***Project 1: Host Setup***

*In this Hands-On Project, you install the server roles and features on your Windows Server 2019 host required for the remaining Hands-On Projects within this module, including the Server for NFS, Client for NFS, File Server Resource Manager, DFS Namespaces, and DFS Replication.*

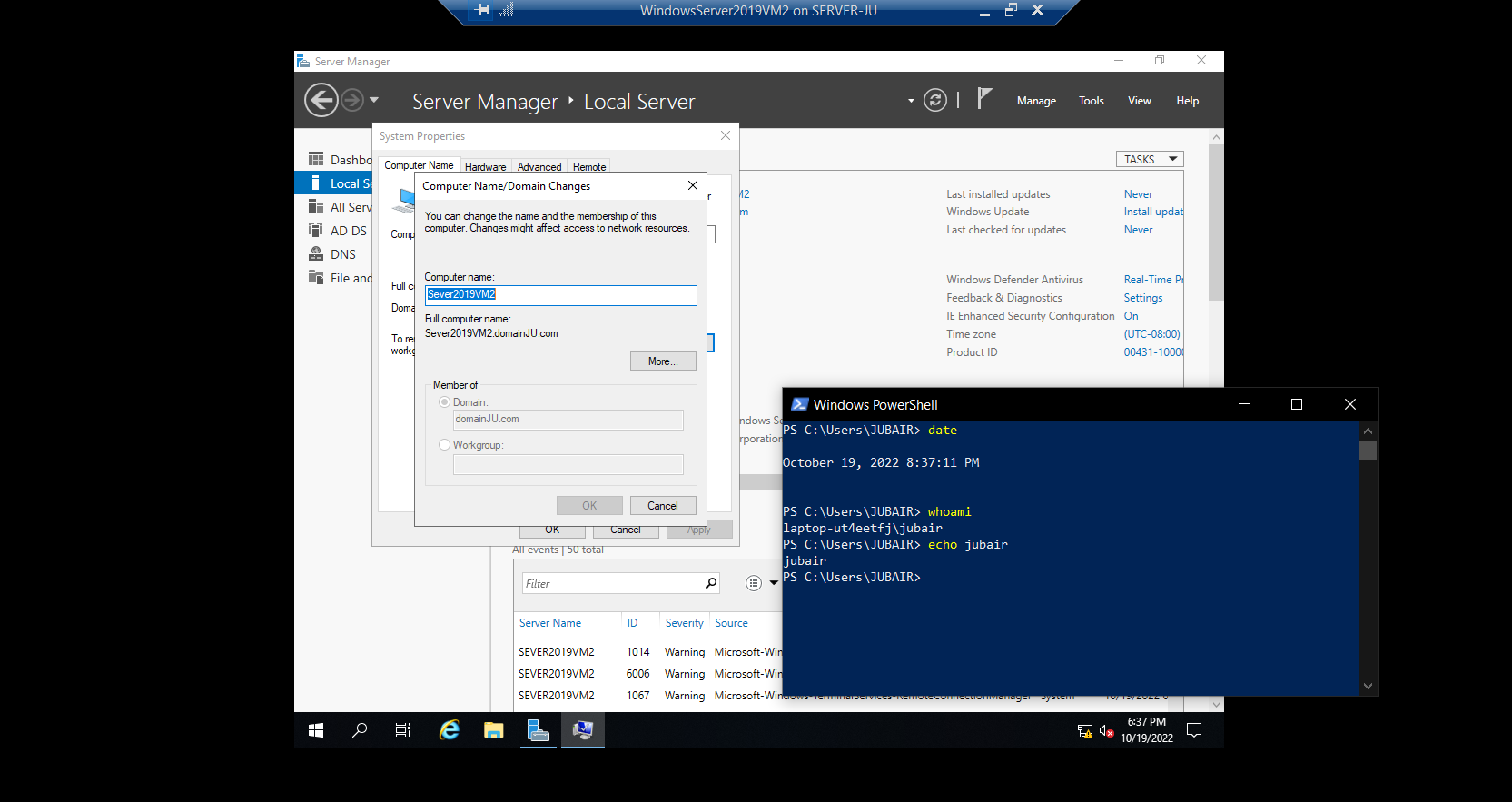
1. Boot your Windows Server 2019 host and log into domain*X*.com as Administrator using the password **Secret555**. Next, click **Start** and then click **Server Manager**.
2. Within Server Manager, click the **Manage** menu and then click **Add Roles and Features**.
3. At the Select installation type page, click **Next**.
4. At the Select destination server page, click **Next**.
5. At the Select server roles page, expand **File and Storage Services**, and then expand **File and iSCSI Services**.
   1. Select **Server for NFS** and click **Add Features** when prompted.
   2. Select **File Server Resource Manager** and click **Add Features** when prompted.
   3. Select **DFS Namespaces** and click **Add Features** when prompted.
   4. Select **DFS Replication**.
6. Click **Next**.
7. At the Select features page, select **Client for NFS** and click **Next**.
8. At the Confirm installation selections page, click **Install** to install the Server for NFS, File Server Resource Manager, DFS Namespaces, and DFS Replication server roles, as well as the Client for NFS feature.
9. At the Installation progress page, click **Close.**

***Project 2: Member Server Setup***

*In this Hands-On Project, you configure your WindowsServer2019VM2 virtual machine as a member server within your Active Directory domain, and then install the DFS Replication role required for Hands-On Project 5-7.*

1. Within Server Manager on your Windows Server 2019 host, select the **Tools** menu and then click **Hyper-V Manager**.
2. Highlight **WindowsServer2019VM2** within the Virtual Machines pane and click **Settings** in the Actions pane.
   1. Highlight **Network Adapter** under the Hardware section.
   2. Select **External Virtual Switch** from the Virtual switch drop-down box to connect your virtual network interface to the external virtual network.
   3. Click **OK** .
3. Highlight **WindowsServer2019VM2** within 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 new virtual machine.
4. At the login screen, click the **Ctrl+Alt+Delete** button within the Virtual Machine Connection window, supply the password **Secret555** for **Administrator** and press **Enter** to log into the system.
5. Click **Start** and then click **Server Manager**. Within Server Manager, click **local Server** within the navigation pane.
   1. Make sure server name is set to **Server2019VM2.** If not, then change the computer name and restart the server.
   2. Next, click the hyperlink next to your Ethernet network interface.
   3. In the Network Connections window, right-click **Ethernet** and click **Properties**.
   4. Highlight **Internet Protocol Version 4 (TCP/IPv4)** within the Ethernet Properties window and click **Properties**. Assign following IPv4 and DNS address:
      * IP address : 192.168.0.20
      * Subnet Mask: 255.255.255.0
      * Default gateway: 192.168.0.2
      * Preferred DNS Server: 192.168.0.10
   5. Click **OK** when finished.
   6. Click **OK** . Click **OK** again to close the Ethernet Properties window.
   7. Close the Network Connections window.
   8. Click the **WORKGROUP** hyperlink within the Properties pane of Server Manager.
   9. At the System Properties window, note your computer name. Next, click **Change**.
   10. At the Computer Name/Domain Changes window, select **domain**, type **domain*X*.com** in the text box and click **OK** .

