Networking - Virtual Cloud Network: Configure Remote VCN Peering

Lab 4-2 Practices

Get Started

Overview

In this lab, you will use Dynamic Routing Gateways (DRGs) to inter-connect two Virtual Cloud Networks (VCNs) in different OCI regions.

Note: This lab requires you to subscribe to two regions. Hence, you will not be able to perform it in Free Tier account.

Remote VCN Peering

Remote VCN peering is the process of connecting two VCNs, typically, but not required to be in different regions. Peering allows VCNs' resources to communicate using private IP addresses.

Dynamic Routing Gateway

A Dynamic Routing Gateway is a powerful virtual router that enables VCN connectivity to on-premises resources and to remote and local VCNs in the current tenancy and in other tenancies.

Summary of Networking Components for Remote Peering

The Networking service components required for a remote peering include:

- DRG attachment to each VCN in the peering relationship.
- A remote peering connection (RPC) on each DRG in the peering relationship.
- A connection between those two RPCs.
- Supporting route rules to enable traffic to flow over the connection.
- Supporting security rules to control the types of traffic allowed to and from the instances in the subnets that need to communicate with the other VCN.

In this lab, you will:

a. Create Virtual Cloud Network 01.

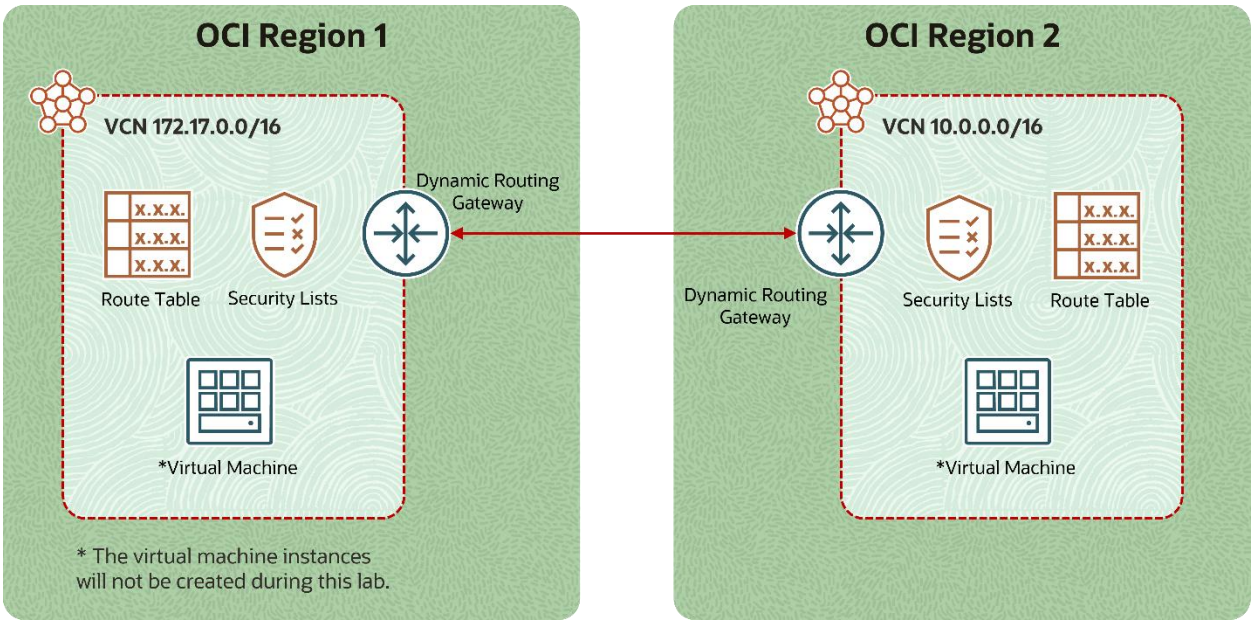
b. Create Virtual Cloud Network 02.

c. Create a Dynamic Routing Gateway in each OCI region.

d. Create Remote Peering Connection attachments and establish the connection between the two DRGs.

e. Add Route Rules.

f. Add Security Rules.



Create Virtual Cloud Network 01

In this section, you will first create the first of two VCNs by using the Start VCN Wizard.

