ORACLE University

Oracle Cloud Infrastructure Architect Associate: Hands-on Workshop

Activity Guide

D1104310GC10

Learn more from Oracle University at ***education.oracle.com***

Disclaimer

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

Trademark Notice

Third-Party Content, Products, and Services Disclaimer

1009262023

Table of Contents

Identity and Access Management (IAM): Enable Multi-Factor Authentication (MFA) 7

Get Started 8

Enable Multi-Factor Authentication 9

Networking - Virtual Cloud Network: Create and Configure a Virtual Cloud Network 11

Get Started 12

Create a Virtual Cloud Network 13

Networking - Virtual Cloud Network: Configure Local VCN Peering 15

Get Started 16

Create Virtual Cloud Network 01 18

Create Virtual Cloud Network 02 19

Add a Local Peering Gateway (LPG) to each VCN 20

Connect the VCNs 21

Add Route Rules 22

Add Security Rules 23

Networking - Virtual Cloud Network: Configure Remote VCN Peering 25

Get Started 26

Create Virtual Cloud Network 01 28

Create Virtual Cloud Network 02 29

Create a Dynamic Routing Gateway in Each OCI Region 30

Create Remote Peering Connection Attachments and Establish the Connection Between the Two DRGs 32

Add Route Rules 34

Add Security Rules 36

Networking: OCI Load Balancer 39

Get Started 40

Create a Virtual Cloud Network 42

Create Two Compute Instances (Back-End Servers) 43

Create a Load Balancer 46

Purge Instructions 48

Networking – DNS Management: Create a Private DNS Zone 51

Get Started 52

Create a Virtual Cloud Network 54

Create Two Compute Instances 55

Create a Private DNS Zone 58

Access the Private DNS Zone from Your Windows Compute Instance 59

Compute: Create a Web Server on a Compute Instance 61
Get Started 62
Launch Cloud Shell 63
Generate SSH Keys 64
Create a Virtual Cloud Network and Its Components 66
Create a Compute Instance 69
Install an Apache HTTP Server on the Instance 71
Compute: Create a Capacity Reservation and Launch Instances 73
Get Started 74
Create a Virtual Cloud Network and a Subnet 75
Create a Capacity Reservation 76
Add a Capacity Configuration 77
Create Instances in a Capacity Reservation 78
Move an Instance out of a Capacity Reservation 80
Adding an Instance to a Capacity Reservation 81
Compute: Configure Metric-Based Autoscaling 83
Get Started 84
Create a Virtual Cloud Network and Its Components 86
Create a Load Balancer 88
Create a Compute Instance and a Custom Image 90
Create an Instance Configuration 94
Create an Instance Pool 95
Create a Metric-Based Autoscaling Configuration 97
Test Autoscaling 99
Object Storage: Create and Manage OCI Object Storage 101
Get Started 102
Create an Object Storage Bucket 105
Upload an Object to a Bucket 107
Configure a Lifecycle Policy Rules for the Bucket 108
Create a Replication Policy for the Bucket 110
Create a Retention Rule for the Bucket 112
Object Storage: Perform Multipart Upload Using CLI (Using Cloud Shell) 115
Get Started 116
Access Cloud Shell via the Console 118
Create a Standard Default Storage Tier Bucket Using CLI (Cloud Shell) 119
Upload a File (Larger than 100 MiB) to Cloud Shell 120
Perform a Multipart Upload Using the CLI (Cloud Shell) 121
Block Storage: Create, Attach, Detach, and Resize a Block Volume 123
Get Started 124

Create a Virtual Cloud Network and Its Components 126
Create a VM Instance 128
Create a Block Volume 131
Attach a Block Volume to a Compute Instance 132
Resize a Block Volume 135
Detach a Block Volume 137
Block Storage: Create a Volume Group and Enable Cross Region Replication 139
Get Started 140
Create Two Block Volumes 141
Create a Volume Group 143
Enable Cross-Region Replication for the Volume Group 145
Activate the Volume Group Replica 147
Disable Replication for a Volume Group 149
File Storage: Create and Mount a File System 151
Get Started 152
Create a Virtual Cloud Network and Its Components 154
Create a VM Instance 157
Create a File System 160
Configure VCN Security Rules for File Storage 162
Mount the File System from an Instance 169
File Storage: Configure NFS Export Options 171
Get Started 172
Create a Virtual Cloud Network and Its Components 174
Create a VM Instance 177
Create a File System 180
Configure VCN Security Rules for File Storage 182
Set Export Options for the File System 189
Mount the File System from Both the Instances 191
Perform Testing 192
Security: Enable Cloud Guard 195
Get Started 196
Create a Virtual Cloud Network 198
Explore Cloud Guard 199
Create a Cloud Guard Target 201
Create a Scenario to Verify Cloud Guard Monitoring 202
Remediate the Problems Identified by Cloud Guard 203
Security: Create a Vault and Encryption Key and Perform Encryption/Decryption of Data 205
Get Started 206
Create a Master Encryption Key 207

Perform Encryption 208
Perform Decryption 210
Observability and Management: Configure Alarms with Notifications and Create Monitoring Queries 213
Get Started 214
Set Up the Environment 216
Create Alarms and View Service Metrics 222
Create CPU Stress and Fire Alarm 226
Create Queries 229
Observability and Management: Configure Logging for a Resource 233
Get Started 234
Set Up the Environment 236
Enable Service Logs 241
Create Custom Logs 243
Search Your Logs 247
Observability and Management: Configure Service Connectors 251
Get Started 252
Set Up the Environment 253
Enable Service Logs 255
Export Logs Using Service Connectors 258

Identity and Access Management (IAM): Enable Multi-Factor Authentication (MFA)

Lab 1-1 Practices

Get Started

Overview

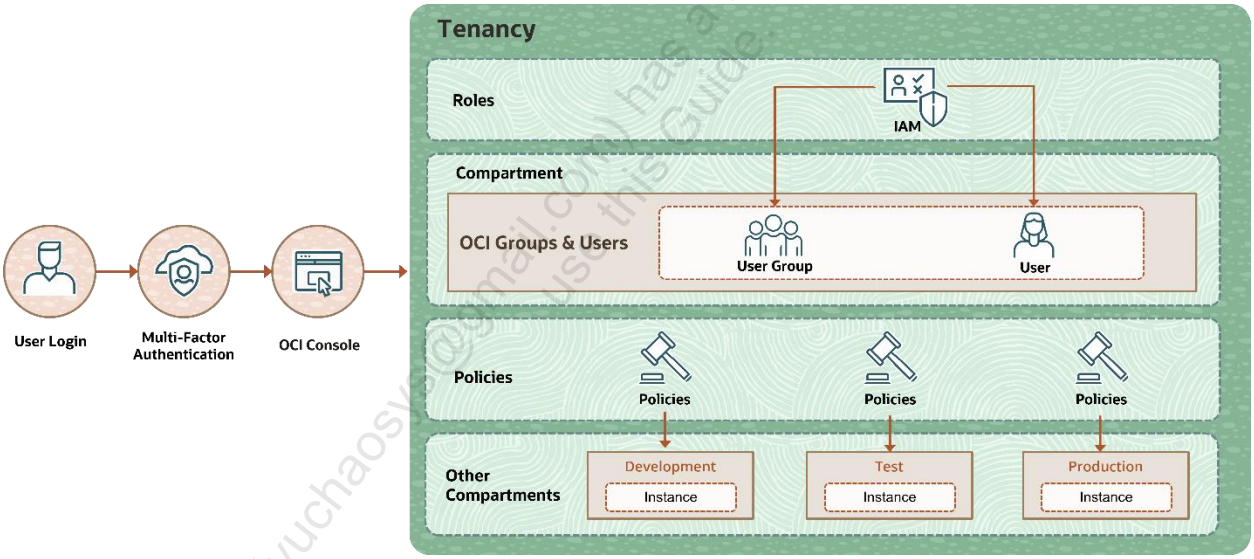
Multi-Factor Authentication (MFA) is a method of authentication that requires the use of more than one factor to verify a user's identity.

With MFA enabled in the IAM service, a user signs in to the Oracle Cloud Infrastructure (OCI) console and is prompted to enter two factors:

- Their username and password, which are things that they *know*
- A verification code from a registered MFA device, which is something that they *have*

The two factors work together, requiring an extra layer of security to verify the user's identity and complete the sign-in process.