**(Take Screenshot)**



* 1. At the Windows Security window, supply the user name [**administrator@domain*X*.com**](mailto:administrator@domainX.com)and password **Secret555** and click **OK** .
  2. Click **OK** at the Computer Name/Domain Changes information window, and then click **OK** again when prompted that you must restart your computer to complete the domain join.
  3. Click **Close** to close the System Properties window and click **Restart Now** when prompted to reboot your virtual machine.

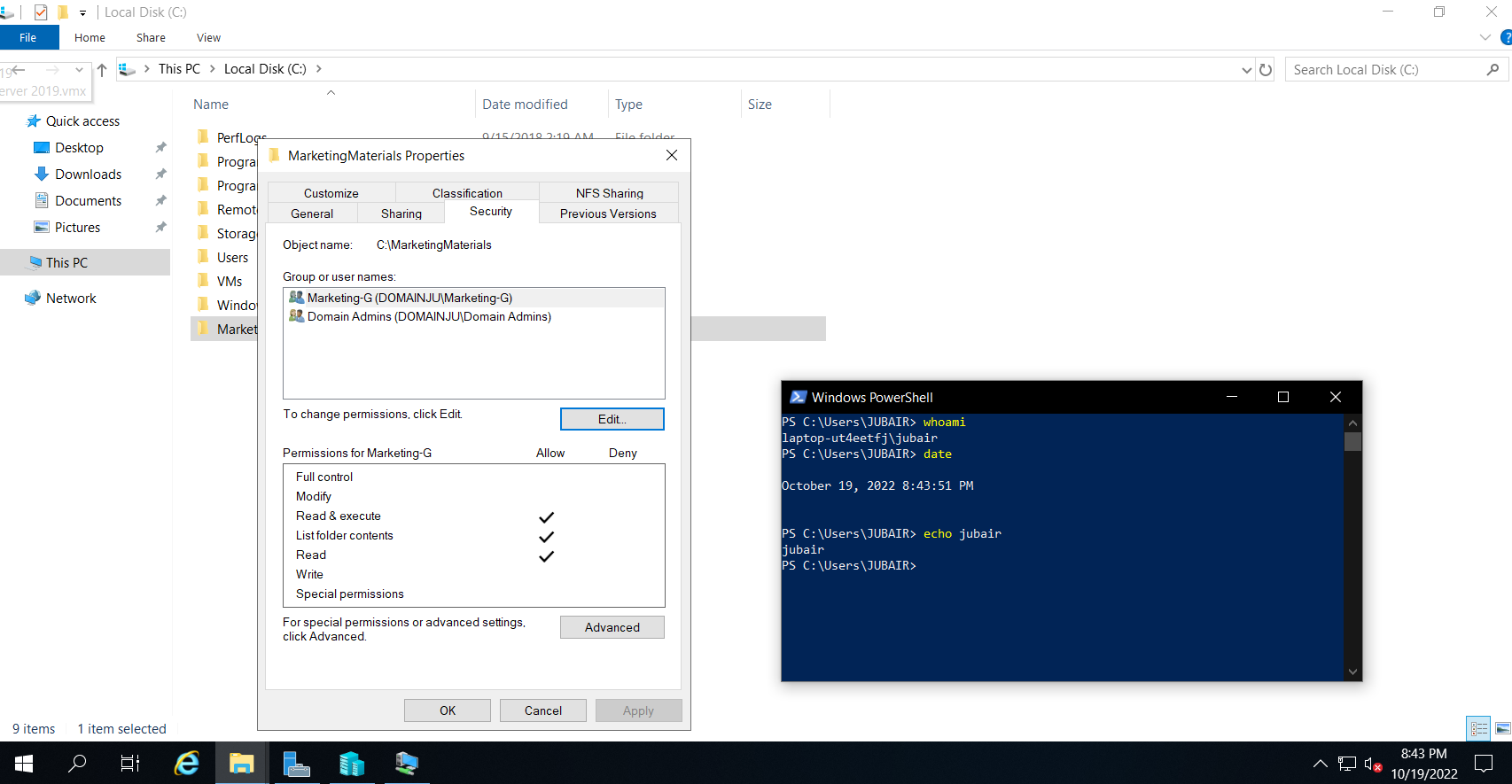
1. After your virtual machine has rebooted, click the **Ctrl+Alt+Delete** button within the Virtual Machine Connection window and then click **other user**. Supply the user name [**administrator@domain*X*.com**](mailto:administrator@domainX.com) and password **Secret555** for the Administrator user within **domain*X*.com** and press **Enter** to log into the system.
2. At the Server Manager information window, select **don’t show this message again** and close the window.
3. Within Server Manager, click the **Manage** menu and then click **Server Manager Properties**. Select **do not start Server Manager automatically at logon** and click **OK** .
4. Within Server Manager, click the **Manage** menu and then click **Add Roles and Features**.
   1. At the Select installation type page, click **Next**.
   2. At the Select destination server page, click **Next**.
   3. At the Select server roles page, expand **File and Storage Services** and then expand **File and iSCSI Services**. Select **DFS Replication** and click **Add Features** when prompted.
   4. Click **Next**.
   5. At the Select features page, click **Next**.
   6. At the Confirm installation selections page, click **Install** to install the DFS Replication role.
   7. At the Installation progress page, click **Close**.
5. Close Server Manager.

***Project 3: Permissions***

*In this Hands-On Project, you configure and verify NTFS permissions on your Windows Server 2019 host.*

1. On your Windows Server 2019 host, click **Start** and then click **File Explorer**.
2. In the navigation pane of File Explorer, expand **This PC** if necessary and highlight **local disk (C:)**.
3. Click the **Home** menu and then click **New folder**. Type **MarketingMaterials** and press **Enter**.
4. Right-click the **MarketingMaterials** folder and click **Properties**.
   1. Highlight the **Security** tab within the **MarketingMaterials** Properties window and note the default permissions assigned to the different groups on the system.
   2. Click **Advanced**. At the Advanced Security Settings for MarketingMaterials window, note that the owner of the folder is the Administrators group.
   3. Click **disable inheritance** and then click **Remove all inherited permissions from this object** when prompted. Click **OK** and then click **Yes** when prompted to close the Advanced Security Settings for **MarketingMaterials** window.
   4. In the MarketingMaterials Properties window, note that all default permissions inherited from C:\ have been removed and click **Edit**.
   5. At the Permissions for MarketingMaterials window, click **Add**. Type **Domain Admins** and click **OK**. Select **Full control** under the Allow permissions column. Click **Add** again. Type **Marketing-G** and click **OK**. Select **Modify** under the Allow permissions column and click **OK**.

