Module 8: Implementing VPNs

Lab: Implementing VPN

(VMs: 20741B-LON-DC1, 20741B-EU-RTR, 20741B-INET1, 20741B-LON-CL1)

Exercise 1: Implementing VPN

Task 1: Verify certificate requirements for IKEv2 and SSTP

Prepare the environment

1. On **LON-DC1**, right-click **Start**, and then click **Windows PowerShell (Admin)**.
2. At the **Windows PowerShell** command prompt, type the following command, and then press Enter: ***cd E:\Labfiles\Mod08***
3. At the **Windows PowerShell** command prompt, type the following command, and then press Enter: ***.\mod8.ps1***
4. Wait for the script to complete, which should take approximately 20 seconds.

Request a certificate for EU-RTR

1. On **EU-RTR**, click **Start**, and then type **Command Prompt**. In the results pane, click **Command Prompt**.
2. At the command prompt, type the following command, and then press Enter: ***mmc***
3. In the **Console** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, click **Certificates**, and then click **Add**.
5. In the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**.
6. In the **Select Computer** dialog box, click **Local computer**, click **Finish**, and then click **OK**.
7. In the **Certificates** snap-in, in the console tree of the **Certificates** snap-in, navigate to **Certificates (Local Computer)\Personal**.
8. Right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
9. On the **Before you begin** page, click **Next**, and then, on the **Select Certificate Enrollment Policy** page, click **Next**.
10. On the **Request Certificates** page, click **Adatum Web Server**, and then click **More information is required to enroll for this certificate. Click here to configure settings.**
11. In the **Certificate Properties** dialog box, on the **Subject** tab, under **Subject name**, under **Type** select **Common name**.

12. In the **Value** text box, type ***131.107.0.10*** and then click **Add**.
13. Click **OK**, click **Enroll**, and then click **Finish**.
14. In the **Certificates** snap-in, expand **Personal** and click **Certificates**, and then, in the **details** pane verify that a new certificate with the name ***131.107.0.10*** is enrolled with **Intended Purposes** of **Server Authentication**.
15. Close the console window.
16. When you receive a prompt to save the settings, click **No**.

Change the HTTPS bindings

1. On **EU-RTR**, open **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Internet Information Services (IIS) Manager**, expand **EU-RTR (ADATUM\Administrator)**.
3. In the **Internet Information Services (IIS) Manager**, in the console tree, expand **Sites**, and then click **Default Web site**.
4. In the **Actions** pane, click **Bindings**, and then click **Add**.
5. In the **Add Site Binding** dialog box, under the **Type** select **https**, in the **SSL Certificate** list, click the **131.107.0.10** certificate, click **OK**, and then click **Close**.
6. Close the **Internet Information Services (IIS) Manager** console.

Task 2: Review the default VPN configuration

1. On **EU-RTR**, in the **Server Manager**, click **Tools**, and then click **Routing and Remote Access**.
2. Maximize the **Routing and Remote Access** window, right-click **EU-RTR (local)**, and then select **Disable Routing and Remote Access**.
3. When you receive a prompt, in the **Routing and Remote Access** dialog box, click **Yes**.
4. Right-click **EU-RTR (local)**, and then select **Configure and Enable Routing and Remote Access**.
5. On the **Welcome to Routing and Remote Access Server Setup Wizard**, click **Next**.
6. On the **Configuration** page, select **Custom configuration**, and then click **Next**.
7. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then click **Next**.
8. On the **Completing the Routing and Remote Access Server Setup Wizard** page, click **Finish**.

9. When you receive a prompt, in the **Routing and Remote Access** dialog box, click **Start service**.
10. Expand **EU-RTR (local)**, right-click **Ports**, and then click **Properties**.
11. In the **Ports Properties** dialog box, verify that five ports exist for Secure Socket Tunneling Protocol (SSTP), Internet Key Exchange version 2 (IKEv2), Point to Point Tunneling Protocol (PPTP), and Layer Two Tunneling Protocol (L2TP).
12. Double-click **WAN Miniport (SSTP)**. In the **Maximum ports** text box, type ***4*** and then click **OK**.
13. In the **Routing and Remote Access** message box, click **Yes**.
14. Repeat steps 12 and 13 for **IKEv2**, **PPTP**, and **L2TP**.
15. To close the **Ports Properties** dialog box, click **OK**.
16. Right-click **EU-RTR (local)**, and then click **Properties**.
17. In the **EU-RTR (local) Properties** dialog box, on the **General** tab, verify that **IPv4 Remote access server** is selected.
18. Click the **Security** tab, click the drop-down arrow next to **Certificate**, and then select **131.107.0.10**.
19. Click **Authentication Methods**, verify that **EAP** is selected as the authentication protocol, and then click **OK**.
20. Click the **IPv4** tab, and then verify that the VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
21. Click the drop-down arrow next to **Adapter**, and then select **London_Network**.
22. To close the **EU-RTR (local) Properties** dialog box, click **OK**, and then, when you receive a prompt click **Yes**.

