Module 10: Automating Windows deployment by using modern deployment techniques

Lab A: Configuring Windows Autopilot for operating system deployment

(VMs: 20695D-LON-DC1, 20695D-LON-SVR2, 20695D-LON-CFG, 20695D-LON-CL1)

Exercise 1: Signing up for Microsoft cloud services

Task 1: Sign up for a Microsoft account

1. On **LON-CL1**, click **Other user** on the sign-in screen. Sign in as **.\Admin** with password **Pa55w.rd**.
2. On the desktop, on the taskbar, click the **Microsoft Edge** icon.
3. In the Microsoft Edge address bar, type ***login.live.com***
4. In the **Sign in** box, look for the "No account?" text, and then click the **Create one!** link.
5. On the **Create account** page, click the **Get a new email address** link. In the **New email** text box, type your username by using the information in the note below to generate a unique username. Then click **Next**.

Note: *Make sure to write down the username and password that you choose. You can choose a username in the YourInitials-Date@outlook.com format; for example, AB-101118@outlook.com. We recommend that you type your working email address in the* ***Alternate email address*** *text box.*

6. In the **Create a password** text box, type a password, clear the **Send me promotional emails from Microsoft** check box, and then click **Next**.
7. On the **Create account** page, type your first and last name, and then click **Next**.
8. On the **Add details** page, select the correct **Country/region** and **Birthdate**, and then click **Next**.
9. On the **Create account** page, type the text displayed in the image, and then click **Next**.
10. On the **Account** page, click **More actions** under your name and email address, and then click **View inbox**.
11. On the **Welcome to Outlook** page, click the right arrow, select an appropriate **Language** and **Time zone**, and then click the right arrow three times to complete

the setup wizard.
12. Click **Let's go**, and then ensure that your Inbox opens.

Task 2: Create a trial Azure subscription

1. On **LON-CL1**, open a new tab in the Microsoft Edge browser by selecting the plus sign (**+**) icon.
2. In Microsoft Edge, in the address bar, type ***http://aka.ms/cu92vo*** and then press Enter.
3. On the **Ready to get started** page, click **Start**.
4. On the **Azure Pass** page, sign in with the Microsoft account that you created in the previous task.
5. When you receive the "Stay signed in" prompt, click **No**.
6. On the **Microsoft Azure** page, verify your details, and then select **Confirm Microsoft Account**.
7. In the **Enter Promo code** text box, type your Azure pass code, and then click **Claim Promo Code**.
8. On the **Thank you for redeeming an Azure Pass** page, click **Activate**. A new tab will open in the Microsoft Edge browser.
9. On the **Azure Pass** page, under **About you**, type your contact phone number in the **Phone** text box. In the **Email address for important notifications** text box, type the outlook.com email address that you just created, and then click **Next**.
10. On the **Azure Pass** page, under **Agreement**, select **I agree to the subscription agreement, offer details, and privacy statement**, and then click **Sign up**.
11. Wait for a few minutes until your Azure subscription has been created.
12. If necessary, in the **Welcome to Microsoft Azure** window, click **Maybe later**.

Note: *Leave the Azure portal open. You will use it in the next task.*

Task 3: Create an Azure AD user and Azure AD groups

1. In Azure portal navigation pane, click **Azure Active Directory**, and then click **Custom domain names**.
2. Record the existing name because it will be necessary in the next exercise. The name of your domain will be based on the email address provided during creation in the ***<initials><date>*****outlook.onmicrosoft.com** format.
3. In the details pane, under **MANAGE**, click **Users**. On the **All users** blade, click the only user that displays.

