# Lab answer key: Implementing and configuring network infrastructure services in Windows Server

## Exercise 1: Deploying and configuring DHCP

### Task 1: Install the DHCP role

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-SVR1**.
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 **Roles & features**.
7. In the **Roles and features** pane, select the **DHCP Server** check box, and then select **Install**.
8. In the **Install Roles and Feature**s dialog box, select **Yes**.
9. Wait until a notification displays indicating that the DHCP role is installed. If necessary, select the **Notifications** icon to verify the current status.
10. In **Microsoft Edge**, select **Windows Admin Center**, and then select **SEA-SVR1**.
11. On the **Tools** pane, select **DHCP**, and then on the **details** pane, select **Install**. If DHCP is not available in the **Tools** pane for **SEA-SVR1**, close **Microsoft Edge** and sign in to **Windows Admin Center** again.
12. Wait for a notification that the DHCP PowerShell tools are installed. If necessary, select the **Notifications** icon to verify the current status.

### Task 2: Authorize the DHCP server

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In **Server Manager**, select **Notifications** in the menu, and then select **Complete DHCP configuration**.
3. In the **DHCP Post-Install configuration wizard** window, on the **Description** screen, select **Next**.
4. On the **Authorization** screen, select **Commit** to use the \*\*Contoso\* credentials.
5. When you complete both tasks, select **Close**.

### Task 3: Create a scope

1. On **SEA-ADM1**, in **Windows Admin Center**, while connected to **SEA-SVR1**, in the **Tools** pane, select **DHCP**, and then select **New scope**.
2. In the **Create a new scope** dialog box, enter the following information, and then select **Create**.
   * Protocol: **IPv4**
   * Name: **ContosoClients**
   * Starting IP address: **10.100.150.50**
   * Ending IP address: **10.100.150.254**
   * DHCP client subnet mask: **255.255.255.0**
   * Router: **10.100.150.1**
   * Lease duration: **4 days**
3. In **Server Manager**, select **Tools**, and then select **DHCP**.
4. In the DHCP window, select **Action**, and then select **Add Server**.
5. In the **Add Server** dialog box, select **This authorized DHCP server**, and then select **OK**.
6. In DHCP window, expand **172.16.10.12**, expand **IPv4**, expand **Scope [10.100.150.0] ContosoClients**, and then select **Scope Options**.
7. Select the **Action** menu, and then select **Configure Options**.
8. In the **Scope Options** dialog box, select the **006 DNS Servers** check box.
9. In the IP address box, enter **172.16.10.10**, select **Add**, and then select **OK**.

### Task 4: Configure DHCP Failover

1. On **SEA-ADM1**, in the DHCP window, select **IPv4**, select the **Action** menu, and then select **Configure Failover**.
2. In the **Configure Failover** window, verify that the **Select all** check box is checked, and then select **Next**.
3. On the **Specify the partner server to use for failover** screen, in the **Partner Server** box, enter **SEA-DC1**, and then select **Next**.
4. On the **Create a new failover relationship** screen, enter the following information, and then select **Next**.
   * Relationship Name: **SEA-SVR1 to SEA-DC1**
   * Maximum Client Lead Time: **1 hour**
   * Mode: **Hot standby**
   * Role of Partner Server: **Standby**
   * Addresses reserved for standby server: **5%**
   * State Switchover Interval: **Disabled**
   * Enable Message Authentication: **Enabled**
   * Shared Secret: **DHCP-Failover**
5. Select **Finish**.
6. In the **Configure Failover** dialog box, select **Close**.
7. Under **172.16.10.12**, select **IPv4**, and then verify that only one scope is listed.
8. Expand **SEA-DC1**, select **IPv4**, and then verify that two scopes are listed.
9. Select **Scope [172.16.0.0] Contoso**, select the **Action** menu, and then select **Configure Failover**.
10. In the **Configure Failover** window, select **Next**.
11. On the **Specify the partner server to use for failover** screen, in the **Partner Server** box, enter **172.16.10.12**, select the **Reuse existing failover relationships configured with this server (if any exist)** check box, and then select **Next**.
12. On the **Select from failover relationships which are already configured on this server** screen, select **Next**, and then select **Finish**.
13. In the **Configure Failover** dialog box, select **Close**.
14. Under **172.16.10.12**, select **IPv4**, and then verify that both scopes are listed. If necessary, select **F5** to refresh.