Task 3: Configure the Remote Access policies

1. On **EU-RTR**, in **Server Manager**, on the **Tools** menu, click **Network Policy Server**.
2. In the **Network Policy Server** console, in the **navigation** pane, expand **Policies**, and then click **Network Policies**.
3. In the navigation pane, right-click **Network Policies**, and then click **New**.
4. In the **New Network Policy Wizard**, in the **Policy name** text box, type: ***Adatum IT VPN***
5. In the **Type of network access server** list, click **Remote Access Server(VPN-Dial up)**, and then click **Next**.

6. On the **Specify Conditions** page, click **Add**.
7. In the **Select condition** dialog box, click **Windows Groups**, and then click **Add**.
8. In the **Windows Groups** dialog box, click **Add Groups**.
9. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** text box, type ***IT*** click **Check Names**, and then click **OK**.
10. Click **OK** again, and then click **Next**.
11. On the **Specify Access Permission** page, verify that **Access granted** is selected, and then click **Next**.
12. On the **Configure Authentication Methods** page, clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
13. To add **EAP Types**, click **Add**.
14. On the **Add EAP** page, click **Microsoft Secured password (EAP-MSCHAP v2)**, and then click **OK**.
15. To add **EAP Types**, click **Add**.
16. On the **Add EAP** page, click **Microsoft: Smart Card or other certificate**, click **OK**, and then click **Next**.
17. On the **Configure Constraints** page, click **Next**.
18. On the **Configure Settings** page, click **Next**.
19. On the **Completing New Network Policy** page, click **Finish**.
20. Close all open windows.

Results*: After completing this exercise, you should have modified the Remote Access server configuration successfully to provide VPN connectivity.*

Exercise 2: Validating the VPN deployment

Task 1: Remove the client computer from the domain

1. Switch to **LON-CL1**.
2. Right-click **Start**, and then click **System**.
3. In the **System** window, click **Advanced system settings**, and then click the **Computer Name** tab.
4. On the **Computer name** tab, click **Change**.
5. In the **Computer Name/Domain Changes** dialog box, click **Workgroup**, in the **Workgroup** text box type ***WORKGROUP*** and then click **OK**.
6. In the **Computer Name/Domain Changes** dialog box, click **OK**.
7. In the **Welcome to the WORKGROUP workgroup** dialog box, click **OK**.
8. To restart the computer, click **OK**.

9. To close **System Properties** dialog box, click **Close**.
10. Click **Restart Now**.

Task 2: Move LON-CL1 to the Internet

1. When the **LON-CL1** computer has restarted, sign in by using the user name ***Admin*** and the password ***Pa55w.rd***
2. If you receive a prompt in the **Networks** dialog box, click **Yes**.
3. Right-click **Start**, and then click **Network Connections**.
4. In the **Network Connections** window, right-click **London_Network**, and then click **Disable**.
5. Right-click **Internet**, and then click **Enable**.
6. Right-click **Internet**, and then click **Properties**.
7. In the **Internet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
8. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, ensure that the following settings display, and then click **OK**:

IP address: **131.107.0.20**
Subnet mask: **255.255.255.0**
Preferred DNS server: **131.107.0.100**

9. In the **Internet Properties** dialog box, click **Cancel**.
10. Close all open windows.
11. On the taskbar, click the **File Explorer** icon.
12. In File Explorer, in the address bar, type ***Lon-DC1*** and then press Enter. Notice that a Network Error message displays.
13. Close all open windows.