4. Click **Edit**, scroll down and under **Settings**, click the drop-down arrow under the **Usage location** box. In the list, select **United States**.
5. Click **Save**, and then close the ***<User>* - Profile** blade by clicking the **X** farthest to the right.
6. On the **User – All users** blade, click **New user**.
7. In the **Name** text box, type **Lara Raisic**, and then in the **User name** text box, type ***lara@<initials><date>outlook.onmicrosoft.com***
8. If necessary, scroll down and select **Show Password**, and then write down the password for later reference. Click **Create**. **Lara Raisic** will display under your Microsoft account.
9. Click **Lara Raisic**, click **Edit** and scroll down, and then under **Settings**, click the drop-down arrow under the **Usage location** box. In the list, select **United States**.
10. Click **Save**, and then close the **Lara Raisic - Profile** blade by clicking the **X** farthest to the right.

Note: *Leave the Azure portal open. You will use it in the next task.*

Note: *You must set a location on each user to which you want to assign an Enterprise Mobility + Security E5 license.*

11. Click **Groups**, and then click **New group**. Click the drop-down arrow under **Group type**, and then select **Security**. In the text box under **Group Name**, type ***Intune Enrollment***
12. Under **Membership type**, click the drop-down arrow, select **Assigned**, and then click **Members, 0 members selected**.
13. On the **Select members** blade, click **Lara Raisic**, and then click **Select**. Back on the **Group** blade, click **Create**.
14. Close the **Group** blade by clicking the **X** in the uppermost right corner.

Task 4: Add a Microsoft Enterprise Mobility + Security trial subscription

1. On the Azure portal, click **Azure Active Directory** in the navigation pane, and then on the **Azure Active Directory** blade, click **Getting Started**.
2. Scroll down in the left-most column, and then under **Getting started with Azure AD**, click the **Get a free trial for Azure AD Premium** link.
3. In the **ENTERPRISE MOBILITY SUITE E5** box, click **Free trial**.
4. In the **Activate Enterprise Mobility + Security E5 trial** area, click **Activate**.
5. In the **AZURE AD PREMIUM P2** box, click **Free trial**.

6. In the **Activate Azure AD Premium P2 trial** area, click **Activate**.
7. Click your username in the top-right corner, and then click **Sign out**.

Note: *You need to sign out and sign in again for the two trials to activate properly.*

8. On the **Pick an account** page, click your Microsoft account, and then on the **Enter password** page, type your password.
9. Click **Azure Active Directory** in the navigation pane, and then click **Licenses**.
10. On the **Licensing** blade, under **MANAGE**, click **All products**.
11. Select **Azure Active Directory Premium P2** and **Enterprise Mobility + Security E5**, and then click **Assign**.
12. On the **Assign license** blade, click **User, None Selected**.
13. On the **Users** blade, click the two users listed, and then click **Select**.
14. Back on the **Assign license** blade, click **Assign**. Verify that you receive a "Licenses assigned" notification.

Results*: After completing this exercise, you should have successfully created an Microsoft Azure Active Directory (Azure AD) tenant and activated Microsoft Enterprise Mobility + Security and Azure AD Premium trial subscriptions.*

Exercise 2: Obtaining hardware IDs and adding devices to Windows Autopilot

Task 1: Create and configure a Windows 10 base workstation

1. On your Hyper-V host, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. In Windows PowerShell, type the following command, and then press Enter:
cd "D:\Program Files\Microsoft Learning\20695\Drives"

Note: *The drive letter might vary based on your host computer's configuration.*

3. Run the following script to create and import the VM that is needed to test Windows Autopilot Deployment: ***.\Mod10-CreateVM.ps1***
4. At the "On which disk drive are the base images extracted?" prompt, type ***C*** and then press Enter.
5. At the "On which disk drive are the course images extracted?" prompt, type ***D*** and then press Enter.

Note: *The drive letter might vary based on your host computer's configuration.*

6. On your Hyper-V host, open **Hyper-V Manager**, and then verify that the **20695D-LON-CL5** VM was created.
7. Start the **20695D-LON-CL5** VM.