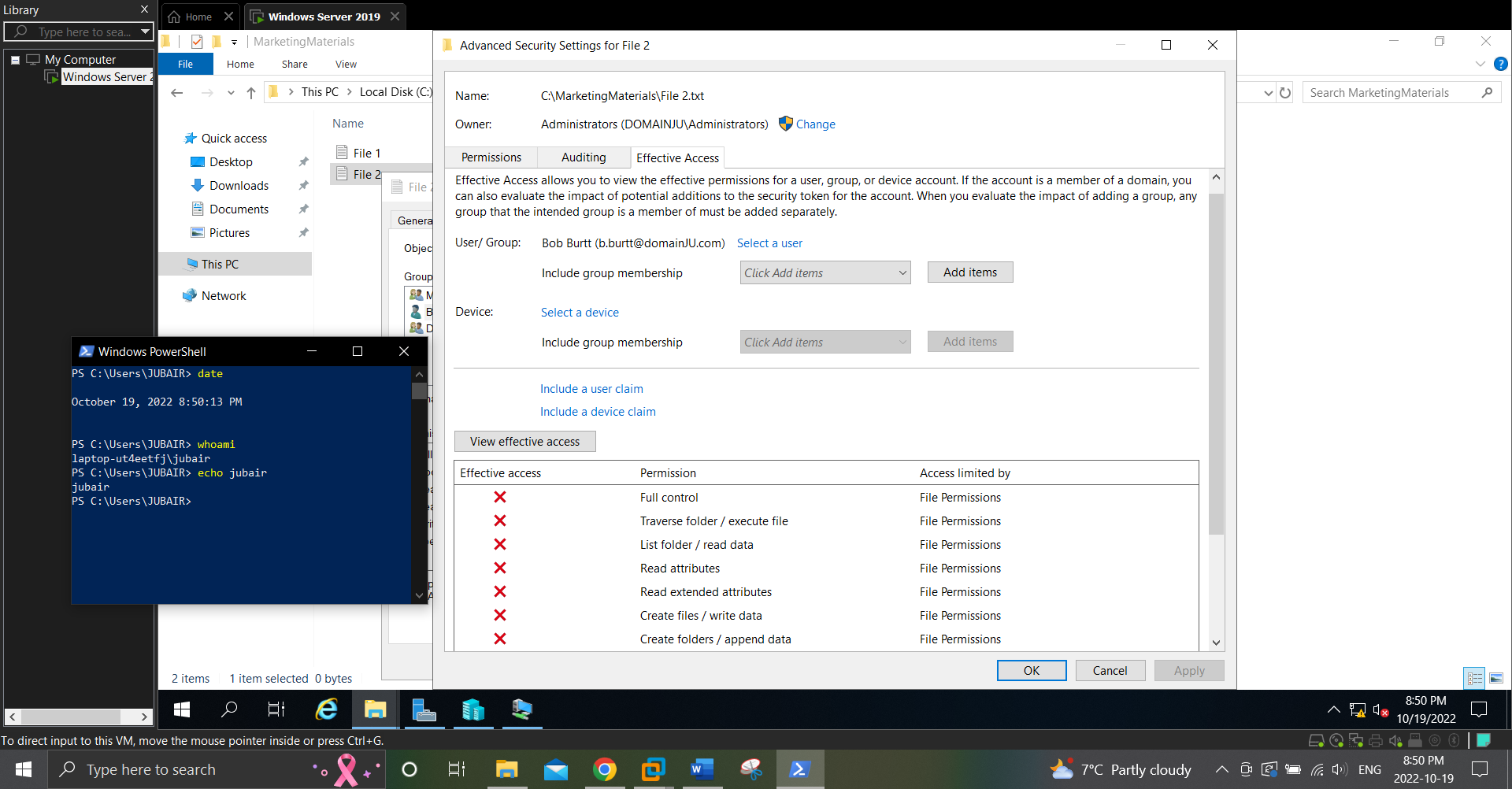
**(Take Screenshot)**



* 1. Click **Advanced**. At the Advanced Security Settings for MarketingMaterials window, highlight the **Marketing-G** permission entry and click **Edit**. Next, click **Show advanced permissions**, note the advanced permissions that comprise the basic Modify permission, and click **OK**. Click **OK** to close the Advanced Security Settings for MarketingMaterials window.
  2. Click **OK** to close the MarketingMaterials Properties window.

1. Double-click the **MarketingMaterials** folder. Next, click the **Home** menu, select the **New item** drop-down box, and click **Text document**. Type **File1** and press **Enter** to create a File1.txt file within the MarketingMaterials folder.
2. Click the **Home** menu, select the **New item** drop-down box, and click **Text document**. Type **File2** and press **Enter** to create a File2.txt file within the MarketingMaterials folder.
3. Right-click **File2** and click **Properties**.
4. Highlight the **Security** tab within the File2 Properties window and note the default permissions inherited from the MarketingMaterials folder.
5. Click **Edit**. At the Permissions for File2 window, click **Add**. Type **Bob Burtt** and click **OK**. Select **Modify** under the Deny permissions column and click **OK**. Read the contents of the Windows Security window and click **Yes**.
6. Click **OK** to close the File2 Properties window.
7. Reopen **File2** Properties window, highlight **security** tab, click **Advanced**. At the Advanced Security Settings for File2 window, highlight the **Effective Access** tab. Recall that both Bob Burtt and Mary Stewart are both members of the Marketing-G group (configured within Hands-On Project 4-7).
8. Click **Select a user**, type **Bob Burtt,** and click **OK**. Next, click **View effective access** and note that Bob Burtt is denied all access because the permissions denied to the Bob Burtt user account override the permissions granted to the Marketing-G group.

**(Take Screenshot)**



1. Click **Select a user**, type **Mary Stewart,** and click **OK**. Next, click **View effective access** and note that Mary Stewart receives the advanced permissions that comprise the basic Modify permission granted to members of the Marketing-G group.
2. Click **OK** to close the Advanced Security Settings for File2 window.
3. Click **OK** to close the File2 Properties window.
4. Right-click the Start menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell. Next, type *Add-ADGroupMember -Identity "Backup Operators" -Members "Marketing-G"* and press **Enter** to add the Marketing-G global group as a member of the Backup Operators built-in group. Close Windows PowerShell when finished.
5. Right-click the **Start** menu and then click **Sign out**.
   1. Press **Ctrl+Alt+Delete** (or the Ctrl+Alt+Delete button within the Virtual Machine Connection window if you use Lab Environment 2) and then click **other user**.
   2. Supply a user name of [**b.burtt@domain*X*.com**](mailto:b.burtt@domainX.com) and password of **Secret555** and press **Enter**.
   3. When prompted to change your password, click **OK**. Type **NewPassword555** in both password text boxes and press **Enter**.
   4. Click **OK** to continue to log into the system.
6. Click **Start** and then click **File Explorer**.
   1. In the navigation pane of File Explorer, expand **This PC**, **local disk (C:)** and highlight **MarketingMaterials.**
   2. Double-click **File1** to open it within Notepad. Type a line of your choice, click the **File** menu and then click **Save**. Close Notepad when finished.
   3. Double-click **File2** and note the error message that you receive. Click **OK** and close Notepad.
7. Right-click the **Start** menu and click **sign out** and then click **Sign out**.
   1. Press **Ctrl+Alt+Delete** (or the Ctrl+Alt+Delete button within the Virtual Machine Connection window if you use Lab Environment 2) and then click **other user**.
   2. Supply a user name of [**administrator@domain*X*.com**](mailto:administrator@domainX.com) and password of **Secret555** and press **Enter** to log into the system.