Note: *The client is unable to open the resources, because it is not on the internal network.*

Task 3: Configure a VPN connection and verify connectivity

Create a VPN profile

1. On **LON-CL1**, right-click **Start**, and then click **Control Panel**.
2. In **Control Panel**, click **Network and Internet**, and then click **Network and Sharing Center**.
3. In **Network and Sharing Center**, click **Set up a new connection or network**.
4. In the **Choose a connection option** window, click **Connect to a workplace**. Click

Next.
5. On the **How do you want to connect?** page, click **Use my Internet connection (VPN)**.
6. On the **Do you want to set up an Internet connection before continuing?** page, click **I´ll set up an Internet connection later**.
7. On the **Type the Internet address to connect to** page, configure the following settings, and then click **Create**:

Internet address: ***131.107.0.10***
Destination name: ***A. Datum VPN***
Select: **Allow other people to use this connection**
Deselect: **Remember my credentials**

8. In **Network and Sharing Center**, click **Change adapter settings**.
9. In the **Network Connections** window, right-click **A. Datum VPN**, and then select **Connect / Disconnect**.
10. On the **VPN** page, select **A. Datum VPN**, and then click **Connect**.
11. In the **Sign in** dialog box, in the **User name** text box, type ***Adatum\Logan*** in the **Password** text box, type ***Pa55w.rd*** and then click **OK**.
12. Switch to the **Network Connections** window.
13. In the **Network Connections** window, verify that **WAN Miniport (PPTP)** displays under **A. Datum VPN**.

Note: *By default, the client will attempt to connect to the VPN server by using a secure connection, such as L2TP with IPsec, IKEv2, or SSTP. In this case, however, because the client does not have a computer certificate or a pre-shared key, the client could not establish an L2TP or IKEv2 connection. Additionally, the client could not establish an SSTP connection because this connection requires that the client trusts the certificate on the VPN server. Therefore, the only possible connection in this case is PPTP with the CHAP v2 authentication.*

Export a root CA certificate
1. Switch to **LON-DC1**.
2. Click **Start**, and then click the **Server Manager** tile.
3. In **Server Manager**, click **Tools**, and then click **Certification Authority**.
4. In the **Certification Authority** console, right-click **AdatumCA**, and then click **Properties**.

5. In the **AdatumCA Properties** dialog box, on the **General** tab, click **View Certificate**.
6. In the **Certificate** window, click the **Details** tab, and then click **Copy to File**.
7. In the **Certificate Export Wizard**, click **Next**.
8. On the **Export file format** page, verify that **DER encoded binary x.509 (.CER)** is selected, and then click **Next**.
9. In the **File Name** text box, type ***\\EU-RTR\C$\AdatumRootCA.cer*** and then click **Next**. Click **Yes** at the prompt.
10. Click **Finish** to close **Certificate Export Wizard**.
11. Click **OK** three times, and then close the **Certification Authority** console.

Import a root CA certificate on a client

1. Switch to **LON-CL1**.
2. On the desktop, on the taskbar, click the **File Explorer** icon.
3. In the **This PC** window, in the address bar, type ***\\131.107.0.10\C$*** and then press Enter.
4. In the **Windows Security** dialog box, click **More choices**, and then click **Use a different account**.
5. In the **Enter network credentials** dialog box, for the username, type ***Adatum\Administrator*** for the password, type ***Pa55w.rd*** and then press Enter.
6. In the **File Explorer** window, right-click **AdatumRootCA.cer**, and then click **Install Certificate**.
7. In the **Open File – Security Warning** dialog box, click **Open**.
8. On the **Welcome to the Certification Import Wizard** page, click **Local Machine**, and then click **Next**.
9. In the **User Account Control** dialog box, click **Yes**.
10. On the **Certificate Store** page, click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, and then click **OK**.
11. On the **Certificate Store** page, click **Next**, and then click **Finish**.
12. Wait for the import to complete. It takes approximately 15 seconds.
13. In the **Certificate Import Wizard**, click **OK**.
14. Right-click **Start**, and then click **Command Prompt**.
15. In the **Command Prompt** window, type ***mmc*** and then press Enter.
16. In the **User Account Control** dialog box, click **Yes**.

17. In the **MMC**, on the **File** menu, click **Add/Remove Snap-in**.
18. In the **Add or Remove Snap-ins** window, from the **Available snap-ins** list, click **Certificates**, and then click **Add**.
19. In the **Certificates snap-in** dialog box, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
20. In the **MMC**, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
21. Verify that **AdatumCA** exists.