Task 2: Obtain hardware ID

1. On **LON-CL5**, sign in as **Admin** with password **Pa55w.rd**.
2. On **LON-CL5**, on the taskbar, right-click **Start**, click **Windows PowerShell (Admin)**, and then select **Yes**.
3. In the Windows PowerShell command-line interface, type the following, and then press Enter: ***Install-Script -Name Get-WindowsAutopilotInfo***
4. You will receive three prompts. Each time, type ***Y*** and then press Enter.
5. Type the following, and then press Enter: ***Set-ExecutionPolicy RemoteSigned***
6. When prompted, type ***Y***, and then press Enter.
7. Type the following, and then press Enter:
Get-WindowsAutopilotInfo.ps1 –OutputFile C:\Computer.csv
8. Type ***C:\Computer.csv***, press Enter, select **Notepad**, and then click **OK**. Review the file content.
9. Close Notepad.
10. Type the following command, and then press Enter:
NET USE F: \\LON-CL1\C$ /user:Administrator Pa55w.rd
11. Type the following command, and then press Enter:
Copy-Item C:\Computer.csv -destination F:
12. Leave the **20695D-LON-CL5** VM running; you will use it later in the lab.
13. Minimize the **20695D-LON-CL5 on <HOSTNAME> - Virtual Machine Connection** window.

Task 3: Add a device to Windows Autopilot

1. On **LON-CL1**, restore the Azure portal, and then click **All services** in the navigation pane.
2. On the **All services** blade, in the text box, type ***Intune***. Click the star to the right of **Intune**. Close the **All services** blade by clicking the **X**.
3. In the navigation pane, scroll down to the bottom, and then click **Intune**.
4. Click **Device enrollment**, and then under **Mobile Device Management Authority**, select **Intune MDM Authority**. Then click **Choose**.

5. In the navigation pane, click **Azure Active Directory**, scroll down, and then click **Mobility (MDM and MAM)**.
6. Click **Microsoft Intune Enrollment**, and then on the **Configure** blade next to **MDM user scope**, click **Some**.
7. Click **Select groups, None Selected**, select the **Intune enrollment** group that you created earlier, and then click **Select**. Back on the **Configure** blade, click **Save**.
8. Close the **Configure** blade by clicking the **X** in the uppermost right corner.
9. In the navigation pane, click **Intune**, and then under **MANAGE**, click **Device Enrollment**.
10. Under **MANAGE**, click **Windows enrollment**, and then on the **Windows enrollment** blade, click **Devices**.
11. On the **Windows Autopilot devices** blade, click **Import**.
12. On the **Add Windows Autopilot devices** blade, click the folder icon next to **Select a file**.
13. In the file browser, click **Local Disk (C:)**, select the **Computer.csv** file, and then click **Open**.
14. On the **Add Windows Autopilot devices** blade, click **Import**.

Note: *Monitor the process and wait for the import to complete. This might take up to 15 minutes.*

15. When the import has completed, click **Sync** and wait a few minutes. Then click **Refresh**.

Note: *If no device is listed, wait 2 minutes, and then click* ***Refresh*** *again.*

16. In the navigation pane, click **Azure Active Directory**.
17. Click **Groups**, and then click **New group**. Click the drop-down arrow under **Group type**, and then select **Security**. In the text box under **Group Name**, type ***Windows Autopilot Devices***
18. Click the drop-down arrow under **Membership type**, and then select **Assigned**.
19. Click **Members, 0 members selected**. On the **Select members** blade, click the device icon with a serial number, and then click **Select**. Back on the **Group** blade, click **Create**.
20. Close the **Group** blade by clicking the **X** in the uppermost right corner.

