**Project 1: Cleanup Tasks**

*In this Hands-On Project, you perform cleanup tasks on your WindowsServer2019VM2 virtual machine to remove the WindowsServer2019VM2 configuration performed during the Module 8 Hands-On Projects. More specifically, you remove the DHCP, DNS, and WINS servers, as well as the second network interface.*

1. Boot your **Windows Server 2019 host** and log into domainX.com as Administrator using

the password **Secret555**. Next, click **Start** and then click **Server Manager**.

1. In Server Manager on your Windows Server 2019 host, select the **Tools** menu and then click **Hyper-V Manager**.

a. 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.

b. 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.

1. In Server Manager, click the **Tools** menu and then click **DHCP**.
2. In the navigation pane of the DHCP tool, highlight **Scope [192.168.0.0] Marketing LAN** and click **More Actions**, **Deconfigure** **Failover** in the Actions pane. Click **OK**. Click **OK** again to remove the failover configuration. Click Close and then **close** the DHCP tool when finished.
3. On your WindowsServer2019VM2 virtual machine, click **Start** and then click **Server**

**Manager**. Next, click the **Manage** menu and then click **Remove Roles and Features.**

a. At the Select destination server page, click **Next**.

b. At the Remove server roles page, de-select **DHCP** **Server** and click **Remove Features** when prompted. Next, de-select **DNS Server** and click **Remove Features** when prompted. Click **Next** when finished.

d. On the Confirm removal selections page, click **Remove** to remove the DHCP and DNS servers.

e. At the Removal progress page, click **Close**.

f. Restart your WindowsServer2019VM2 virtual machine.

**Project 2: Configuring a VPN Server**

*In this Hands-On Project, you configure your Windows Server 2019 host as a VPN server and DHCP relay agent to allow access to the 172.16.0.0/24 network.*

1. In Server Manager on your Windows Server 2019 host, click the **Manage** menu and then click **Add Roles and Features**.

a. At the Select installation type page, click **Next**.

b. At the Select destination server page, click **Next**.

c. At the Select server roles page, select **Remote Access** and click **Next**.

d. At the Select features page, click **Next**.

e. At the Remote Access page, click **Next**.

f. At the Select role services page, select **DirectAccess and VPN (RAS)** and click **Add Features** when prompted. Next, select **Routing** and click **Next**.

g. At the Confirm installation selections page, click **Install**.

h. At the Installation progress page, click **Open the Getting Started Wizard** and then click Close to **close** the Add the Roles and Features Wizard.

1. At the Configure Remote Access wizard, click **Deploy VPN only** to open the Routing and Remote Access tool.
2. Close the Configure Remote Access window and click **OK** when prompted.
3. In the navigation pane of the Routing and Remote Access tool, right-click **SERVERX** and click **Configure and Enable Routing and Remote Access**.

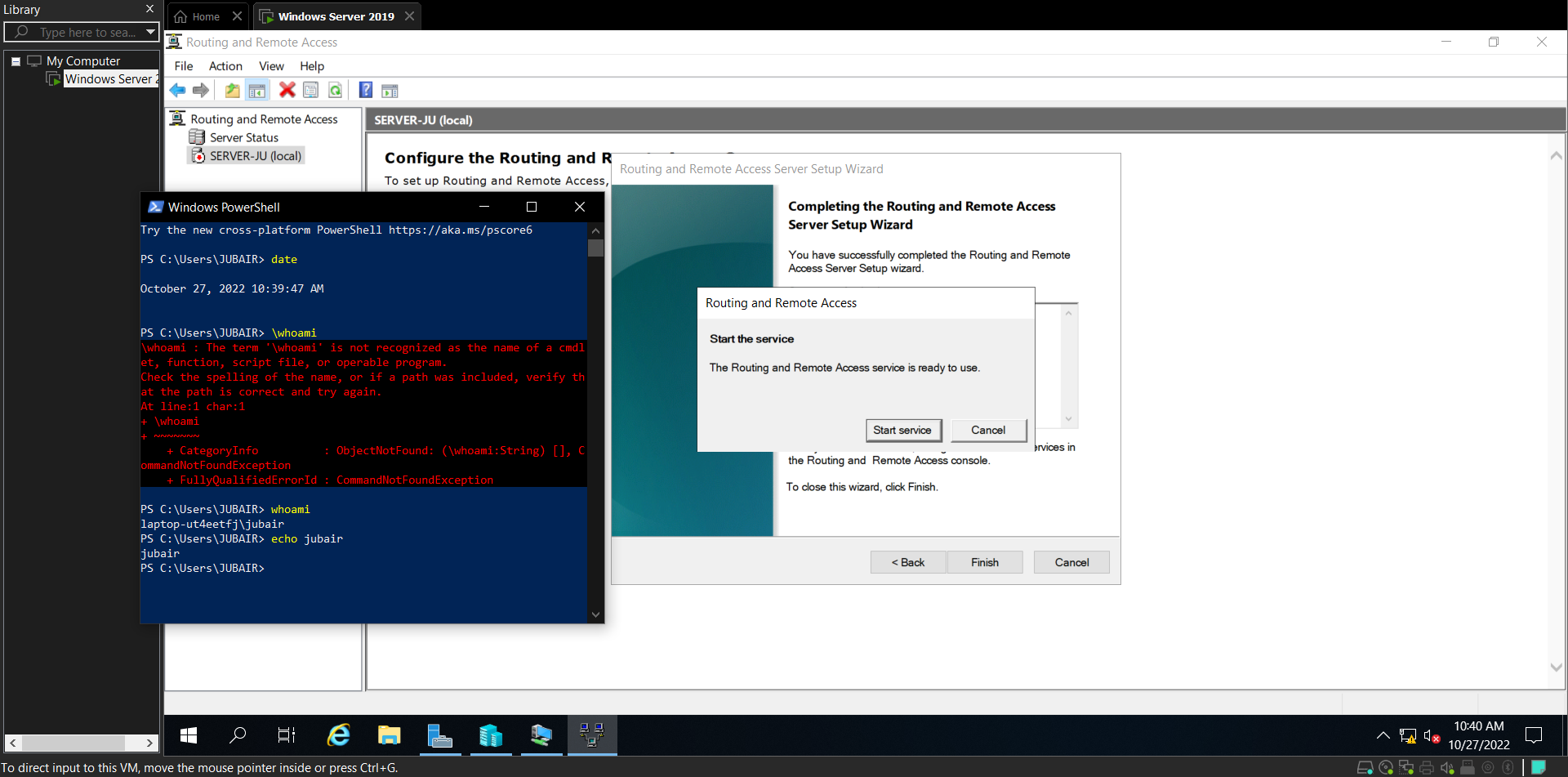
a. At the first page of the Routing and Remote Access Server Setup Wizard, click **Next**.

