View**.
17. In the **Create Custom View** dialog box, select the **Critical** and **Error** check boxes, and then click **OK**.
18. In the **Save Filter to Custom View** dialog box, in the **Name** box, type **LON-DC1 errors**, and then click **OK**.
19. Examine any listed events. The list may be empty.
20. Close all apps and open windows.

    Results: After completing this exercise, you will have successfully configured monitoring by using Event Viewer.

7.2 Exercise 2: Monitoring Reliability and Performance

7.2.1 Task 1: Use Performance Monitor to gather a baseline

1. On **LON-CL1**, click **Start**, type **administrative**, click **Windows Administrative Tools**, and then click **Performance Monitor**.
2. In **Performance Monitor**, in the navigation pane, expand **Data Collector Sets**.
3. Expand **User Defined**, right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
4. In the **Create new Data Collector Set Wizard**, on the **How would you like to create this new data collector set?** page, in the **Name** text box, type **Adatum Baseline**.
5. Click **Create manually (Advanced)**, and then click **Next**.
6. On the **What type of data do you want to include?** page, select the **Performance counter** check box, and then click **Next**.
7. On the **Which performance counters would you like to log?** page, in the **Sample interval** field, type **1**, and then click **Add**.
8. In the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add**.
9. In the **Available counters** list, expand **Network Interface**, select **Packets/sec**, and then click **Add**.
10. In the **Available counters** list, expand **Physical Disk**, click **% Disk Time**, and then click **Add**.
11. Under **Physical Disk**, click **Avg. Disk Queue Length**, and then click **Add**.
12. In the **Available counters** list, expand **Processor**, click **% Processor Time**, and then click **Add**.
13. In the **Available counters** list, expand **System**, click **Processor Queue Length**, click **Add**, and then click **OK**.
14. On the **Which performance counters would you like to log?** page, click **Next**.

15. On the **Where would you like the data to be saved?** page, click **Next**.
16. On the **Create the data collector set** page, click **Finish**.
17. In **Performance Monitor**, in the navigation pane, right-click **Adatum Baseline**, and then click **Start**.
18. Click **Start**, and then click **Word 2016**.
19. Click **Start**, and then click **Excel 2016**.
20. Click **Start**, and then click **PowerPoint 2016**.
21. Close all open Microsoft Office 2016 apps, and then switch to **Performance Monitor**.
22. In the navigation pane, right-click **Adatum Baseline**, and then click **Stop**.
23. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **Adatum Baseline**, and then click the report that has a name beginning with **LON-CL1**.
24. View the chart. On the menu bar, click the drop-down arrow, and then click **Report**.
25. Record the following values:

- Memory Pages per second
- Network Interface Packets per second
- Physical Disk % Disk Time
- Physical Disk Avg. Disk Queue Length
- Processor % Processor Time
- System Processor Queue Length

7.2.2 Task 2: Load the suspect app

1. On **LON-CL1**, if necessary, sign by in using the following credentials:

- User name: **Adatum\Administrator**
- Password: **Pa55w.rd**

2. Run the **E:\Labfiles\Mod11\Scenario.vbs** script.
3. The script starts to generate the load.

7.2.3 Task 3: Use Performance Monitor to identify possible bottlenecks

1. Switch to **Performance Monitor**.
2. Under **Data Collector Sets**, click **User Defined**.
3. Right-click **Adatum Baseline**, and then click **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?

   Answers will vary depending upon the usage scenario and host configuration, although central processing unit (CPU) and network are likely to be used heavily.
6. After a few minutes, in the **Windows Script Host** prompt, click **OK**. Check the taskbar to see if this dialog may be hidden.
7. Close the instance of **C:\Windows\System32\cmd.exe** that the script launched.
8. Switch to **Performance Monitor**.
9. In the navigation pane, right-click **Adatum Baseline**, and then click **Stop**.
10. In **Performance Monitor**, in the navigation pane, expand **Reports**, expand **User Defined**, expand **Adatum Baseline**, and then click the **second report** that has a name beginning with **LON-CL1**.
11. View the chart.
12. On the menu bar, click the drop-down arrow, and then click **Report**.

13. Record the component details:
    - Memory Pages per second
    - Network Interface Packets per second
    - Physical Disk % Disk Time
    - Physical Disk Avg. Disk Queue Length
    - Processor % Processor Time
    - System Processor Queue Length
13. In your opinion, which components is the script affecting the most?

    The script is affecting the CPU and network, but it is also affecting all counters.
14. Close all open windows and apps.