***Project 4: Auditing***

*In this Hands-On Project, you enable, configure, and test file auditing on your Windows Server 2019 host.*

1. On your Windows Server 2019 host, click **Start** and then click **Server Manager**.
2. Within Server Manager, click the **Tools** menu and then click **Group Policy Management**.
3. Within the navigation pane of the Group Policy Management window, expand Forest: **domainX.com, Domains, domainX.com.**
4. Right-click **Default Domain Policy** and click **Edit**.
5. In the navigation pane of the Group Policy Management Editor window, expand **Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies,** and highlight **Audit Policy**.
6. Double-click **Audit object access** in the right pane. In the Audit object access Properties window, select **Define these policy settings**. Next, select **Failure** and click **OK**.

**(Take Screenshot)**

1. Close the Group Policy Management Editor window and then close the Group Policy Management window.
2. Click **Start** and then click **File Explorer**.
3. In the navigation pane of File Explorer, expand **This PC, Local Disk (C:)** and highlight **MarketingMaterials**.
4. Right-click **File2** and click **Properties**.
5. Highlight the **Security** tab within the File2 Properties window and click **Advanced**.
6. At the Advanced Security Settings for File2 window, highlight the **Auditing** tab. Note that no auditing entries are created by default.
7. Click **Add**. In the Auditing Entry for File2 window, click **Select a principle**, type **Marketing-G**, and click **OK**. Next, select **Fail** from the Type drop-down box, select Full control permission within the Basic permissions section, and click OK. This will create an auditing entry that records failures of any permission level on File2 for members of the Marketing-G group.
8. Click **OK** to close the Advanced Security Settings for File2 window.
9. Click **OK** to close the File2 Properties window.
10. Right-click the **Start** menu and then click **Sign out**.
11. Press **Ctrl+Alt+Delete** (or the Ctrl+Alt+Delete button within the Virtual Machine Connection window if you use Lab Environment 2) and then click **Other user**.
12. Supply a user name of **b.burtt@domainX.com** and password of **NewPassword555** and press **Enter** to log into the system.
13. Click **Start** and then click **File Explorer**.
14. In the navigation pane of File Explorer, expand **This PC, Local Disk (C:)** and highlight **MarketingMaterials**.
15. Double-click **File2** to generate an error message due to denied permissions. Click **OK** and close Notepad.
16. Right-click the **Start** menu and then click **Sign out**.
17. Press **Ctrl+Alt+Delete** (or the Ctrl+Alt+Delete button within the Virtual Machine Connection window if you use Lab Environment 2) and then click **Other user**.
18. Supply a user name of **administrator@domainX.com** and password of **Secret555** and press **Enter** to log into the system.
19. Right-click the Start menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell. Next, type *Get-EventLog Security -EntryType FailureAudit -Newest 3 | Format-List* and press **Enter** to view the details for the most recent three failure audit entries within the Security log. Note that Bob Burtt’s failed attempt to access File2.txt using Notepad was recorded.

**(Take Screenshot)**

1. Close Windows PowerShell.

***Project 5: Attributes***

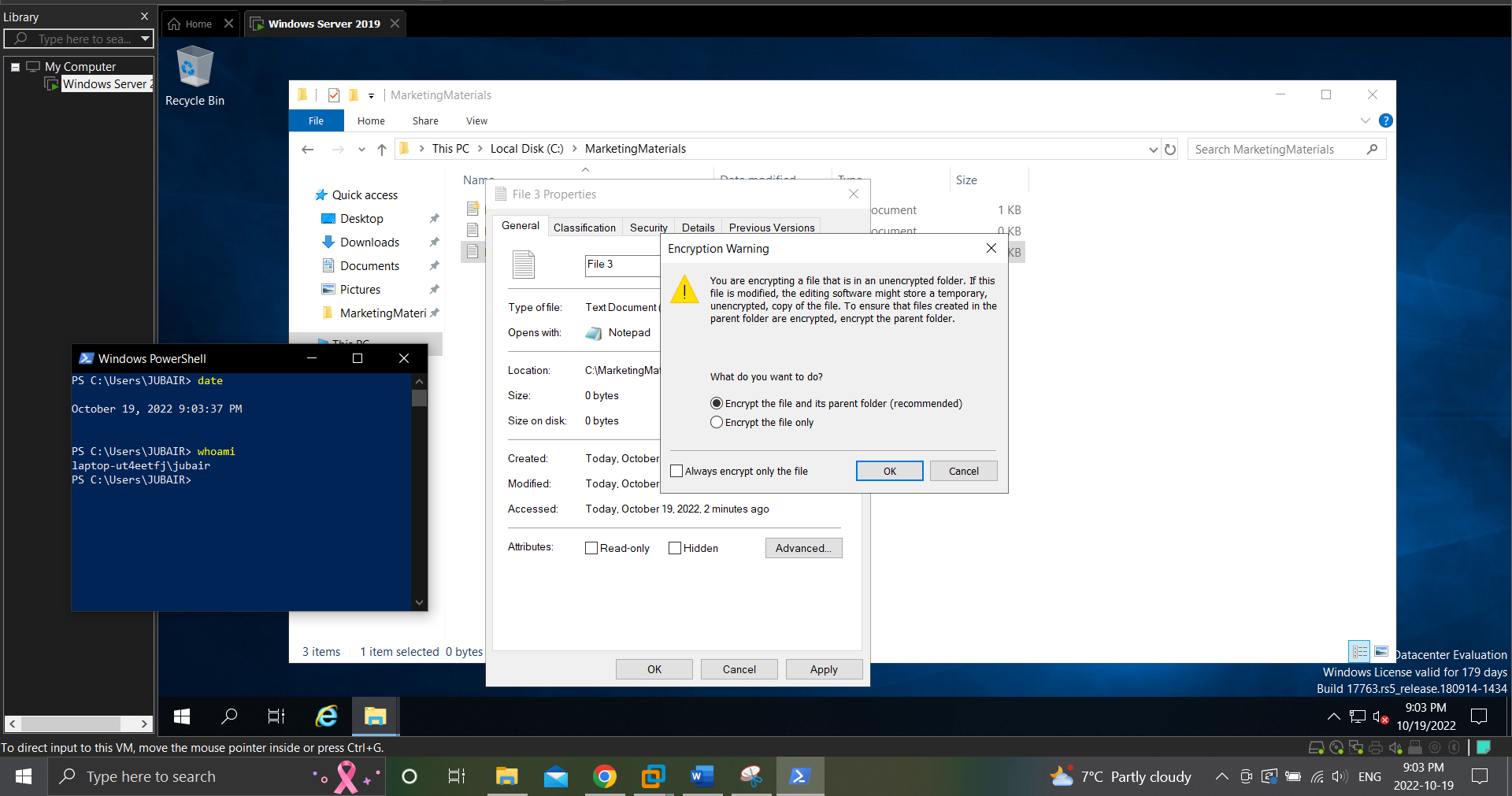
*In this Hands-On Project, you configure and test file attributes on your Windows Server 2019 host.*

