# Lab answer key: Deploying network workloads

## Lab setup

For this demonstration, you will use the following virtual machines:

* **WS-011T00A-SEA-DC1**
* **WS-011T00A-SEA-ADM1**
* **WS-011T00A-SEA-SVR1**
* **WS-011T00A-SEA-SVR3**
* **WS-011T00A-SEA-CL1**

Sign in by using the following credentials:

* User Name: \*\*Contoso\*
* Password: **Pa55w.rd**

**Tip:** You don't need to sign in to **WS-011T00A-SEA-DC1** as you don't use this machine in this lab.

### Exercise 1: Implementing Web Application Proxy

#### Task 1: Install AD FS on SEA-DC1

1. On **SEA-SVR1**, enter **powershell.exe**, and then select Enter.
2. At the Windows PowerShell prompt, enter C:\Labfiles\Mod03\InstallADFS.ps1, and then select Enter.
3. Wait for the restarting message to display.

#### Task 2: Create DNS entries for AD FS and Web Application Proxy

1. On **SEA-ADM1**, on the taskbar, select **Microsoft Edge**.
2. In **Microsoft Edge**, select **Windows Admin Center**.
3. In the **Windows Security** dialog box, sign in as **Contoso\* with the password** Pa55w.rd\*\*.
4. In **Windows Admin Center**, select **SEA-DC1**.
5. In the **Specify your credentials** dialog box, select **Use another account for this connection**, and then sign in as **Contoso\* with the password** Pa55w.rd\*\*.
6. On the **Tools** pane, select **DNS**, and then on the right **details** pane, select **Install**.
7. When the DNS PowerShell tools installation is complete, select **Contoso.com**, and then select **Create new DNS record**.
8. In the **Create a new DNS record** dialog box, enter the following information, and then select **Create**:
   * DNS record type: **Host (A)**
   * Record name: **remoteapp**
   * IP address: **172.16.10.14**
   * Time to live: **3600**
9. Select **Create a new DNS record**, enter the following information, and then select **Create**:
   * DNS record type: **Host (A)**
   * Record name: **fs**
   * IP address: **172.16.10.12**
   * Time to live: **3600**

#### Task 3: Install Remote Access management tools

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Windows Admin Center**, and then select **sea-adm1.contoso.com [gateway]**.
2. On the **Tools** pane, select **Roles & features**.
3. On the **Roles and features** pane, under **Features**, expand **Remote Server Administration Tools**, expand **Role Administration Tools**, select the **Remote Access Management Tools** check box, and then select **Install**.
4. In the **Install Roles and Features** dialog box, select **Yes**.

#### Task 4: Install Web Application Proxy

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Windows Admin Center**, and then select **SEA-SVR3**.
2. In the **Specify your credentials** dialog box, select **Use another account for this connection**, and then sign in as **Contoso\* with the password** Pa55w.rd\*\*.
3. On the **Tools** pane, select **Roles & features**.
4. On the **Roles and features** pane, expand **Remote Access**, select the **Web Application Proxy** check box, and then select **Install**.
5. In the **Install Roles and Features** dialog box, select **Yes**.

#### Task 5: Configure Web Application Proxy

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In **Server Manager**, select **Tools**, and then select **Remote Access Management**.
3. In the **Remote Access Management Console**, on the **Tasks** pane, select **Manage a Remote Server**.
4. In the **Manage a Remote Server** dialog box, enter **SEA-SVR3**, and then select **OK**.
5. In the **Remote Access Management Console**, select **Web Application Proxy**, and then select **Run the Web Application Proxy Configuration Wizard**.
6. In the **Web Application Proxy Configuration Wizard**, select **Next**.
7. On the **Federation Server** screen, enter the following information, and then select **Next**:
   * Federation service name: **fs.Contoso.com**
   * User name: **Contoso\Administrator**
   * Password: **Pa55w.rd**
8. On the **AD FS Proxy Certificate** screen, in the **Select a certificate to be used by the AD FS proxy** box, select **fs.contoso.com**, and then select **Next**.
9. On the **Confirmation** screen, read the information, and then select **Configure**.
10. On the **Results** screen, select **Close**.

**Note:** If you get an error in **Remote Access Management Console** indicating that cmdlets are not found, restart **Remote Access Management Console**.

#### Task 6: Configure a web application

1. On **SEA-ADM1**, in the **Remote Access Management Console**, in the **Tasks** pane, select **Publish**.
2. In the **Publish New Application Wizard**, on the **Welcome** screen, select **Next**.
3. On the **Preauthentication** screen, select **Pass-through**, and then select **Next**.
4. On the **Publishing Settings** screen, enter the following information, and then select **Next**.
   * Name: **RemoteApp**
   * External URL: **https://remoteapp.contoso.com**
   * External certificate: **remoteapp.contoso.com**
   * Backend server URL: **https://SEA-ADM1.contoso.com**

* **Note:** You will receive a warning that external URL and backend URL are different. You can ignore this warning.