***Results**: After completing this exercise, you will have created a virtual machine (VM) that you're going to deploy by using Windows Autopilot. Furthermore, you will have upload the hardware ID of the VM to Intune and added the device to an Azure AD group.*

Exercise 3: Creating and applying the Windows Autopilot deployment profile

Task 1: Customize Azure AD company branding

1. On **LON-CL1**, on the Microsoft Azure portal, in the navigation pane, select **Azure Active Directory**.
2. On the **Azure Active Directory** blade, select **Company Branding**, and then select **Configure**.
3. On the **Configure company branding** blade, configure the following settings:
o Sign-in page background image: Select **Browse**, browse to **C:\Labfiles\Mod10**, select **Background.jpg**, and then select **Open**.
o Banner logo: Select **Browse**, select **Adatum280.jpg**, and then select **Open**.
o Sign-in page text: **A. Datum Cloud Sign-in**
o Square logo image: Select **Browse**, select **Adatum240.jpg**, and then select **Open**.
o Square logo image, dark theme: Select **Browse**, select **Adatum_dark.jpg**, and then select **Open**.
o Show option to remain signed in: Select **Yes**.
4. Select **Save**, and then close the **Configure company branding** blade.
5. On the **Azure Active Directory** blade, in the navigation pane, click **Properties**.
6. In the **Name** text box, type ***A. Datum Azure AD***, and then click **Save**.

Task 2: Create the Autopilot deployment profile

1. On **LON-CL1**, in the navigation pane, click **Intune**, and then click **Device Enrollment** under **MANAGE**.
2. Click **Windows enrollment** under **MANAGE**, and then on the **Windows enrollment** blade, click **Deployment Profiles**.
3. On the **Windows Autopilot deployment profiles** blade, click **Create profile**.
4. On the **Create profile** page, under the **Name** text box, type **A. Datum Pilot**.
5. Under **Deployment mode**, verify that **User Driven** is selected.
Note: Don't change the Deployment mode, because this will cause a failure later

in the lab.
6. Click the drop-down arrow under the **Join Azure AD as** box, select **Azure AD joined**, and then click **Out-Of-box experience (OOBE), Defaults configured**.
7. On the **Out-of-box experience (OOBE)** blade, verify that the **End user agreement** is set to **Hide**.
8. Verify that **Privacy Settings** is set to **Hide**, and then verify that **User account type** is set to **Standard**.
9. Click **Save**, and then click **Create**.
10. Close the **Create profile** blade by clicking the **X**.
11. On the **Windows Autopilot deployment profiles** blade, click the **A. Datum Pilot** profile.
12. Click **Assignments** under **MANAGE**, and then on the **A. Datum Pilot – Assignments** blade, click **+ Select groups**.
13. On the **Select groups** blade, click **Windows Autopilot Devices**, click **Select**, and then click **Save**.
14. Close all the open blades by clicking the **X**.
15. Click **Intune**, and then under **MANAGE**, click **Device Enrollment**.
16. Click **Windows enrollment** under **MANAGE**, and then on the **Windows enrollment** blade, click **Devices**.
17. In the details pane, verify that the **PROFILE STATUS** column for the device indicates **Assigned**.

Note: *If* ***Not Assigned*** *or* ***Assigning*** *displays in the* ***PROFILE STATUS*** *column, wait one minute, and then click* ***Refresh****. Continue this process until* ***Assigned*** *displays before you continue.*

Task 3: Deploy the setting to a Windows 10 device

1. Switch to **LON-CL5**, click **Start**, and then click the **Settings** app.
2. On the **Settings** page, click **Update & Security**, and then click **Recovery**.
3. Click **Get started** under **Recovery**, and then in the **Choose an option** window, click **Remove everything**.
4. In the **Do you want to clean the drives, too?** window, click **Just remove my files**.
5. In the **Ready to reset this PC** window, click **Reset**.

***Note: LON-CL5** will restart after a few minutes. Windows 10 will then be reinstalled on the computer. The entire process takes about 15 minutes.*

6. On the **Let's start with region. Is this right?** page, select your country/region, and then click **Yes**.
7. On the **Is this the right keyboard layout** page, select your keyboard layout, and then click **Yes**.
8. On the **Want to add a second keyboard layout?** page, click **Skip**.
9. On the **Welcome to A. Datum Azure AD!** page, verify that the page is customized with the A. Datum company branding that you added earlier.
10. In the **someone@example.com** text box, type: ***Lara@yourinitialsMMDDYYoutlook.onmicrosoft.com***, and then click **Next**.
11. On the **Enter your password** page, verify that a custom graphic is present, in addition to text at the bottom of the page. In the **Password** text box, type ***Pa55w.rd***, and then click **Next**.
12. On the **Update your password** page, type your current password, specify a new strong password, and then click **Sign in**.