b. At the Configuration page, select **Custom configuration** and click **Next**.

c. At the Custom Configuration page, select **VPN access**. Next select **LAN routing** and click **Next**.

d. Click **Finish**. Next, click **Start service** to start the Routing and Remote Access service.

**(Take Screenshot)**



1. Right-click **Ports** in the navigation pane and click **Properties**. Note the default number of ports configured for each VPN type by default and click **OK**.
2. Right-click **SERVERX** in the navigation pane and click **Properties**. On the General tab, note that your server is configured for IPv4 routing and remote access.

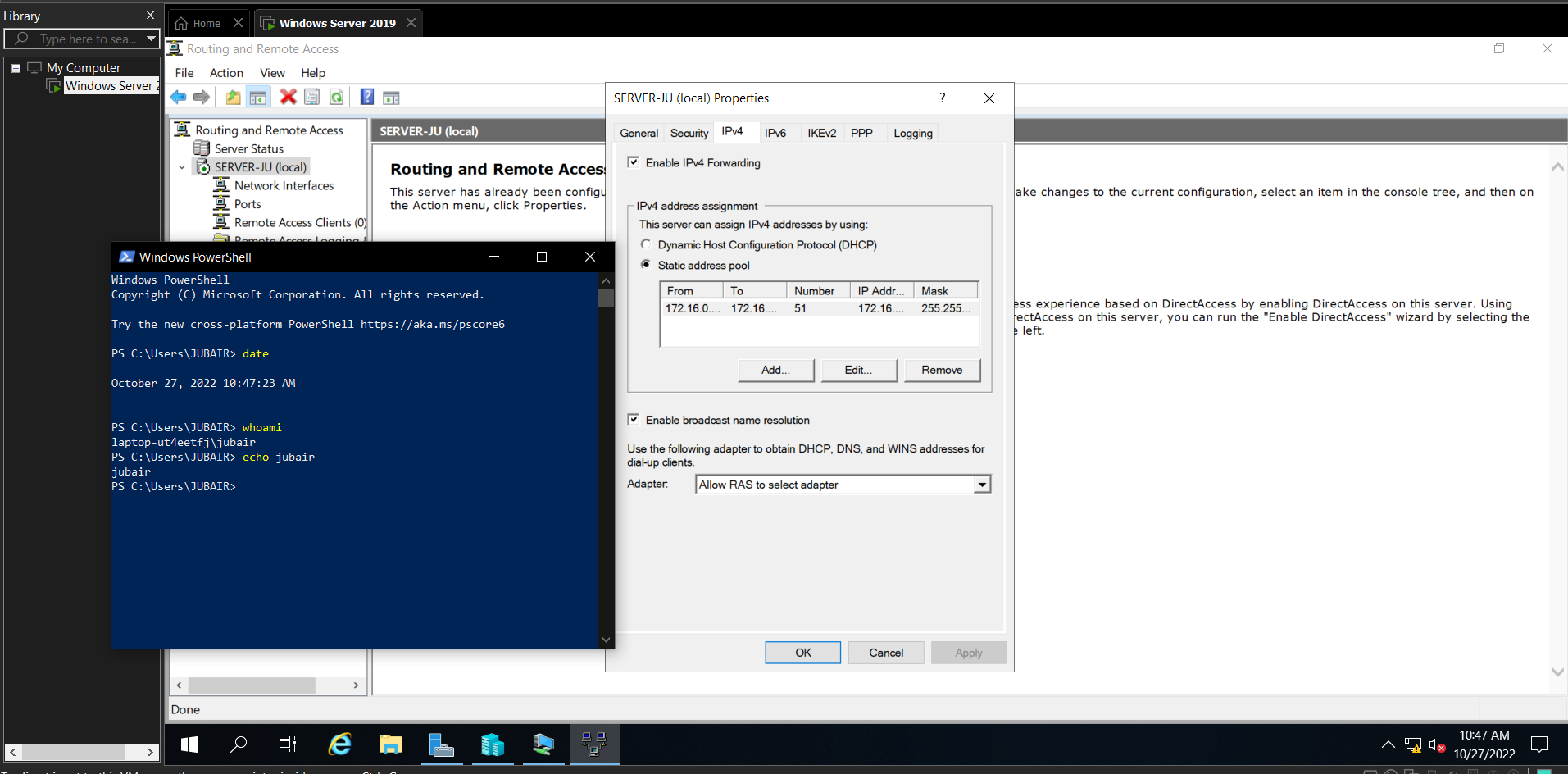
a. Highlight the **Security** tab. Note that your VPN server is configured to use Windows Authentication to authenticate remote access clients by default.

