Module 10: Securing a SharePoint 2016 deployment

Lab: Securing a SharePoint 2016 deployment

Exercise 1: Configuring SharePoint Server communication security

▶ Task 1: Configure SQL Server to use a nonstandard TCP port

1. Access the virtual machine: **20339-1A-NYC-DB1-E**. On the **Start** screen, type **SQL Server 2014 Configuration Manager**, and then press Enter.
2. In SQL Server Configuration Manager, in the navigation pane, expand **SQL Server Network Configuration**, and then click **Protocols for MSSQLSERVER**.
3. In the details pane, right-click the **TCP/IP** row, and then click **Properties**.
4. In the **TCP/IP Properties** dialog box, on the **IP Addresses** tab, locate the **IPAll** section.
5. In the **IPAll** section, in the **TCP Port** row, change the port number to **55555**, and then click **OK**.
6. In the **Warning** dialog box, click **OK**.
7. In the navigation pane, click **SQL Server Services**.
8. In the details pane, right-click **SQL Server (MSSQLSERVER)**, and then click **Restart**.
9. Close SQL Server Configuration Manager.

▶ Task 2: Configure SharePoint to communicate with SQL Server on a specific port

1. Sign in to the **NYC-SP1** virtual machine as **Contoso\Administrator** with the password **Pa$$w0rd**.
2. On the **Start** screen, click **Internet Explorer**.
3. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
4. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
5. Verify that the page displays an error message.

Note: This is because SharePoint is currently unable to communicate with the SQL Server instance on the database server.

6. Close Internet Explorer.
7. On the **Start** screen, type **cliconfg**, and then press Enter.
8. In SQL Server Client Network Utility, on the **Alias** tab, make sure that **ContosoDB** is selected, and then click **Edit**.
9. In the **Edit Network Library Configuration** dialog box, clear **Dynamically determine port**.
10. In the **Port number** text box, type **55555**, and then click **OK**.
11. In SQL Server Client Network Utility, click **OK**.
12. On the **Start** screen, click **Internet Explorer**.
13. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.

14. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
15. Verify that the page loads successfully.
16. Close Internet Explorer.

▶ Task 3: Encrypt Central Administration

1. On the **Start** screen, type **IIS**, and then press Enter.
2. In Internet Information Services (IIS) Manager, in the **Connections** pane, click **NYC-SP1 (CONTOSO\Administrator)**.
3. If it appears, in the **Internet Information Services (IIS) Manager** dialog, click **No**.
4. In Features View, under **IIS**, double-click **Server Certificates**.
5. Under **Actions**, click **Create Domain Certificate**.
6. Enter the **Distinguished Name Properties**. The **Common name** should be the URL that points to **Central Administration: nyc-sp1.contoso.com**.
7. Enter the following values for the remaining fields:
   - Organization: **Contoso**
   - Organizational Unit: **IT**
   - City/locality: **Raleigh**
   - State/province: **NC**
8. Click **Next**, and then specify the Online Certification Authority by clicking **Select**. Choose **NYC-DC1.Contoso.com**. It should be your only option.
9. Enter a **Friendly name**: **Contoso sp1 Certificate**, and then click **Finish**.
10. Open **SharePoint 2016 Management Shell**, and then enter the following cmdlet: **Set-SPCentralAdministration –Port 443**
11. Type **Y** to confirm the command.
12. In Internet Information Services (IIS) Manager, under **Sites**, click **SharePoint Central Administration V4**. Under **Actions**, click **Bindings**.
13. In the **Site Bindings** dialog box, select the row with the value as **https**, and then click **Edit**.
14. In the **Edit Site Binding** dialog box, in the **Host name** enter **NYC-SP1.contoso.com**.
15. Select the **Require Server Name Indication** check box.
16. Click **OK** after adding the SSL Certificate.
17. Select the newly created certificate in the **SSL certificate** drop-down list.
18. Open **SharePoint 2016 Central Administration**: type **https://nyc-sp1.contoso.com** in Internet Explorer.
19. If you are prompted for credentials, enter the following:
    - User: **Contoso\Administrator**
    - Password: **Pa$$w0rd**
20. Click **Application Management**, and then select **Configure alternate access mappings**.

21. You will see **https://nyc-sp1** under the **Internal URL** column. Click the URL. This will bring you to the **Edit Internal URLs** page.
22. Change **https://nyc-sp1** to **https://nyc-sp1.contoso.com** in the **URL protocol, host, and port** text box.
23. Click **OK**.

Results: After completing this exercise, you should have configured communications over port a nonstandard port.

