Networking – DNS Management: Create a Private DNS Zone

Lab 6-1 Practices

Get Started

Overview

In this practice, you will configure a private DNS zone and create a DNS A record that corresponds to a private IP address. You will create two compute instances, one running Oracle Linux that will be used as a web server, and another running Microsoft Windows, which will be used as a client.

Private DNS Zones

Private DNS zones contain DNS data that is accessible only from within a Virtual Cloud Network (VCN). A private DNS zone has capabilities similar to an Internet DNS zone but provides responses only for clients that can reach it through a private VCN. Each zone belongs to a single view.

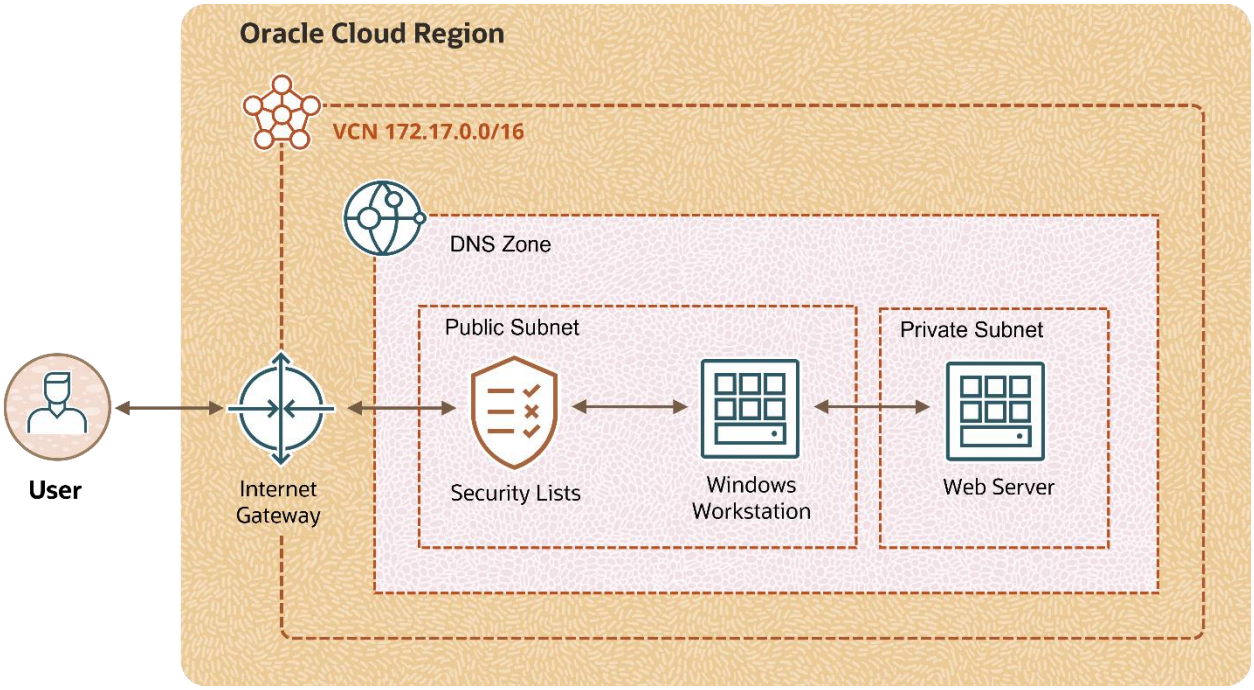
In this lab, you will:

a. Create a Virtual Cloud Network

b. Create two compute instances

c. Create a private DNS zone

d. Access the private DNS zone from your Windows compute instance



Prerequisites

- You will use Remote Desktop Connection (RDC) to access a Windows compute instance from your personal workstation. You can download RDC here.

Note: Oracle does not provide support for Remote Desktop Connection.

Create a Virtual Cloud Network

In this practice, you will create a VCN and associated resources by using the VCN Wizard.