Note: *You perform the above steps to import the AdatumCA certificate into the Trusted Root Certification Authorities store on* ***LON-CL1*** *and to verify that the AdatumCA certificate is imported into Trusted Root Certification Authorities of* ***LON-CL1****. This enables the clients to trust the certificate on the VPN server and to establish a VPN connection by using the SSTP protocol.*

Connect to VPN by using IKEv2 and SSTP

1. Switch to **Network Connections**, right-click **A. Datum VPN**, and then click **Properties**.
2. In the **A. Datum VPN Properties** dialog box, click the **Security** tab.
3. In the **Type of VPN** list, click **IKEv2**, and then click **Use Extensible Authentication Protocol (EAP)**.
4. Click **OK** twice.
5. In the **Network Connections** window, double-click the **A. Datum VPN** icon, and then click **Disconnect**. If you receive a prompt, click **OK**.
6. In the **Network Connections** window, right click **A. Datum VPN**, and then click **Connect / Disconnect**.
7. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
8. If the **Network sign-in** dialog box appears, in the **User name** box, type ***Adatum\Logan*** in the **Password** box, type ***Pa55w.rd*** and then click **OK**.
9. Switch to the **Network Connections** window, and then verify that the connection is established by using the IKEv2 protocol.
10. In the **Network Connections** window, right-click **A. Datum VPN**, and then click **Properties**.
11. In the **Properties** dialog box, click the **Security** tab.
12. In the **Type of VPN** list, click **Secure Socket Tunneling Protocol (SSTP)**, and ensure that **Use Extensible Authentication Protocol (EAP)** is selected.

13. Click **OK** twice.
14. In the **Network Connections** window, double-click the **A. Datum VPN** icon, and then click **Disconnect**.
15. In the **Network Connections** window, double click the **A. Datum VPN** icon.
16. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
17. If the **Network sign-in** dialog box displays, in the **User name** box, type ***Adatum\Logan*** in the **Password** box, type ***Pa55w.rd*** and then click **OK**.
18. Switch to the **Network Connections** window, and then verify that the connection is established by using the **SSTP** protocol.

Note: *Do not disconnect the A. Datum VPN connection.*

Task 4: Sign in to the domain by using VPN

1. On **LON-CL1**, right-click **Start**, and then click **Command Prompt**.
2. In the **Command prompt** window, type **mmc**, and then press Enter. Click **Yes** at the User Account Control prompt.
3. In the **Console** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, select **Group Policy Object Editor**, and then click **Add**.
5. In the **Select Group Policy Object** dialog box, click **Finish**.
6. In **Add or Remove Snap-in** window, click **OK**.
7. In the **Console** window, expand **Local Computer Policy**, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
8. Double-click **Interactive logon: Do not require CTRL+ALT+DEL**.
9. In the **Interactive logon: Do not require CTRL+ALT+DEL Properties** window, select **Enabled**, and then click **OK**.
10. Close the **Console** window, and do not save changes.
11. Right-click **Start**, and then click **System**.
12. In the **System** window, click **Advanced system settings**, and then click the **Computer Name** tab.
13. On the **Computer name** tab, click **Change**.
14. In the **Computer Name/Domain Changes** dialog box, click **domain**, in the **Domain** text box, type ***Adatum.com*** and then click **OK**.
15. In the **Windows Security** dialog box, type ***Adatum\Administrator*** in the **User name** text box and ***Pa55w.rd*** in the **Password** text box, and then click **OK**.

16. In the **Welcome to the adatum.com domain** dialog box, click **OK**.
17. In the **Computer Name/Domain Changes** dialog box, click **OK**.
18. To close the **System Properties** dialog box, click **Close**.
19. Click **Restart Now**.

Task 5: Verify connectivity

1. When **LON-CL1** has restarted, press Ctrl+Alt+End.
2. On the **sign-in** screen, click the **Network sign-in** icon.
3. On the **Network sign-in** screen, sign in by using the user name **Adatum\Logan** and the password **Pa55w.rd**.