1. On the **Confirmation** screen, select **Publish**.
2. On the **Results** screen, select **Close**.

#### Task 7: Configure Windows Defender Firewall to allow remote access

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Windows Admin Center**, and then select **sea-adm1.contoso.com[gateway]**.
2. In the **Tools** pane, select **Firewall**.
3. In the **Firewall** pane, select **Incoming rules**, and then select **New**.
4. In the **New Rule** dialog box, enter the following information, and then select **Create**:
   * Name: **SecureWeb**
   * Direction: **Incoming**
   * Action: **Allowed**
   * Enable firewall rule: **Yes**
   * Protocol: **TCP**
   * Local port: **443**
   * Remote port: **blank**
   * ICMP types: **blank**
   * Profiles: **Select All**

#### Task 8: Test the web application

1. On **SEA-CL1**, on the taskbar, select **Microsoft Edge**.
2. In **Microsoft Edge**, in the address bar, enter **https://remoteapp.contoso.com**, and then select Enter.
3. In the **Windows Security** dialog box, sign in as **Contoso\Administrator** with the password **Pa55w.rd**.

### Exercise 2: Implementing VPN in Windows Server

#### Task 1: Configure RRAS service and NPS policies for VPN

1. On **SEA-ADM1**, right-select (or access the context menu) the **Start** button, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: Install-WindowsFeature -name RemoteAccess,Routing -IncludeManagementTools
3. Wait for the command to complete, which should take approximately 1 minute.
4. Leave the **Administrator: Windows PowerShell** window open.

##### Request certificate for SEA-ADM1

1. On SEA-ADM1, in the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: mmc
2. In the **Console** window, select **File**, and then select **Add/Remove Snap-in**.
3. In the **Available snap-ins** list, select **Certificates**, and then select **Add**.
4. In the **Certificates snap-in** dialog box, select **Computer account**, and then select **Next**.
5. In the **Select Computer** dialog box, verify that **Local computer** is selected, select **Finish**, and then select **OK**.
6. In the **Certificates** snap-in, in the console tree of the **Certificates** snap-in, navigate to \*\*Certificates (Local Computer)\*.
7. Right-click (or access the context menu) **Personal**, point to **All Tasks**, and then **select Request New Certificate**.
8. On the **Before you begin** page, select **Next**, and then on the **Select Certificate Enrollment Policy** page, select **Next**.
9. On the **Request Certificates** page, select **Contoso Web Server**, and then select the **More information is required to enroll for this certificate. Click here to configure settings** link.
10. In the **Certificate Properties** dialog box, on the **Subject** tab, under **Subject name**, under **Type**, select **Common name**.
11. In the **Value** text box, enter **vpn.contoso.com**, and then select **Add**.
12. Select the **General** tab, and in the **Friendly name** field, enter **Contoso VPN**.
13. Select **OK**, select **Enroll**, and then select **Finish**.
14. In the **Certificates** snap-in, expand **Personal** and then select **Certificates**.
15. In the **details** pane, verify that a new certificate with the name **vpn.contoso.com** is enrolled with **Intended Purposes** of **Server Authentication**.
16. In the **Microsoft Management Console (MMC)**, select **File**, and then select **Exit**. When you receive a prompt to save the settings, select **No**.

##### Change the HTTPS bindings

1. On **SEA-ADM1**, open **Server Manager**, select **Tools**, and then select **Internet Information Services (IIS) Manager.**
2. In the **Internet Information Services (IIS) Manager**, expand **SEA-ADM1 (CONTOSO)**.
3. In the **Internet Information Services (IIS) Manager**, in the console tree, expand **Sites**, and then select **Default Web site**.
4. In the **Actions** pane, select **Bindings**, and then select **Add**.
5. In the **Add Site Binding** dialog box, under the **Type** select **https**, in the SSL Certificate list, select the **Contoso VPN** certificate, select **OK**, select **Yes** when prompted, and then select **Close**.
6. Close the **Internet Information Services (IIS) Manager** console.