b. Click the **Authentication Methods** button. Note that EAP and MS-CHAP v2 authentication methods are enabled by default, and click **OK**.

c. Highlight the **IPv4** tab. Under IPv4 address assignment, select **Static address pool.** Click **Add** and enter 172.16.0.50 – 172.16.0.100 in the address range dialog. Click **OK**.

d. Click **OK**.

**(Take Screenshot)**



1. In Server Manager, click the **Tools** menu and then **click Active Directory Users and Computers**.

a. Highlight the **Users** folder under domainX.com in the navigation pane.

b. Right-click the **Administrator** user account and click **Properties**.

c. Highlight the Dial-in tab, select **Allow access**, and click **OK**.

d. Close the Active Directory Users and Computers tool.

**Project 3: Connecting to a VPN**

*In this Hands-On Project, you connect to the VPN server on your Windows Server 2019 host from your WindowsServer2019VM2 virtual machine. Following this, you enable split tunneling on the VPN connection.*

1. On your WindowsServer2019VM2 virtual machine, right-click **Start** and click **Network** **Connections**.
2. In the navigation pane of the Settings window, highlight **VPN** and click **Add a VPN connection**.

a. Select **Windows (built-in)** from the VPN provider drop-down box.

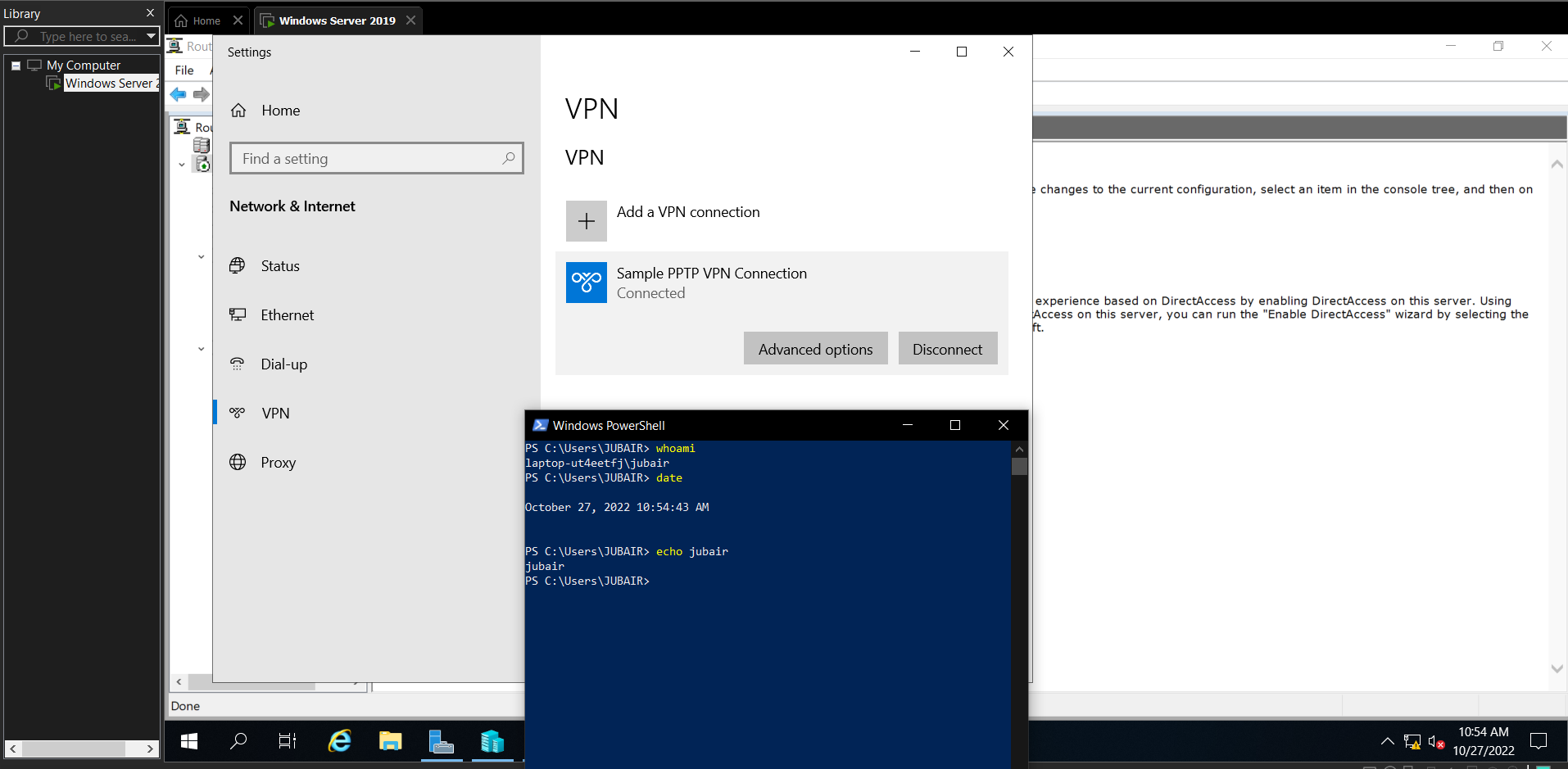
b. Type **Sample PPTP VPN Connection** in the Connection name text box.