Tasks

1. Log in to the Oracle Cloud Infrastructure (OCI) console.
2. In the console ribbon at the top of the screen, open the **Regions** menu and select **Germany Central (Frankfurt).**
3. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
4. Click **Start VCN Wizard**.
5. Select the **Create VCN with Internet Connectivity** option, and then click **Start VCN Wizard.**
6. Enter the following values:
   - **VCN Name:** `FRA-AA-LAB04-2-VCN-01`
   - **Compartment:** Select your assigned <*compartment name*>
   - **VCN CIDR Block**: `172.17.0.0/16`
   - **Public Subnet CIDR Block:** `172.17.0.0/24`
   - **Private Subnet CIDR Block:** `172.17.1.0/24`
7. Leave the default values for the remaining fields. Click **Next**.
8. Review and understand the list of resources that the OCI VCN Wizard will create. Notice that the wizard will configure CIDR block ranges for VCN IP addresses, and for the public and private subnets. It will also set up security list rules and route table rules to enable basic access to the VCN.
9. Click **Create**.
10. When complete, click **View Virtual Cloud Network**.

Create Virtual Cloud Network 02

In this section, you will first create the second of two VCNs by using the Start VCN Wizard.

Tasks

1. In the console ribbon, at the top of the screen, open the **Regions** menu and select **US West (Phoenix)**.
2. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
3. Click **Start VCN Wizard**.
4. Select the **Create VCN with Internet Connectivity** option and then click **Start VCN Wizard.**
5. Enter the following values:
   - **VCN Name:** `PHX-AA-LAB04-2-VCN-01`
   - **Compartment:** Select your assigned <*compartment name*>.
   - **VCN CIDR Block**: `10.0.0.0/16`
   - **Public Subnet CIDR Block:** `10.0.0.0/24`
   - **Private Subnet CIDR Block:** `10.0.1.0/24`
6. Leave the default values for the remaining fields. Click **Next**.
7. Review and understand the list of resources that the OCI VCN Wizard will create. Notice that the wizard will configure CIDR block ranges for VCN IP addresses, and for the public and private subnets. It will also set up security list rules and route table rules to enable basic access to the VCN.
8. Click **Create**.
9. When complete, click **View Virtual Cloud Network**.

Create a Dynamic Routing Gateway in Each OCI Region

In this section, you will create two DRGs, one in each OCI region, and attach them to the VCNs you just created.

Tasks

1. In the console ribbon at the top of the screen, open the **Regions** menu and select **Germany Central (Frankfurt).**
2. From the **Main Menu**, select **Networking**, and under **Customer Connectivity** click **Dynamic Routing Gateways**.
3. In the left navigation pane, under **List Scope** select your *<assigned compartment>.*
4. Click **Create Dynamic Routing Gateway**.
5. In the **Name** field enter `FRA-AA-LAB04-2-DRG-01`.
6. In the **Compartment**, select your assigned *<compartment name>.*
7. Click **Create Dynamic Routing Gateway**.
8. Click **Create Virtual Cloud Network Attachment**.
9. Leave the **Attachment name** field blank.
10. Select **FRA-AA-LAB04-2-VCN-01** from the **Virtual Cloud Network in**…
11. Click **Create Virtual Cloud Network Attachment** to attach your VCN to the DRG.
12. Open the **Regions** menu and select **US West (Phoenix).**
13. Click **Create Dynamic Routing Gateway**
14. In the **Name** field, enter `PHX-AA-LAB04-2-DRG-01`.
15. Set the **Create in Compartment** select your assigned *<compartment name>.*
16. Click **Create Dynamic Routing Gateway**.
17. Click **Create Virtual Cloud Network Attachment**.
18. Leave the **Attachment name** field blank.

19. Select **PHX-AA-LAB04-2-VCN-01** from the **Virtual Cloud Network in**…

20. Click **Create Virtual Cloud Network Attachment** to attach your VCN to the DRG.

Create Remote Peering Connection Attachments and Establish the Connection Between the Two DRGs

In this section, you will establish the remote peering connection between the two DRGs.

