Module 3: Troubleshooting startup and performing system recovery

Lab: Troubleshooting startup and performing system recovery

**Scenario**

You’re reviewing open tickets on the helpdesk system. There are a couple that relate to startup problems on computer running Windows 11. You decide to investigate and resolve the problems.

**Objectives**

After completing this lab, you will be able to:

* Explore Windows RE
* Perform a System Restore
* Recover a BitLocker encrypted drive

Exercise 1: Exploring Windows RE

**Scenario**

In this exercise, you will explore safe mode and how it is different from the standard Windows 11 environment. You will also test other advanced startup options.

The main tasks for this exercise are as follows:

1. Explore safe mode.
2. Use advanced startup options.

Task 1: Explore safe mode

1. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm) and login as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. In **LON-CL1**, click **start**, type [**service**](urn:gd:lg:a:send-vm-keys) , and then click **Services**.
3. In the **Services** window, click the **Status** column to sort the services, scroll down, verify that many services (more than 75 services) are running, and then close Services.
4. Right-click **Start**, select **Run**, and in the **Open** box, type [**shutdown /r /o**](urn:gd:lg:a:send-vm-keys), and then press Enter.
5. In the **You're about to be signed out** dialog box, click **Close**.
6. On the **Choose an option** page, click **Troubleshoot**.
7. On the **Troubleshoot** page, click **Advanced options**.
8. On the **Advanced options** page, click **Startup Settings**, click **Restart** , and then press 4 to select **Enable Safe Mode**.
9. When the computer starts, sign in as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
10. Verify that the words **Safe Mode** appear in all four corners of the desktop. Right-click **Start**, and then click **Device Manager**.
11. In Device Manager, right-click **Generic PnP Monitor**, click **Properties**, and then verify that the status of the device is not available when the computer is running in safe mode.
12. Click the **Driver** tab and verify that you can still use the **Update Driver** or **Uninstall Device** options while the computer is running in safe mode. Click **OK**.
13. Right-click **Start**, and then click **Computer Management**.
14. In Computer Management, in the navigation pane, expand **Services and Applications**, and then click **Services**. In the details pane, click the **Status** column to sort the services, scroll down, and verify that only a few services (fewer than 25 services) are running when the computer is in safe mode.

Task 2: Use advanced startup options

1. In **LON-CL1**, restart your computer and sign in as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. Click **Start**, click **Settings**, and then click **Recovery**.
3. On the **Advanced startup** tile, click **Restart now**.
4. When prompted, click **Restart now** again.
5. Windows 11 starts into recovery. Click **Troubleshoot** and then click **Advanced options**.
6. Click **System Restore**.
7. In the **System Restore** dialog box, click **Cancel**. There are currently no restore points available.

**Note:** You can use System Restore from the Windows Recovery Environment (Windows RE).

1. On the **Choose an option** page, click **Troubleshoot**.
2. On the **Advanced options** page, click **Command Prompt**.
3. At the command prompt, type **bcdedit** , and then press Enter.
4. bcdedit
5. Review the output and verify that Windows 11 appears as the default Windows Boot Loader operating system.
6. At the command prompt, type **diskpart** , and then press Enter.
7. diskpart
8. At the command prompt, type **list disk** , and then press Enter.
9. list disk
10. At the command prompt, type **list volume** , and then press Enter.
11. list volume
12. At the command prompt, type **exit** twice, and then press Enter.

exit

1. On the **Choose an option** page, click **Troubleshoot**.
2. On the **Advanced options** page, click **Startup Repair**. Startup Repair starts diagnosing your PC.
3. After a few seconds, the **Startup Repair** couldn't repair your PC page appears. This is because there is nothing wrong with your computer. Click **Advanced options** , and then click **Continue**.

**Results** : After completing this exercise, you will have used safe mode and other advanced startup options.

Exercise 2: Recovering a device with a restore point

**Scenario**

In this exercise, you will turn on System Protection, create restore points, perform several configuration changes, and then apply a previous restore point. You will verify which configuration changes reverted and which did not revert when you applied the restore point.