In this lab, you'll enable Multi-Factor Authentication in OCI.



Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.
- You must install a supported authenticator app (Oracle Mobile Authenticator or Google Authenticator) on the mobile device you intend to register for MFA.

Enable Multi-Factor Authentication

You will learn how to enable Multi-Factor Authentication (MFA) for your Oracle Cloud Infrastructure (OCI) account.

In this practice, you will also learn the sign-in process after enabling MFA.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console by using the Direct Sign-In method.

   Note: If the **Customize your Console** pop-up window appears, select the profiles that best describe your Oracle Cloud Infrastructure work or interests.

2. In the console ribbon at the top of the screen, click the **Profile** icon and click the *<username>* with which you logged in to the OCI Console.
3. On the User Details page, click **Enable Multi-Factor Authentication** to open a dialog box.
4. Follow the instructions in the dialog box:

   a. Install Oracle Mobile Authenticator or a similar authenticator app on your mobile device**.**

   b. Open the app and add a new account. Scan the QR code from the dialog box when prompted.

   c. Enter the code displayed by the app.

5. After you've entered the code into the **Verification Code** box, click **Verify.** Multi-Factor Authentication is now enabled.
6. Click the **Profile** icon at the top right of the screen and click **Sign out.**
7. Sign in to your Oracle Cloud Infrastructure (OCI) Console by using the Direct Sign-In method:

   a. Enter your <*username*> in the **User Name** field.

   b. Enter your <*password*> in the **Password** field.

   c. Click **Sign In**.

Note: After your username and password are authenticated, you have successfully supplied the first factor for authentication. The second factor appears on an authentication page and prompts you to enter a one-time passcode.

8. Open the Oracle Mobile Authenticator app on your registered mobile device and then open the account for your Oracle Cloud Infrastructure (OCI) tenancy.

9. Enter the passcode displayed by your authenticator app and then click **Sign In**. You are now successfully signed in to the OCI Console.

   Important: The authenticator app generates a new time-based, one-time passcode every 30 seconds. You must enter a code while the code is still valid. If you miss the time window for one passcode, you can enter the next one that is generated.

Networking - Virtual Cloud Network: Create and Configure a Virtual Cloud Network

Lab 3-1 Practices

Get Started

Overview

In this practice, you will configure and deploy a Virtual Cloud Network (VCN).

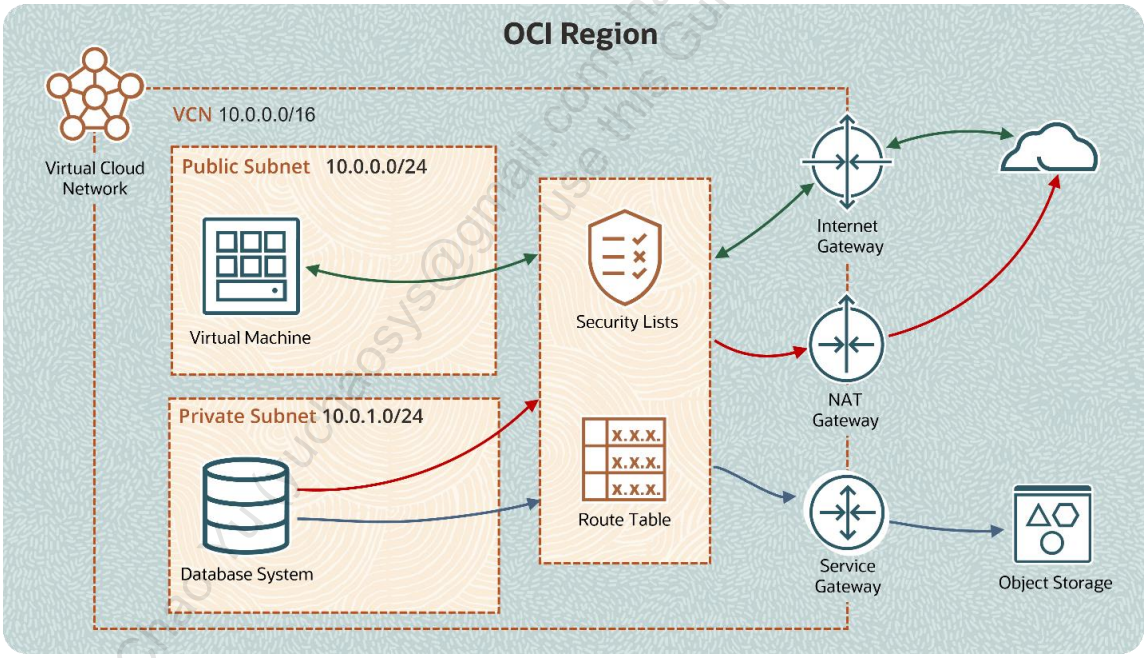
A VCN is a software-defined network specific to your OCI tenancy or a compartment in a specified region.

Upon creation, a VCN automatically includes route tables, security lists (with default security rules), and a set of DHCP options. The VCN also has access to a DNS resolver.

A VCN that is launched with the OCI VCN Wizard tool automatically creates the following:

- Public and Private subnets
- Internet Gateway (IG)
- NAT Gateway (NAT)
- Service Gateway (SG)
- Two Route Tables (RT)
- Two Security Lists (SL)

For more information about Virtual Cloud Networks, see the [OCI Networking Documentation](): https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/landing.htm



Prerequisites

- You need to have service limits for all the resources listed above.
- You need to be in a group that has manage access to virtual-network-family.

Create a Virtual Cloud Network

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

Steps

1. Log in to the Oracle Cloud Infrastructure (OCI) console.
2. In the console ribbon at the top of the screen, click the Region icon to expand the menu. Ensure that you are in the correct region, Germany Central (Frankfurt).
3. Click the **Main Menu**, click **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:

   Name: `FRA-AA-LAB03-VCN-01`

   Compartment: Select your <*assigned compartment*>.
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**.

Networking - Virtual Cloud Network: Configure Local VCN Peering

Lab 4-1 Practices

Get Started

Overview

In this practice, you will configure Local Peering Gateways (LPGs) to interconnect two Virtual Cloud Networks (VCNs).

Local VCN Peering

Local VCN peering is the process of connecting two VCNs in the same region so that their resources can communicate using private IP addresses.

Local Peering Gateway

A Local Peering Gateway is a component on a VCN for routing traffic to a locally peered VCN.

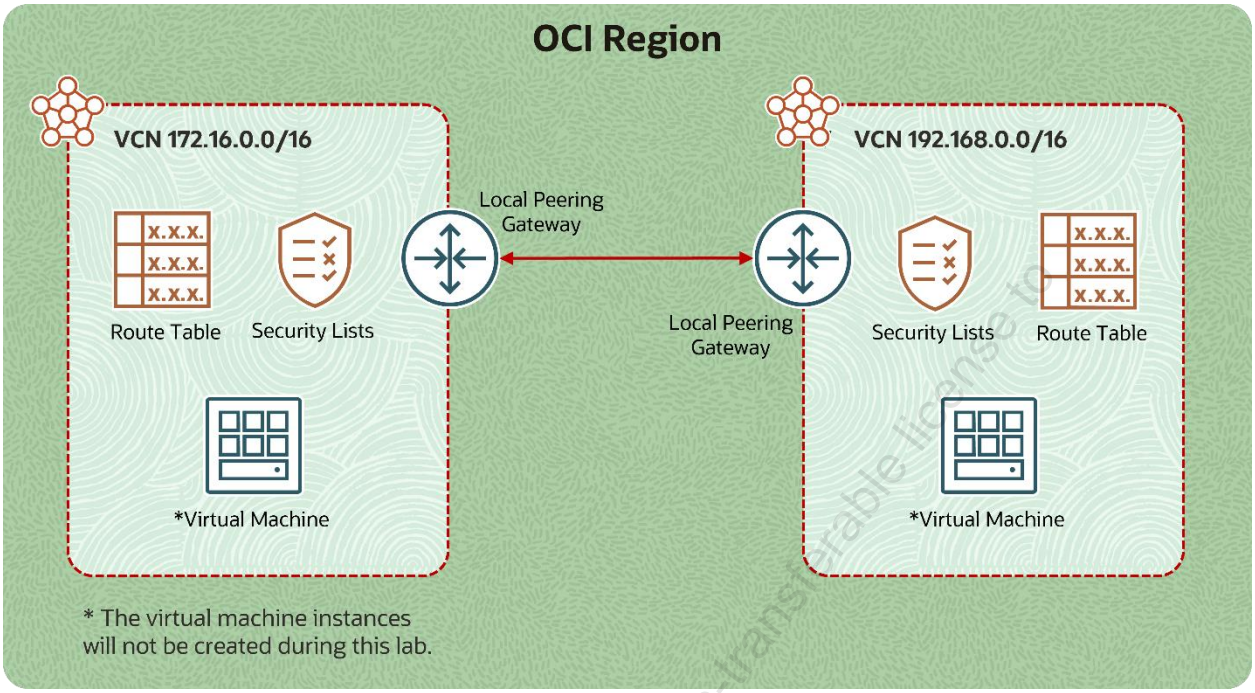
Summary of Networking Components for Peering Using an LPG

The Networking service components required for a local peering include:

- Two VCNs with non-overlapping CIDRs, in the same region
- A local peering gateway (LPG) on each VCN in the peering relationship
- A connection between those two LPGs
- 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:

1. Create Virtual Cloud Network 01.
2. Create Virtual Cloud Network 02.
3. Add a Local Peering Gateway (LPG) to each VCN.
4. Connect the VCNs.
5. Add Route Rules.
6. Add Security Rules.



