Module 6: Remote access in Windows Server 2016

Lab: Implementing Web Application Proxy

(VMs: LON-DC1, EU-RTR, LON-SVR1, LON-SVR2, INET1, LON-CL1)

Exercise 1: Implementing Web Application Proxy

Task 1: Prepare the environment

Disable Routing and Remote Access on EU-RTR

1. Switch to **EU-RTR**.
2. Click the **Start** button, and then click the **Server Manager** tile.
3. In **Server Manager**, on the upper-right side, click **Tools**, and then click **Routing and Remote Access**.
4. In the **Routing and Remote Access** console, in the left pane, right-click **EU-RTR (local)**, and then click **Disable Routing and Remote Access**.
5. In the **Routing and Remote Access** dialog box, click **Yes**, and then close the **Routing and Remote Access** window.

Note: *Routing and Remote Access is preconfigured on the virtual machine for the purpose of other labs in this course. The Web Application Proxy configuration in this lab will not work properly if you leave Routing and Remote Access enabled on the virtual machine.*

Task 2: Remove the client computer from a domain

1. Switch to **LON-CL1**.
2. Right-click the **Start** button, 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 the **Change** button.
5. In the **Computer Name/Domain Changes** dialog box, click **Workgroup**, in the **Workgroup** 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 the **System Properties** dialog box, click **Close**.
10. Click **Restart Now**, and then wait for the computer to restart.

Import a root CA certificate on the client

1. When the **LON-CL1** computer restarts, sign in with the user name ***Admin*** and the password ***Pa55w.rd***
2. When prompted by **Networks**, click **Yes**.
3. On the desktop, on the taskbar, click the **File Explorer** icon.
4. In the **File Explorer** window, in the address bar, type ***\\172.16.0.10\C$*** and then press Enter.
5. When prompted for the user name, 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. In the **Certificate Import Wizard**, click **OK**.
13. Right-click the **Start** button, and then click **Command Prompt**.
14. In the **Command Prompt** window, type ***mmc*** and then press Enter.
15. In the **User Account Control** dialog box, click **Yes**.
16. In the **MMC**, on the **File** menu, click **Add/Remove Snap-in**.
17. In the **Add or Remove Snap-ins** window, from the **Available snap-ins** list, click **Certificates**, and then click **Add**.
18. In the **Certificates snap-in** dialog box, click **Computer** account, click **Next**, click **Finish**, and then click **OK**.
19. In the **MMC**, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
20. Verify that **AdatumCA** exists.

Note: *You perform the preceding steps to import the AdatumCA certificate into the Trusted Root Certification Authorities of* ***LON-CL1*** *and then to verify that the AdatumCA certificate is imported into the Trusted Root Certification Authorities of*

LON-CL1*. This enables the client to trust the certificates issued by the Adatum Certification Authority.*

Move the computer to the Internet

1. To move the client from the internal network to the Internet, on **LON-CL1**, right-click the **Start** button, and then click **Network Connections**.
2. In **Network Connections**, right-click **London_Network**, and then click **Disable**.
3. Right-click **Internet**, and then click **Enable**.
4. On the taskbar, click the **Microsoft Edge** icon.
5. In Microsoft Edge, in the **Search or enter web address** box, type ***https://lon-svr1.adatum.com*** and then press Enter. Notice that a Network Error message displays.
6. Right-click the **Start** button, and then click **Run**. In the **Run** dialog box type ***mstsc*** and then press Enter.
7. In the **Remote Desktop Connection** app, in the **Computer** box, type ***lon-dc1*** and then press Enter.

Notice that you cannot connect to **lon-dc1**, because the computer cannot be found on the network.

8. Close all open windows.

Note: *You are unable to open the internal website running on* ***lon-svr1*** *and connect to* ***lon-dc1*** *by using Remote Desktop because the client cannot access the internal network.*

Task 3: Install the Web Application Proxy role service

1. Switch to **EU-RTR**.
2. Click the **Start** button, and then click the **Server Manager** tile.
3. On the **Dashboard** page, click **Add roles and features**.
4. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**, on the **Select installation type** page, click **Next**, and then on the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, expand **Remote Access**, click **Web Application Proxy** and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.

