Module 11: Troubleshooting Apps

Lab: Troubleshooting Apps

**Scenario**

Your users are experiencing problems running a number of apps. You’ve been asked to investigate. Later, you need to provision a computer for the reception area. You decide to use Windows Configuration Designer to create a provisioning package.

**Objectives**

After completing this lab, you will be able:

* Configure AppLocker.
* Provision a kiosk

Exercise 1: Configuring AppLocker

**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 Record** |
| --- |
| **Incident Reference Number**: 723401 |
| Date of Call: January 4 |
| Time of Call: 13:22 |
| User: Benjamin Kavo (Marketing Department) |
| Status: OPEN |
| **Incident Details** |
| Users are installing unauthorized applications in the Marketing department. |
| **Additional Information** |
| Benjamin Kavo, one of the marketing managers, has reported that users are installing unauthorized desktop apps. |
| The AppLocker policies that are in place do not appear to be working. |
| You must determine why these policies are not being enforced. |
| **Plan of Action** |
| **Resolution** |

Task 1: Review the help-desk Incident Record for incident 723401

* Review the help-desk Incident Record 723401 in the Student Handbook exercise scenario.

Task 2: Discuss recommendations

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

Task 3: Verify the problem

1. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm)
2. Sign in by using the following credentials:
   * Username: **[Adatum\Benjamin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)**
   * Password: [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
3. On the taskbar, select the **File Explorer** icon.
4. In the File Explorer address bar, enter [**\\lon-dc1\Apps\XmlNotepad.msi**](urn:gd:lg:a:send-vm-keys), and then select Enter.
5. When installation starts, select **Cancel**.

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

1. Sign out of **LON-CL1**.
2. Sign in to **LON-CL1** as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) by using the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)

Task 4: Attempt to resolve the problem

1. Switch to [**LON-DC1**](urn:gd:lg:a:select-vm), send the [**CTRL+ALT+DEL**](urn:gd:lg:a:send-vm-key-combo) command 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. On **LON-DC1**, in the Server Manager window, select **Tools**, and then select **Group Policy Management**.
3. In the Group Policy Management window, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, expand **Group Policy Objects**, and then select **Marketing**.
4. Right-click **Marketing** and then select **Edit**.
5. 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 select **Windows Installer Rules**.
6. Right-click **Windows Installer Rules** or activate its context menu, and then select **Create Default Rules**.
7. Right-click **Windows Installer Rules** or activate its context menu, and then select **Create New Rule**.
8. On the **Before You Begin** page, select **Next**.
9. On the **Permissions** page, select **Deny**, and then select **Next**.
10. On the **Conditions** page, select **Path**, and then select **Next**.
11. On the **Path** page, select **Browse Files**.
12. In the **File name** text box, enter [**\\lon-dc1\apps**](urn:gd:lg:a:send-vm-keys), and then select Enter.
13. In the **Open** dialog box, double-click **XmlNotepad.msi** or select it and select Enter, and then select **Next**.
14. On the **Exceptions** page, select **Next**, and then select **Create**.
15. Select **Yes** to create the default rules, if necessary.
16. In the navigation pane, right-click **AppLocker** or activate its context menu, and then select **Properties**.
17. In the **AppLocker Properties** dialog box, under Windows Installer rules, select the **Configured** check box, and then select **OK**.
18. In the navigation pane, select **System Services**, and then double-click **Application Identity**,or select it and then select Enter.
19. In the **Application Identity Properties** dialog box, select the **Define this policy setting** check box, select **Automatic**, and then select **OK**.
20. Close the Group Policy Management Editor window.
21. Right-click the **Marketing** OU and then select **Link an Existing GPO**. Select **Marketing**, and then select **OK**.
22. Close Group Policy Management.
23. In the Server Manager window, select **Tools**, and then select **Active Directory Users and Computers**.
24. In **Active Directory Users and Computers**, expand **Adatum.com**, and then select **Computers**.
25. Right-click **LON-CL1** or activate its context menu, and then select **Move**.
26. In the **Move** dialog box, select **Marketing**, and then select **OK**.
27. Switch to [**LON-CL1**](urn:gd:lg:a:select-vm)
28. On **LON-CL1**, right-click **Start** or activate its context menu, and then select **Windows Terminal (Admin)**.
29. In the Windows PowerShell Command Prompt window, at the command prompt, enter the following command:
30. gpupdate /force
31. At the command prompt, enter the following command:
32. shutdown /r /t 0
33. When **LON-CL1** has restarted, sign in by using the following credentials:
    * Username: **[Adatum\Benjamin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)**
    * Password: [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
34. On the taskbar, select the **File Explorer** icon.
35. In the File Explorer address bar, enter [**\\lon-dc1\Apps\XmlNotepad.msi**](urn:gd:lg:a:send-vm-keys), and then select Enter.
36. In the **Windows Installer** dialog box, select **OK**.

**Note:** If you are able to progress the installation, select **Cancel**, and then repeat steps 28 through 30 while signed in as **adatum\administrator**.

1. Update the **Resolution** section of the incident record with the following comments:
   * Enabled Default Windows Installer rules.
   * 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.

Exercise 2: Provisioning a kiosk device

**Scenario**

In the reception area at head office, it’s necessary to deploy several computers as kiosk devices. These devices will provide guests the ability to sign in to the security system. You decide to use provisioning to configure kiosk settings on these devices. Before you begin, you undertake a trial of using Windows Configuration Designer to create the appropriate provisioning packages.