Prerequisites

- You need to have service limits for all resources listed above.
- You need to be in a group that has manage access to VCN and LPG resources.

Create Virtual Cloud Network 01

In this section, you will 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, click the Region and select **Germany Central (Frankfurt)**.
3. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
4. In the left navigation pane, under **List Scope** select your <*assigned compartment*>.
5. Click **Start VCN Wizard**.
6. Select the **Create VCN with Internet Connectivity** option, and then click **Start VCN Wizard**.
7. Enter the following values:
   - **VCN Name:** `FRA-AA-LAB04-1-VCN-01`
   - **Compartment:** Select your <*assigned compartment*>.
   - **VCN CIDR Block**: `172.16.0.0/16`
   - **Public Subnet CIDR Block:** `172.16.0.0/24`
   - **Private Subnet CIDR Block:** `172.16.1.0/24`
8. Leave the default values for the remaining fields. Click **Next**.
9. 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.
10. Click **Create**.
11. When complete, click **View Virtual Cloud Network**.

Create Virtual Cloud Network 02

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

Tasks

1. In the console ribbon at the top of the screen, click the Region and select **Germany Central (Frankfurt).**
2. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
3. In the left navigation pane, under **List Scope** select your *<assigned compartment>.*
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-LAB04-1-VCN-02
   - **Compartment:** Select your *<assigned compartment>*.
   - **VCN CIDR Block**: `192.168.0.0/16`
   - Public Subnet CIDR Block: `192.168.0.0/24`
   - Private Subnet CIDR Block: `192.168.1.0/24`
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. Once complete, click View Virtual Cloud Network.

Add a Local Peering Gateway (LPG) to each VCN

In this section, you will add LPGs to the VCNs.

Tasks

1. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
2. In the left navigation pane, under **List Scope** select your *<assigned compartment>*.
3. Select **FRA-AA-LAB04-1-VCN-01**.
4. In the left navigation pane, under **Resources,** click **Local Peering Gateways (0).**
5. Click **Create Local Peering Gateway**.
6. In the **Name** field, enter: `FRA-AA-LAB04-1-LPG-01`.
7. Click **Create Local Peering Gateway**.
8. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
9. Select **FRA-AA-LAB04-1-VCN-02**.
10. In the left menu, under **Resources**, click **Local Peering Gateways (0)**.
11. Click **Create Local Peering Gateway**.
12. In the **Name** field, enter**:** `FRA-AA-LAB04-1-LPG-02`.
13. Click **Create Local Peering Gateway**.

Connect the VCNs

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

Tasks

1. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
2. Select **FRA-AA-LAB04-1-VCN-01**.
3. In the left navigation pane, under **Resources,** click on **Local Peering Gateways (1).**
4. Click the three dots to the right of **FRA-AA-LAB04-1-LPG-01** to open the Actions menu and select (**Establish Peering Connection**).
5. Click **Browse Below**.
6. Select **FRA-AA-LAB04-1-VCN-02** in **Virtual Cloud Network**.
7. Select **FRA-AA-LAB04-1-LPG-02** from the **Unpeered Peer Gateway** list.
8. Click **Establish Peering Connection**.
9. Wait for the **Peering Status** field to change to **Peered - Connected to a peer**.
10. Verify that **Peer Advertised CIDRs** is 192.168.0.0/16.
11. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
12. Select **FRA-AA-LAB04-1-VCN-02**.
13. In the left menu, under **Resources**, click **Local Peering Gateways (1)**.
14. Verify that **Peering Status** is **Peered - Connected to a peer**.
15. Verify that **Peer Advertised CIDRs** is 172.16.0.0/16.

Add Route Rules

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

Tasks

1. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
2. Select **FRA-AA-LAB04-1-VCN-01**.
3. In the left navigation pane, under **Resources,** click **Route Tables (2)**
4. Click **Default Route Table** for **FRA-AA-LAB04-1-VCN-01**.
5. Click **Add Route Rules**.
6. Select **Local Peering Gateway** under **Target Type**.
7. In the **Destination CIDR Block** field, enter 192.168.0.0/24.
8. Select **FRA-AA-LAB04-1-LPG-01** under **Target Local Peering Gateway** in ***<assigned compartment>***
9. Click **Add Route Rules**.
10. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
11. Select **FRA-AA-LAB04-1-VCN-02**.
12. In the left navigation pane, under **Resources,** click **Route Tables (2).**
13. Click **Default Route Table for FRA-AA-LAB04-1-VCN-02**.
14. Click **Add Route Rules**.
15. Select **Local Peering Gateway** under **Target Type**.
16. In the **Destination CIDR Block** field, enter 172.16.0.0/24.
17. Select **FRA-AA-LAB04-1-LPG-02** under **Target Local Peering Gateway in *<assigned compartment>***
18. 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. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
2. Select **FRA-AA-LAB04-1-VCN-01**.
3. In the left navigation pane, under **Resources,** click **Security Lists (2).**
4. Click **Default Security List for FRA-AA-LAB04-1-VCN-01**.
5. Click **Add Ingress Rules**.
6. In the **Source CIDR** field, enter 192.168.0.0/24.
7. Select **ICMP** under **IP Protocol**.
8. In the **Type** field**,** enter 8.
9. Click **Add Ingress Rules**.
10. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
11. Select **FRA-AA-LAB04-1-VCN-02**
12. In the left navigation pane, under **Resources,** click **Security Lists (2).**
13. Click **Default Security List for FRA-AA-LAB04-1-VCN-02**.
14. Click **Add Ingress Rules**.
15. Enter 172.16.0.0/24 in the **Source CIDR** field.
16. In the **IP Protocol** field, select **ICMP.**
17. In the **Type** field**,** enter 8.
18. Click **Add Ingress Rules**.

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.

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.

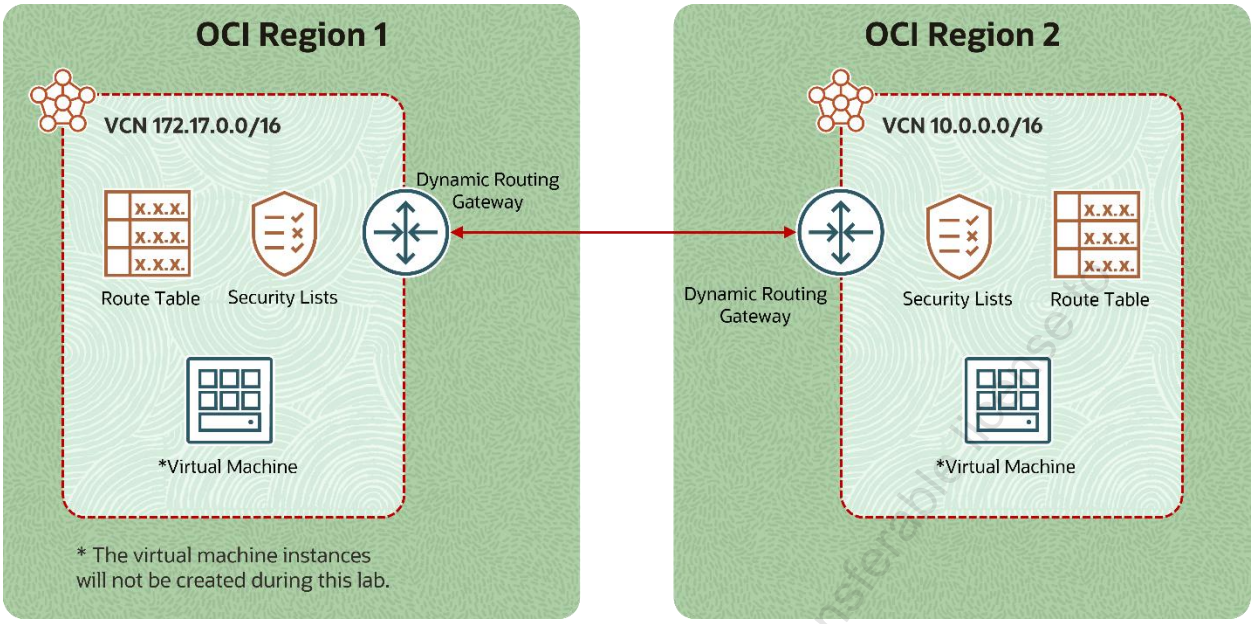
b. Create Virtual Cloud Network 02.

