**Project 1: Configuring Group Policy**

*In this Hands-On Project, you configure GPOs on your Windows Server 2019 host, as well as test their application on your WindowsServer2019VM2 virtual machine.*

1. Boot your Windows Server 2019 host and log into domainX.com as Administrator using the password **Secret555**. Next, click **Start** and then click **File Explorer**.
2. In the navigation pane of File Explorer, expand **This PC**, and highlight **Local Disk (C:).**
3. Click the **Home** menu and then click **New folder**. Type **Software** and press **Enter**. Click the **Home** menu again and then click **New folder**. Type **UserData** and press **Enter.**
4. Right-click the **Software folder** and click **Properties**.
5. Highlight the **Sharing** tab in the Software Properties window, and click **Advanced Sharing**.
6. In the Advanced Sharing window, select **Share this folder**.
7. Click **Permissions**, select **Full Control** under the Allow column and click **OK**.
8. Click **OK** to close the Advanced Sharing window and click **Close** to close the Software Properties window.
9. Right-click the **UserData** folder and click **Properties**.
10. Highlight the **Sharing** tab in the UserData Properties window, and click **Advanced Sharing**.
11. In the Advanced Sharing window, select **Share this folder**.
12. Click **Permissions**, select **Full Control** under the Allow column and click **OK**.
13. Click **OK** to close the Advanced Sharing window and click **Close** to close the UserData Properties window.
14. Close File Explorer.
15. Open a Web browser and navigate to **https://sourceforge.net/projects/notepadmsi/**. Follow the website instructions to download the latest version of the Notepad++ program.
16. When the download has completed, Right-click the Notepad++ Windows Installer (.msi) file and click **Copy**.
17. In the navigation pane of File Explorer, expand **This PC, Local Disk (C:)**, right-click **Software**, and click **Paste**.
18. Close File Explorer.
19. Click **Start** and then click **Server Manager**. Next, click the **Tools** menu and then click **Group Policy Management**.
20. In the navigation pane of the Group Policy Management window, expand **Forest: domainX.com, Domains, domainX.com**.
21. Right-click **Default Domain Policy** and click **Edit**.
22. In the navigation pane of the Group Policy Management Editor window, expand **Computer Configuration, Policies, Software Settings**.
23. Right-click **Software installation** and click **New, Package**.
24. Type **\\serverX.domainX.com\software** in the File name text box and click Open.
25. Select the **Notepad++version.msi** file and click **Open**.

**(Take Screenshot)**

1. At the Deploy Software window, note the default selection of Assigned and click **OK**.
2. Right-click **Notepad++**, click **Properties**, and highlight the **Deployment** tab.
3. Select **Uninstall this application when it falls out of the scope of management** and click **OK.**
4. In the navigation pane, expand **Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies** and highlight **Password Policy**. Note the default values.
5. Under Account Policies, highlight **Account Lockout Policy**.
6. Double-click **Account lockout threshold**, select **Define this policy** setting, type **3** in the text box, and click **OK**. At the Suggested Value Changes window, click **OK**.
7. Double-click **Reset Account lockout counter after**, type **10** in the text box, and click **OK**.
8. Double-click **Account lockout duration**, type **60** in the text box, and click **OK**. Note that your configuration locks user accounts for 60 minutes after 3 invalid logins within 10 minutes.

**(Take Screenshot)**

1. In the navigation pane, expand **User Configuration, Policies, Administrative Templates** and highlight **Desktop**. Double-click **Hide and disable all items on the desktop**, select **Enabled**, and click **OK**.
2. In the navigation pane, expand **User Configuration, Preferences, Windows Settings**.
3. Right-click **Drive Maps** and click **New, Mapped Drive**.
4. Select **Create** from the Action drop-down box.
5. Type **\\domainX.com\warehouse** in the Location text box.
6. Select **Reconnect** and type **Data Warehouse** in the Label as text box
7. Select **W** from the Use drop-down box and click **OK**. Note the new drive map configuration shown.