1. On your Windows Server 2019 host, click **Start** and then click **File Explorer**.
2. In the navigation pane of File Explorer, expand **This PC, Local Disk (C:)** and highlight **MarketingMaterials**.
3. Right-click **File1** and click **Properties**.
4. On the General tab of File1 Properties, select **Read-only** and **Hidden** and click

**Advanced**.

1. At the Advanced Attributes window, note the attributes selected by default. Select **Compress contents to save disk space** and click **OK**.
2. Click **OK** to close the File1 Properties window. Note that File1 disappears from view after a few moments.
3. Click the **View** menu within File Explorer and select **Hidden items**. Note that File1 appears again, but has a grey icon with a blue compression arrow symbol.
4. Double-click File1 to open it within Notepad. Type a line of your choice, click the **File** menu, and then click **Save**. Instead of saving the changes, Notepad displays a Save As window that will allow you to save the file to a different file name, because File1 has the read-only attribute. Click **Cancel**, close Notepad, and click **Don’t Save** when prompted.
5. Right-click **File1** and click **Properties**.
6. On the General tab of File1 Properties, deselect **Read-only** and **Hidden** and click **Advanced**.
7. At the Advanced Attributes window, select **Encrypt contents to secure data**, note that the compression attribute was automatically deselected, and click **OK**.
8. Click **OK** to close the File1 Properties window. Select **Encrypt the file only** when prompted and click **OK**. Note that the File1 icon now has a yellow lock symbol.
9. Double-click File1 to open it within Notepad. Type a line of your choice, click the **File** menu, and then click Save. Close Notepad when finished.
10. Right-click the **Start** menu and click **Sign out**.
11. Press **Ctrl+Alt+Delete** (or the Ctrl+Alt+Delete button within the Virtual Machine Connection window if you use Lab Environment 2) and then click **Other user**.
12. Supply a user name of **b.burtt@domainX.com** and password of **NewPassword555** and press **Enter** to log into the system.
13. Click **Start** and then click **File Explorer**.
14. In the navigation pane of File Explorer, expand **This PC, Local Disk (C:)** and highlight **MarketingMaterials**.
15. Double-click **File1** and note the error message. Click **OK** and close Notepad.
16. Click the **Home** tab, select the **New item** drop-down box, and click **Text Document**. Type **File3** and press **Enter** to create a File3.txt file within the MarketingMaterials folder.
17. Double-click **File3** to open it within Notepad. Type a line of your choice, click the File menu and then click **Save**. Close Notepad when finished.
18. Right-click **File3**, click **Properties**, and then click **Advanced**.
19. At the Advanced Attributes window, select **Encrypt contents to secure data** and click **OK**.