8. On the **Installation progress** page, verify that the installation is successful, and then click **Close**.

Task 4: Configure access to an internal website

Obtain a certificate for the ADFSWAP farm

1. On **EU-RTR**, right-click the **Start** button, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type ***mmc*** and then press Enter.
3. In the **MMC**, on the **File** menu, click **Add/Remove Snap-In**.
4. In the **Add or Remove Snap-ins** window, click **Certificates**, click **Add**, click **Computer account** and then click **Next**.
5. Verify that **Local Computer** is selected, click **Finish**, and then click **OK**.
6. In the **MMC**, expand **Certificates (local Computer)**, right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
7. On the **Before You Begin** page, click **Next**.
8. On the **Select Certificate Enrollment Policy** page, click **Next**.
9. On the **Request Certificates** page, click **Adatum Web Server**, and then click the **More information is required to enroll for this certificate. Click here to configure settings** link.
10. In the **Subject name** section, under the **Type** box, click the drop-down list, select **Common name**, in the **Value** box, type ***adfswap.adatum.com*** and then click **Add**.
11. In the **Alternative name** list, under the **Type** box, click the drop-down list, and then select **DNS**. In the **Value** box, type ***adfswap.adatum.com*** and then click **Add**.
12. In the **Alternative name** list, click **DNS**, in the **Value** box, type: ***rdgw.adatum.com*** and then click **Add**.
13. In the **Alternative name** list, click **DNS**, in the **Value** box, type: ***lon-svr1.adatum.com*** and then click **Add**.
14. Click **OK** to close the **Certificate Properties** dialog box.
15. Click **Enroll** to proceed with Certificate Enrollment.
16. Click **Finish** to close the **Certificate Enrollment** dialog box.

Configure Web Application Proxy

1. In **Server Manager**, from the **Tools** menu, open the **Remote Access Management** console.
2. In the navigation pane, click **Web Application Proxy**.
3. In the middle pane, click **Run the Web Application Proxy Configuration Wizard**.

4. In the **Web Application Proxy Configuration Wizard**, on the **Welcome** page, click **Next**.
5. On the **Federation Server** page, perform the following steps:
a. In the **Federation service name** box, type ***adfswap.adatum.com***, which is the FQDN of the federation service.
b. In the **User name** box, type ***Administrator***, in the **Password** box, type ***Pa55w.rd*** and then click **Next**.
6. On the **AD FS Proxy Certificate** page, in the list of certificates currently installed on the Web Application Proxy server, click **adfswap.adatum.com** and then click **Next**.
7. On the **Confirmation** page, review the settings. If necessary, you can copy the Windows PowerShell cmdlet to automate additional installations. Click **Configure**.
8. On the **Results** page, verify that the configuration is successful, and then click **Close**.

Note: *If you receive an error message, check if* ***LON-SVR2*** *is started and if the AD FS service is running on* ***LON-SVR2****. Then return to step 2 to run the* ***Web Application Proxy Configuration Wizard*** *again.*

Publish the internal website
1. On the Web Application Proxy server, in the **Remote Access Management** console, in the navigation pane, click **Web Application Proxy**, and then in the **Tasks** pane, click **Publish**.
2. In the **Publish New Application Wizard**, on the **Welcome** page, click **Next**.
3. On the **Preauthentication** page, click **Pass-through** and then click **Next**.
4. On the **Publishing Settings** page, perform the following steps:
a. In the **Name** box, type ***Adatum LOB Web App (LON-SVR1)***
b. In the **External URL** box, type ***https://lon-svr1.adatum.com***
c. In the **External certificate** list, click **adfswap.adatum.com**
d. In the **Backend server URL** box, ensure that **https://lon-svr1.adatum.com** is listed, and then click **Next**.

Note: *The value for* ***Backend server URL*** *is automatically entered when you type the external URL.*

5. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the Windows PowerShell command to set up additional published

applications.
6. On the **Results** page, ensure that the application published successfully, and then click **Close**.

Configure internal website authentication
1. Switch to **LON-SVR1**.
2. Click the **Start** button, and then click the **Server Manager** tile. Click the **Tools** menu, and then click **Internet Information Services (IIS) Manager**.
3. In the **Internet Information Services (IIS) Manager** console, expand **LON-SVR1 (ADATUM\administrator)**.
4. Expand **Sites**, and then click **Default Web site**.
5. In the **Internet Information Services (IIS) Manager** console, in the **Default Web Site Home** pane, double-click **Authentication**.
6. In the **Internet Information Services (IIS) Manager** console, in the **Authentication** pane, right-click **Windows Authentication** and then click **Enable**.
7. In the **Internet Information Services (IIS) Manager** console, in the **Authentication** pane, right-click **Anonymous Authentication** and then click **Disable**.
8. Close the **Internet Information Services (IIS) Manager** console.