***Note:** You're seeing the **Update your password** page because it's the first time that **Lara Raisic** has signed in.*

***Note:** While Lara is signing in, notice that you weren't asked for privacy settings. You disabled that in the Windows Autopilot deployment profile.*

13. On the **Your organization requires Windows Hello** page, select **Set up PIN**, close the **Help us protect your account** page, and then click **Skip for now**.
14. Click **Start,** and then click the **Settings** app.
15. On the **Windows Settings** page, click **Accounts**.
16. Verify that you're signed in as **Lara Raisic**. Notice that she is a normal user and that the text "Administrator" isn't displayed under her name. Close the Settings app.

***Results**: After completing this exercise, you will have successfully implemented Azure AD company branding. You will also have successfully implemented Windows Autopilot and used it to deploy a Windows 10 device.*

Task 4: Prepare for the next lab

When you finish the lab, revert the virtual machines to their initial state. To do

this, complete the following steps:
1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20695D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20695D-LON-CL1**.
5. Right-click **20695D-LON-CL5**, and then click **Shut Down**.
Leave **MT17B-WS2016-NAT** running.

Lab B: Using Windows Configuration Designer to provision Windows devices

Exercise 1: Create a provisioning package

Task 1: Create a new provisioning package for all Windows 10 editions

1. On **LON-CFG**, click the **Start** button and expand **Windows Kits**.
2. Click **Windows Imaging and Configuration Designer**.
3. On the **WCD Start** page, click the **Advanced provisioning** tile.
4. In the **New project** wizard, on the **Enter project details** page, in the **Name** field, type ***DevConfig***.
5. In the **Project folder** field, click **Browse**.
6. In the **Browse for Folder** dialog box, click **Allfiles (E:)**, and then click **Images**.
7. Click **Make New Folder**, and then in the text box, type ***WCD***. Ensure that **WCD** is selected, and then click **OK**.
8. In the **Description** text box, type ***Windows Defender exclusion of the C:\DevProjects Folder***. Then click **Next**.
9. On the **Choose which settings to view and configure** page, click **All Windows desktop editions**, and then click **Next**.
10. On the **Import a provisioning package (optional)** page, click **Finish**. This creates the new **DevConfig** project and the **DevConfig** customization page will open.
11. In the **Available customization** pane, next to **View**, ensure that **All settings** is selected.
12. Expand **Runtime** settings and expand **Policies**, and then click the **Defender** node.
13. Click **ExcludedPaths**, and in the details pane, in the **Any text** field type

C:\DevProject.
14. On the menu bar, click **Export** and then click **Provisioning package**.
15. In the **Build** window, under **Owner**, in the **OEM** drop-down list, change the value to **IT Admin**, and then click **Next**.
16. On the **Select security details for the provisioning package** page, click **Next**.
17. On the **Select where to save the provisioning package** page, click **Next**.
18. On the **Build the provisioning package** page, click **Build**, and then click **Finish**.
19. In the **Windows Configuration Designer** console, click the **File** menu item, and select **Close** project in the context menu.
20. On the taskbar, open **File Explorer**, and in the **File Explorer** console tree, browse to **E:\Images\WICD**.
21. Note the file named **DevConfig.ppkg**. This is the provisioning package that you will apply to your devices.