**(Take Screenshot)**

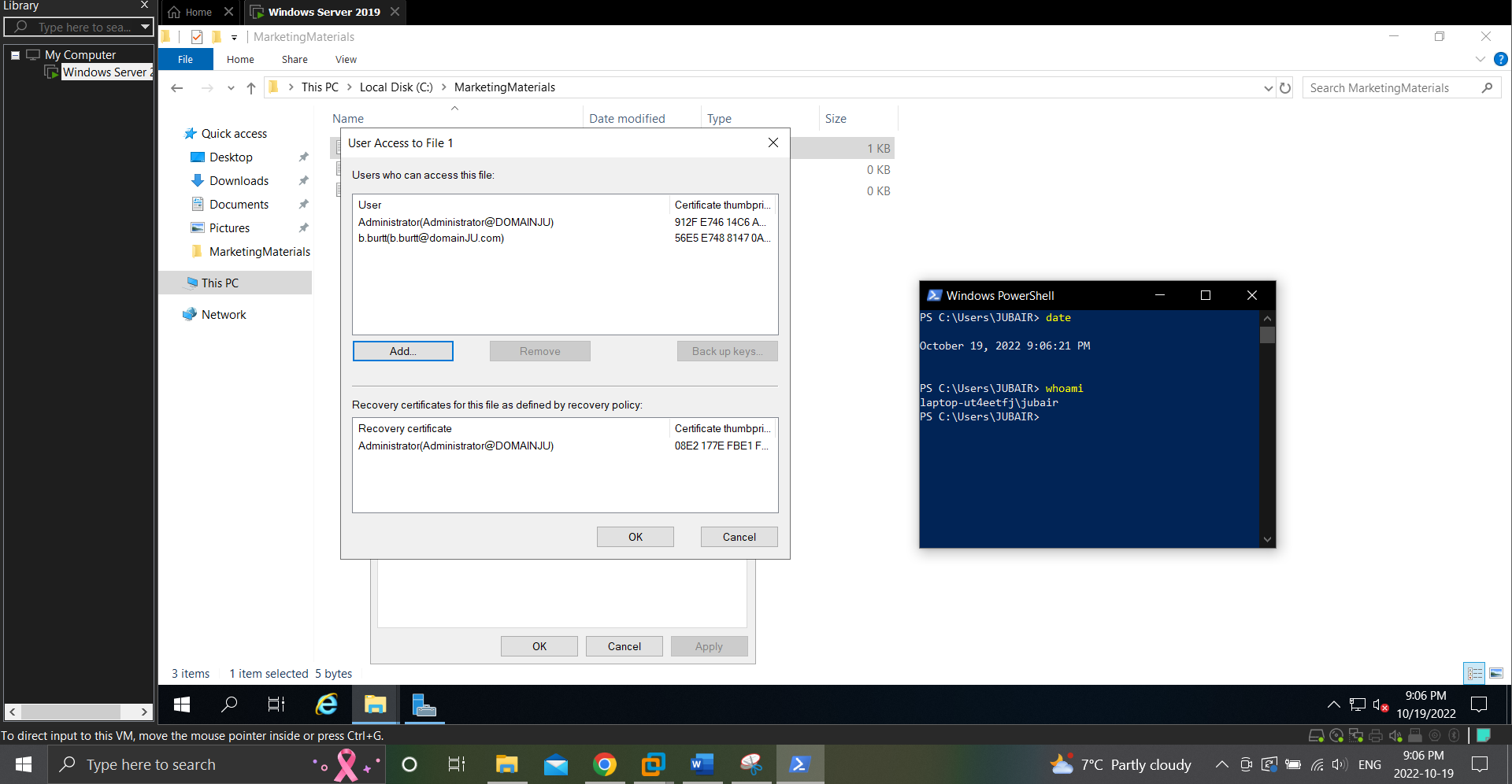


1. Click OK to close the **File3** Properties window. Select **Encrypt the file only** when prompted and click **OK**.
2. Right-click the **Start** menu and click **Shut down or sign out** and then click **Sign out**.
3. Press **Ctrl+Alt+Delete** (or the Ctrl+Alt+Delete button within the Virtual Machine Connection window if you use Lab Environment 2) and then click **Other user**.
4. Supply a user name of **administrator@domainX.com** and password of **Secret555** and press **Enter** to log into the system.
5. Click **Start** and then click **File Explorer**.
6. In the navigation pane of File Explorer, expand **This PC, Local Disk (C:)** and highlight

**MarketingMaterials**.

1. Double-click **File3** and note that you were able to access it even though Bob Burtt encrypted it. Close Notepad.
2. Right-click **File3**, click **Properties**, and then click **Advanced**.
3. At the Advanced Attributes window, click **Details**, note that Administrator is listed as a recovery agent within the domain by default, and click **OK**.
4. Click **OK** to close the Advanced Attributes window and click **OK** to close the File3 Properties window.
5. Right-click **File1**, click **Properties**, and then click **Advanced**.
6. At the Advanced Attributes window, click **Details**.
7. At the User Access to File1 window, click **Add**, select **b.burtt@domainX.com**, and click **OK** to allow Bob Burtt to access File1 using EFS.

**(Take Screenshot)**



1. Click **OK** to close the User Access to File1 window, click **OK** to close the Advanced

Attributes window, and click **OK** to close the File1 Properties window.

1. Close File Explorer.

***Project 6: Sharing Folders***

*In this Hands-On Project, you share folders using SMB.*

1. On your Windows Server 2019 host, click **Start** and then click **File Explorer.**
2. In the navigation pane of File Explorer, expand **This PC** and highlight **Local Disk (C:).**
3. Right-click the **MarketingMaterials** folder and click **Properties.**
4. Highlight the **Sharing** tab within the MarketingMaterials Properties window and click **Advanced Sharing.**
5. In the Advanced Sharing window, select **Share this folder** and note the default share name and number of simultaneous connections allowable.
6. Click **Permissions** and note that the Everyone group has Read shared folder permission by default. Select **Full Control** under the Allow column and click **OK**.
7. Click **Caching**, note that manual offline file caching is enabled by default, and click **OK**.
8. Click **OK** to close the Advanced Sharing window and click **Close** to close the MarketingMaterials Properties window.
9. Close File Explorer.
10. Right-click Start and click **Run**. Type **\\serverX\MarketingMaterials** in the Run dialog box and click **OK**. Note that you have access to File1, File2, and File3 using SMB. Optionally modify the content of each file, saving your changes when finished.
11. Within Hyper-V Manager on your Windows Server 2019 host, highlight **WindowsServer2019VM2** within the virtual machines pane and click **Connect** in the Actions pane. Click the **Ctrl+Alt+Delete** button within the Virtual Machine Connection window, supply the password **Secret555** for **administrator@domainX.com**, and press **Enter** to log into the system.
12. Click **Start** and then click **File Explorer**.
13. In the navigation pane of File Explorer, expand **This PC** and highlight **Local Disk (C:).**
14. Click the **Home** menu and then click **New folder**. Type **MarketingMaterials** and press **Enter**.
15. Right-click the **MarketingMaterials** folder and click **Properties**.
16. Highlight the **Security** tab within the MarketingMaterials Properties window and click **Advanced**.
17. At the Advanced Security Settings for MarketingMaterials window, click **Disable inheritance** and then click **Remove all inherited permissions from this object** when prompted. Click **OK** and then click **Yes** when prompted to close the Advanced Security Settings for MarketingMaterials window.
18. In the MarketingMaterials Properties window, click **Edit**.
19. At the Permissions for MarketingMaterials window, click **Add**. Type **Domain Admins** and click **OK**. Select **Full control** under the Allow permissions column. Click **Add** again. Type **Marketing-G** and click **OK**. Select **Modify** under the Allow permissions column, and click **OK**.
20. Highlight the **Sharing** tab within the MarketingMaterials Properties window and click **Advanced Sharing**.
21. In the Advanced Sharing window, select **Share this folder** and note the default share name and number of simultaneous connections allowable.
22. Click **Permissions** and note that the Everyone group has Read shared folder permission by default. Select **Full Control** under the Allow column and click **OK**.
23. Click **OK** to close the Advanced Sharing window and click **Close** to close the MarketingMaterials Properties window.
24. Right-click **Start** and click **Run**. Type **\\Server2019VM2\MarketingMaterials** in the Run dialog box, and click **OK**. Note that you have access to the shared folder on the server but there are no contents. We will use this shared folder in the following Hands-On Project.
25. Close File Explorer.

**Project 7: DFS**

*In this Hands-On Project, you configure a DFS namespace shared folder to provide access to the MarketingMaterials shared folder, as well as configure DFS replication for the MarketingMaterials shared folder available on your Windows Server 2019 host and WindowsServer2019VM2 virtual machine.*