**(Take Screenshot)**

1. Close the Group Policy Management Editor window.
2. In the navigation pane of the Group Policy Management window, right-click **Marketing** and click **Block Inheritance.**
3. Right-click **Marketing** and click **Create a GPO in this domain, and Link it here**. Type **Marketing Group Policy** in the Name text box and click **OK**.
4. Expand **Marketing** in the navigation pane and note the GPO link for the Marketing Group Policy.
5. Right-click **Marketing Group Policy** and click **Edit**.
6. In the navigation pane of the Group Policy Management Editor window, expand **User Configuration, Policies, Windows Settings, Folder Redirection**.
7. Right-click **Documents** and click **Properties**.
8. At the Documents Properties window, select **Basic – Redirect everyone’s folder to the same location** from the Setting drop-down box.
9. Type **\\serverX.domainX.com\UserData** in the Root Path text box, and note that a target folder will be created for each user under this path using the example shown.
10. Highlight the **Settings** tab, note the default option that grants the user exclusive permissions to the folder, and click **OK**.
11. Note the warning and click **Yes** to add the configuration.
12. In the navigation pane, expand **User Configuration, Policies, Administrative Templates** and highlight **Control Panel**. Double-click P**rohibit access to Control Panel and PC settings**, select **Enabled**, and click **OK**.

**(Take Screenshot)**

1. Close the Group Policy Management Editor window.
2. In the navigation pane of the Group Policy Management window, select **Marketing Group Policy** and then highlight the **Settings** tab. Note that Computer Configuration settings have not been configured. Highlight the **Details** tab, select **Computer configuration settings disabled** from the GPO Status drop-down box, and click **OK**.
3. Close the Group Policy Management window.
4. In Server Manager, select the **Tools** menu and then click **Hyper-V Manager**.
5. Highlight **WindowsServer2019VM2** in the virtual machines pane of Hyper-V Manager and click **Connect** in the Actions pane. In the Virtual Machine Connection window, click **Start** to boot your virtual machine.
6. At the login screen, click the **Ctrl+Alt+Delete** button in the Virtual Machine Connection window, supply the password **Secret555** for Administrator, and press **Enter** to log into the system.
7. Note that no items appear on your desktop. This is because the User Configuration of the Default Domain Policy GPO was applied to the Administrator user account located under the default Users folder in the domain.
8. Click **Start** and note that Notepad++ is listed under the *Recently added* section. This is because the Computer Configuration of the Default Domain Policy GPO was applied to the computer account for the WindowsServer2019VM2 virtual machine located under the default Computers folder in the domain.

**(Take Screenshot)**

1. Select **File Explorer** from the Start menu, expand **This PC**, and note that you have a mapped drive (W:\) for DomainX Warehouse. This is because the Group Policy preferences from the User Configuration of the Default Domain Policy GPO was applied to Administrator.

**(Take Screenshot)**

1. Right-click **Start**, click **Shut down or sign out, Sign out**.
2. At the login screen, click the **Ctrl+Alt+Delete** button in the Virtual Machine Connection window, click **Other user**, and supply a user name of **b.burtt@domainX.com**. Supply the password **Secret555** and press **Enter** to log into the system.
3. Note that the Recycle Bin appears on your desktop. This is because the User Configuration of the Default Domain Policy GPO was not applied to the Bob Burtt user account located under the Marketing OU due to the Block Inheritance setting.
4. Right-click **Start** and click **Settings**. Note that you are unable to access the Settings window. This is because the User Configuration of the Marketing Group Policy GPO was applied to the Bob Burtt user account located under the Marketing OU.
5. Click **Start** and click **Control Panel**. Note the error message that you receive and click **OK**.

**(Take Screenshot)**

1. Click **Start** and click **File Explorer**. Right-click Documents and click Properties. Note that Bob Burtt’s documents folder has been redirected to \\serverX.domainX.com\UserData\b.burtt and click **OK**.

**(Take Screenshot)**

1. Right-click **Start**, click **Shut down or sign out, Sign out**.
2. At the login screen, click the **Ctrl+Alt+Delete** button in the Virtual Machine Connection window, supply an invalid password for Bob Burtt and press **Enter**. Repeat this process three more times and note the message indicating that the Bob Burtt user account has been locked.

**(Take Screenshot)**

1. In Server Manager on your Windows Server 2019 host, click the **Tools** menu and then click **Active Directory Users and Computers**.
2. Highlight the **Marketing** OU under domainX.com.
3. Right-click **Bob Burtt**, click **Properties**, and highlight the **Account** tab. Note that the account is currently locked.
4. Select **Unlock account** and click **OK**.
5. Close Active Directory Users and Computers.
6. On your WindowsServer2019VM2 virtual machine, click the **Ctrl+Alt+Delete** button in the Virtual Machine Connection window, click **Other user** and supply the user name **administrator@domainX.com**. Supply the password **Secret555** and press **Enter** to log into the system.
7. Right-click **Start** and click **Windows PowerShell (Admin)**. At the prompt, type gpresult /r and press **Enter**. Note that the User Configuration and Computer Configuration of the Default Domain Policy GPO was applied, but that the Local Group Policy was not applied because it contained no settings. Close Windows PowerShell when finished.