### Task 5: Verify DHCP functionality

1. On **SEA-CL1**, select **Start**, and then select **Settings**.
2. In the **Settings** window, select **Network & Internet**, and then select **Network and Sharing Center**.
3. In **Network and Sharing Center**, select **Ethernet**, and then select **Properties**.
4. In the **Ethernet Properties** dialog box, select **Internet Protocol Version 4 (TCP/IPv4)**, and then select **Properties**.
5. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Obtain an IP address automatically**, select **Obtain DNS server address automatically**, and then select **OK**.
6. Select **Close**, and then select **Details**.
7. In the **Network Connection Details** dialog box, verify that DHCP is enabled, an IP address was obtained, and that the **SEA-SVR2 (172.16.10.12)** DHCP server issued the lease.
8. Select **Close**, and then select **Disable**.
9. On **SEA-ADM1**, in the **DHCP** window, under **172.16.10.12**, under **IPv4**, expand **Scope [172.16.0.0] Contoso**, and then select **Address Leases**.
   1. Verify that **SEA-CL1** is listed as a lease.
10. Under **SEA-DC1**, under **IPv4**, expand **Scope [172.16.0.0] Contoso**, and then select **Address Leases**.
11. Verify that **SEA-CL1** is listed as a lease.
12. Select **172.16.10.12**, select the **Action** menu, select **All Tasks**, and then select **Stop**.
13. Close all open windows on **SEA-ADM1**.
14. On **SEA-CL1**, in the **Network and Sharing Center**, on the left **navigation** pane, select **Change adapter settings**.
15. In the **Network Connections** window, right-click or access the context menu for **Ethernet**, and then select **Enable**.
16. In the menu bar, select **View status of this connection**, and then select **Details**. Verify that the DHCP server is now **SEA-DC1 (172.16.10.10)**.
17. Close all open windows on **SEA-CL1**.

## Exercise 2: Deploying and configuring DNS

### Task 1: Install the DNS role

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-SVR1**.
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. In the **Tools** pane, select **Roles & features**.
7. In the **Roles and features** pane, select the **DNS Server** check box, and then select **Install**.
8. In the **Install Roles and Features** dialog box, select **Yes**.
9. Wait until a notification appears indicating that the DNS role is installed. If necessary, select the **Notifications** icon to verify the current status.
10. In **Microsoft Edge**, select **Windows Admin Center**, and then select **SEA-SVR1**.
11. In the **Tools** pane, select **DNS**, and then on the **details** pane, select **Install**. If DNS is not available in the **Tools** pane for **SEA-SVR1**, close **Microsoft Edge** and sign in to **Windows Admin Center** again.
12. Wait until a notification appears indicating that the DNS PowerShell tools are installed. If necessary, select the **Notifications** icon to verify the current status.

### Task 2: Create a DNS zone

1. On **SEA-ADM1**, in **Windows Admin Center**, select **Create a new DNS zone**.
2. In the **Create a new DNS zone** dialog box, enter the following information, and then select **Create**:
   * Zone type: **Primary**
   * Zone name: **TreyResearch.net**
   * Zone file: **Create a new file**
   * Zone file name: **TreyResearch.net.dns**
   * Dynamic update: **Do not allow dynamic update**
3. Select **TreyResearch.net**, and then select **Create a new DNS record**.
4. In the **Create a new DNS record** dialog box, enter the following information, and then select **Create**:
   * DNS record type: **Host (A)**
   * Record name: **TestApp**
   * IP address: **172.30.99.234**
   * Time to live: **600**
5. Select **Start**, and then select **Windows PowerShell**.
6. At the **Windows PowerShell** prompt, enter the following, and then select Enter:

* Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net

1. Close the **Windows PowerShell** prompt.

### Task 3: Configure forwarding

1. On **SEA-ADM1**, select **Start**, and then select **Server Manager**.
2. In **Server Manager**, select **Tools**, and then select **DNS**.
3. In **DNS Manager**, select **DNS**, select **Action**, and then select **Connect to DNS Server**.
4. In the **Connect to DNS Server** dialog box, select **The following computer**, enter **SEA-SVR1**, and then select **OK**.
5. In **DNS Manager**, select **SEA-SVR1**, select **Action**, and then select **Properties**.
6. In the **SEA-SVR1 Properties** dialog box, select the **Forwarders** tab, and then select **Edit**.
7. In the **Edit Forwarders** dialog box, in the **IP addresses for forwarding servers** box, enter **131.107.0.100**, and then select **OK**.
8. In the **SEA-SVR1 Properties** dialog box, select **OK**.