The main tasks for this exercise are as follows:

1. Configure System Restore.
2. Use System Restore.

Task 1: Configure System Restore

1. On **LON-CL1**, in File Explorer, in the navigation pane, right-click **This PC**, and then click **Properties**.
2. In **Settings**, click **System protection**.
3. In the **System Properties** dialog box, in the **Protection Settings** section, click **Local Disk (C:) (System)**, click **Configure** , click **Turn on system protection** ,move the **Max Usage** slider between **5 GB** and **10 GB** , and then click **OK**.
4. In the **System Properties** dialog box, click **Create**.
5. In the **System Protection** dialog box, type [**Initial settings**](urn:gd:lg:a:send-vm-keys) , click **Create** , and then click **Close**.
6. In the **System Properties** dialog box, click **OK**.
7. Right-click the desktop, point to **New**, click **Text Document**, type [**My document**](urn:gd:lg:a:send-vm-keys) as its name, and then press Enter.
8. In **LON-CL1**, right-click **Start**, and then select **Device Manager**.
9. In Device Manager, expand **Keyboards**, right-click **Microsoft Hyper-V Virtual Keyboard**, and then click **Properties**.
10. In the **Microsoft Hyper-V Virtual Keyboard Properties** dialog box, select the **Driver** tab, and then confirm that the **Roll Back Driver** button is not available. Click **Update Driver**.
11. In the **Update Drivers - Microsoft Hyper-V Virtual Keyboard** dialog box, click **Browse my computer for drivers**.
12. On the **Browse for drivers on your computer** page, click **Let me pick from a list of available drivers on my computer**.
13. On the **Select the device driver you want to install for this hardware** page, clear the **Show compatible hardware** check box.
14. In the **Manufacturer** section, click **Microsoft**, in the **Model** section, click **Microsoft USB Internet Keyboard**, click **Next**, in the **Update Driver Warning** box, click **Yes**, and then click **Close** twice.

Task 2: Use System Restore

1. In **LON-CL1**, in File Explorer, in the navigation pane, right-click **This PC**, and then select **Properties**.
2. In **Settings**, click **System protection**.
3. In the **System Properties** dialog box, click **System Restore**.
4. In the **System Restore** dialog box, click **Next**.
5. Select the **Initial settings** restore point, and then click **Next**.
6. Click **Finish**, and then click **Yes**. Wait until **LON-CL1** has restarted.
7. On **LON-CL1**, sign in as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
8. In the **System Restore** dialog box, click **Close**. Verify that **My document.txt** is still on the desktop.
9. Right-click the **Start** icon, and then click **Device Manager**.
10. Verify that your keyboard has reverted to the **Microsoft Hyper-V Virtual Keyboard Properties** driver.
11. On the taskbar, click **File Explorer**.
12. In File Explorer, in the navigation pane, right-click **This PC**, and then click **Properties**.
13. In **Settings** click **System protection**.
14. In the **System Properties** dialog box, click **System Restore**.
15. In the **System Restore** dialog box, select **Choose a different restore point**, and then click **Next**.
16. In the **System Restore** dialog box, verify that the additional restore point with the description **Restore Operation** and the type **Undo** was created. Click **Cancel**, click **OK**, and then close the System window.

**Results** : After completing this exercise, you will have used System Restore to revert the computer to an earlier restore point, and explored the effects of applying the restore point.