Exercise 2: Hardening a SharePoint server farm

▶ Task 1: Enable Windows Firewall on the Database server

1. Switch to the **NYC-DB1** server.
2. On the **Start** screen, type **Windows Firewall with Advanced Security**, and then press Enter.
3. In the Windows Firewall with Advanced Security window, in the **Overview** section, click **Windows Firewall Properties**.
4. In the **Windows Firewall with Advanced Security on Local Computer** dialog box, on the **Domain Profile** tab, in the **Firewall state** list, click **On (recommended)**, and then click **OK**.
5. Close the Windows Firewall with Advanced Security window.
6. Switch to the **NYC-SP1** virtual machine.
7. On the **Start** screen, click **Internet Explorer**.
8. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
9. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
10. Verify that the page displays **HTTP 500 Internal Server Error**.
11. Close Internet Explorer.

Note: This is because the firewall on the database server is currently preventing SharePoint from communicating with the database server.

▶ Task 2: Configure Windows Firewall with Advanced Security exceptions on the database server

1. Switch to the **NYC-DB1** server.
2. On the **Start** screen, type **Windows Firewall with Advanced Security**, and then press Enter.
3. In the Windows Firewall with Advanced Security window, in the navigation pane, click **Inbound Rules**.
4. In the **Actions** pane, click **New Rule**.
5. In the New Inbound Rule Wizard, on the **Rule Type** page, click **Port**, and then click **Next**.
6. On the **Protocol and Ports** page, make sure that **TCP** is selected.
7. In the **Specific local ports** text box, type **55555**, and then click **Next**.

8. On the **Action** page, make sure **Allow the connection** is selected, and then click **Next**.
9. On the **Profile** page, leave **Domain** selected, clear **Private** and **Public**, and then click **Next**.
10. On the **Name** page, in the **Name** text box, type **SQL Server inbound TCP traffic from SharePoint**, and then click **Finish**.
11. Close the Windows Firewall with Advanced Security window.
12. Switch to the **NYC-SP1** server.
13. On the **Start** screen, click **Internet Explorer**.
14. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
15. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
16. Verify that the page loads successfully.
17. Close Internet Explorer.

▶ Task 3: Enable Windows Firewall with Advanced Security on the SharePoint 2016 server

1. On NYC-SP1, on the **Start** screen, type **Windows Firewall with Advanced Security**, and then press Enter.
2. In the Windows Firewall with Advanced Security window, in the **Overview** section, click **Windows Firewall Properties**.
3. In the **Windows Firewall with Advanced Security on Local Computer** dialog box, on the **Domain Profile** tab, in the **Firewall state** list, click **On (recommended)**, and then click **OK**.
4. In the navigation pane, click **Inbound Rules**.
5. Review the existing inbound rules, and notice that they include the following rules to allow communication between servers in the SharePoint farm:
   - The **SharePoint - sharepoint.contoso.com80** rule allows the SharePoint web application to receive TCP traffic over port 80.
   - The **SharePoint Central Administration v4** rule allows Central Administration to receive TCP traffic over port 50000.
   - The **SharePoint Search** rule allows various components of the search service to receive the TCP traffic over ports 16500-16519.
   - The **SharePoint Web Services** rule allows various Windows Communication Foundation (WCF)–based SharePoint web services to listen on TCP ports 32843-32845.
   - The **SPUserCodeV4** rule enables the user code service for sandboxed solutions to listen on TCP port 32846.
6. Close the Windows Firewall with Advanced Security window.
7. On the **Start** screen, click **Internet Explorer**.
8. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
9. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.

10. Verify that the page loads successfully.
11. Close Internet Explorer.

> **Note:** You do not need to configure an inbound firewall exception for SQL Server traffic on port 55555 on the SharePoint server, because database communication takes place on the outbound port 55555.

Results: After completing this exercise, you should have configured firewalls on a database server and a SharePoint server.

Exercise 3: Configuring blocked file types

▶ Task 1: Configure blocked file types

1. On the NYC-SP1 virtual machine, on the **Start** screen, type **SharePoint 2016 Central Administration**, and then press Enter.
2. If you are prompted by **Windows Security**, enter the user name **Contoso\Administrator** with a password of **Pa$$w0rd**.
3. On Central Administration, under **Application Management**, click **Manage web applications**.
4. Click **SharePoint - sharepoint.contoso.com80**.
5. On the ribbon, on the **Web Applications** tab, in the **Security** group, click **Blocked File Types**.
6. In the **Blocked File Types** dialog box, on a new line, type **bmp**.
7. On a new line, type **dib**, and then click **OK**.