Tasks

1. In the console ribbon at the top of the screen, open the **Regions** menu and select **US West (Phoenix).**
2. From the **Main Menu**, select **Networking**, and then under **Customer Connectivity** click **Dynamic Routing Gateways.**
3. Click **PHX-AA-LAB04-2-DRG-01.**
4. In the left navigation pane, under **Resources,** click **Remote Peering Connections Attachments (0).**
5. Click the **Create Remote Peering Connection** button.
6. Enter `PHX-AA-LAB04-2-RPC-01` in the **Name** field.
7. Set the **Create in compartment** field to your assigned *<compartment name>.*
8. Click **Create Remote Peering Connection**.
9. Select **PHX-AA-LAB04-2-RPC-01** in the **Remote Peering Connection** list.
10. Click to **Copy** the RPC **OCID** and save the value to Notepad for later use.
11. Open the **Regions** menu and select **Germany Central (Frankfurt)**.
12. Click **FRA-AA-LAB04-2-DRG-01**.
13. Under **Resources,** click **Remote Peering Connections Attachments (0).**
14. Click **Create Remote Peering Connection**.
15. Enter `FRA-AA-LAB04-2-RPC-01` in the **Name** field.
16. Set the **Create in compartment** field to your assigned *<compartment name>.*
17. Click **Create Remote Peering Connection**.

18. Select **FRA-AA-LAB04-2-RPC-01** in the **Remote Peering Connection** list.

19. Click **Establish Connection**.

20. In the console ribbon at the top of the screen, open the **Regions** menu and select **US West (Phoenix). (us-phoenix-1)**

21. Paste the OCID you previously copied and saved to your Notepad into the **Remote Peering Connection OCID** field.

22. Click **Establish Connection**.

Add Route Rules

In this section, you will add route rules to the route table to enable traffic over the peered connection.

Tasks

1. In the console ribbon at the top of the screen, from the **Regions** menu, select **Germany Central (Frankfurt)**.
2. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
3. Select **FRA-AA-LAB04-2-VCN-01.**
4. In the left navigation pane, under **Resources,** click **Route Tables (2).**
5. Click **Default Route Table for FRA-AA-LAB04-2-VCN-01**.
6. Click **Add Route Rules**.
7. Select **Dynamic Routing Gateway** under **Target Type**.
8. Set the **Destination CIDR Block** field to `10.0.0.0/24`.
9. Notice that for **Target Dynamic Routing Gateway**, the DRG**: FRA-AA-LAB04-2-DRG-01** is automatically selected, as well as your assigned Compartment.
10. Click the **Add Route Rules** button.

    Note: The route rules that will route traffic from Frankfurt to Phoenix via the DRG have been successfully added. Now we will configure the return direction.

11. In the console ribbon at the top of the screen, open the **Regions** menu and select **US West (Phoenix).**
12. Select **PHX-AA-LAB04-2-VCN-01**.
13. In the left navigation pane, under **Resources,** click **Route Tables (2)**.
14. Click **Default Route Table for PHX-AA-LAB04-2-VCN-01**.
15. Click **Add Route Rules**.
16. Select **Dynamic Routing Gateway** under **Target Type**.

17. Set the **Destination CIDR Block** field to `172.17.0.0/24`.

18. Note that the value for **Target Dynamic Routing Gateway** is automatically set to **PHX-AA-LAB04-2-DRG-01** along with your assigned *<compartment name>.*

19. Click **Add Route Rules**.

Add Security Rules

In this section, you will enable ICMP from the private IP addresses to the public subnet, allowing ping communications.

Tasks

1. In the console ribbon at the top of the screen, from the **Regions** menu, select **US West (Phoenix)**.
2. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
3. Select **PHX-AA-LAB04-2-VCN-01**.
4. In the left navigation pane, under **Resources,** click **Security Lists (2)**.
5. Click **Default Security List for PHX-AA-LAB04-2-VCN-01**.
6. Click **Add Ingress Rules**.
7. Enter `172.17.0.0/24` in the **Source CIDR** field.
8. Select **ICMP** from the **IP Protocol** field.
9. In the **Type field** enter `8`**.**
10. Click **Add Ingress Rules.**
11. In the console ribbon at the top of the screen, open the **Regions** menu and select **Germany Central (Frankfurt).**
12. Select **FRA-AA-LAB04-2-VCN-01**
13. In the left navigation pane, under **Resources,** click **Security Lists (2).**
14. Click **Default Security List for FRA-AA-LAB04-2-VCN-01**.
15. Click **Add Ingress Rules**.
16. Enter `10.0.0.0/24` in the **Source CIDR** field.
17. Select **ICMP** in the **IP Protocol** field.

18. In the **Type** field, enter `8`.

19. Click **Add Ingress Rules.**

This completes the lab.

.