c. Type the IP address of your Windows Server 2019 host (192.168.0.10) in the Server name or address box.

d. Select **Point to Point Tunneling Protocol (PPTP)** from the VPN type drop-down box and click Save.

1. Click **Sample PPTP VPN Connection** and then click **Connect**. Type **administrator@domainX.com** in the User name text box, type **Secret555** in the Password text box, and click **OK**. Note that your VPN displays a Connected status.

**(Take Screenshot)**



1. Right-click **Start** and click **Windows PowerShell**. At the Windows PowerShell prompt, type **ipconfig /all** and press **Enter**. Note that you have two network interfaces:

• Ethernet adapter Ethernet should list the IP configuration for your network connection to the External Virtual Switch.

• PPP adapter Sample PPTP VPN Connection should contain an IP address on the 172.16.0.0/16 network that was obtained from the DHCP server on your Windows Server 2019 host via the DHCP relay agent. This IP address represents the client side of the PPTP VPN tunnel. Also note that the default gateway for this network interface is set to 0.0.0.0 to ensure that all traffic passes through the VPN connection.

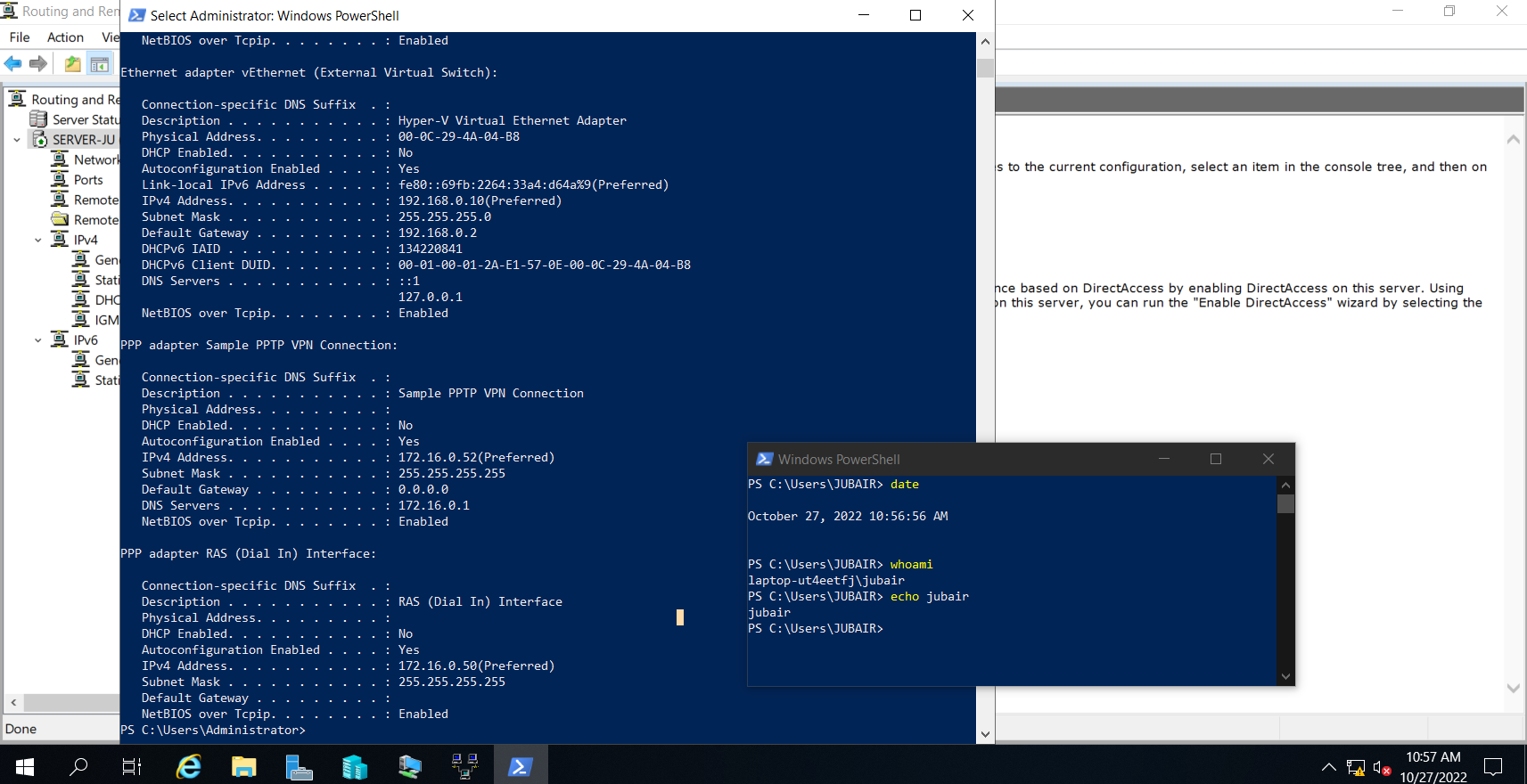
1. On your Windows Server 2019 host, right-click **Start** and click **Windows PowerShell**. At the Windows PowerShell prompt, type **ipconfig /all** and press **Enter**. Note that you have three network interfaces:

• Ethernet adapter vEthernet (External Virtual Switch) should list the IP configuration for your network connection to the External Virtual Switch.

• Ethernet adapter vEthernet (Internal Virtual Switch) should list the IP address 172.16.0.1 that was manually configured for your network connection to the Internal Virtual Switch.

• PPP adapter RAS (Dial In) Interface should contain an IP address on the 172.16.0.0/16 network that matches the server side of the PPTP VPN tunnel to allow VPN clients the ability to connect to the VPN server. Note this IP address for the following step.

**(Take Screenshot)**



1. On your WindowsServer2019VM2 virtual machine, right-click **Start** and click **Run**.

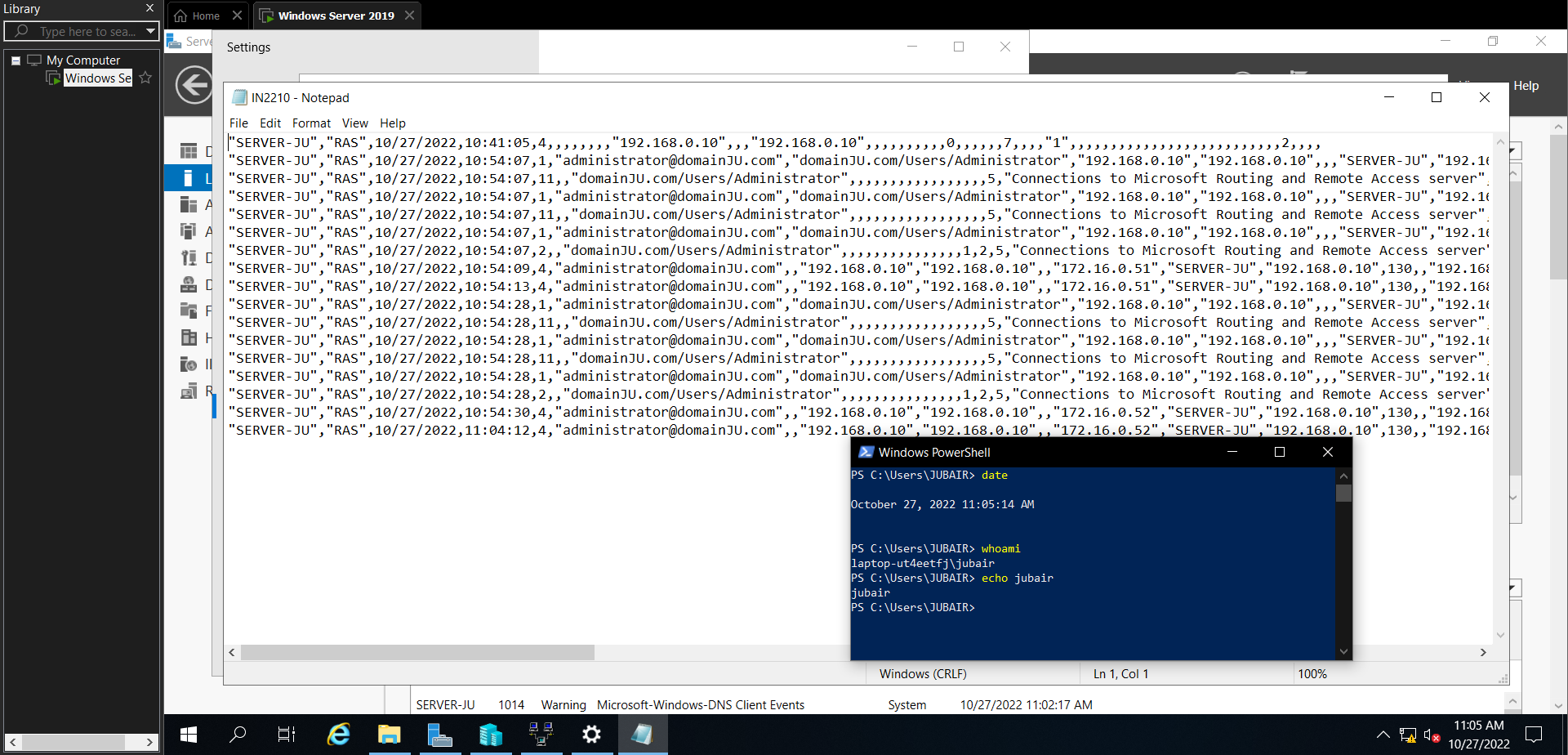
a. Type **\\IPaddress\MarketingMaterials** in the Run dialog box and click **OK**, where IPaddress is the IP address of your Windows Server 2019 host on the External Virtual Switch. Note that you can continue to access the MarketingMaterials SMB shared folder on your Windows Server 2019 host using an unencrypted connection, as you have previously. Close the File Explorer window.