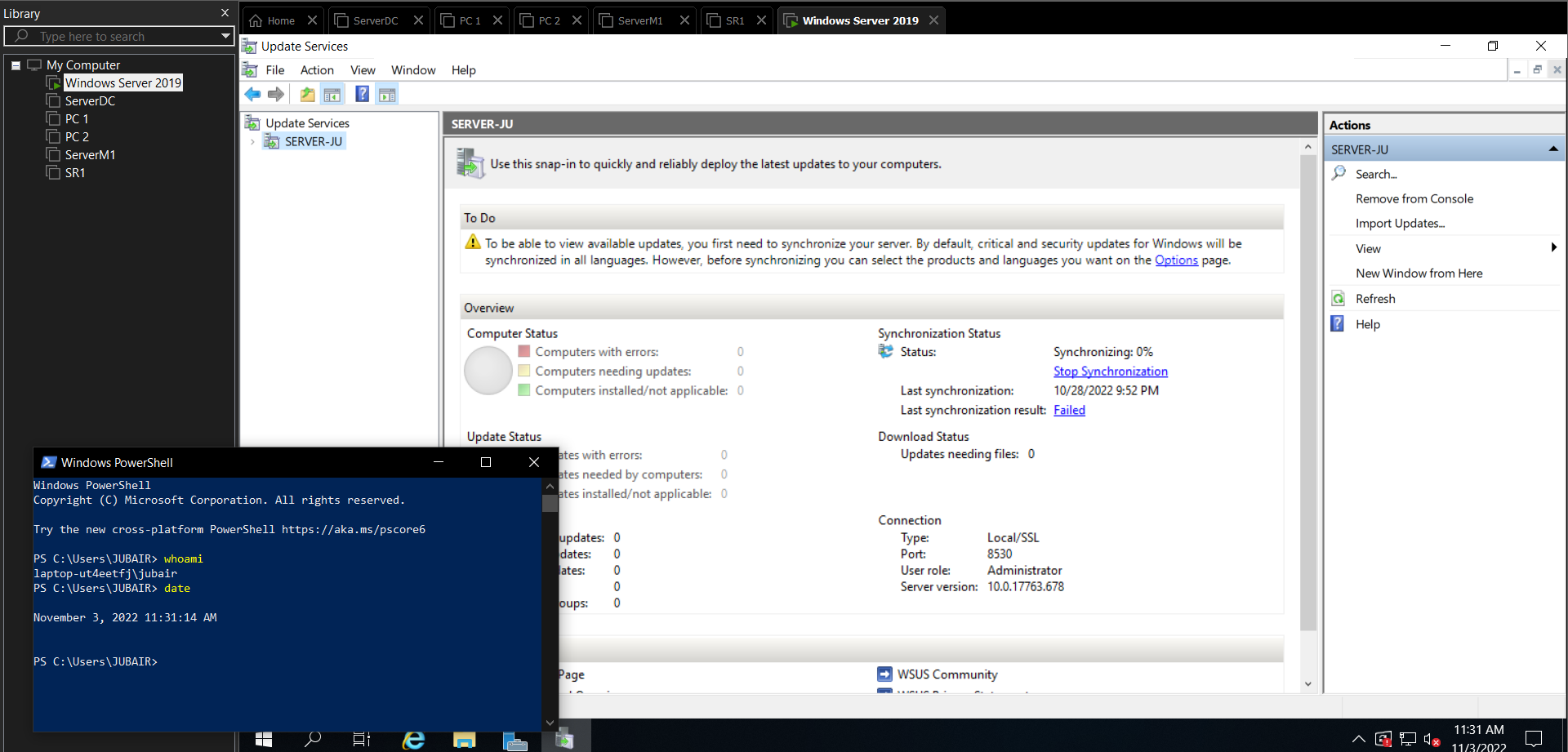
**(Take Screenshot)**

**Project 2: Configuring WSUS**

*In this Hands-On Project, you install and configure WSUS to provide critical and security updates for Windows systems in your Active Directory domain.*