▶ Task 2: Verify file-type blocking

1. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
2. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
3. In the **Quick Launch** navigation pane, click **Site Contents**.
4. On the **Site Contents** page, click **Site Assets**.
5. On the **Site Assets** page, click **new document**.
6. In the **Add a document** dialog box, click **Browse**.
7. In the **Choose Files to Upload** dialog box, browse to the **E:\Labfiles\Mod10** folder, click **ContosoHeader.bmp**, and then click **Open**.
8. In the **Add a document** dialog box, click **OK**.
9. In the **Error** dialog box, verify that you receive an error message that states that your file has been blocked by the administrator, and then click **GO BACK TO SITE**.
10. On the **Site Assets** page, click **new document**.
11. In the **Add a document** dialog box, click **Browse**.
12. In the **Choose Files to Upload** dialog box, browse to the **E:\Labfiles\Mod10** folder, click **ContosoHeader.jpg**, and then click **Open**.

13. In the **Add a document** dialog box, click **OK**.
14. Verify that the image is added to the **Site Assets** page.
15. Close Internet Explorer.

Results: After completing this exercise, you should have configured blocked file types.

Exercise 4: Configuring Web Part security

▶ Task 1: Upload documents as another user

1. Open Internet Explorer, and then browse to **sharepoint.contoso.com**.
2. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
3. In the top-right corner, you should see several navigation elements: **SHARE**, **FOLLOW**, and **EDIT**.
4. Click **EDIT**.
5. In the top tab, click **Insert**.
6. In the top navigation bar, click **Web Part**. Under **Parts**, select **Documents** and click the **Add** button. Click **Save** in the upper-left corner.
7. Click **SHARE**.
8. In the **Share 'Contoso Intranet Portal'** dialog box, enter **Kate** in the text box that states **Enter names, email, or 'Everyone'**. You should see Kate Herrera populate in the drop-down.
9. Click the blue **Share** button.
10. Close Internet Explorer.
11. Click the **Windows** button in the lower left hand corner. This will present the **Start** menu. Right click Internet Explorer and select **Run as different user**.
12. In the Windows Security login, enter **Contoso\Kate** as the username with the password **Pa$$w0rd**.
13. In the address bar of Internet Explorer, browse to **sharepoint.contoso.com**.
14. If you are prompted for credentials, sign in as **Contoso\Kate** with the password **Pa$$w0rd**.
15. If Internet Explorer 11 prompts you, click **Use recommended security and compatibility settings** and click **OK**.
16. In the left navigation under **Home**, click **Documents**.
17. Click **Upload**.
18. Click the **Browse** button.
19. In the **Choose File to Upload** dialog box, enter the following path: **E:\Labfiles\Mod10\Contracts**.
20. Hold down the Ctrl key and select **Litware Inc Contract.docx**, **Northwind Traders Contract.docx**, and **Proseware Inc Contract.docx**. Click the **Open** button.
21. Click **OK**.
22. Close Internet Explorer.

▶ Task 2: Create a Web Part connection

1. On the **Start** screen, click **Internet Explorer**.
2. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
3. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
4. When the page loads, notice that the **Documents** Web Part displays three documents.
5. On the toolbar at the top of the page, click **EDIT**.
6. Click the content area below the **Documents** Web Part.
7. On the ribbon, on the **INSERT** tab, click **Web Part**.
8. In the **Categories** list, click **Filters**.
9. In the **Parts** list, click **Current User Filter**, and then click **Add**.
10. Click the new Web Part, which is rendered as an empty rectangle.
11. On the ribbon, on the **WEB PART** tab, click **Web Part Properties**.
12. On the **Current User Filter** Web Part, on the drop-down menu, point to **Connections**, point to **Send Filter Values To**, and then click **Documents**.
13. In the **Internet Explorer blocked a pop-up from sharepoint.contoso.com** message box, on the **Options for this site** drop-down menu, click **Always allow**.
14. In the **Message from webpage** dialog box, click **OK**.
15. In the **Windows Internet Explorer** dialog box, click **Retry**.
16. In the **Choose Connection** dialog box, in the **Connection Type** list, click **Get Filter Values From**, and then click **Configure**.
17. In the **Configure Connection** dialog box, in the **Consumer Field Name** list, click **Created By**, and then click **Finish**.
18. On the ribbon, on the **PAGE** tab, click **Save**.
19. Notice that the **Documents** Web Part does not display any documents. The documents are filtered out because you did not create them. If SharePoint displays a **Save Conflict** dialog box, click **Overwrite the Page**, and then click **OK**.
20. Close Internet Explorer.

▶ Task 3: Configure Web Part security settings

1. On the **Start** screen, type **SharePoint 2016 Central Administration**, and then press Enter.
2. If you are prompted by **Windows Security**, enter the user name **Contoso\Administrator** with a password of **Pa$$w0rd**.
3. On Central Administration, under **Application Management**, click **Manage web applications**.
4. Click **SharePoint - sharepoint.contoso.com80**.
5. On the ribbon, on the **WEB APPLICATIONS** tab, in the **Security** group, click **Web Part Security**.
6. In the **Security For Web Part Pages** dialog box, under **Web Part Connections**, click **Prevents users from creating connections between Web Parts, and helps to improve security and performance**.
7. Under **Online Web Part Gallery**, click **Prevents users from accessing the Online Web Part Gallery, and helps to improve security and performance**, and then click **OK**.

8. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
9. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
10. Verify that the **Documents** Web Part no longer filters the list of documents.
11. On the toolbar at the top of the page, click **EDIT**.
12. Click the **Current User Filter** Web Part, which is rendered as an empty rectangle.
13. On the ribbon, on the **WEB PART** tab, click **Web Part Properties**.
14. Notice that the **Current User Filter** Web Part displays a warning message stating that the filter is not connected.
15. On the **Current User Filter** Web Part, on the drop-down menu, verify that there is no longer a menu option for connecting the Web Part.
16. Close Internet Explorer.
17. In the **Message from webpage** dialog box, click **OK**.

Results: After completing this exercise, you should have configured Web Part security settings to prevent users from connecting Web Parts or accessing the Online Web Part Gallery.

Exercise 5: Implementing security auditing

▶ Task 1: Configure site-collection audit settings

1. On the **Start** screen, click **Internet Explorer**.
2. In Internet Explorer, in the address bar, type **sharepoint.contoso.com**, and then press Enter.
3. If you are prompted for credentials, sign in as **Contoso\Administrator** with the password **Pa$$w0rd**.
4. On the **Settings** menu, click **Site settings**.
5. On the **Site Settings** page, under **Site Collection Administration**, click **Site collection audit settings**.
6. On the **Configure Audit Settings** page, under **Automatically trim the audit log for this site**, click **Yes**.
7. Under **Optionally**, specify the number of days of audit log data to retain, and in the text box, type **28**.
8. Under **Documents and Items**, select the following:
   - **Moving or copying items to another location in the site**
   - **Deleting or restoring items**
9. Under **Lists, Libraries, and Sites**, select **Editing users and permissions**, and then click **OK**.

▶ Task 2: Create audit data

1. On the Quick Launch navigation menu, click **Documents**.
2. On the ribbon, on the **LIBRARY** tab, click **Library Settings**.
3. On the **Document/Settings** page, under **Permissions and Management**, click **Permissions for this document library**.

4. On the ribbon, on the **PERMISSIONS** tab, click **Stop Inheriting Permissions**.
5. In the **Message from webpage** dialog box, click **OK**.
6. Select **Contoso Intranet Portal Visitors**, and then on the ribbon, click **Remove User Permissions**.
7. In the **Message from webpage** dialog box, click **OK**.
8. On the Quick Launch navigation menu, click **Documents**.
9. Click the **Litware Inc Contract.docx** row, and then on the ribbon, on the **FILES** tab, click **Delete Document**.
10. In the **Message from webpage** dialog box, click **OK**.

▶ Task 3: View audit reports

1. On the **Settings** menu, click **Site settings**.
2. On the **Site Settings** page, under **Site Collection Administration**, click **Audit log reports**.
3. On the **View Auditing Reports** page, under **Content Activity Reports**, click **Deletion**.
4. On the **Customize Report** page, under **File Location**, click **Browse**.
5. In the **Select List or Library** dialog box, click **Documents**, and then click **OK**.
6. On the **Customize Report** page, click **OK**.
7. On the **Operation Completed Successfully** page, click **Click here to view the report**.
8. You may receive an **Open Document** prompt stating that some files may be harmful. Click **OK**.
9. If you are prompted by **Windows Security**, enter the user name **Contoso\Administrator** with a password of **Pa$$w0rd**.
10. Review the report, and verify that it records the document that you deleted in the previous task.
11. Close the Excel Web Access browser window.
12. On the **Operation Completed Successfully** page, click **OK**.
13. On the **Site Settings** page, under **Site Collection Administration**, click **Audit log reports**.
14. On the **View Auditing Reports** page, under **Security and Site Settings Reports**, click **Security settings**.
15. On the **Customize Report** page, under **File Location**, click **Browse**.
16. In the **Select List or Library** dialog box, click **Documents**, and then click **OK**.
17. On the **Customize Report** page, click **OK**.
18. On the **Operation Completed Successfully** page, click **Click here to view the report**.
19. You may receive an **Open Document** prompt stating that some files may be harmful. Click **OK**.
20. If you are prompted by **Windows Security**, enter the user name **Contoso\Administrator** with a password of **Pa$$w0rd**.

21. The report loads in an Excel Web Access browser window.
22. Review the report, and verify that it refers to the permission changes that you made in the previous task.
23. Close Internet Explorer.

Results: After completing this exercise, you should have configured a site collection's audit settings.

▶ Task 4: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20339-1A-NYC-DC1-E**, and then click **Revert.**
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20339-1A-NYC-DB1-E** and **20339-1A-NYC-SP1-E**.