Tasks

1. In the console ribbon at the top of the screen, click the **Regions icon** to expand the menu. Ensure that you are in the correct region, **Germany Central (Frankfurt).**
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:
   - **Name:** `FRA-AA-LAB06-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`
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. Once complete, click **View Virtual Cloud Network**.
10. Under **Resources**, select **Security Lists**
11. Select **Security List for Private Subnet-FRA-AA-LAB06-VCN-01**.
12. Click **Add Ingress Rules** and enter the following:
    - **Source CIDR:** `172.16.0.0/12`
    - **Destination Port Range:** `80`
13. Click **Add Ingress Rules.**

Create Two Compute Instances

In this practice, you will create two compute instances. One will run Oracle Linux and the Apache web server and the other will run Microsoft Windows as its operating system.

Tasks

Build the First Compute Instance

1. In the console ribbon at the top of the screen, click the **Regions icon** to expand the menu. Ensure that you are in the correct region, **Germany Central (Frankfurt)**.

2. From the **Main Menu**, select **Compute**, and then click **Instances**.

3. In the left navigation pane, under **List Scope**, select your assigned *<compartment name>*.

4. Click **Create Instance** and enter the following values:
   - **Name**: `FRA-AA-LAB06-VM-01`
   - **Compartment**: Your assigned *<compartment name>*
   - **Placement**: AD-1
   - **Image:** Oracle Linux
   - **Shape:** Click **Change Shape**
     - **Instance Type:** Virtual Machine
     - **Shape Series**: Ampere
     - **Shape Name:** VM.Standard.A1.Flex (1 OCPU, 6 GB Memory)
   - Click **Select Shape.**
   - **Networking:**
     - **Primary network:** Select an existing virtual cloud network.
     - **Virtual Cloud Network in *<assigned compartment>***: FRA-AA-LAB06-VCN-01
     - **Subnet in *<assigned compartment>***: Private Subnet-FRA-AA-LAB06-VCN-01 (regional)
   - **Add SSH Key:** No SSH Keys
   - Click **Show advanced options.**
   - On the Management tab, click **Paste cloud-init script** under **Initialization script.**

- Copy and paste the following into the **Cloud-init script** field:

```
#!/bin/bash -x
iptables -A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
yum -y install httpd
systemctl enable httpd.service
systemctl start httpd.service
firewall-offline-cmd --add-service=http
firewall-offline-cmd --add-service=https
systemctl enable firewalld
systemctl restart firewalld
echo Hello World! My name is FRA-AA-LAB06-WS-01>
/var/www/html/index.html
```

Note: This script configures and enables the compute instance's firewall and httpd processes.

5. Click **Create** and wait for the status to become Active.

   Note: The process will take approximately three minutes.

6. **Locate** the compute instance's **Private IP** address under **Primary VNIC**. Copy the value to Notepad for later use.

7. Under **Instance details**, click **Virtual cloud network: FRA-AA-Lab06-VCN-01.**

8. Under Resources, click **Security List (2)**.

9. Under **Security Lists in <*Your Compartment*> Compartment,** click **Default Security List for FRA-AA-LAB06-VCN-01**.

10. Click **Add Ingress Rules** and enter the following:
    - **Source CIDR:** `172.16.0.0/12`
    - **Destination Port Range:** `80`
    - Click **+ Another Ingress Rule**
    - Under **Ingress Rule 2**, in the **Source CIDR** field enter `0.0.0.0/0`
    - **Destination Port Range:** `3389`

11. Click **Add Ingress Rules.**

Build the Second Compute Instance

1. In the console ribbon at the top of the screen, click the **Regions** icon to expand the menu. Ensure that you are in the correct region, **Germany Central (Frankfurt)**.