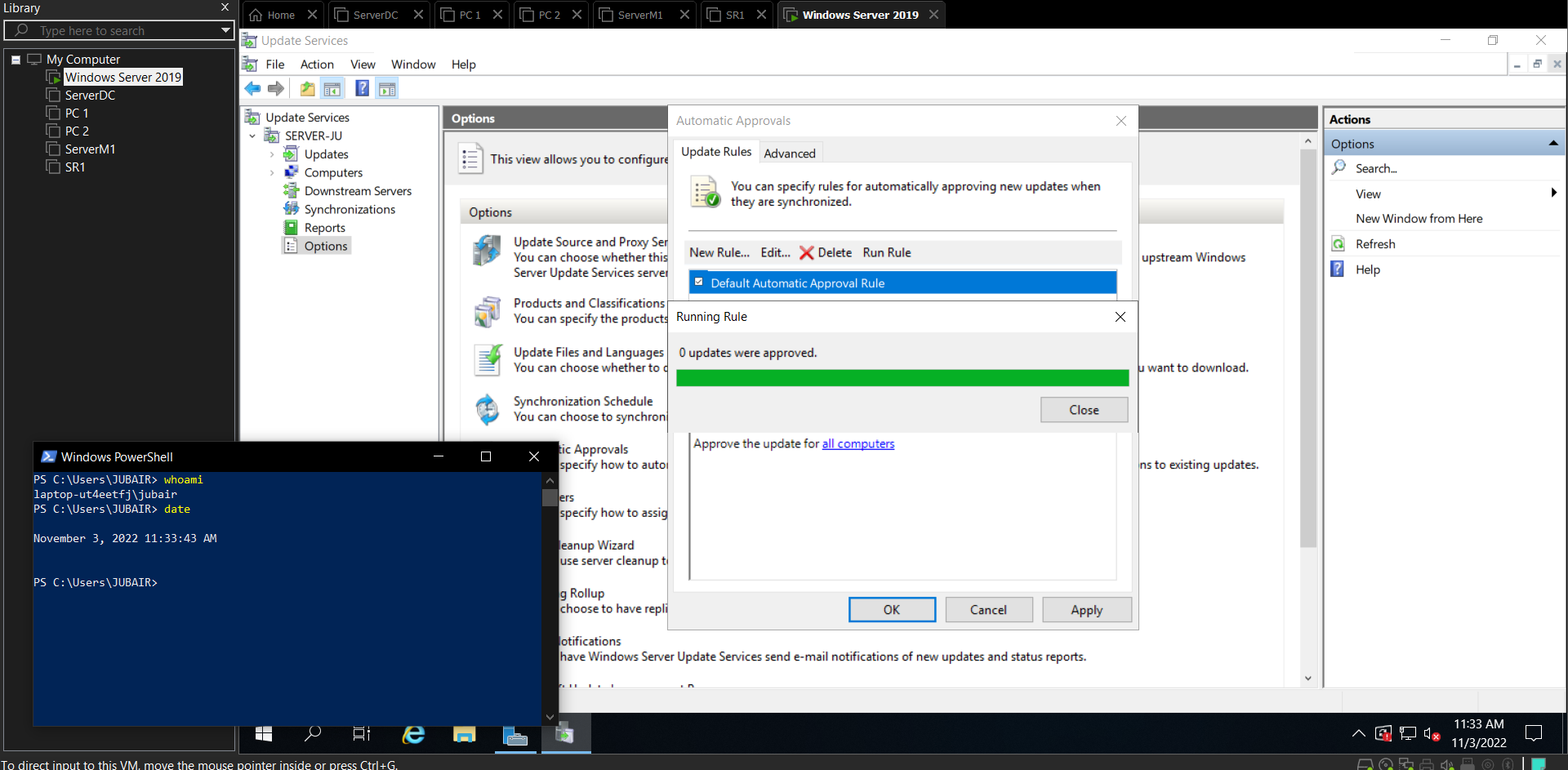
1. In Server Manager on your Windows Server 2019 host, click the **Manage** menu and then click **Add Roles and Features**.
2. At the Select installation type page, click **Next**.
3. At the Select destination server page, click **Next**.
4. At the Select server roles page, select **Windows Server Update Services** and click **Add Features** when prompted. Click **Next**.
5. At the Select features page, click **Next**.
6. At the Windows Server Update Services page, note the default selections and click **Next**.
7. At the Content location selection page, deselect **Store updates in the following location** and click **Next**.
8. At the Confirm installation selections page, click **Install**.
9. At the Installation progress page, click **Launch Post-Installation tasks** and then click **Close** to close the Add Roles and Features Wizard.
10. In Server Manager, select the **Tools** menu and then click **Windows Server Update Services** to start the Windows Server Updates Services Configuration Wizard.
11. At the Before You Begin page, click **Next**.
12. At the Microsoft Update Improvement Program page, deselect **Yes, I would like to join the Microsoft Update Improvement Program** and click **Next**.
13. At the Choose Upstream Server page, note the default selection that synchronizes from Microsoft Update and click **Next**.
14. At the Specify Proxy Server page, click **Next**.
15. At the Connect to Upstream Server page, click **Start Connecting**. This will download the Windows Catalog and may take several minutes, depending on the speed of your Internet connection. When finished click **Next**. *(It can take up-to half hour to download information)*
16. At the Choose Products page, note the default selections for Windows operating system products and click **Next**.
17. At the Choose Classifications page, deselect **Definition Updates** and **Upgrades** and click **Next**.
18. At the Configure Sync Schedule page, select **Synchronize automatically**, specify **1:00:00 AM** in the First synchronization text box, and click **Next**.