    Results: After completing this exercise, you will have successfully determined the cause of a performance bottleneck.

8 Lab A: Troubleshooting Desktop Apps

8.1 Exercise 1: Troubleshooting AppLocker Policy Applications

8.1.1 Task 1: Review the help-desk Incident Record

Scenario: Your manager has come to you indicating that there are reports of staff in one department who are installing unauthorized programs. Your manager indicates that the AppLocker policies in place should be preventing this. You need to investigate why they are not working.

Incident Reference Number: 723401

Incident Reference Number: 723401 **Date of Call:** January 4 **User:** Alan Steiner (Marking Dept) **Status:** Open
Incident Details Users are installing unauthorized applications in the Marketing department.
Additional Information Alan Steiner, one of the marketing managers, has reported that users are installing unauthorized
Plan of Action
Resolution

The main tasks for this exercise are as follows:

1. Read the help-desk Incident Record for incident 723401.
2. Discuss recommendations.
3. Verify the problem.
4. Attempt to resolve the problem.

8.1.2 Task 2: Discuss recommendations

1. Read the Additional Information section of the incident record in the Student Handbook exercise scenario.
2. Discuss your recommendations with other students:
    1. Visit the user's computer.
    2. Sign in as a member of the Marketing group and verify the application of the AppLocker restriction policy.
    3. If the policy is not applying, use the Group Policy Object (GPO) troubleshooting techniques to determine why.
    4. Assuming that the GPO is applying, examine the settings for the AppLocker policy.
    5. Check for AppLocker enforcement requirements:
        1. Application identity is service running.
        2. Default rules are being applied.

3. Enforcement is enabled in the AppLocker policy.
    - more
    - more
        - even more

8.1.3 Task 3: Verify the problem

1. Switch to **LON-CL1**.
2. Sign in by using the following credentials:

- User name: **Adatum\Benjamin**
- Password: **Pa55w.rd**

3. On the desktop, on the taskbar, click the **File Explorer** icon.
4. In the File Explorer address bar, type **\\lon-dc1\Apps\XmlNotepad.msi**, and then press **Enter**.
5. When installation starts, cancel it by clicking **Cancel,** then click **Yes,** then **Finish.**

   Note: This step shows that the AppLocker policy is not being enforced.

8.1.4 Task 4: Attempt to resolve the problem with an App Locker policy

1. Switch to **LON-DC1.**
2. **Sign in** to LON-DC1 as **Adatum\Administrator** with the password of **Pa55w.rd**.
3. On LON-DC1, in the Server Manager window, click **Tools**, and then click **Group Policy Management**.
4. In the Group Policy Management window, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, expand **Group Policy Objects**, and then click **Marketing**.
5. Right-click **Marketing**, and then click **Edit**.
6. In the Group Policy Management Editor window, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Application Control Policies**, expand **AppLocker**, and then click **Windows Installer Rules**.
7. Right-click **Windows Installer Rules**, and then click **Create Default Rules**.
8. Right-click **Windows Installer Rules**, and then click **Create New Rule**.
9. On the Before You Begin page, click **Next**.
10. On the Permissions page, select **Deny**, and then click **Next**.
11. On the Conditions page, select **Path**, and then click **Next**.
12. On the Path page, click **Browse Files**.
13. In the File name text box, type **\\lon-dc1\apps**, and then press **Enter**.
14. In the Open dialog box, double-click **XmlNotepad.msi**, and then click **Next**.
15. On the Exceptions page, click **Next**, and then click **Create**.
16. In the navigation pane, right-click **AppLocker**, and then click **Properties**.
17. In the AppLocker Properties dialog box, under Windows Installer rules, select the **Configured** check box, and then click **OK**.
18. In the navigation pane, click **System Services**, and then double-click **Application Identity**.
19. In the Application Identity Properties dialog box, select the **Define this policy setting** check box, click **Automatic**, and then click **OK**.
20. **Close** the Group Policy Management Editor window.