##### Configure and enable VPN configuration

1. On **SEA-ADM1**, in the **Server Manager**, select **Tools**, and then select **Routing and Remote Access**.
2. Right-click (or access the context menu) **SEA-ADM1 (local)**, and then select **Configure and Enable Routing and Remote Access**.
3. On the **Welcome to Routing and Remote Access Server Setup Wizard**, select **Next**.
4. On the **Configuration** page, select **Custom configuration**, and then select **Next**.
5. On the **Custom Configuration** page, select **VPN access** and **LAN routing**, and then select **Next**.
6. On the **Completing the Routing and Remote Access Server Setup Wizard** page, select **Finish**.
7. When you receive a prompt, select the **Routing and Remote Access** dialog box, and then select **Start service**.
8. Expand **SEA-ADM1 (local)**, right-click (or access the context menu) **Ports**, and then select **Properties**.
9. In the **Ports Properties** dialog box, verify that 128 ports exist for **WAN Miniport (SSTP)**, **WAN Miniport (IKEv2)**, **WAN Miniport (L2TP)**, and **WAN Miniport (PPTP)**.
10. Select **WAN Miniport (SSTP)** and select **Configure**. In the **Maximum ports** text box, enter **5**, and then select **OK**.
11. In the **Routing and Remote Access** message box, select **Yes**.
12. Repeat steps 10 and 11 for IKEv2 and L2TP.
13. Select **WAN Miniport (PPTP)** and select **Configure**. In the **Configure Device - WAN Miniport (PPTP)** windows, remove the check mark next to **Remote access connections (inbound only)** and **Demand-dial routing connections (Inbound and outbound)**, and then select **OK**.
14. To close the **Ports Properties** dialog box, select **OK**.
15. Right-click (or access the context menu) **SEA-ADM1 (local)**, and then select **Properties**.
16. In the **SEA-ADM1 (local) Properties** dialog box, on the **General** tab, verify that **IPv4 Remote access server** is selected.
17. Select the **Security** tab, and then select **Authentication Methods**. Verify that **Extensible authentication protocol (EAP)** is selected as the authentication protocol, and then select **OK**.
18. On the **Security** tab, select the drop-down arrow next to **Certificate**, and then select **vpn.contoso.com**.
19. Select the **IPv4** tab, and then verify that the VPN server is configured to assign IPv4 addressing by using **Dynamic Host Configuration Protocol (DHCP)**.
20. To close the **SEA-ADM1 (local) Properties** dialog box, select **OK** and then select **Yes** when prompted.

##### Configure the Remote Access policies on NPS

1. On **SEA-ADM1**, in **Server Manager**, on the **Tools** menu, select **Network Policy Server**.
2. In the **Network Policy Server** console, in the **navigation** pane, expand **Policies**, and then select **Network Policies**.
3. In the **navigation** pane, right-click (or access the context menu) **Network Policies**, and then select **New**.
4. In the **New Network Policy** Wizard, in the **Policy name** text box, enter **Contoso IT VPN**.
5. In the **Type of network access server** list, select **Remote Access Server(VPN-Dial up)**, and then select **Next**.
6. On the **Specify Conditions** page, select **Add**.
7. In the **Select condition** dialog box, select **Windows Groups**, and then select **Add**.
8. In the **Windows Groups** dialog box, select **Add Groups**.
9. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** text box, enter **IT**, select **Check Names**, and then select **OK** select **OK** again, and then select **Next**.
10. On the **Specify Access Permission** page, verify that **Access granted** is selected, and then select **Next**.
11. On the **Configure Authentication Methods** page, clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
12. To add **EAP Types**, select **Add**.
13. On the **Add EAP** page, select **Microsoft Secured password (EAP-MSCHAP v2)**, and then select **OK**.
14. To add **EAP** types, select **Add**.
15. On the **Add EAP** page, select **Microsoft: Smart Card or other certificate**, select **OK**, and then select **Next**.
16. On the **Configure Constraints** page, select **Next**.
17. On the **Configure Settings** page, select **Next**.
18. On the **Completing New Network Policy** page, select **Finish**.
19. Close all open windows.

#### Task 2: Configure a client VPN connection

1. On **SEA-CL1**, right-click (or access the context menu) the **Start** button, and then select **Network Connections**.
2. In **Network & Internet**, select **VPN**, and then select **Add a VPN connection**.
3. In the **Add a VPN connection** wizard, configure the following settings, and then select **Save**:
   * VPN provider: **Windows (built-in)**
   * Connection name: **Contoso VPN**
   * Server name or address: **vpn.contoso.com**
   * VPN type: **Secure Socket Tunneling Protocol (SSTP)**
   * Type of sign-in info: **User name and password**
   * Remember my sign-in info: **Cleared**. You might need to scroll down to find this setting.