Task 2: Apply the provisioning package to a Windows 10 device

1. If you have not already done so, sign in to **LON-CL2** as ***.\Admin*** with the password ***Pa55w.rd***
2. Click the **Start** button and then click **Settings**.
3. In the Settings app, click **Update and Security**.
4. On the **Update & Security** page, click **Windows Defender**.
5. On the **Windows Defender** page, click **Open Windows Defender Security Center**.
6. On the **Windows Defender Security Center** page, click **Settings** in the lower left corner.
7. On the **Settings** page, click **Virus & threat protection settings**.
8. On the **Virus & threat protection settings** page, scroll down to **Exclusions** and click **Add or remove exclusions**.
9. On the **Exclusion** page, verify that no exclusions have been configured. Close the **Exclusions** page by clicking the **X** in the right upper corner. Minimize the **Windows Defender** page.
10. On the taskbar, click the **File Explorer** icon and in the File Explorer address bar, type ***\\lon-cfg\e$\images***, and then press Enter.
11. In the **Windows Security** dialog box, in the **Name** field, under **Enter network credentials**, type ***adatum\administrator***, and in the **Password** field, type ***Pa55w.rd***, and then click **OK**.

12. In File Explorer, right-click **WCD**, and then click **Copy**.
13. In the File Explorer console tree, click **Local Disk (C:)**.
14. Right-click in the empty space of the **C:** details pane and click **Paste**.
15. Double-click **WCD** and then double-click **DevConfig.ppkg**.
16. In the **User Account Control** dialog box, click **Yes**.
17. In the **Is this package from a source you trust?** dialog box, click **Yes, add it**.
18. Close File Explorer, and then maximize the **Windows Defender** page.
19. On the **Windows Defender** page, click **Open Windows Defender Security Center**.
20. On the **Windows Defender Security Center** page, click **Settings** in the lower left corner.
21. On the **Settings** page, click **Virus & threat protection settings**.
22. On the **Virus & threat protection settings** page, scroll down to **Exclusions** and click **Add or remove exclusions**.
23. On the **Exclusion** page, verify that **C:\DevProjects** has been added as an exclusion.

***Results**: After completing this exercise, you should have created a provisioning package, saved it in a shared folder, and applied it to Windows 10 device.*

Task 3: Prepare for the next lab

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:
1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20695D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20695D-LON-CFG** and **20695D-LON-CL2**.

Leave **MT17B-WS2016-NAT** running.

Lab C: Using Configuration Manager servicing plans to manage Windows 10 devices

Exercise 1: Configuring software updates to support Windows 10 upgrades

Task 1: Modify software update classifications and verify products to support

Windows 10 servicing

1. On **LON-CFG**, click the **Configuration Manager Console** icon on the taskbar.
2. Click the **Administration** workspace, expand **Site Configuration**, and then click **Sites**.
3. In the results pane, right-click **S01 – Adatum Site, point to Configure Site Components**, and then click **Software Update Point**.
4. In the **Software Update Point Component Properties** dialog box, click the **Classifications** tab, and then select **Upgrades**. When prompted about **Windows 10 Servicing Prerequisite**, click **OK**.
5. Click the **Products** tab, and then verify that **Windows 10** is selected.
6. To close the **Software Update Point Component Properties** dialog box, click **OK**.
7. In the **Configuration Manager** console, click **Servers and Site System Roles**, and then in the preview pane under **Site System Roles**, right-click **Service connection point**, and then click **Properties**.
8. In the **Service connection point Properties** window, click **Online, persistent connection (recommended)**, and then click **OK**.

Task 2: Create and populate a target collection

1. In the **Configuration Manager** console, click the **Assets and Compliance** workspace.
2. Right-click the **Device Collection** node, and then click **Create Device Collection**.
3. In the **Create Device Collection Wizard**, on the **General** page, type ***W10 v1803 servicing – Ring 1 – IT Pilot*** in the **Name** text box.
4. Click **Browse** next to the **Limiting Collection** box, select **All System**, and then click **OK**.
5. Click **Summary**, click **OK** when prompted, click **Next**, and then click **Close**.
6. Click the **Device Collections** node, right-click the **W10 v1803 servicing – Ring 1 – IT Pilot** collection, and then click **Add Resources**.
7. In the **Add Resources to Collection** window, type ***CL1*** in the **Name string contains** text box, click **Search**, and then verify that **LON-CL1** displays in the **Search** results box.
8. Click **Add**, and then click **OK**.
9. Right-click the **All Systems** collection, select **Update Membership**, and then click **Yes** when prompted.