1. On your Windows Server 2019 host, click **Start** and then click **Server Manager**. Within Server Manager, click the **Tools** menu and then click **DFS Management**.
2. In the navigation pane of the DFS Management tool, highlight **Namespaces** and note that no namespace shared folder exists by default. Click **New Namespace** within the Actions pane.
3. On the Namespace Server page of the New Namespace Wizard, type **server-X** within the Server text box and click **Next**.
4. On the Namespace Name and Settings page, type **warehouse** within the Name text box and click **Edit Settings**. Note the default path and permissions for the shared folder, click **OK**, and then click **Next**.
5. On the Namespace Type page, note the default options and UNC for the shared folder and click **Next**.
6. On the Review Settings and Create Namespace page, click **Create**.
7. On the Confirmation page, click **Close**.
8. In the navigation pane of the DFS Management tool, expand **Namespaces** (if necessary) and highlight **\\domainX.com\warehouse**.
9. Click **Properties** in the Actions pane.
10. In the \\domainX.com\warehouse Properties window, highlight the **Advanced** tab.
11. Select **Enable access-based enumeration for this namespace** and click **OK**.
12. Click **New Folder** within the Actions pane.
13. In the New Folder window, type **MarketingMaterials** within the Name text box.
14. Click **Add**, type **\\serverX\MarketingMaterials** within the text box, and click **OK**.
15. Click **Add**, type **\\Server2019VM2\MarketingMaterials** within the text box, and click **OK**.
16. Click **OK** to close the New Folder window. When prompted to configure a replication group (to keep the contents of the two shared folder locations within the MarketingMaterials target synchronized using DFS replication), click **Yes**.
17. At the Replication Group and Replicated Folder Name page of the Replicate Folder Wizard, note the default names and click **Next**.
18. At the Replication Eligibility page, click **Next**.
19. At the Primary Member page, select **SERVERX** from the Primary member drop-down box and click **Next**.
20. At the Topology Selection page, note the default option and click **Next**.
21. At the Replication Group Schedule and Bandwidth page, note the default options and click **Next**.
22. At the Replication Settings and Create Replication Group page, click **Create**.
23. At the Confirmation page, click **Close**. Click **OK** at the Replication Delay information window.
24. In the navigation pane of the DFS Management tool, expand **Replication** and highlight **Domain System Volume**. Note that the SYSVOL share (which provides Active Directory object replication using DFS) is shown within the DFS Management console because your system is a domain controller.
25. Under Replication in the navigation pane of the DFS Management tool, highlight **domainX.com\warehouse\marketingmaterials** and note the two paths and servers shown on the Memberships tab.
26. Highlight the **C:\MarketingMaterials** path for SERVERX and click **Properties** in the Actions pane. Highlight the **Staging** tab and note the default location and maximum size of the DFS staging folder. Click **Cancel** when finished.
27. Highlight the **Connections** tab, select **SERVERX**, and click **Replicate Now** in the Actions pane.
28. Click **OK** at the Replication Now window to perform the replication immediately and click **OK** to close the Resume Schedule Successful information window.

**(Take Screenshot)**

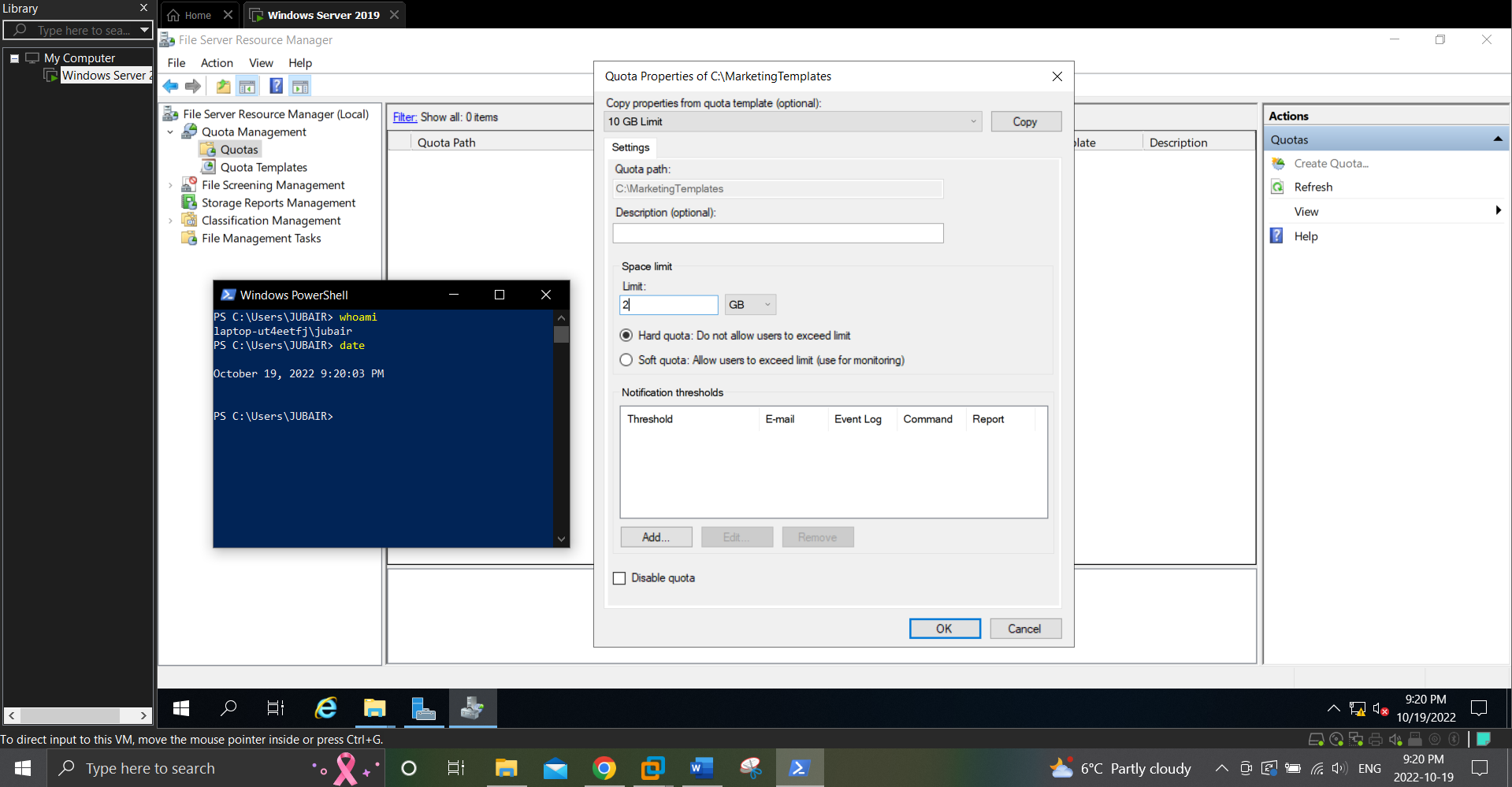
1. Click **Properties** in the Actions pane. Note that replication is enabled and uses remote differential compression. Highlight the **Schedule** tab and click **View** **Schedule**. Note that replication occurs at all times of the day. Click **Cancel** and click **Cancel** again when finished.
2. Close the DFS Management window.
3. Right-click **Start** and click **Run**. Type **\\domainX.com\warehouse** in the Run dialog box and click **OK**. Note that you have access to the MarketingMaterials as the target.
4. Double-click **MarketingMaterials** and note that you can access File1, File2, and File3. Optionally modify the content of each file, saving your changes when finished.
5. Right-click **Start** and click **Run**. Type **\\**Server2019VM2**\MarketingMaterials** in the Run dialog box, and click **OK**. Note that File2 is available because it was replicated from the MarketingMaterials share on serverX using DFS. (Note: to sync File1 and File3, encryption has to be disabled.)
6. Close File Manager.