b. Right-click **Start** and click **Run**. Type **\\IPaddress\MarketingMaterials** in the Run dialog box and click **OK**, where IPaddress is the IP address of your Windows Server 2019 host on the PPP adapter RAS (Dial In) Interface from Step 5. Note that you can now access the MarketingMaterials SMB shared folder on your Windows Server 2019 host using an encrypted connection through the VPN tunnel. Close the File Explorer window.

c. Right-click **Start** and click **Run**. Type **\\172.16.0.1\MarketingMaterials** in the Run dialog box and click **OK.** Note that the VPN server allows you to access existing hosts on the 172.16.0.0/24 network via the VPN tunnel. Close the File Explorer window.

1. In the Routing and Remote Access tool on your Windows Server 2019 host, highlight **Ports** in the navigation pane. Note that you have one active PPTP port. Right-click this port, click **Status**, and note the statistics and VPN client IP address. Click **Disconnect** to close the VPN tunnel and then click **Close** to close the Port Status window.
2. Open File Explorer and navigate to the **C:\Windows\system32\logfiles** folder. Double-click the **INDDMM.log** file (where DD is the day of the month, and MM is the month of the year) to open it in Notepad. View the entries for your VPN connection and note that EAP-MSCHAP v2 was used as the authentication method. Close Notepad when finished.

**(Take Screenshot)**



1. In the Settings window on your WindowsServer2019VM2 virtual machine, click **Network and Sharing Center** under the Related settings section.

a. Click **Change adapter settings** to open the Network Connections section of Control Panel.

b. Right-click **Sample PPTP VPN Connection**, click **Properties**, and highlight the **Networking** tab.

c. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

d. Click **Advanced**.

e. Deselect **Use default gateway on remote network** and click **OK**.

f. Click **OK** to close the Internet Protocol Version 4 (TCP/IPv4) Properties window.

g. Click **OK** to close the Sample PPTP VPN Connection Properties window.

1. Right-click **Sample PPTP VPN Connection** in the Network Connections window and click **Connect / Disconnect**. Next, click **Sample PPTP VPN Connection** and click **Connect**.
2. Right-click **Start** and click **Run**. Type **\\172.16.0.1\MarketingMaterials** at the Run dialog box and click **OK**. Note that you have access to hosts on the 172.16.0.0/24 network via the VPN tunnel. Close the File Explorer window.
3. In the Windows PowerShell window, type **ipconfig /all** and press **Enter**. Note that Sample PPTP VPN Connection does not have a default gateway listed. As a result, the default gateway on the Ethernet network interface will be used for any traffic that is not destined for the 172.16.0.0/16 network on the remote access client.
4. 13. Right-click **Sample PPTP VPN Connection** in the Network Connections window and click **Connect / Disconnect**. Next, click **Sample PPTP VPN Connection** and click **Disconnect**. Close the Network Connections window when finished.

**Project 4: RADIUS**

*In this Hands-On Project, you install and configure the Network Policy and Access Services role on your Windows Server 2019 host, as well as configure a remote access policy for Marketing department users. To test the application of this remote access policy, you configure its settings to disconnect active users after 1 minute and view the results.*

1. In Server Manager on your Windows Server 2019 host, click the **Manage** menu and then click **Add Roles and Features**.

a. At the Select installation type page, click **Next**.

b. At the Select destination server page, click **Next**.

c. At the Select server roles page, select **Network Policy and Access Services** and click **Add Features** when prompted. Click **Next**.

d. At the Select features page, click **Next**.

e. At the Network Policy and Access Services page, click **Next**.

f. At the Confirm installation selections page, click **Install**.

g. At the Installation progress page, click **Close** to close the Add the Roles and Features Wizard.

1. In the navigation pane of the Routing and Remote Access tool, right-click **SERVERX**, click **Properties**, and highlight the **Security** tab. Note that your remote access server is automatically configured to use RADIUS for authentication and logging because the Network Policy and Access Services role was installed on the same computer. Click **OK** when finished.
2. In Server Manager, click the **Tools** menu and then click **Network Policy Server**.
3. In the navigation pane of the Network Policy Server tool, right-click **NPS (Local)** and note that the Register server in Active Directory is unavailable. This is because the RADIUS server is installed on a domain controller and automatically registered as a result. Press **Escape**.
4. Expand **Policies** in the navigation pane and highlight **Network Policies**. Note the two default remote access policies that deny dial-in permission for all VPN (Routing and Remote Access server) requests and requests from other servers.
5. Right-click **Network Policies** and click **New** to open the New Network Policy wizard.

a. At the Specify Network Policy Name and Connection Type page, type **Marketing Remote Access Policy** in the Policy name text box. From the Type of network access server drop-down box, select **Remote Access Server (VPN-Dial up)** and click **Next**.

b. At the Specify Conditions page, click **Add**.

i. Highlight **User Groups** and click **Add**.

ii. Click **Add Groups**.

iii. Type **Marketing-G** in the Select Group dialog box and click **OK**.

iv. Click **OK** to close the Windows Groups window.

v. Click **Next**.

c. At the Specify Access Permission page, note the default option that allows dial-in permission and click **Next**.