10. Right-click the **W10 v1803 servicing – Ring 1 – IT Pilot** collection, select **Update Membership**, and then click **Yes** when prompted.
11. Click the **W10 v1803 servicing – Ring 1 – IT Pilot** collection, and then press F5 after 10 seconds.
12. When the **Member Count** column changes to **1**, right-click the **W10 v1803 servicing – Ring 1 – IT Pilot** collection, and then select **Show Members**. You should now be able to see the computer that you added.

Task 3: Perform a software update sync

1. In the **Configuration Manager** console, click the **Software Library** workspace, expand **Software Updates**, and then click **All Software Updates**.
2. Right-click **All Software Updates**, click **Synchronize Software Updates**, and then click **Yes**.
3. Click the **Monitoring** workspace, and then click **Software Update Point Synchronization Status**.
4. In the preview pane, note the synchronization status. It will take from 15 to 20 minutes for this to complete. Refresh the console to view the updated status. You can also view the **Wsyncmgr.log** file to monitor the synchronization status.

Note: *The* ***Wsyncmgr.log*** *file is located in* ***Drive:\Program Files \Microsoft Configuration Manager\Logs****.*

5. Continue to monitor and refresh the **Software Update Point Synchronization Status** until the **Synchronization Status** displays **Completed**.
6. Click the **Software Library** workspace, expand **Windows 10 Servicing**, and then click **All Windows 10 Updates**. In the preview pane, verify that updates are displayed.

Results*: After completing this exercise, you should have successfully configured and verified all prerequisites for supporting Windows 10 servicing in Microsoft System Center Configuration Manager (Configuration Manager). Furthermore, you will have successfully created a collection for your pilot computers and performed a software update sync.*

Exercise 2: Creating a Windows 10 servicing plan

Task 1: Create a Windows 10 servicing plan

1. On **LON-CFG**, if necessary, click the **Configuration Manager Console** icon on the taskbar.
2. In the **Configuration Manager** console, click the **Software Library** workspace, expand **Windows 10 Servicing**, right-click **Servicing Plans**, and then click **Create Servicing Plan**.
3. On the **General** page of the **Create Servicing Plan Wizard**, in the **Name** text box, type ***W10 v1803 servicing – Ring 1 – IT Pilot*** and then click **Next**.
4. On the **Servicing Plan** page, click **Browse**, select the **W10 v1803 servicing – Ring 1 – IT Pilot** collection, click **OK**, and then click **Next**.
5. On the **Deployment Ring** page, verify that **Semi-Annual Channel (Targeted)** is selected, and then click **Next**.
6. On the **Upgrades** page, select **Title** in the **Property filters** box, and then under **Search criteria**, click **<text to find>**.
7. In the **Search Text** window, type ***(business editions), version 1803, en-us***, click **Add**, and then click **OK**.
8. On the **Upgrades** page, click **Preview**. You should see **Feature update to Windows 10 (business editions), version 1803, en-us** listed. Click **Close**, and then click **Next**.
9. On the **Deployment Schedule** page, click **Next**.
10. On the **User Experience** page, select **Display in Software Center and show all notifications**, and then click **Next**.
11. On the **Deployment Package** page, select **Create a new Deployment** package. Fill in the following details, and then click **Next**:
o Name: **W10 v1803 Upgrade**
o Package source: **\\LON-CFG\e$\Sources\W10Upgrade**
12. On the **Distribution Points** page, click **Add**, and then select **Distribution Point**.
13. In the **Add Distribution Points** dialog box, select **LON-CFG.ADATUM.COM**, click **OK**, and then click **Next**.
14. On the **Download Location** page, click **Download software updates from a location on my network**.
15. In the text box, type ***\\LON-CFG\e$\Software Updates*** and then click **Next**.
16. On the **Language Selection** page, verify that only **English** is selected, and then click **Next**.