2. From the **Main Menu**, select **Compute**, and then click **Instances**.

3. In the left navigation pane, under **List Scope**, select your assigned *<compartment name>*.

4. Click **Create Instance** and enter the following values:
   - **Name**: `FRA-AA-LAB06-VM-02`
   - **Compartment**: Your assigned *<compartment name>*
   - **Placement**: AD-2
   - **Image and Shape:** Click **Change Image**.
     - Select **Windows** (Windows Server 2022 Standard)
     - Select **I have reviewed and accept the following documents Oracle and Microsoft Windows Terms of Use.**

       Note: It is your responsibility to read and understand the terms of use before accepting.
     - Click **Select image**.
   - Click **Change shape**.
     - **Instance Type:** Virtual Machine
     - **Shape Series**: AMD
     - **Shape Name:** VM.Standard.E4.Flex (1 OCPU, 8 GB Memory)
   - Click **Select shape**.
   - **Networking:**
     - **Primary network:** Select **Existing virtual cloud network**.
     - **Virtual Cloud Network in *<assigned compartment>***: FRA-AA-LAB06-VCN-01
     - **Subnet in *<assigned compartment>***: Public Subnet-FRA-AA-LAB06-VCN-01 (regional)
5. Click **Create**.

Create a Private DNS Zone

In this practice, we will create a private DNS zone and access it from the Windows compute instance located on the same Virtual Cloud Network where the web server is.

Tasks

1. In the console ribbon at the top of the screen, click the **Regions icon** to expand the menu. Ensure that you are in correct region, **Germany Central (Frankfurt).**
2. From the **Main Menu**, select **Networking**, Under **DNS Management**, click **Zones**.
3. In the left navigation pane, under **List Scope**, select your assigned <*compartment name*>.
4. Click the **Private Zones** tab.
5. Click **Create Zone** and enter the following values:
   - **Zone Name**: `FRA-AA-LAB06-PrivateZone-01.com`
   - Under **DNS Private View**, click **Selecting existing DNS Private View**.
   - Under **DNS Private View in *<assigned compartment>***, select **FRA-AA-LAB06-VCN-01.**
6. Click **Create**.
7. Click **Add Record**.
8. Under **Record Type**, select **A-IPv4 Address.**
9. Under **TTL**, click the lock and set **TTL** to **30 seconds.**
10. In the **Address** field, enter the web server's private IP address that you previously pasted into Notepad.
11. Click **Submit.**
12. Click **Publish Changes**.
13. Click **Publish Changes** to confirm.

Access the Private DNS Zone from Your Windows Compute Instance

In this practice, you will connect to your Windows compute instance from your personal workstation by using Remote Desktop Connection, launch Internet Explorer, and access the private DNS zone URL, FRA-AA-LAB06-PrivateZone-01.com.

Tasks

1. In the console ribbon at the top of the screen, click the **Regions icon** to expand the menu. Ensure that you are in the correct region, **Germany Central (Frankfurt).**
2. From the **Main Menu**, select **Compute**, and then click **Instances**.
3. In the left navigation pane, under **List Scope**, select your assigned <*compartment name*>.
4. Click **FRA-AA-LAB06-VM-02.**
5. Under **Instance Access**, click **Copy** to save your **Initial password to your clipboard.**
6. Save the copied value to your Notepad.
7. Copy the **Public IP Address.**
8. On your personal workstation, open **Remote Desktop Connection.**
9. Paste the public IP address of your Windows compute instance into the **Computer** field, and click **Connect**.

Note: If there is a warning message, click **Yes**. If you are connected to any VPN or working on a restricted network connection, you will not be able to connect to the Windows machine by using RDP (Remote Desktop Protocol).

10. Paste the Initial password value that you pasted to Notepad in the **Password** field.
11. Click **Connect.**

    Note: You will be prompted to change your password upon your first connection. Do so and proceed.

12. Once connected to your Windows compute instance with RDC, launch **Internet Explorer (IE).**

13. In the top right of the browser window, click the configuration icon and select **Internet Options.**

14. Click the **Security** tab.

15. Deselect **Enable Protected Mode** and click **OK**.

    Note: You must restart Internet Explorer for the setting to take effect.

16. Restart Internet Explorer.

17. In the address field, enter `FRA-AA-LAB06-PrivateZone-01.com`.

18. You will see the custom message: **Hello World! My name is FRA-AA-LAB06-WS-01**.