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.



Prerequisites

- You need to have service limits for all resources listed above.
- You need to be in a group that has manage access to VCN and DRG resources.

Regions

For this lab, the tenancy needs to subscribe to the Germany Central (Frankfurt) and US West (Phoenix) regions.

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.

Networking: OCI Load Balancer

Lab 5-1 Practice

Get Started

Overview

In this practice, you will configure a Public Load Balancer, including a set of two back-end compute instances.

Load Balancer

The OCI Load Balancer provides automated traffic distribution from one entry point to multiple back-end servers in your VCN. It operates at the connection level and balances incoming client connections to healthy back-end servers. The service offers a load balancer with your choice of a regional public or private IP address and provisioned bandwidth.

Summary of Components for OCI Load Balancer Used in This Lab

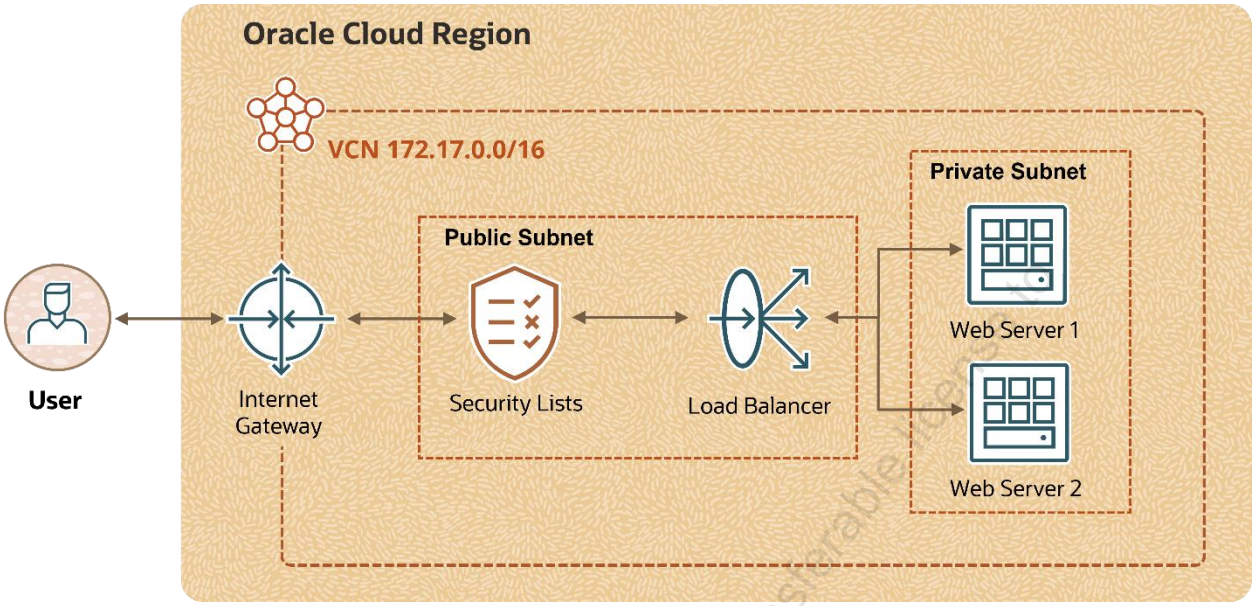
- **Listener:** A logical entity that checks for incoming traffic on the load balancer's IP address
- **Back-end server:** An application server responsible for generating content in reply to the incoming traffic
- **Back-end set:** A logical entity defined by a list of backend servers
- **Load balancing policy:** A load-balancing policy tells the load balancer how to distribute incoming traffic to the back-end servers
- **Health check:** A test to confirm the availability of back-end servers
- **Shape:** The Bandwidth capacity of the load balancer

In this lab, you will:

a. Create a Virtual Cloud Network

b. Create two compute instances

c. Create a load balancer



Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Create a Virtual Cloud Network

In this practice, you will create a VCN and associated resources 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-LAB05-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. When complete, click **View Virtual Cloud Network**.
10. In the left navigation pane, under **Resources**, click **Security Lists**.
11. Select **Default Security List for FRA-AA-LAB05-VCN-01**.
12. Click **Add Ingress Rule.**
    a. For **Source CIDR**, enter `0.0.0.0/0`.
    b. For **Destination Port Range**, enter `80`.
    c. Click **Add Ingress Rules**.

Create Two Compute Instances (Back-End Servers)

In this lab, you will create two compute instances and configure them to provide web services. They will serve as the back-end servers, and will reside in a private subnet.

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-LAB05-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 existing virtual cloud network.
     - **Virtual Cloud Network in *<assigned compartment>***: `FRA-AA-LAB05-VCN-01`
     - **Subnet in *<assigned compartment>***: Private Subnet-`FRA-AA-LAB05-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 (**Tip:** Copy the below script in a notepad and ensure that the last 2 lines of the script are copied in a single line as a single command):

```
#!/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-LAB05-WS-01> 
/var/www/html/index.html
```

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

5. Click **Create.**

Note: The process will take approximately two minutes.

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-LAB05-VM-02`
   - **Compartment**: Your assigned <*compartment name*>
   - **Placement**: AD-2
   - **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 existing virtual cloud network.
  - **Virtual Cloud Network in <*assigned compartment*>**: FRA-AA-LAB05-VCN-01
  - **Subnet in <*assigned compartment*>**: Private Subnet-FRA-AA-LAB05-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 (**Tip:** Copy the below script in a notepad and ensure that the last 2 lines of the script are copied in a single line as a single command):

```
#!/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-LAB05-WS-02>
/var/www/html/index.html
```

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

5. Click **Create.**

Note: The process will take approximately two minutes.

Create a Load Balancer

In this lab, you will create a Load Balancer, and configure the listener, the health check, and back-end set. You will then add a security rule to the security list of the private subnet.

Tasks

1. From the **Main Menu**, select **Networking**, and then click **Load Balancers.**
2. In the left navigation pane, under **List Scope**, select your assigned <*compartment name*>.
3. Click **Create Load Balancer**.
4. Select **Load Balancer**, click **Create Load Balancer** and enter the following values:
   - **Load Balancer Name**: `FRA-AA-LAB05-LB-01`
   - **Choose visibility type:** Public
   - **Assign a public IP address:** Ephemeral IP Address
   - In the **Bandwidth** section, under **Shapes,** select **Flexible Shapes (Specify Minimum Bandwidth as 10 Mbps and Maximum Bandwidth as 20 Mbps)**.
   - Under **Choose Networking,** for the **Virtual Cloud Network in *<compartment name>,*** select FRA-AA-LAB05-VCN-01 and for the **Subnet in *<compartment name>,*** select **Public** Subnet-FRA-AA-LAB05_VCN-01.
   - Click **Next**.
   - Under **Choose Backends** select **Weighted Round Robin**.
   - Click **Add Backends**.
   - Select both **FRA-AA-LAB05-VM-01** and **FRA-AA-LAB05-VM-02**.
   - Click **Add Selected Backends**.
   - Leave all values at defaults in the **Specify Health Check Policy** section.
   - Click **Next**.
   - On the **Configure Listener** page, enter the following values:
     - **Listener Name:** FRA-AA-LAB05-Listener-01
     - **Specify the type of traffic you listener handles:** HTTP

       Note: The **Specify the port your listener monitors for ingress traffic** value will become 80.
   - Click **Next**.
   - On the **Manage** Logging page, set **Error Logs** to **Not Enabled**.
5. Click **Submit** and wait for the status to become **Active.**

Note: The process will take approximately three minutes.