8.1.5 Task 5: Apply the AppLocker policy

1. In the Group Policy Management window, right-click the **Marketing OU**, and then click **Link an Existing GPO**. Select **Marketing**, and then click **OK**.
2. **Close** Group Policy Management.
3. In the Server Manager window, click **Tools**, and then click **Active Directory Users and Computers**.
4. In Active Directory Users and Computers, expand **Adatum.com**, and then click **Computers**.
5. Right-click **LON-CL1**, and then click **Move**.
6. In the Move dialog box, click **Marketing**, and then click **OK**.
7. Switch to **LON-CL1** and restart LON-CL1.
8. **Sign in** to LON-CL1 as **Adatum\Administrator** with the password of **Pa55w.rd**.
9. In LON-CL1, click **Start**, and type **cmd**, right-click on **Command Prompt**, and select **Run as Administrator**.
10. In the Command Prompt window, at the command prompt, type the following command, and then press **Enter**:

```
gpupdate /force
```

1. **Sign out** of LON-CL1, then sign in by using the following credentials:

- User name: **Adatum\Benjamin**
- Password: **Pa55w.rd**

2. On the desktop, on the taskbar, click the **File Explorer** icon.
3. In the File Explorer address bar, type **\\lon-dc1\Apps\XmlNotepad.msi**, and then press **Enter**.
4. In the Windows Installer dialog box, click **OK**.
5. Update the Resolution section of the incident record with the following comments:

- Enabled Default Windows Installerrules.
- Verified the installer path in the Deny rule.
- Turned on AppLocker enforcement.
- Configured policy to start the Application Identity service.
- Moved a computer, LON-CL1, to Marketing OU to test the policy.

Results: After completing this exercise, you should have successfully resolved the AppLocker policy application problem.

8.2 Exercise 2: Troubleshooting Application Compatibility Issues

8.2.1 Task 1: Identify compatibility issues

1. If necessary, sign in to **LON-CL1** as **Adatum\Benjamin** with the password **Pa55w.rd**.
2. On the desktop, on the taskbar, click the **File Explorer** icon.
3. Navigate to **C:\Program Files (x86)\StockViewer**, and then double-click **StockViewer**.
4. In the Permission denied dialog box, click **OK**.
5. On the Stock Viewer toolbar, click **Trends**.
6. In the Error dialog box, click **OK**.
7. On the Tools menu, click **Options**.
8. In the Stock Viewer dialog box, click **Continue**.
9. On the Tools menu, click **Show Me a Star**.
10. In the Unsupported Version dialog box, click **OK**.
11. **Close** Stock Viewer.
12. If a Program Compatibility Assistant window opens, click **This program ran correctly**.

13. In the File Explorer window, right-click **StockViewer**, and then click **Run as administrator**.
14. In the User Account Control dialog box, provide the following credentials, and then click Yes:

- User name: **Adatum\Administrator**
- Password: **Pa55w.rd**

15. On the Stock Viewer toolbar, click **Trends**.
16. On the Tools menu, click **Options**, and then click **OK**.
17. On the Tools menu, click **Show Me a Star**, and then click **OK**.
18. **Close** Stock Viewer, and then **sign out** of LON-CL1.

8.2.2 Task 2: Create a compatibility fix

1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa55w.rd**.
2. Click the Start button. In the list of apps, click **Windows Kits**, and then click **Compatibility Administrator (32bit)**.
3. In the **Compatibility Administrator (32-bit) – New Database (1) [Untitled_1]** dialog box, right-click **New Database(1) [Untitled_1]**, and then click **Rename**.
4. Type **AdatumACT**, and then press **Enter**.
5. In the Compatibility Administrator window, right-click **AdatumACT [Untitled_1]*,** click **Create New**, and then click **Application Fix**.
6. In the Create New Application Fix Wizard, in the Name of the program to be fixed text box, type **StockViewer**.
7. Click Browse.
8. In the Find Binary window, browse to **C:\Program Files (x86)\StockViewer\StockViewer.exe**, and then click **Open**.
9. In the Create new Application Fix window, click **Next**.
10. On the Compatibility Modes page, select the **Run this program in compatibility mode** for check box, click the **drop-down list**, and then click **Windows XP**.
11. In the Additional compatibility modes section, scroll down, select the **RunAsAdmin** check box, and then click **Next**.
12. On the Compatibility Fixes page, click **Next**.
13. On the Matching Information page, click **Finish**.
14. In the Compatibility Administrator window, click **Save**.
15. In the Save Database window, browse to **c:**.
16. In the File name text box, type **AdatumACT**, and then click **Save**.
17. Close the Compatibility Administrator window.
18. **Sign out** of LON-CL1.