Task 5: Configure access to Remote Desktop Gateway
Install Remote Desktop Gateway
1. Switch to **LON-SVR2**.
2. Click the **Start** button, and then click the **Server Manager** tile.
3. On the **Dashboard** page, click **Add roles and features**.
4. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**, on the **Select installation type** page, click **Next**, and then on the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, click **Remote Desktop Services** and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Remote Desktop Services** page, click **Next**.
8. On the **Select role services** page, click **Remote Desktop Gateway**. When you receive a prompt, click **Add Features**, and then click **Next**.
9. On the **Network Policy and Access Services** page, click **Next**.
10. On the **Web Server Role (IIS)** page, click **Next**.

11. On the **Select role services** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**.
13. On the **Installation progress** page, verify that the installation is successful, and then click **Close**.

Obtain a certificate for the Remote Desktop Gateway server

1. On **LON-SVR2**, right-click the **Start** button, and then click **Windows PowerShell**.
2. In the **Windows PowerShell** window, type ***mmc*** and then press Enter.
3. In the **MMC**, on the **File** menu, click **Add/Remove Snap-In**.
4. In the **Add or Remove Snap-ins** window, click **Certificates**, click **Add**, click **Computer account** and then click **Next**.
5. Verify that **Local Computer** is selected, click **Finish** and then click **OK**.
6. In the **MMC**, expand **Certificates (local Computer)**, right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
7. On the **Before You Begin** page, click **Next**.
8. On the **Select Certificate Enrollment Policy** page, click **Next**.
9. On the **Request Certificates** page, click **Adatum Web Server**, and then click the **More information is required to enroll for this certificate. Click here to configure settings** link.
10. In the **Subject Name** section, under the **Type** box, click the drop-down list select **Common name**, in the **Value** box, type ***rdgw.adatum.com*** and then click **Add**.
11. Click **OK** to close the **Certificate Properties** dialog box.
12. Click **Enroll** to proceed with Certificate Enrollment.
13. Click **Finish** to close the **Certificate Enrollment** dialog box.

Configure the Remote Desktop Gateway server

1. In **Server Manager**, on the **Tools** menu, select **Remote Desktop Services**, and then click **Remote Desktop Gateway Manager**.
2. In the **RD Gateway Manager**, click **LON-SVR2 (Local)**.
3. In the details pane, under **RD Gateway Server Status: LON-SVR2**, click the **View or modify certificate properties** link.
4. On the **SSL Certificate** tab in the **LON-SVR2 Properties** dialog box, click **Import Certificate**.
5. In the **Import Certificate** dialog box, click the **rdgw.adatum.com** certificate, and then click **Import**.

Verify that the information about the certificate is now listed on the **SSL Certificate** tab.
6. Click the **SSL Bridging** tab, and then click **Use SSL Bridging**. Verify that **HTTPS – HTTPS bridging (terminate SSL requests and initiate new HTTPS requests)** is selected. Click **OK**, and when prompted by RD Gateway, click **Yes**.
7. In the **RD Gateway Manager**, expand **LON-SVR2 (Local)**, right-click **Policies** and then click **Create New Authorization Policies**.
8. On the **Create Authorization Policies for RD Gateway** page, verify that **Create a RD CAP and a RD RAP (recommended)** is selected, and then click **Next**.

Note: *An RD CAP allows you to select the users that can connect to a remote computer by using the RD Gateway server.*

9. On the **Create an RD CAP** page, type ***Adatum Admins*** and then click **Next**.
10. On the **Select Requirements** page, in the **User group membership (required)** section, click **Add Group**.
11. In the **Select Groups**, type ***Domain admins***, click **Check Names**, and then click **OK**. On the **Select Requirements** page, click **Next**.
12. On the **Enable or Disable Device Redirection** page, click **Disable device redirection for the following client device types** and then click **Next**.
13. On the **Set Session Timeout** page, click **Enable idle timeout**, in the value box, type ***15*** and then click **Next**.
14. On the **RD CAP Settings Summary** page, verify your selections, and then click **Next**.