6. Verify that the **Backend Set Health** status is **OK.**
7. Locate and copy the Load Balancer's **IP Address.**
8. Paste the copied value into your browser's address bar to visit the site.
9. A webpage stating **Hello World! My name is FRA-AA-LAB05-WS-01** will appear.
10. Reload the page to see the other back-end server has provided the message, **Hello World! My name is FRA-AA-LAB05-WS-02.**

Purge Instructions

Purge Load Balancer

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 navigation menu, select **Networking**, and then click **Load Balancers.**
3. In the left navigation pane, under **List Scope**, select your assigned <*compartment name*>.
4. Click **FRA-AA-LAB05-LB-01.**
5. Click **Terminate**.
6. Click **Terminate** when prompted.

Purge the First Oracle Linux 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 navigation menu, select **Compute**, and click **Instances.**
3. In the left navigation pane, under **List Scope**, select your assigned <compartment name>.
4. Click **FRA-AA-LAB05-VM-01.**
5. Click **Terminate**.
6. Check **Permanently delete the attached boot volume** when prompted**.**
7. Click **Terminate instance.**

   Note: The status for the compute instance will show **Terminating.**
8. Eventually you will see the status of the compute instance will show **Terminated** and all buttons for administrative tasks for this Linux Machine will be disabled.

Purge the Second Oracle Linux 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 navigation menu, select **Compute**, and click **Instances.**
3. In the left navigation pane, under **List Scope**, select your assigned <compartment name>.
4. Click **FRA-AA-LAB05-VM-02.**
5. Click **Terminate**.
6. Check **Permanently delete the attached boot volume** when prompted**.**
7. Click **Terminate instance.**

   Note: The status for the compute instance will show **Terminating.**
8. Eventually you will see the status of the compute instance will show **Terminated** and all buttons for administrative tasks for this Linux machine will be disabled.

Purge VCN

1. Click the navigation menu, click **Networking**, and then click **Virtual Cloud Networks**.
2. In the left navigation pane, under **List Scope**, select your assigned compartment from the **Compartment** drop-down menu.
3. In the list of VCNs, click the three dots on the right of **FRA-AA-LAB05-1-VCN-01** to open the Actions menu. Select **Delete**.
4. Make sure that the **Search compartments for resources associated with this VCN** check box is selected.
5. In the white box that starts with **Select which compartments to search for associated resources**, select the **Specific compartments** option and select your assigned compartment from the drop-down menu.
6. Click **Scan.**

7. After the scan is completed, click **Delete All**.

Note: This process can take up to 2 minutes.

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.

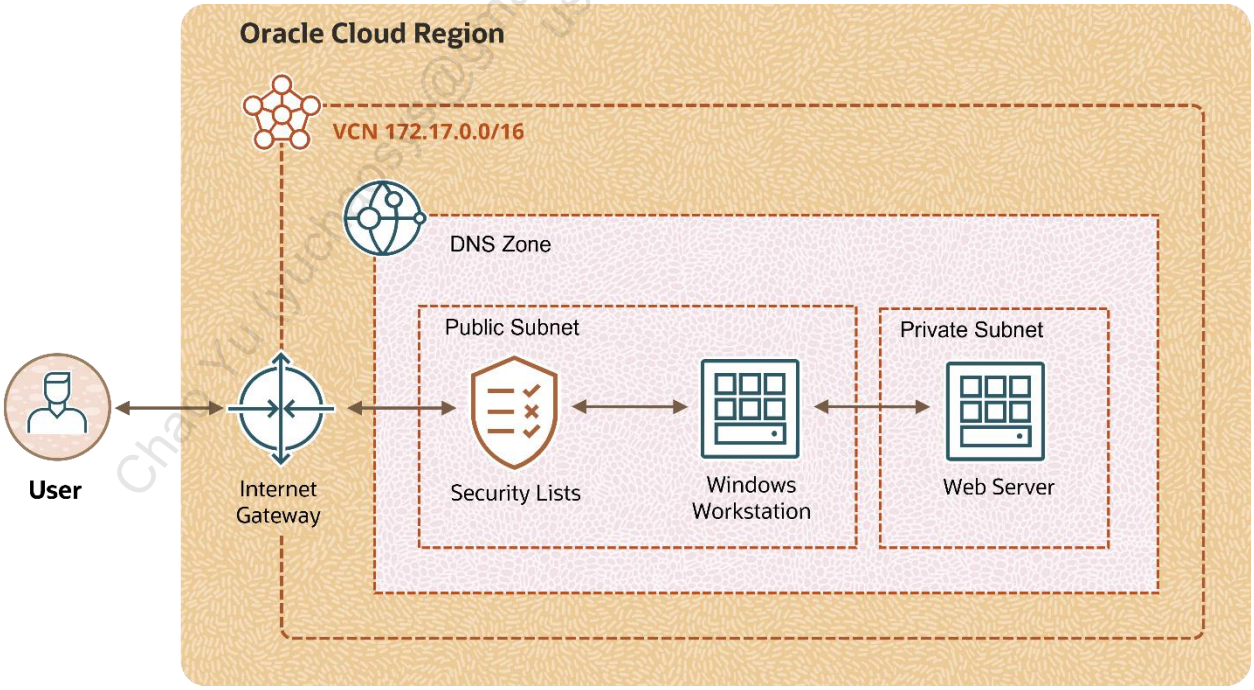
In this lab, you will:

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 need to have service limits for all resources listed above.
- 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**.

Compute: Create a Web Server on a Compute Instance

Lab 07-1 Practices

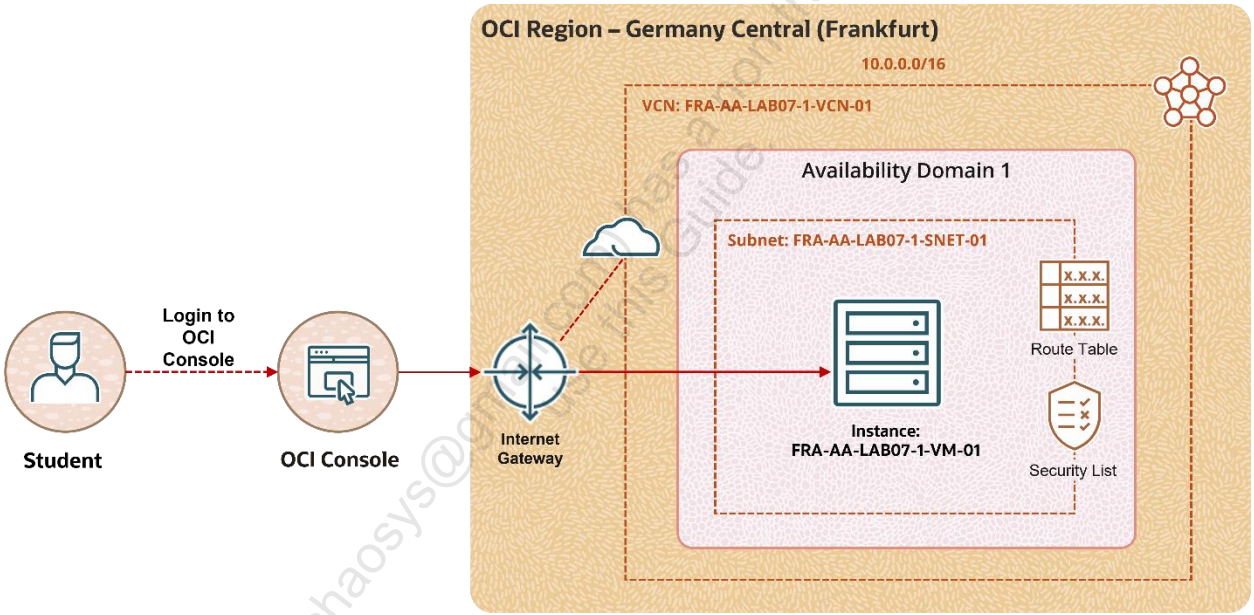
Get Started

Overview

The Oracle Cloud Infrastructure (OCI) Compute lets you provision and manage compute hosts, known as instances. You can launch instances as needed to meet your compute and application requirements. In this lab, you will create a web server on a compute instance.