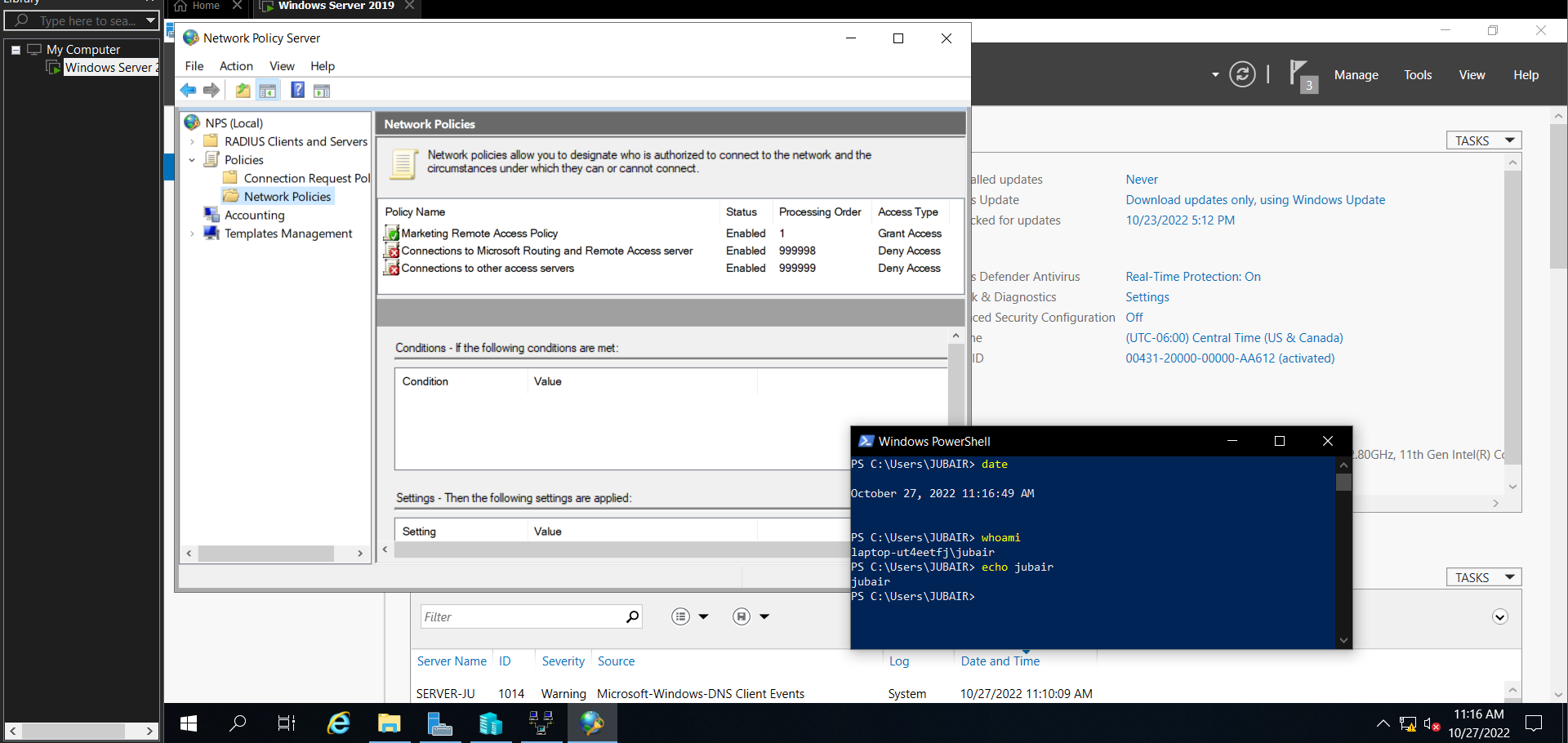
d. At the Configure Authentication Methods page, note the default authentication methods chosen and click **Add**. Select **Microsoft: Secure password (EAP-MSCHAP v2)** and click **OK**. Click **Next**.

e. At the Configure Constraints page, select **Session Timeout**, check the **Disconnect after the following maximum session time** option and note the default value of 1 minute. Click **Next**.

f. At the Configure Settings page, select **IP Settings** and note the default value that obtains IP configuration using the method specified on the remote access server. Click **Next**.

g. Click **Finish**. Note that the Processing Order for the Marketing Remote Access Policy is listed as 1 to ensure that it is processed before the two default remote access policies.

**(Take Screenshot)**



1. Highlight Accounting in the navigation pane and note that remote access connections are logged to the C:\Windows\system32\LogFiles folder by default.

a. Click **Change Log File Properties** and highlight the **Log File tab**. Note the file name format of INyymm.log.

b. Select **Daily** and note the new file name format of INyymmdd.log.

c. Click **OK** to close the Log File Properties window.