#### Task 3: Test the VPN connection

1. Still in **Network & Internet**, select **Contoso VPN**, and then select **Connect**.
2. In the **Sign in** dialog box, in the **User name** text box, enter **contoso\jane**, in the **Password text** box, enter **Pa55w.rd**, and then select **OK**.
3. Verify that **Connected** displays under **Contoso VPN**, indicating that you are now connected to the VPN server.
4. In **Network & Internet**, select **Ethernet** and then under **Related settings**, select **Network and Sharing Center**.
5. In **Network and Sharing Center**, select **Change Adapter settings**.
6. Verify that **WAN Miniport (SSTP)** displays under **Contoso VPN**.

#### Verify connection on client and VPN server

1. On **SEA-CL1**, right-click (or access the context menu) the **Start** button, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: Get-NetIPConfiguration
3. Examine the output and verify that **Contoso VPN** is listed next to **InterfaceAlias**. Also verify that the **Contoso VPN** interface has been issued an IP Address. This is the IP address for VPN connection assigned by RRAS.
4. Switch to **SEA-ADM1** and maximize the **Routing and Remote Access** snap-in.
5. In the **Routing and Remote Access** snap-in, select **Remote Access Clients (0)** and verify that **Contoso\* is listed under the** User Name\*\* column. This indicates that the user is connected to the VPN Server.
6. Maximize **Server Manager**, select the **Tools** menu, and then select **Remote Access Management**.
7. In the **Remote Access Management** console, select **Remote Client Status** and verify that **CONTOSO\* is listed in the** details\*\* pane under **Connected Clients**. Notice that the VPN protocol displays under the **Protocol/Tunnel** field as **Sstp**.

**Question:** Why did you disable the PPTP authentication protocol when you configured the ports of the VPN Server?

**Answer:** The PPTP protocol is considered highly insecure and you shouldn't use it.

**Results**: After completing this exercise, you should have installed and configured the Remote Access server to successfully provide VPN access.

### Exercise 3: Deploying and configuring web server

#### Task 1: Install the Web Server role

1. On **SEA-SVR1**, in the **Administrator C:32.exe** window, enter the following command, and then select Enter: powershell
2. In the **Administrator C:32.exe - powershell** window, enter the following command, and then select Enter: Install-WindowsFeature -name Web-Server -IncludeManagementTools
3. Wait for the command to complete, which should take approximately one minute.
4. Verify that **True** displays under **Success** in the output.

##### Verify the Web Server installation

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, if not already open.
2. In the Windows PowerShell command prompt, enter the following command, and then select Enter: Get-eventLog System -After (Get-Date).AddHours(-1) Verify that no errors display under the **EntryType** column.
3. Still in the Windows PowerShell command prompt, enter the following command, and then select Enter: Get-eventLog Application -After (Get-Date).AddHours(-1) Verify that only errors with word **License** display under the **Message** column.

##### Verify that the Windows Firewall rules for HTTP and HTTPS traffic are enabled

1. On **SEA-SVR1**, in a Windows PowerShell command prompt, enter the following command, and then select Enter:Get-NetFirewallProfile -Name Domain | Get-NetFirewallRule | where-Object {$\_.DisplayName -like "World Wide Web\*"}
2. This will return information about two rules. One for HTTP and one for HTTPS. Verify that both rules are enabled and allow inbound traffic.
3. Examine the **Enabled** value. It should display **True**. Also examine the **Direction** value, which should display **Inbound**.
4. Leave the Windows PowerShell command prompt open.

##### Test the default website

1. Switch to **SEA-ADM1** and in the taskbar select the Microsoft edge icon, which is to the right of the **File Explorer** icon.
2. In Microsoft Edge, enter **http://SEA-SVR1** in the address bar, and then select Enter.
3. Verify that IIS displays the default, **Internet Information Services** webpage.
4. In Microsoft Edge, enter **http://172.16.10.12** in the address bar, and then select Enter.
5. Verify that IIS displays the default, **Internet Information Services webpage**.
6. Leave Microsoft Edge open.

#### Task 2: Configure Web Server options

##### Configure DNS for the default website

1. On **SEA-ADM1**, right-click (or access the context menu) the **Start** button, and then select **Windows PowerShell (Admin)**.
2. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: Add-DnsServerResourceRecordA -ComputerName SEA-DC1 -Name "www" -ZoneName "contoso.com" -AllowUpdateAny -IPv4Address "172.16.10.12"
3. In the **Administrator: Windows PowerShell** window, enter the following command, and then select Enter: Get-DnsServerResourceRecord -ComputerName SEA-DC1 -ZoneName "contoso.com"
4. In the output, verify **www** displays in the **HostName** column and that **172.16.10.12** displays under the **RecordData** column in the same row as the **www** entry.