In this lab, you will:

- Launch Cloud Shell
- Generate SSH keys
- Create a Virtual Cloud Network and its components
- Create a compute instance
- Install an Apache HTTP server on the instance



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- Select the region available in the tenancy allotted to you. In this lab, **Germany Central (Frankfurt)** is considered as your region.
- You must be familiar with navigating the OCI Console.

Launch Cloud Shell

The OCI Cloud Shell is a web browser–based terminal accessible from the OCI Console. It provides access to a Linux shell, with a pre-authenticated OCI CLI.

In this practice, you will access Cloud Shell via the OCI Console.

Tasks

1. Sign in to your Oracle Cloud Infrastructure Console.
2. In the Console ribbon at the top of the screen, click the Region icon to expand the menu. Ensure that you are in the correct region, **Germany Central (Frankfurt)**.
3. Click the **Cloud Shell** icon next to the Region in the Console ribbon.

   Note: The OCI CLI running in the Cloud Shell will execute commands against the region selected in the Console's region selection menu when the Cloud Shell is started.

   This displays the Cloud Shell in a "drawer" at the bottom of the console.
4. You can use the icons in the top-right corner of the Cloud Shell window to minimize, maximize, and close your Cloud Shell session.

Generate SSH Keys

In this practice, you will generate SSH keys using Cloud Shell.

Tasks

1. From the OCI Console, click the **Cloud Shell** icon next to the region in the Console ribbon.
2. After the Cloud Shell has started, run the following commands:

   ```
   $ mkdir .ssh
   ```

   Important: In case you get an error that says, "cannot create director: File exists", you can skip running the first command.

   ```
   $ cd .ssh
   ```

   ```
   $ ssh-keygen -b 2048 -t rsa -f <<sshkeyname>>
   ```

   Replace `<<sshkeyname>>` with **ociaalab7key**. Select the key name you can remember. This will be the key name you will use to connect to the compute instance you create.

   Note: If you receive an error message for the above command, enter the command manually.

   Remember:

   - After entering the third command, press **Enter** twice for no passphrase.
   - Do not include the angle brackets «» and `$` symbol when pasting code into Cloud Shell.

3. Examine the two files that you just created by running the following command:

   ```
   $ ls
   ```

   Note: In the output, there are two files, a private key: <<sshkeyname>> and a public key: <<sshkeyname>>.pub. Keep the private key safe and don't share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems as well as copied and pasted to facilitate secure communications in the cloud.

4. To list the contents of the public key, run the following command:

   ```
   $ cat <<sshkeyname>>.pub
   ```

   Replace <<*sshkeyname*>> with **ociaalab7key**.

   Note: The angle brackets «» should not appear in your code.

5. Copy the contents of the public key as you will require this in a subsequent step. Make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

Create a Virtual Cloud Network and Its Components

In this practice, you will create a Virtual Cloud Network (VCN), subnet, and Internet gateway and add route rules in the route table.

Tasks

1. From the **Main Menu**, under **Networking**, click **Virtual Cloud Networks**.
2. Click **Create VCN**.
3. In the **Create a Virtual Cloud Network** dialog box, populate the following information:
   a. **Name**: FRA-AA-LAB07-1-VCN-01
   b. **Create in Compartment**: <*your compartment*>
   c. **IPv4 CIDR Blocks**: 10.0.0.0/16 (Press **Enter** to add.)
4. Keep the other options default and click **Create VCN**.

   You can see that the VCN is created successfully.
5. Click **FRA-AA-LAB07-1-VCN-01** VCN to view the details page.
6. Click **Create Subnet**.
7. In the **Create Subnet** dialog box, populate the following information:
   a. **Name**: FRA-AA-LAB07-1-SNET-01
   b. **Create in Compartment**: <*your compartment*>
   c. **Subnet Type**: Regional
   d. **IPv4 CIDR Blocks**: 10.0.1.0/24
   e. **Subnet Access**: Public Subnet
8. Keep the other options default and click **Create Subnet**.

   You can see that the subnet is created successfully, and the state is Available.
9. Under **Resources** in the left navigation panel, click **Internet Gateways**.

10. Click **Create Internet Gateway**.
11. In the **Create Internet Gateway** dialog box, populate the following information:
    a. **Name**: FRA-AA-LAB07-1-IG-01
    b. **Create In Compartment**: <*your compartment*>
12. Click **Create Internet Gateway**.

    You can see that Internet Gateway is created successfully and the state is Available.
13. Under **Resources** in the left navigation panel, click **Route Tables**.
14. Click **Default Route Table** for FRA-AA-LAB07-1-VCN-01.
15. Click **Add Route Rules**.
16. In the **Add Route Rules** dialog box, populate the following information:
    a. **Target Type**: Internet Gateway
    b. **Destination CIDR Block**: 0.0.0.0/0
    c. **Target Internet Gateway**: FRA-AA-LAB07-1-IG-01
17. Click **Add Route Rules**.

    You can see that the route rule is successfully added in the default Route Table.
18. Navigate back to the **Virtual Cloud Networks** page from the **Main Menu**.
19. Click **FRA-AA-LAB07-1-VCN-01** VCN to view the details page.
20. Under **Resources** in the left navigation panel, click **Security Lists**.
21. Click **Default Security List** for FRA-AA-LAB07-1-VCN-01.
22. Here, you need to open port 80. Click **Add Ingress Rules**.

23. In the **Add Ingress Rules** dialog box, populate the following information:

    a. **Source Type**: CIDR

    b. **Source CIDR**: 0.0.0.0/0

    c. **IP Protocol**: TCP

    d. **Destination Port Range**: 80

    Note: Do not select the **Stateless** check box. The **Source Port Range** field is set to **All** by default.

24. Click **Add Ingress Rule**.

    You can see that the rule is successfully added.

Create a Compute Instance

In this practice, you will launch a compute instance and connect to it.

Tasks

1. From the OCI Console **Main Menu**, under **Compute**, click **Instances**.
2. Click **Create instance**.
3. In the **Create compute instance** dialog box, populate the following information:
   a. **Name**: FRA-AA-LAB07-1-VM-01
   b. **Create in compartment**: <*your compartment*>
   c. **Placement (Availability domain)**: AD 1

      Click **Show advanced options** and select **On-demand capacity** under Capacity type.
   d. **Image**: Oracle Linux 8
   e. **Shape**: Select VM.Standard.A1.Flex (1 OCPU, 6GB Memory) [Shape series: Ampere]
   f. **Primary network**: Select an existing virtual cloud network.
   g. **Virtual cloud network in *<your compartment>***: FRA-AA-LAB07-1-VCN-01
   h. **Subnet**: Select an existing subnet.
   i. **Subnet in *<your compartment>***: FRA-AA-LAB07-1-SNET-01 (regional)
   j. **Public IP address**: Assign a public IPv4 address.
   k. **Add SSH keys**: Paste public keys.
   l. **SSH Keys**: <*public key*> (Paste the public key which you copied in Step 5 of Generate SSH Keys practice.)

   Note: Keep the default option for **Boot volume**.
4. Click **Create**.

   You will see that the Instance is created successfully, and the state is **Running**.

5. Copy the Public IP corresponding to the **FRA-AA-LAB07-1-VM-01** instance and paste it in the Notepad.

6. Click the **Cloud Shell** icon next to the Region at the top of the screen.

7. Run the following command using SSH to connect to your instance:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address>
   ```

   a. The `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.

   b. The `<username>` is the default user `opc`.

   c. The `<public-ip-address>` is the public IP address of the instance.

   Note: Enter **`yes`** in response to - Are you sure you want to continue connecting (yes/no)?

You are now connected to the instance FRA-AA-LAB07-1-VM-01.

Install an Apache HTTP Server on the Instance

The HTTP Server is an open-source web server developed by the Apache Software Foundation. The Apache server hosts web content and responds to requests for this content from web browsers such as Chrome or Firefox.

In this practice, you will install an Apache HTTP web server and connect to it over the public Internet.

Tasks

1. On the OCI Console, click the **Cloud Shell** icon at the top of the screen.
2. While connected to your compute instance via SSH, run the following commands:
   a. Install Apache HTTP:

```
$ sudo yum install httpd -y
```

   b. Start the Apache server and configure it to start after system:

```
$ sudo apachectl start

$ sudo systemctl enable httpd
```

   c. Run a quick check on Apache configurations:

```
$ sudo apachectl configtest
```

   d. Create firewall rules to allow access to the ports on which the HTTP server listens:

```
$ sudo firewall-cmd --permanent --zone=public --add-
service=http

$ sudo firewall-cmd --reload
```

   e. Create an index file for your web server.