1. On your WindowsServer2019VM2 virtual machine, right-click **Start** and click **Network Connections.**

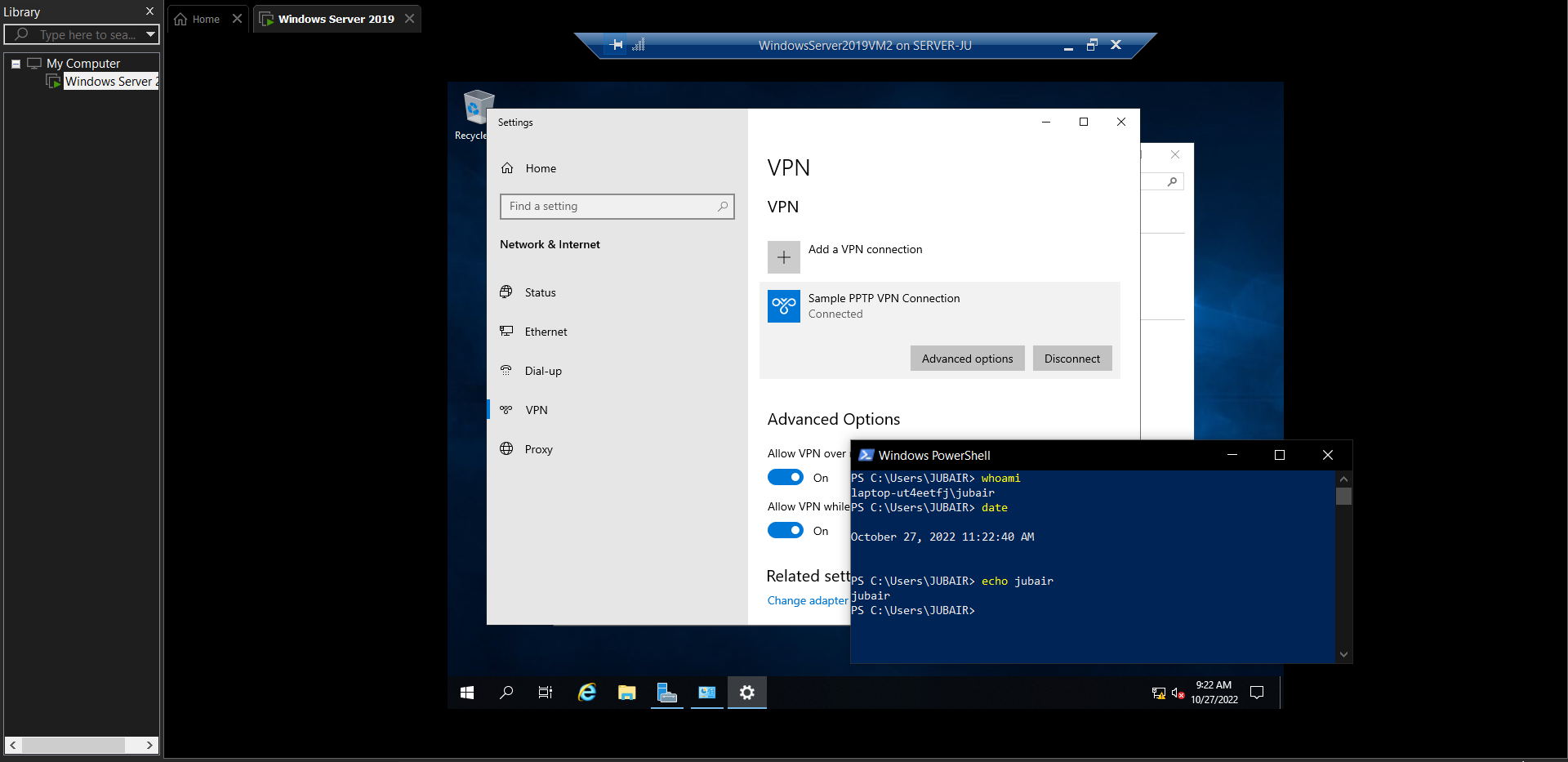
a. In the navigation pane of the Settings window, highlight **VPN**.

b. Click **Sample PPTP VPN Connection** and then click **Advanced options**.

c. Click Clear **sign-in info** and then click the **back arrow** in the upper left of the Settings window.

d. Click **Sample PPTP VPN Connection** and then click **Connect**. Type **b.burtt@ domainX.com** in the User name text box, type **Secret555** in the Password text box, and click **OK**. Note that your VPN displays a Connected status.

**(Take Screenshot)**



e. Wait for 1 minute. Note that your VPN is automatically disconnected using the session timeout value you specified in your remote access policy.

f. Close the Settings window.

1. On your Windows Server 2019 host, open **File Explorer** and navigate to the **C:\Windows\system32\logfiles folder**. Note that you now have a **INddmmyy.log** file (where dd is the day of the month, and mm is the month of the year, and yy is the year) that was created by your RADIUS server using the daily log format. Double-click this file to open it in Notepad. Note the recent VPN connection from user **b.burtt@domainX.com** and close Notepad when finished.

**(Take Screenshot)**