**(Take Screenshot)**



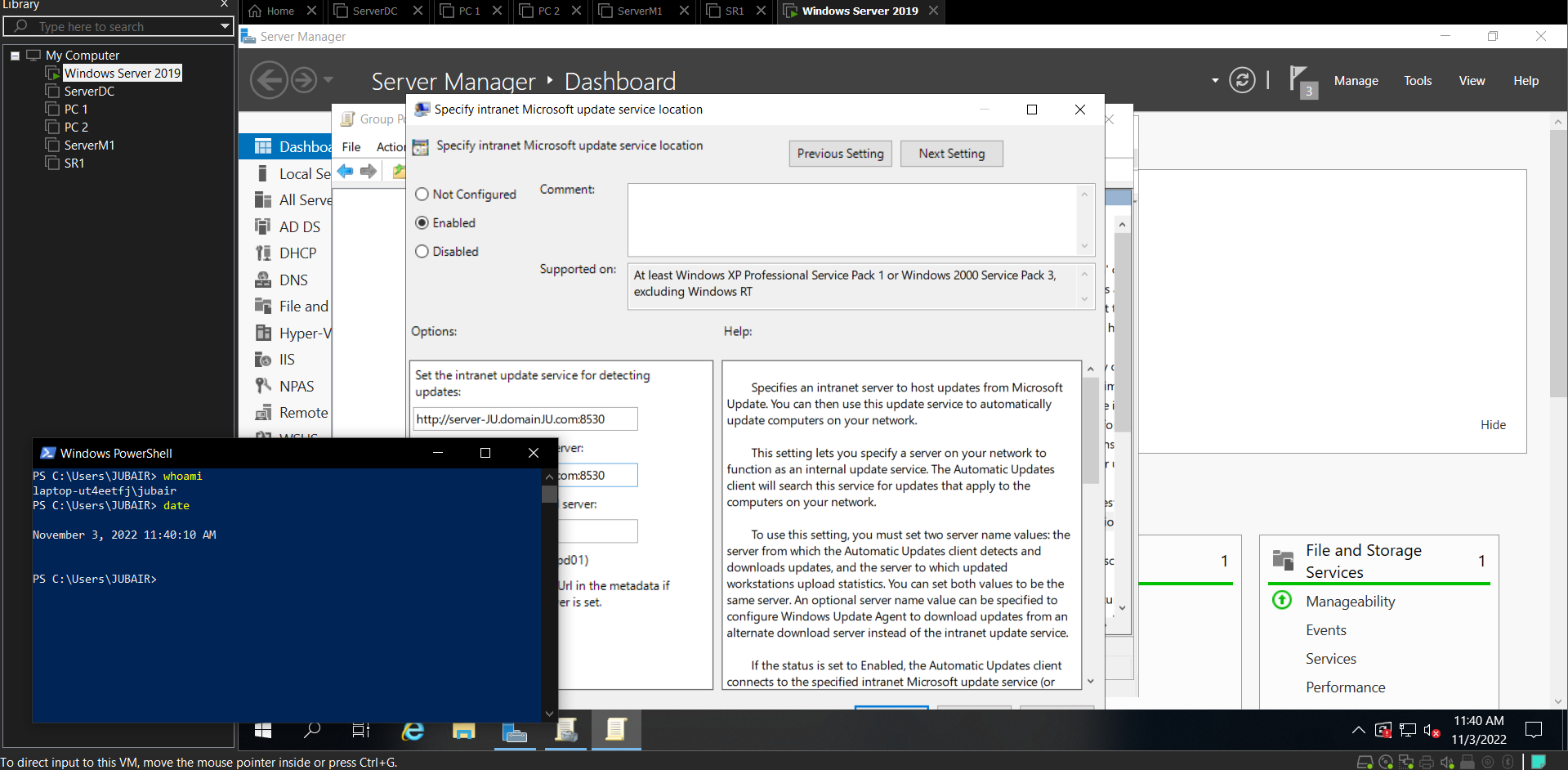
1. At the Finished page, select **Begin initial synchronization** and click **Finish** to close the Windows Server Updates Services Configuration Wizard, and open the Update Services tool.
2. In the Update Services tool, expand **SERVERX** in the navigation pane and highlight **Options**.
3. Click **Automatic Approvals** in the Options pane and check the **Default Automatic Approval Rule**
4. Click **Run rule** to approve critical and security updates that have already been synchronized on the WSUS server.