```
$ sudo bash -c 'echo This is my Web-Server running on Oracle
Cloud Infrastructure >> /var/www/html/index.html'
```

3. Open your browser and enter `http://Public-IPAddress` in the address bar (the IP Address of the Compute Instance).

You should see the index page of the web server we created in the second step (last point).

```
This is my Web-Server running on Oracle Cloud Infrastructure.
```

Compute: Create a Capacity Reservation and Launch Instances

Lab 08-1 Practices

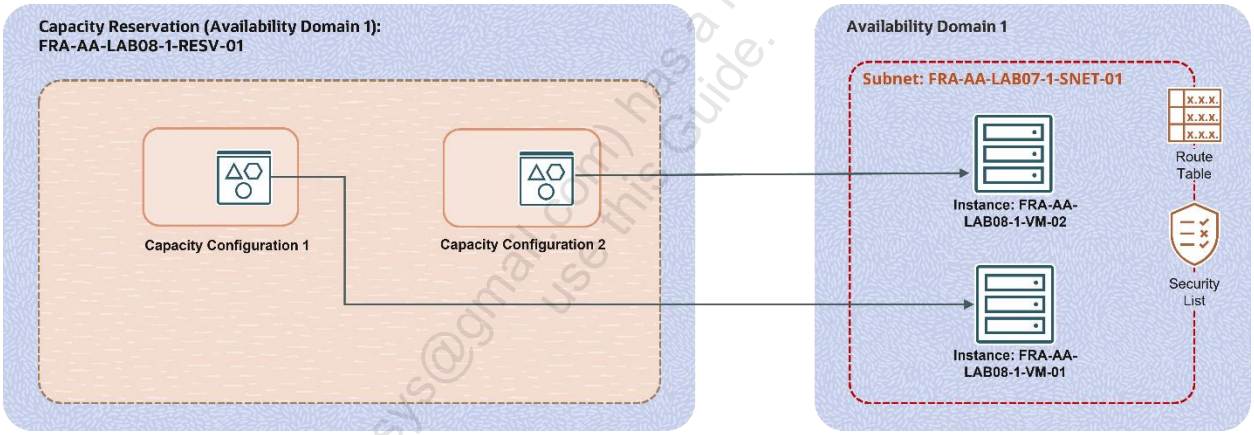
Get Started

Overview

The capacity reservations allow you to reserve compute capacity in advance and use this capacity when you create instances against the reservation. There is no minimum time or size commitment. You can create, modify, and terminate your capacity reservation at any time.

In this lab, you will:

- Create a Virtual Cloud Network and a subnet
- Create a capacity reservation
- Add a capacity configuration
- Create instances in a capacity reservation.
- Move an instance out of a capacity reservation.
- Add an instance to a capacity reservation



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- You must be familiar with navigating the OCI Console.
- Select the region available in the tenancy allotted to you. In this lab, **Germany Central (Frankfurt)** is considered as your region.

Create a Virtual Cloud Network and a Subnet

In this practice, you will create a Virtual Cloud Network (VCN) and a subnet.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) Console.
2. From the **Main Menu**, under **Networking**, select **Virtual Cloud Networks.**
3. Click **Create VCN.**
4. In the **Create a Virtual Cloud Network** dialog box, populate the following information:
    a. **Name**: FRA-AA-LAB08-1-VCN-01.
    b. **Create In Compartment**: <*your compartment*>
    c. **IPv4 CIDR Blocks:** 10.0.0.0/16 (Press **Enter** to add.)
5. Keep all the other options default and click **Create VCN**.

    You can see that the VCN is created successfully.
6. Click **FRA-AA-LAB08-1-VCN-01** VCN to view the details page and click **Create Subnet**.
7. In the **Create Subnet** dialog box, populate the following information:
    a. **Name**: FRA-AA-LAB08-1-SNET-01
    b. **Create In Compartment**: <*your compartment*>
    c. **Subnet Type**: Regional (Recommended)
    d. **IPv4 CIDR Blocks**: 10.0.1.0/24.
    e. **Subnet Access**: Public Subnet
8. Keep all the other options default and click **Create Subnet.**

    You can see that the subnet is created successfully, and the state is Available.

Create a Capacity Reservation

In this practice, you will create a capacity reservation.

Tasks

1. From the **Main Menu**, under **Compute**, click **Capacity Reservations**.
2. Click **Create capacity reservation**.
3. In the **Create capacity reservation** dialog box, populate the following information in the **Add basic details** section:
    a. **Name**: FRA-AA-LAB08-1-RESV-01
    b. **Create in compartment:** <*your compartment*>
    c. **Availability domain:** <*first availability domain*>

    Note: Do not select the **Make this reservation the default for this availability domain** check box.
4. Click **Next.**
5. In the **Add capacity configurations** dialog box, populate the following information:
    a. **Fault Domain**: First available
    b. **Shape:** VM.Standard.A1.Flex (1 OCPU, 6 GB Memory)
    c. **Count:** 1
6. Click **Next.**
7. Review the capacity reservation and capacity configuration information.
8. Click **Create.**

You can now see that the capacity reservation is created successfully.

Add a Capacity Configuration

In this practice, you will add a capacity configuration to an existing capacity reservation.

Tasks

1. From the **Main Menu**, under **Compute**, select **Capacity Reservations**.
2. Click the capacity reservation **FRA-AA-LAB08-1-RESV-01**.
3. Click **Add capacity configuration**.
4. In the **Add capacity configurations** dialog box, populate the following information:
    a. **Fault Domain**: First available
    b. **Shape:** VM.Standard.E4.Flex (1 OCPU, 8 GB Memory)
    c. **Count:** 1
5. Click **Add configuration**.

    You can now see two capacity configurations in the capacity reservation.

Create Instances in a Capacity Reservation

In this practice, you will create instances in a capacity reservation.

Tasks

1. From the **Main Menu**, under **Compute**, select **Capacity Reservations**.
2. Click the capacity reservation **FRA-AA-LAB08-1-RESV-01.**
3. Under **Resources** in the left navigation panel, click **Created instances.**
4. Click **Create instance** and populate the following information:
    a. **Name:** FRA-AA-LAB08-1-VM-01
    b. **Create in compartment:** <*your compartment*>
    c. **Placement (Availability domain):** AD 1
    d. **Capacity type:** Capacity reservation
    e. **Capacity reservation:** FRA-AA-LAB08-1-RESV-01
    f. **Fault Domain:** Let Oracle choose the best fault domain.
    g. **Image**: Oracle Linux 8
    h. **Shape:** VM.Standard.A1.Flex (1 OCPU, 6GB Memory)

    Note: If the capacity reservation doesn't have a configuration for a shape, you will see this icon ⓘ in front of the Shape name.

    i. **Networking**: FRA-AA-LAB08-1-VCN-01
    j. **Subnet**: FRA-AA-LAB08-1-SNET-01 (regional)
    k. **Public IP address**: Do not assign a public IPv4 address.
    l. **Add SSH keys**: No SSH keys

    Note: Keep the default option for **Boot volume**.

5. Click **Create**.

   In a couple of minutes, you can see that the instance is created successfully, and the state is Running.

6. Navigate back to the **Capacity Reservations** page under **Compute** from the **Main Menu**.

7. Click the capacity reservation **FRA-AA-LAB08-1-RESV-01**.

   Under **Capacity configurations**, you can see that the **Used capacity** for VM.Standard.A1.Flex Instance type is 1, and the **Reserved capacity** is 1.

8. Repeat steps 1 through 5 to create another instance with the following changes:

   a. **Name:** FRA-AA-LAB08-1-VM-02