Note: *An RD RAP allows you to select the network resources that users can connect to remotely by using the RD Gateway server.*

15. On the **Create an RD RAP** page, type ***Adatum admins – allow access to all computers*** and then click **Next**.
16. On the **Select User Groups** page, verify that **ADATUM\Domain Admins** displays under **User group membership (required)**, and then click **Next**.
17. On the **Select Network Resources** page, click **Allow users to connect to any network resource (computer)**, and then click **Next**.
18. On the **Select Allowed Ports**, click **Next**.
19. On the **RD RAP Settings Summary** page, verify your selection, and then click

Finish.
20. On the **Confirm Creation of Authorization Policies** page, click **Close**.

Publish the Remote Desktop Gateway server
1. Switch to **EU-RTR**.
2. On the Web Application Proxy server, in the **Remote Access Management** console, in the navigation pane, click **Web Application Proxy**, and then in the **Tasks** pane, click **Publish**.
3. In the **Publish New Application Wizard**, on the **Welcome** page, click **Next**.
4. On the **Preauthentication** page, click **Pass-through**, and then click **Next**.
5. On the **Publishing Settings** page, perform the following steps:
a. In the **Name** box, type ***Adatum RD Gateway***
b. In the **External URL** box, type ***https://rdgw.adatum.com***
c. In the **External certificate** list, click **adfswap.adatum.com**
d. In the **Backend server URL** box, ensure that **https://rdgw.adatum.com** is listed, and then click **Next**.

Note: *The value for* ***Backend server URL*** *is automatically entered when you type the external URL.*

6. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the Windows PowerShell command to set up additional published applications.
7. On the **Results** page, ensure that the application published successfully, and then click **Close**.

Results*: After completing this exercise, you should have successfully implemented Web Application Proxy.*

Exercise 2: Validating the Web Application Proxy deployment

Task 1: Verify access to the internal website from the client computer

1. Switch to **LON-CL1**.
2. On the taskbar, click the **Microsoft Edge** icon.
3. In the **Search or enter web address** box, type ***https://lon-svr1.adatum.com*** and then press Enter.
4. When you receive a prompt, in the **Microsoft Edge** dialog box, type ***Adatum\Logan*** for the user name and ***Pa55w.rd*** for the password, and then click

OK.
5. Verify that the default IIS 9.0 webpage for **LON-SVR1** opens.

Task 2: Verify access to the internal Remote Desktop Gateway server and remote desktop access to LON-DC1

1. Right-click the **Start** button and then click **Run**. In the **Run** dialog box, type ***mstsc*** and then press Enter.
2. In the **Remote Desktop Connection** app, click **Show Options**, and then click the **Advanced** tab.
3. On the **Advanced** tab, in the drop-down box under **If server authentication fails**, click **Connect and don´t warn me**.

Note: *In real life, you would leave this setting at* ***Warn me****. However, because the certificate revocation list distribution point (CDP) is not reachable to* ***LON-CL1*** *in this lab, you change it.*

4. Click **Settings**, and then in the **RD Gateway Server Settings** dialog box, click **Use these RD Gateway server settings**. In the **Server name** box, type ***rdgw.adatum.com***. In the **Logon settings** section, click **Use my RD Gateway credentials for the remote computer**. Click **OK**.

Note: *If you do not choose the* ***Use my RD Gateway credentials for the remote computer*** *setting, you have to validate twice—once for the Remote Desktop Gateway server and once for the server you are connecting to.*

5. Click the **General** tab, in the **Computer** box, type ***lon-dc1*** and then click **Connect**.
6. In the **Windows Security** dialog box, type ***Adatum\administrator*** for the user name and ***Pa55w.rd*** for the password, and then click **OK**.
7. Verify that you can connect to **LON-DC1** by using Remote Desktop.

Note: *It will take approximately 20 seconds to connect to* ***LON-DC1****.*

Results*: After completing this exercise, you will have verified that external users are able to access the internal application through the Web Application Proxy.*

Task 3: 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-LON-SVR1**, **20741B-LON-SVR2**, **20741B-EU-RTR**, **20741B-INET1**, and **20741B-LON-CL1**.