17. On the **Summary** page, click **Next**.
18. On the **Completion** page, click **Close**.

Task 2: Verify Windows 10 servicing plan and deployment creation

1. In the **Configuration Manager** console, click **Servicing Plans**.
2. In the details pane, right-click the **W10 v1803 servicing – Ring 1 – IT Pilot** servicing plan that you just created, and then click **Run Now**. When prompted, click **OK**.
3. Expand **Software Updates**, and then click the **Software Update Groups** node. Wait for approximately 5 minutes, and then press F5 to refresh. Continue until **W10 v1803 servicing – Ring 1 – IT Pilot** *<creation date and time>* is displayed.
4. Click the **Monitoring** workspace, and then click the **Deployments** node. A deployment called **W10 v1803 servicing – Ring 1 – IT Pilot** *<current date and time>* is displayed as well.

Results*: After completing this exercise, you should have successfully created a functioning servicing plan and deployed it to your pilot collection.*

Exercise 3: Deploying a Windows 10 servicing plan to Configuration Manager client devices

Task 1: Verify the version of Windows 10 that is currently installed

1. On **LON-CL1**, right-click **Start**, and then click **System**.
2. On the **About** page, scroll down and verify that the Windows 10 version is **Windows 10 Enterprise**, **Version 1709**, **OS Build 16299.15**.

Task 2: Run the upgrade on a Windows 10 computer

1. On **LON-CL1**, click **Start**, type **control**, and then press Enter.
2. In Control Panel, click **System and Security**, and then click **Configuration Manager**.
3. In the **Configuration Manager Properties** dialog box, click the **Actions** tab.
4. On the **Actions** tab, click **Machine Policy Retrieval & Evaluation Cycle**, click **Run Now**, and then click **OK**.
5. On the **Actions** tab, click **Software Updates Deployment Evaluation Cycle**, click **Run Now**, and then click **OK**.
6. Click **OK** to close the **Configuration Manager Properties** dialog box.

7. Close Control Panel.
8. Wait approximately 2 minutes until a “Software Changes are required” notification displays. Click it, and then a **Software Center** window will open.
9. In the **Software Center** window, click the down arrow next to **More information**, and then click **View in Software Center**.
10. Close the **Software Center** window by clicking the **X** in the top-right corner.
11. In Software Center, click the **Updates** tab. On the **Updates** page, you should now see **Feature update to Windows 10 (business editions), version 1803, en-us** with a status of **Schedule to install after...**.
12. In Software Center, click the **Scheduled to install** text, and then click **Install**. In the **Software Center** window, click **Install** again.

Note: Installing *will display for up to 45 minutes. When the preparation for the upgrade is complete, a* ***Restart*** *button will appear. If time permits, leave the upgrade running on* ***LON-CL1*** *while the instructor starts the next module. The upgrade itself will take about 20 minutes. Otherwise, go to the next task for information about reverting the VMs.*

13. In Software Center, click **Restart**, and then in the **Software Center** window, click **Restart** again. The computer will restart, and the actual upgrade will begin.

Note: *The computer will restart several times during the upgrade.*

14. When the upgrade is complete, sign in to **LON-CL1** as **ADATUM\Administrator** with the password **Pa55w.rd**.
15. On **LON-CL1**, right-click **Start**, and then click **System**.
16. On the **About** page, scroll down and verify that the Windows 10 version is **Windows 10 Enterprise**, **Version 1803**, **OS Build 17134.112**.

Results*: After completing this exercise, you will have successfully upgraded your Windows 10 computer to version 1803.*

Task 3: Prepare for the next module

When you finish the lab, revert the VMs to their initial state. To do this, complete the following steps:
1. On the host computer, start **Hyper V Manager**.
2. In the **Virtual Machines** list, right-click **20695D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.

4. Repeat steps 2 and 3 for **20695D-LON-SVR2**, **20695D-LON-CFG**, and **20695D-LON-CL1**.