The main tasks for this exercise are as follows:

1. Configure general settings in the provisioning package.
2. Configure kiosk settings.
3. Create and distribute the package.
4. Apply the package.
5. Verify application of the package.

Task 1: Configure general settings in the provisioning package

1. Switch to [**LON-CL2**](urn:gd:lg:a:select-vm)
2. Login as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
3. Select **Start**, scroll down the list of installed apps, and then expand **Windows Kits**.
4. Select **Windows Imaging and Configuration Designer**.
5. In Windows Configuration Designer, select the **Provision kiosk devices** tile.
6. In the **New Project** Wizard, on the **Enter project details** page, in the **Name** box, enter **[Adatum Reception Test](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** and select **Finish**.
7. In the **Adatum Reception Test** project, under the **Steps** list, on the **Set up device** tab, in the **Device name** box, enter [**Reception-%RAND:3%**](urn:gd:lg:a:send-vm-keys),and then select the **Account management** tab.
8. In the details pane, ensure that **Enroll into Active Directory** is selected.
9. In the **Domain name** box, enter [**Adatum.com**](urn:gd:lg:a:send-vm-keys).
10. In the **User name** box, enter **[adatum\adatumadmin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)**.
11. In the **Password** box, enter [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).

Task 2: Configure kiosk settings

1. Select the **Configure kiosk account and app** tab.
2. Under the **Create a kiosk user account** heading, in **User name**, enter [**kiosk1**](urn:gd:lg:a:send-vm-keys).
3. In Password, enter [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
4. Under the **Configure the kiosk mode app** heading, in the **User name** box, enter [**kiosk1**](urn:gd:lg:a:send-vm-keys).
5. In the **App type** list, select **Universal Windows app**.
6. Right-click **Start** or activate its context menu, and then select **Windows Terminal (Admin)**.
7. In the Windows PowerShell (Admin) window, enter the following command:
8. Get-startapps -name edge
9. Use your cursor to select the AppID for Microsoft Edge, which will be like the following:
10. Microsoft.MicrosoftEdge\_8wekyb3d8bbwe!MicrosoftEdge
11. Select CTRL+C to copy this text (and only this text).
12. Switch to Windows Configuration Designer, and in the **Enter the AUMID for the app** text box, select CTRL+V to paste the text.
13. Select the **Configure kiosk common settings** tab. There's nothing to configure here, so select the **Finish** tab.

Task 3: Create and distribute the package

1. In the **Adatum Reception Test** project, select **Create**.
2. The package is created, and a link to the package is displayed beneath the **Create** button. select the following link: **C:\Users\Administrator.ADATUM\Documents\Windows Imaging and Configuration Designer (WICD)\Adatum Reception Test**.
3. File Explorer opens. Select CTRL, and then select the following files:
   * **Adatum Reception Test.cat**
   * **Adatum Reception Test.ppkg**
4. Select CTRL+C to copy the files.
5. On the taskbar, right-click **File Explorer**, and then select **File Explorer**.
6. In the address bar, enter [**\\LON-DC1\Apps**](urn:gd:lg:a:send-vm-keys), and then select Enter.
7. Select CTRL+V to paste the files.

Task 4: Apply the package

1. Switch to [**LON-CL4**](urn:gd:lg:a:select-vm)
2. Sign in as [**.\Admin**](urn:gd:lg:a:send-vm-keys) by using the password of [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys)
3. On the taskbar, select **File Explorer**.
4. In the address bar, enter [**\\LON-DC1\Apps**](urn:gd:lg:a:send-vm-keys), and then select Enter.

If you are unable to connect to the location, restart LON-DC1.

1. In the **Windows Security** dialog box, in the **User name** box, enter **[Adatum\AdatumAdmin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)**
2. In the **Password** box, enter [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys) and then select Enter.
3. Select both files that begin **Adatum Reception Test** and copy them to the **Downloads** library.
4. In Downloads, open **Adatum Reception Test.ppkg**.
5. In the **User Account Control** dialog box, select **Yes**.
6. In the **Is this package from a source you trust** dialog box, review the changes in the package, and then select **Yes, add it**.
7. The package applies, and the device will restart.

Task 5: Verify application of the package

1. Switch to [**LON-DC1**](urn:gd:lg:a:select-vm) and switch to **Server Manager**.
2. Select **Tools**, and then select **Active Directory Users and Computers**.
3. Expand **Adatum.com** and select **Computers**. Verify the presence of a computer with the prefix of RECEPTION-, and then a three digit suffix.
4. Switch to [**LON-CL4**](urn:gd:lg:a:select-vm)
5. On the sign in page, select **Other user**, and then sign in as [**.\Kiosk1**](urn:gd:lg:a:send-vm-keys) by using the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). After a moment, you are signed in. This verifies that the local account, kiosk1, was created.
6. Microsoft Edge opens (although you are unable to access any specific webpages). This verifies that the kiosk application was assigned.
7. Log out and sign in as **[Adatum\AdatumAdmin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)**
8. Select **Start**, and then select **Settings**.
9. Select the **Accounts** node, and then select the **Other users** tab.
10. Notice the kiosk1 account.
11. Sign out.

**Results**: After completing this exercise, you should have successfully configured a new computer to run a specific app in the Kiosk mode.

**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.