##### Test the website by using DNS names

1. In Microsoft Edge, enter **http://www.contoso.com** in the address bar, and then select Enter.
2. Verify that IIS displays the default, **Internet Information Services webpage**.

##### Enable remote management of IIS using IIS Manager

1. On **SEA-SVR1**, open a Windows PowerShell command prompt, if it's not already open.
2. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter: Install-WindowsFeature -Name Web-Mgmt-Service Wait for the command to complete, which should take approximately one minute.
3. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\WebManagement\Server' -Name EnableRemoteManagement -Value 1
4. On **SEA-SVR1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:Restart-Service wmsvc

**Note:** Setting this registry key to 1 will enable remote management of IIS. You must restart the **Web Management Service (wmsvc)** after changing the registry key.

1. On **SEA-ADM1**, open a Windows PowerShell command prompt, if it's not already open.
2. On **SEA-ADM1**, in the Windows PowerShell command prompt, enter the following command, and then select Enter:Install-WindowsFeature -Name Web-Mgmt-Console,Web-Scripting-Tools. Wait for the command to complete, which should take approximately one minute.

**Note:** The output from this command will return **NoChangeNeeded** under the **Exit Code** column. This is because, you already installed the management tools during exercise 1. This step has been left here intentionally to show the complete process of enabling remote management of IIS.

1. On **SEA-ADM1**, select the **Start** button, and then select the **Server Manager** tile. In **Server Manager**, select **Tools**, and then select **Internet Information Services (IIS) Manager**.
2. On the **Start Page**, under **Connection tasks**, select **Connect to a server**. Use the following information and select **Finish** to complete the wizard:
   * Server name: **SEA-SVR1**
   * User name: \*\*contoso\*
   * Password: **Pa55w.rd**
   * When prompted by the **Server Certificate Alert** dialog window, select **Connect**
   * Connection name: **SEA-SVR1**
3. In the **Connections** pane, select **Start Page**. Notice **Recent connections**, **Connection tasks**, **Online resources**, and **IIS News**.
4. In the **Connections** pane, select **SEA-SVR1 (contoso)**. Notice the icons listed in the **Features View** pane. In the **Actions** pane, notice the list of **Manage Server** actions.
5. In the **Connections** pane, expand **SEA-SVR1 (contoso)**, and then select **Sites**. In the **Features View** pane, notice the **Name** of the listed website and its **Status**.
6. In the **Actions** pane, select **Set Website Defaults**. In the **Website Defaults** dialog box, notice the **Application Pool** setting. Select **Cancel**.
7. Leave **Internet Information Services (IIS) Manager** open.

#### Task 3: Create and configure a new site

##### Create a webpage in the default website

1. Switch to **SEA-SVR1**, and in the **Administrator C:32.exe - powershell** window, enter the following command, and then select Enter: notepad
2. In **Notepad**, enter the following:**<p>Contoso intranet running on SEA-SVR1</p>**
3. In the menu bar, select **File**, and then select **Save As**. In the **Save As** dialog box, select **File name**, and then delete \***.txt**. In the **File name** box, enter **c:.htm**.
4. In the **Text Documents (\*.txt)** drop-down box, select **All Files**. Then select **Save**. Close **Notepad**.

##### Request a new Web Server certificate

1. On **SEA-SVR1**, in the **Administrator C:32.exe - powershell** window, enter the following command, and then select Enter:Get-Certificate -Template ContosoWebServer -DnsName www.contoso.com -CertStoreLocation cert:\LocalMachine\My.
2. Wait for the command to complete, which should take approximately 30 seconds.
3. In the output, verify that **Issued** displays under **Status**.

#### Task 4: Verify site functionality

1. Switch to **SEA-ADM1**, and in the **Internet Information Services (IIS) Manager**, right-click (or access the context menu) **Default Web Site** and select **Bindings...**
2. In the **Site Bindings** dialog box, select **Add** and under **type**, select **https**.
3. Under **SSL certificate**, select the certificate displayed with a GUID, select **OK** and then select **Close**. The GUID will be similar to: **35B56A0F8D0AC682579BA893524EDFC6EC8FBA83**.
4. In Microsoft Edge, enter **http://www.contoso.com** in the address bar, and then select Enter.
5. Verify that IIS displays the default **Internet Information Services webpage**. Notice that **Not secure** displays next to **www.contoso.com**.
6. In the address bar, enter **https://www.contoso.com**. Verify that IIS displays the website. Notice that a padlock displays next to **www.contoso.com**. This means that the website is protected using SSL.

©2019 Microsoft Corporation. All rights reserved. The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are ***not*** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.