Note: *You now are signed in to the domain via the VPN connection.*

4. Sign out of **LON-CL1**.

Results*: After completing this exercise, you should have verified that the clients that cannot connect by using DirectAccess now can connect by using VPN, and that they can use Network Sign-in to sign in directly to the domain.*

Exercise 3: Troubleshooting VPN access

Task 1: Read the help-desk incident record for incident IN24578

Read the help-desk **Incident Record IN24578** under the **Exercise Scenario**.

Task 2: Update the Plan of Action section of the incident record

1. Read the **Additional Information** section of the incident record in the Student Handbook exercise scenario.
2. Update the **Plan of Action** section of the incident record with your recommendations:

Visit Logan´s computer.
Try to connect to the VPN by using the A. Datum VPN profile.
Document the error message when connection.
Fix the connection issue and test the connection.

Task 3: Try to connect by using the A. Datum VPN connection on Logan´s computer (LON-CL1)

1. On **LON-CL1**, sign in by using the user name ***.\Admin*** and the password ***Pa55w.rd***
2. If you receive a prompt in the **Networks** dialog box, click **Yes**.

3. On **LON-CL1**, right-click **Start**, and then click **Command Prompt (Admin)**. When you receive a prompt in **User Account Control** (UAC), click **Yes**.
4. At the command prompt, type the following command, and then press Enter: ***cd C:\Labfiles\Mod08***
5. At the command prompt, type the following commands, and then press Enter after each one: ***PowerShell .\Mod8LabB.ps1***
6. Wait for the script to complete.
7. If you receive a prompt in the **Networks** dialog box, click **Yes**.
8. Right-click **Start**, and then click **Network Connections**.
9. In the **Network Connections** window, double-click the **A. Datum VPN** icon.
10. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
11. If the **Network sign-in** dialog box displays, in the **User name** text box, type ***Adatum\Logan*** and in the **Password** text box, type ***Pa55w.rd*** and then click **OK**.
12. Wait for the connection to fail, and then write down the error message in the **Plan of Action** section of the incident record in the Student Handbook. (If the connection is successful, disconnect and the re-attempt the connection. It should fail.)

Task 4: Implement the fix, and test the solution

1. On **LON-CL1**, right-click the **File Explorer** icon and click **File Explorer**.
2. In the **This PC** window, in the address bar, type ***\\172.16.0.10\C$*** and then press Enter.
3. In the **Windows Security** dialog box, type ***Adatum\Administrator*** in the **User name** text box, type ***Pa55w.rd*** in the **Password** text box, and then press Enter.
4. In the **File Explorer** window, right-click **AdatumRootCA.cer**, and then click **Install Certificate**.
5. In the **Open File – Security Warning** dialog box, click **Open**.
6. On the **Welcome to the Certification Import Wizard** page, click **Local Machine**, and then click **Next**.
7. In the **User Account Control** dialog box, click **Yes**.
8. On the **Certificate Store** page, click **Place all certificates in the following store**, click **Browse**, click **Trusted Root Certification Authorities**, and then click **OK**.
9. On the **Certificate Store** page, click **Next**, and then click **Finish**.
10. Wait for the import to complete. It takes approximately 15 seconds.
11. In the **Certificate Import Wizard**, click **OK**.

12. Right-click **Start**, and then click **Command Prompt**.
13. In the **Command Prompt** window, type ***mmc***, and then press Enter.
14. If the **User Account Control** dialog box is displayed, click **Yes**.
15. In the **MMC**, on the **File** menu, click **Add/Remove Snap-in**.
16. In the **Add or Remove Snap-ins** window, from the **Available snap-ins** list, click **Certificates**, and then click **Add**.
17. In the **Certificates snap-in** dialog box, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
18. In the **MMC**, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
19. Verify that **AdatumCA** exists.
20. In the **Network Connections** window, double click the **A. Datum VPN** icon.
21. On the **VPN** page, click **A. Datum VPN**, and then click **Connect**.
22. In the **Network sign-in** dialog box, in the **User name** text box, type ***Adatum\Logan*** in the **Password** text box, type ***Pa55w.rd*** and then click **OK**.
23. Verify that you are now able to connect to the **A. Datum** VPN server.

Results*: After completing this exercise, you should have resolved the VPN access issue successfully, and Logan should be able to connect to the A. Datum VPN.*

Task 5: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20741B-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for: **20741B-EU-RTR**, **20741B-INET1**, and **20741B-LON-CL1**.