8.2.3 Task 3: Test the compatibility fix

1. Sign in to **LON-CL1** as **Adatum\Benjamin** with the password **Pa55w.rd**.
2. Click **Start**, and type **cmd**, right-click on **Command Prompt**, and select **Run as Administrator**.
3. In the User Account Control dialog box, enter the following credentials, and then click **Yes**:
    - User name: **Adatum\administrator**
    - Password: **Pa55w.rd**
4. At the command prompt, type the following command, and then press **Enter**:

```
Sdbinst C:\\AdatumACT.sdb
```

5. On the desktop, on the taskbar, click the **File Explorer** icon.
6. In File Explorer, navigate to **C:\Program Files (x86)\StockViewer** and then double-click **StockViewer**.
7. In the User Account Control dialog box, enter the following credentials, and then click **Yes**:
   - User name: **Adatum\administrator**
   - Password: **Pa55w.rd**
8. On the Stock Viewer toolbar, click **Trends**.
9. On the Tools menu, click **Options**.
10. Click **OK** to close the message box.
11. On the Tools menu, click **Show Me a Star**, and then click the star.
12. **Close** the Stock Viewer application.
13. If the Program Compatibility Assistant window opens, click **Yes**, this program worked correctly.
14. **Sign out** of LON-CL1.

    Results: After completing this exercise, you should have successfully resolved the issues with the Stock Viewer application.

9 Lab B: Troubleshooting Access to Company Web Applications

9.1 Exercise 1: Troubleshooting Microsoft Internet Explorer Issues

9.1.1 Task 1: Verify the issue

1. In **LON-CL1**, sign in as **Adatum\Harry** with the password **Pa55w.rd**.
2. Click the Start button, and in the list of apps, click **Windows Accessories**, and then click **Internet Explorer.**
3. In the Internet Explorer 11 window, click **Use recommended security and compatibility settings**, and then click **OK**.
4. In the Internet Explorer Address bar, type **http://intranet.adatum.com**, and then press **Enter**.
5. Verify that the website displays correctly. If you press the **ALT** key, click the **Tools menu**, and then verify that the Enterprise Mode menu item is not visible.
6. **Sign out** of LON-CL1.

9.1.2 Task 2: Create a policy for Internet Explorer Enterprise Mode

1. Switch to **LON-DC1**.
2. On LON-DC1, on the taskbar, click the **File Explorer** icon.
3. In File Explorer, click **E:**, and then click **Labfiles**.
4. Double-click the **EMIESiteListManager.msi** file.
5. In the Enterprise Mode Site List Manager Setup window, click **Next**.
6. On the End-User License Agreement page, select the check box for **I accept the terms in the License Agreement**, and then click **Next**.
7. On the Destination Folder page, click **Next**.
8. On the Ready to install Enterprise Mode Site List Manager page, click **Install**.
9. On the Completed the Enterprise Mode Site List Manager Setup Wizard page, click **Finish**.
10. Click the **Start** button, type **Enterprise**, and then click **Enterprise Mode Site List Manager**.
11. In the Enterprise Mode Site List Manager for Windows 10 window, click **Add**.

12. In the Add new website window, in the URL text box, type **intranet.adatum.com**. In the Compat Mode drop-down list box, click **IE9 Document Mode**, and then click **Save**.
13. If a dialog box opens, click **Yes**.
14. Click the **File menu**, and then click **Save to XML**.
15. In the Save as… dialog box, navigate to **c:\inetpub\wwwroot**. In the File name text box, type **AdatumEnterpriseMode**, and then click **Save**.
16. **Close** Enterprise Mode Site List Manager.
17. Click the **Start** button, and then click **Internet Explorer**.
18. In the Internet Explorer window, in the Address bar, type **http://lon-dc1.adatum.com/AdatumEnterpriseMode.xml**, and then press **Enter**.
19. Verify that the XML file opens correctly.
20. **Close** Internet Explorer.

9.1.3 Task 3: Enable Internet Explorer Enterprise Mode

1. Switch to the **Server Manager** window, click **Tools**, and then click **Group Policy Management**.
2. If necessary, in the Group Policy Management window, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, expand **Group Policy Objects**.
3. Right-click **Group Policy Objects**, and then click **New**. Name the new policy **Internet Explorer Enterprise Mode Policy**. Click **OK**.
4. Right-click **Internet Explorer Enterprise Mode Policy**, and then click **Edit**.
5. In the Group Policy Management Editor window, in the left pane, expand **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then click **Internet Explorer**.
6. Notice that the **Let users turn on and use Enterprise Mode from the Tools menu** setting is not configured.
7. Leave the Group Policy Management Editor window open.
8. Switch to the **File Explorer** window.
9. In the File Explorer window, in the address bar, type **C:\Windows**, and then press **Enter**.
10. In the content pane, right-click **PolicyDefinitions**, and then click **Copy**.
11. In the address bar, type **\\LON-DC1\SYSVOL\Adatum.com\Policies**, and then press **Enter**.
12. In the content pane, right-click **any empty space**, and then click **Paste**.
13. Switch to **LON-CL1**.
14. Sign in as **Adatum\Administrator** with the password **Pa55w.rd**.
15. Click **Start**, and type **cmd**, and press **Enter**.
16. In the Command Prompt window, type the following two commands, press **Enter** after each command, and press **Y** and **Enter** when asked to overwrite the files:

```
Copy c:\Windows\PolicyDefinitions\inetres.admx \\LON-DC1\SYSVOL\Adatum.com\Policies\PolicyDefinitions\i
Copy c:\Windows\PolicyDefinitions\en-US\inetres.adml \\LON-DC1\SYSVOL\Adatum.com\Policies\PolicyDefinit
```