Exercise 3: Recovering a BitLocker encrypted drive

**Scenario**

Allan cannot start his computer. He has logged a call with the help desk. Your job is to resolve the incident. A work colleague has determined a plan of action. You must attempt a resolution based on this plan.

| **Incident Record** |
| --- |
| **Incident Reference Number:** 802151 |
| Date and time of call: August 30 14:27 |
| User: Allan Yoo (Sales Department) |
| Status: OPEN |
| **Incident Details:** Allan cannot remember his BitLocker password and cannot start his computer. |
| --- |
| **Additional Information** The user has a recovery key somewhere but has no idea what to do with it. (Record the recovery key saved from Task 1.) **Recovery Key:** |
| **Plan of Action** |
| Visit the user's computer and verify the problem. |
| Locate the recovery key. |
| Attempt to recover the drive by entering the recovery key. |
| **Resolution** |

Task 1: Enable BitLocker

1. On [**LON-CL1**](urn:gd:lg:a:select-vm), sign in as **[Adatum\AdatumAdmin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. Click **Start** and then type **[gpedit.msc](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** and press Enter.
3. In the Local Group Policy Editor, navigate to **Computer Configuration\ Administrative Templates\ Windows Components\ BitLocker Drive Encryption\ Operating System Drives**.
4. Double-click **Require additional authentication at startup**.
5. Click **Enabled** and click **OK**.
6. Close the editor.
7. On the taskbar, click **File Explorer**.
8. In the navigation pane, right-click **Local Disk (C:)**, and then click **Turn on BitLocker**.
9. On the **Choose how to unlock your drive at startup** page, click **Enter a password**.
10. On the **Create a password to unlock this drive** page, enter [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys) in both fields and click **Next**.
11. On the **How do you want to back up your recovery key?** page, click **Save to a file**.
12. In the **Save BitLocker recovery key as** dialog box, click **All files (D:)**.
13. On the File Explorer toolbar, click **New folder**, type [**BitLocker**](urn:gd:lg:a:send-vm-keys), and then press Enter.
14. In the **Save BitLocker recovery key as** dialog box, click **Open**, click **Save**, and then click **Next**.
15. On the **Choose how much of your drive to encrypt** page, click **Next**.
16. On the **Choose which encryption mode to use** page, ensure that **New encryption mode (best for fixed drives on this device)** is selected, and then click **Next**.
17. On the **Are you ready to encrypt this drive?** page, click **Start encrypting**.
18. Restart **LON-CL1**.

Task 2: Verify BitLocker

1. On **LON-CL1**, sign in as **[Adatum\AdatumAdmin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. On the taskbar, click **File Explorer**.
3. Notice that **Local Disk (C:)** is encrypted and unlocked. The TPM unlocked the drive automatically.
4. Right-click **Local Disk (C:)**, select **Show more options**, and then click **Manage BitLocker**.
5. Review the status of the drive. It will probably be **BitLocker Encrypting**.
6. On the taskbar, select the **File Explorer** icon.
7. Navigate to **D:\Bitlocker** and open the text file that starts with **BitLocker Recovery Key**.
8. Write down the **Recovery Key** (or screenshot it).
9. Close all open windows and apps.

Task 3: Review the help-desk Incident record for incident 802151

* Review the help-desk Incident Record 802151 in the student handbook exercise scenario.

Task 4: Review the Plan of Action section in the Incident Record

1. Review the **Additional Information** section of the Incident Record. Update it with the recovery key that you recorded earlier.
2. Review the **Plan of Action** section of the Incident Record.

Task 5: Verify the problem

1. Right-click **Start**, point to **Shut down or sign out**, and then select **Restart**.
2. During the restart sequence, when the **BitLocker** screen displays, in the **Enter the password to unlock this drive** box, enter **incorrect password**, and then select Enter.
3. The drive doesn't unlock.

Task 6: Attempt to resolve the problem

1. Press **Esc** and in the **Enter the recovery key for this drive** text box, enter the recovery key and press Enter. Windows starts.

**Note:** You do not need to enter the hyphens in the recovery key, because the Windows operating system adds them automatically.

1. Update the **Resolution** section in the Incident Record:
   * Entered the recovery key, and was able to start Windows normally.

**Results**: After completing this exercise, you should have recovered a BitLocker-encrypted drive and enabled the computer to start up.

**Congratulations!** You have now completed this lab. To continue to the next lab click End Lab in the Tools Menu . If you wish to contiue with this lab at a later date ensure you save the lab environment rather than ending it.