**(Take Screenshot)**



1. Click **Close** to close the Running Rule window.
2. Click **OK** to close the Automatic Approvals window.
3. Close the Update Services tool.
4. In Server Manager, click the **Tools** menu and then click **Group Policy Management**.
5. In the navigation pane of the Group Policy Management window, expand **Forest: domainX.com, Domains, domainX.com**.
6. Right-click **Default Domain Policy** and click **Edit**.
7. In the navigation pane of the Group Policy Management Editor window, expand **Computer Configuration, Policies, Administrative Templates, Windows Component**s, and highlight **Windows Update**.
8. Double-click **Configure Automatic Updates**, select **Enabled**, and then select **4 – Auto download and schedule the install** from the *Configure automatic updating* drop-down box. Next, specify **1:00** in the *Scheduled install time* drop-down box and click **OK**.
9. Double-click **Specify intranet Microsoft update service location** and select **Enabled**. Next, type **http://serverX.domainX.com:8530** in both the *Set the intranet update service for detecting updates* and *Set the intranet statistic* server text boxes and click **OK**.

**(Take Screenshot)**



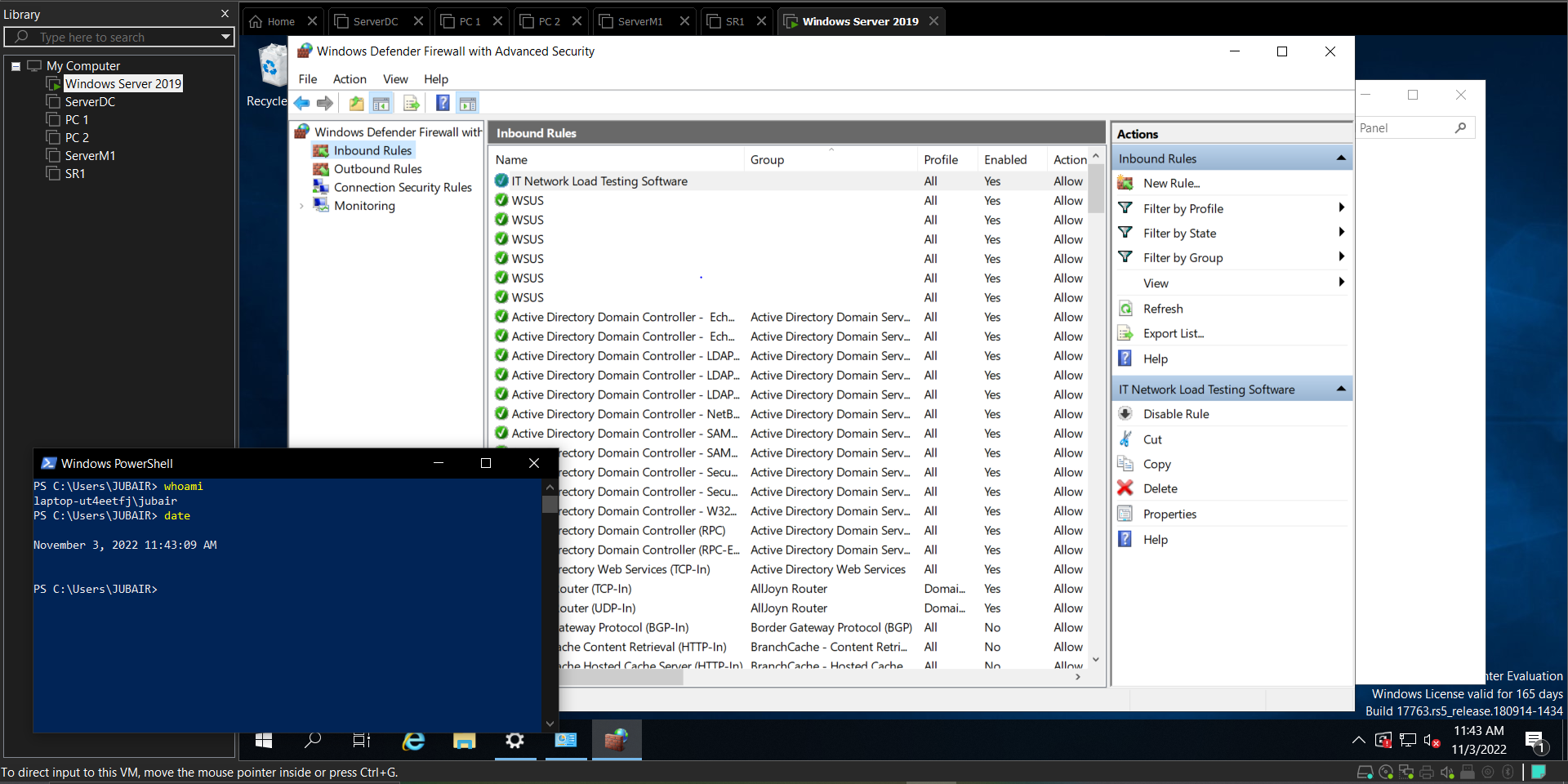
1. Close the Group Policy Management Editor window.
2. Close the Group Policy Management window.