**Project 8: Quotas and File Screens**

*In this Hands-On Project, you explore the configuration of user quotas, folder quotas, and file screens.*

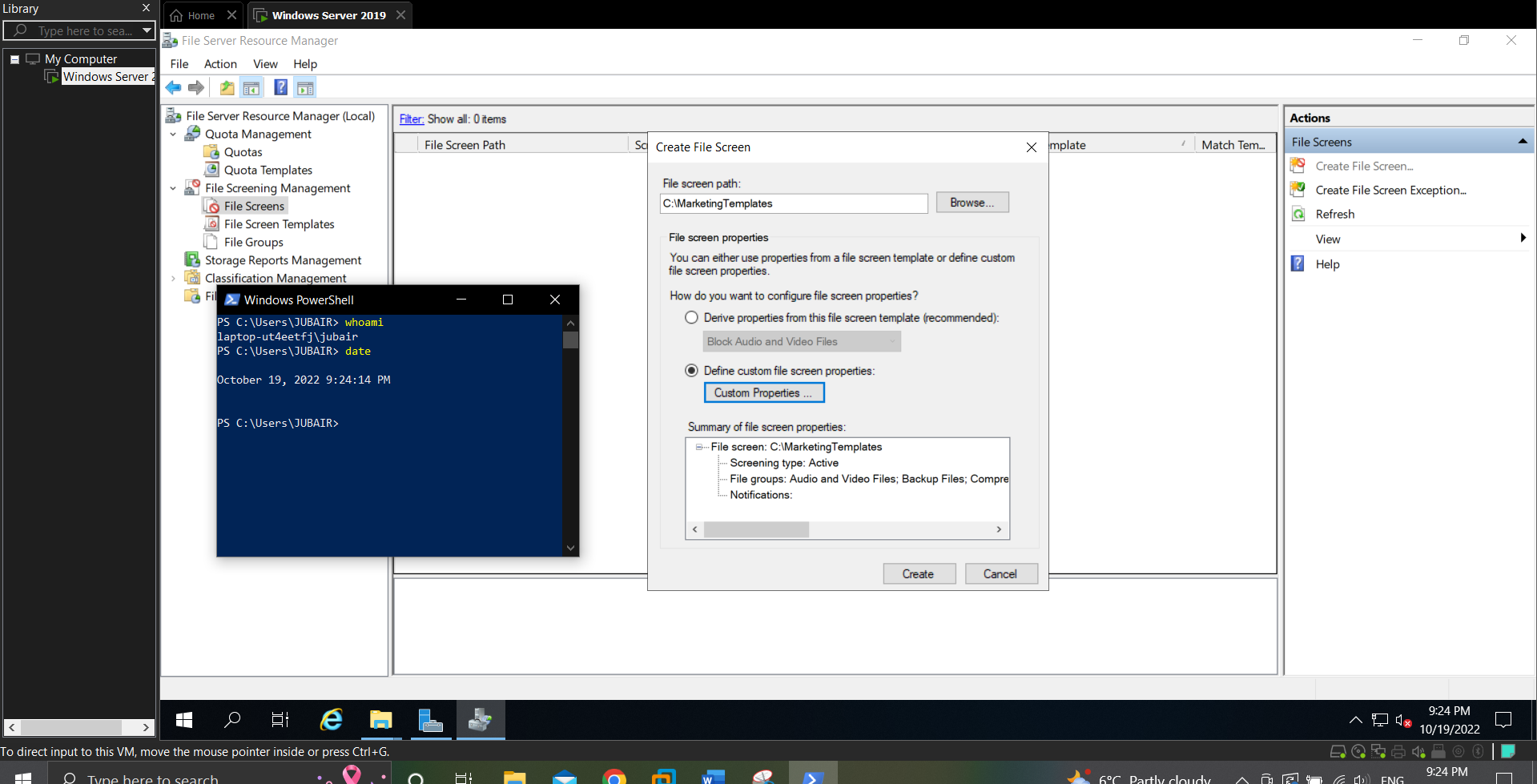
1. On your Windows Server 2019 host, click **Start** and then click **File Explorer**.
2. Create a new folder named **MarketingTemplates** under Local Disk(C:) drive.
3. Navigate inside MarketingTemplates folder and create a new text document and name it **file4.txt**.
4. In the navigation pane of File Explorer, expand **This PC**, right-click **Local Disk (C:),** and click **Properties.**
5. Highlight the **Quota** tab within the Local Disk (C:) Properties window and select **Enable quota management**. Note the default limit and warning level settings.
6. Select **Deny disk space to users exceeding quota limit, Log event when a user exceeds their quota limit**, and **Log event when a user exceeds their warning level**, and click **OK**.
7. At the Disk Quota window, note the warning and click **OK**.
8. Click **OK** to close the Local Disk (C:) Properties window.
9. Click **Start** and then click **Server Manager**. Within Server Manager, click the **Tools** menu and then click **File Server Resource Manager**.
10. In the navigation pane of the File Server Resource Manager tool, expand **Quota** **Management** and highlight **Quota Templates**. Note the default templates available, including their limits and type.
11. Highlight Quotas in the navigation pane and click **Create Quota** in the Actions pane.
12. At the Create Quota window, type **C:\MarketingTemplates** in the Quota path text box, select **Define custom quota properties**, and click **Custom Properties**.
13. At the Quota Properties of c:\MarketingTemplates window, select **2 GB Limit** from the Copy properties from quota template (optional) drop-down box and click **Copy**. Note the default quota type and warning thresholds and click **OK**.

**(Take Screenshot)**



1. Click **Create**.
2. At the Save Custom Properties as a Template window, type **Marketing Quota** in the Template name text box and click **OK**.
3. Expand **File Screening Management** and highlight **File Groups**. Note the default file groups available, including the related file extensions.
4. Highlight **File Screen Templates** in the navigation pane and note the default templates available, including their screening type and the file groups that they contain.
5. Highlight **File Screens** in the navigation pane and click **Create File Screen** in the Actions pane.
6. At the Create File Screen window, type **C:\MarketingTemplates** in the Quota path text box, select **Define custom file screen properties** and click **Custom Properties**.
7. At the File Screen Properties of c:\MarketingTemplates window, note that Active screening is the default type. Within the File groups section, select all file groups except for Office Files and click **OK.**

**(Take Screenshot)**



1. Click **Create**.
2. At the Save Custom Properties as a Template window, type **Marketing Screen** in the Template name text box and click **OK**.
3. Close the File Server Resource Manager and Server Manager windows.
4. In the navigation pane of File Explorer, expand **This PC**, expand **Local Disk (C:)**, and highlight **MarketingTemplates**. Note that File4.txt is available within the folder as it was created prior to applying the file screen. Click the **Home** menu and then click **New item, Text Document**. Note the error that you receive and click **Cancel**. Close File Manager when finished.