### Task 4: Configure conditional forwarding

1. On **SEA-ADM1**, in **DNS Manager**, expand **SEA-SVR1**, and then select **Conditional Forwarders**.
2. Select **Action**, and then select **New Conditional Forwarder**.
3. In the **New Conditional Forwarder** dialog box, in the **DNS Domain** box, enter **Contoso.com**.
4. In the **IP addresses of the master servers** box, enter **172.16.10.10**, and then select **Enter**.
5. Select **OK**.
6. Close **DNS Manager** and **Server Manager**.
7. Select **Start**, and then select **Windows PowerShell**.
8. At the **Windows PowerShell** prompt, enter the following, and then select Enter:

* Resolve-DnsName -Server sea-svr1.contoso.com -Name sea-dc1.contoso.com

1. Close the Windows PowerShell prompt.

### Task 5: Configure DNS policies

1. On **SEA-ADM1**, in Windows Admin Center, while connected to **SEA-SVR1**, use PowerShell to sign in remotely.
2. At the **Password** prompt, enter **Pa55w.rd**, and then select **Enter**.
3. To create a head office subnet, enter the following, and then select Enter:

* Add-DnsServerClientSubnet -Name "HeadOfficeSubnet" -IPv4Subnet "172.16.10.0/24"

1. To create a zone scope for head office, enter the following, and then select Enter:

* Add-DnsServerZoneScope -ZoneName "TreyResearch.net" -Name "HeadOfficeScope"

1. To add a new resource record for the head office scope, enter the following, and then select Enter:

* Add-DnsServerResourceRecord -ZoneName "TreyResearch.net" -A -Name "testapp" -IPv4Address "172.30.99.100" -ZoneScope "HeadOfficeScope"

1. To create a new policy that links the head office subnet and the zone scope, enter the following, and then select Enter:

* Add-DnsServerQueryResolutionPolicy -Name "HeadOfficePolicy" -Action ALLOW -ClientSubnet "eq,HeadOfficeSubnet" -ZoneScope "HeadOfficeScope,1" -ZoneName "TreyResearch.net"

1. Close **Windows Admin Center**.

### Task 6: Verify DNS policy functionality

1. On **SEA-CL1**, right-click or access the context menu for **Start**, and then select **Windows PowerShell**.
2. At the **Windows PowerShell** prompt, enter **ipconfig**, and then select **Enter**. Note that the Ethernet adapter has an IP address that is part of the HeadOfficeSubnet configured in the policy.
3. Enter **Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net**, and then select **Enter**. The name resolves to the IP address 172.30.99.100 that was configured in the HeadOfficePolicy.
4. Select **Start**, and then select **Settings**.
5. In the **Settings** window, select **Network & Internet**, and then select **Network and Sharing Center**.
6. In **Network and Sharing Center**, select **Ethernet**, and then select **Properties**.
7. In the **Ethernet Properties** dialog box, select **Internet Protocol Version 4 (TCP/IPv4)**, and then select **Properties**.
8. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select **Use the following IP address**, enter the following information, and then select **OK**:
   * IP Address: **172.16.11.100**
   * Subnet mask: **255.255.0.0**
   * Default gateway: **172.16.10.1**
   * Preferred DNS server: **172.16.10.10**
9. Select **Close** twice.
10. At the **Windows PowerShell** prompt, enter the following, and then select Enter:

* Resolve-DnsName -Server sea-svr1.contoso.com -Name testapp.treyresearch.net

1. Notice that the name resolves to **172.30.99.234** because the client is no longer on the HeadOffice subnet.
2. Close all open windows.

* **Note:** When the client is on the HeadOffice subnet **(172.16.10.0/24)** the record testapp.treyresearch.net resolves to **172.30.99.100**. When the client is moved off of the HeadOffice subnet, testapp.treyresearch.net resolves to **172.30.99.234**.

©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.