**Project 3: Configuring Windows Defender**

*In this Hands-On Project, you explore Windows Defender settings, as well as configure a firewall rule using the Windows Defender Firewall with Advanced Security tool.*

1. On your Windows Server 2019 host, click **Start**, type **Windows Defender settings**, and press **Enter** to open the Windows Security section of Settings.
2. Click **Open Windows Security** and note that all areas of your system are protected by default.
3. Click **Virus & threat protection**.
4. Click **Quick scan** to perform a malware scan on your system.
5. Click **Threat history** and view the results. Click the back arrow in the upper left of the Windows Security window.
6. Click **Manage ransomware protection** and note that Controlled folder access is not enabled by default. Click the back arrow twice in the upper left of the Windows Security window.
7. Click **Firewall & network protection**.
8. Note that the firewall is enabled for the active (Domain network) profile.
9. Click **Allow an app through firewall** and note the default firewall rules that you can configure.
10. Click **Cancel** and then click the back arrow in the upper left of the Windows Security window.
11. Click **App & browser control**.
12. Note the default action that warns users of unrecognized apps.
13. Click **Exploit protection settings** and note that all system settings are enabled by default.
14. Click **Program settings** and note that you can modify protection settings for programs on the system. Click the back arrow twice in the upper left of the Windows Security window.
15. Click **Device security**.
16. Note whether core isolation and secure boot are enabled on your Windows Server 2019 host.
17. Click **Core isolation details** and note that core isolation is disabled by default.
18. Close the Windows Security window, and then close the Settings window.
19. Right-click **Start** and click **Run**. Type wf.msc in the Run dialog box and click **OK** to open Windows Defender Firewall with Advanced Security.
20. Highlight **Inbound Rules** in the navigation pane and note the default rules available for each firewall profile.
21. Click **New Rule** in the Actions pane.
22. At the New Inbound Rule Wizard, select **Port** and click **Next**.
23. At the Protocols and Ports page, note the default selection of TCP, type **27950, 27952, 27960, 27965** in the *Specific local ports* text box, and click **Next**.
24. At the Action page, note the default action that allows the connection and click **Next**.
25. At the Profile page, note the default selection of all firewall profiles and click **Next**.
26. At the Name page, type **IT Network Load Testing Software** in the Name text box and click **Finish**. Note that your new inbound rule is enabled for all profiles.

**(Take Screenshot)**



1. Close Windows Defender Firewall with Advanced Security.