17. **Sign out** of LON-CL1.
18. Switch to **LON-DC1**.
19. On LON-DC1, switch to Group Policy Management Editor window. You should still see the available Internet Explorer policy settings in the content pane.
20. In the content pane, double-click **Let users turn on and use Enterprise Mode from the Tools menu**.
21. Click **Enabled**, and then click **OK**.

22. In the content pane, double-click **Use the Enterprise Mode IE website list**.
23. Click **Enabled**, in the Type the location (URL) of your Enterprise Mode IE website list text box, type **http://lon-dc1.adatum.com/AdatumEnterprisemode.xml**, and then click **OK**.
24. **Close** the Group Policy Management Editor window.
25. In the Group Policy Management window, right-click the **Adatum.com domain**, and then click **Link an existing GPO**.
26. In the Select GPO window, click **Internet Explorer Enterprise Mode Policy**, and click **OK**.

9.1.4 Task 4: Verify that the issue is resolved

1. In LON-CL1, sign in as **Adatum\Harry** with the password **Pa55w.rd**.
2. Click the **Start** button, type **gpupdate**, and then press **Enter,** and wait for the policy update to complete.
3. Click the **Start** button, and in the list of apps, click **Windows Accessories**, click **Internet Explorer**, and then wait two minutes.
4. In the Internet Explorer window, press the **ALT** key, click the **Tools** menu, and then click **Enterprise Mode**.
5. In the Internet Explorer Address bar, type **http://intranet.adatum.com**, and then press **Enter**.
6. Verify that the website displays correctly, and if you press the **ALT** key, click the **Tools** menu, and then verify that Enterprise Mode is greyed out because the site runs in Enterprise Mode.
7. **Sign out** of LON-CL1.

   Results: After completing this exercise, you should have successfully resolved the Internet Explorer 11 issue by configuring Enterprise Mode.

9.2 Exercise 2: Troubleshooting Microsoft Edge Issues

9.2.1 Task 1: Review the help-desk Incident Record

Scenario: Your company is has recently migrated users to Windows 10. You are in a sub-group of the Help Desk that is responsible for handling support calls related to post-deployment issues. A ticket has been opened regarding a user's browser favorties are now missing after migration.

1. Read the following help-desk Incident Record.

Incident Reference Number: 723415

Date of Call: January 8**Time of Call:** 08:50 **User:** Finlay Butcher (Research Department) **Status:** OPEN
Incident Details: User cannot find the Favorites tab that he used in Internet Explorer when he uses Microsoft Edge.
Additional Information: Finlay wants the same Favorites tab in Microsoft Edge that he has in Internet Explorer, but it
Plan of Action
Resolution

9.2.2 Task 2: Discuss recommendations

1. Read the Additional Information section of the incident record in the Student Handbook exercise scenario.
2. Discuss your recommendations with other students:
   1. Visit the user's computer and view the problem.
   2. Review the Microsoft Edge configuration options.
   3. Enable the Home button.
   4. Import favorites from Internet Explorer.

9.2.3 Task 3: Attempt to resolve the problem

1. Switch to **LON-CL1**.
2. Sign in as **Adatum\Finlay** with the password **Pa55w.rd**.

3. On the desktop, on the taskbar, click the **Microsoft Edge** icon.
4. Click on the **Hub** (three horizontal lines). Notice that there are no favorites.
5. Click **Import favorites**, and then click **Import**.
6. **Close** the hub, and then **reopen the hub**.
7. Notice that the favorites from Internet Explorer now display in Microsoft Edge.
8. Update the Resolution section of the Incident Record with the following text:
   - Turned on home button in advanced settings.
   - Clicked Import favorites in the hub to import Internet Explorer favorites.

   Results: After completing this exercise, you should have successfully resolved the Microsoft Edge issue.