   b. **Shape:** VM.Standard.E4.Flex (1 OCPU, 8 GB Memory)

      For changing Shape, click **Change Shape** and click **AMD** under **Shape series.** Then select **VM.Standard.E4.Flex**

9. Populate all other fields as per Step 4 and click **Create**.

10. Navigate back to the **Capacity Reservations** page from the **Main Menu**.

11. Click the capacity reservation **FRA-AA-LAB08-1-RESV-01**.

    Under **Capacity configurations**, you can see that the **Used capacity** for VM.Standard.E4.Flex Instance type is 1. The **Reserved capacity** is 1.

Move an Instance out of a Capacity Reservation

In this practice, you will move an instance out of a capacity reservation.

Tasks

1. From the **Main Menu**, under **Compute**, select **Instances**.
2. Click the instance **FRA-AA-LAB08-1-VM-02**.
3. From the **More Actions** drop-down menu, select **Edit.**
4. Click **Show advanced options**, and then click the **Placement** tab.
5. Deselect the **Apply a capacity reservation** check box.
6. Click **Save changes.**
7. Navigate back to the **Main Menu** and click **Compute**. Under **Compute**, click **Capacity Reservations**.
8. Click the capacity reservation **FRA-AA-LAB08-1-RESV-01**.
9. Under **Capacity configurations**, you can see that the **Used capacity** for VM.Standard.E4.Flex Instance type is 0.

Adding an Instance to a Capacity Reservation

In this practice, you will add an instance to a capacity reservation.

Tasks

1. From the **Main Menu**, under **Compute**, select **Instances**.
2. Click the instance **FRA-AA-LAB08-1-VM-02**.
3. From the **More Actions** drop-down menu, select **Edit.**
4. Click **Show advanced options**, and then click the **Placement** tab.
5. Select the **Apply a capacity reservation** check box.
6. Select **FRA-AA-LAB08-1-RESV-01** under Capacity reservation.
7. Click **Save changes.**
8. Navigate back to the **Main Menu** and select **Compute**. Under **Compute**, click **Capacity Reservations**.
9. Click the capacity reservation **FRA-AA-LAB08-1-RESV-01**.
10. Under **Capacity configurations**, you can see that the **Used capacity** for VM.Standard.E4.Flex Instance type is 1.

Compute: Configure Metric-Based Autoscaling

Lab 09-1 Practices

Get Started

Overview

Autoscaling lets you automatically adjust the number or the lifecycle state of compute instances in an instance pool. This helps you provide consistent performance for your end users during periods of high demand, and reduce your costs during periods of low demand.

In this lab, you will:

a. Create a Virtual Cloud Network (VCN) and its components

b. Create a load balancer

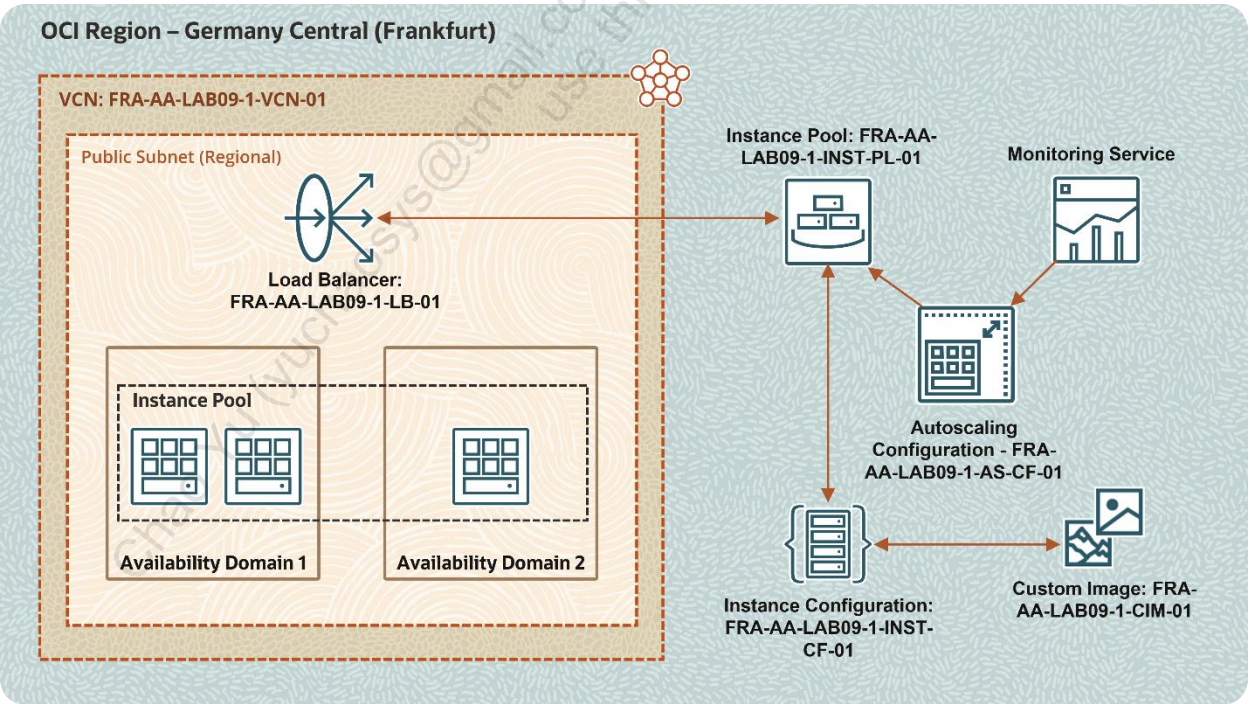
c. Create a compute instance and a custom image

d. Create an instance configuration

e. Create an instance pool

f. Create a metric-based autoscaling configuration

g. Test autoscaling



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab has all the IAM policies added (that's required for your lab).

Assumptions

- You must be familiar with navigating the OCI Console.
- Select the region available in the tenancy allotted to you. In this lab, Germany Central (Frankfurt) region will be considered.

Create a Virtual Cloud Network and Its Components

In this practice, you will create a Virtual Cloud Network (VCN), subnet, and Internet gateway, and add route rules in the route table.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) Console.
2. From the navigation menu, under **Networking**, select **Virtual Cloud Networks.**
3. Click **Create VCN.**
4. In the **Create a Virtual Cloud Network** dialog box, populate the following information:
   - **Name**: `FRA-AA-LAB09-1-VCN-01`
   - **Create In Compartment**: <*your compartment*>
   - **IPv4 CIDR Blocks**: `10.0.0.0/16`
5. Keep all the other options default and click **Create VCN**.

   Note: You can see that the VCN is created successfully.
6. Click **FRA-AA-LAB09-1-VCN-01** to view the details and click **Create Subnet**.
7. In the **Create Subnet** dialog box, populate the following information:
   - **Name**: `FRA-AA-LAB09-1-SNET-01`
   - **Create In Compartment**: <*your compartment*>
   - **Subnet Type**: Regional
   - **IPv4 CIDR Blocks**: `10.0.1.0/24`
   - **Subnet Access**: Public Subnet
8. Keep all the other options default and click **Create Subnet.**
9. Under **Resources** in the left navigation panel, click **Internet Gateways.**

10. Click **Create Internet Gateway** and populate the following information:
    - **Name**: `FRA-AA-LAB09-1-IG-01`
    - **Create In Compartment**: <*your compartment*>
11. Click **Create Internet Gateway**.

    You can see that the internet gateway is created successfully, and the state is Available.
12. Under **Resources** in the left navigation panel, click **Route Tables**.
13. Click **Default Route Table** for FRA-AA-LAB09-1-VCN-01.
14. Click **Add Route Rules** and populate the following information:
    - **Target Type**: Internet Gateway
    - **Destination CIDR Block**: `0.0.0.0/0`
    - **Target Internet Gateway**: FRA-AA-LAB09-1-IG-01
15. Click **Add Route Rules**.
16. Using the breadcrumb list at the top of the screen, return to the VCN page by selecting **FRA-AA-LAB09-1-VCN-01**.
17. Under **Resources** in the left navigation panel, click **Security Lists**.
18. Click **Default Security List** for FRA-AA-LAB09-1-VCN-01.
19. Click **Add Ingress Rule** and populate the following information:
    - **Source Type**: CIDR
    - **Source CIDR**: `0.0.0.0/0`
    - **IP Protocol**: TCP
    - **Source Port Range**: All
    - **Destination Port Range**: `80`

      Note: Do not select Stateless.
20. Click **Add Ingress Rules**.

Create a Load Balancer

The Oracle Cloud Infrastructure (OCI) Load Balancer provides automated traffic distribution from one entry point to multiple servers reachable from your VCN. A load balancer improves resource utilization, facilitates scaling, and helps ensure high availability.

In this practice, you will create a public load balancer.

Tasks

1. From the navigation menu, under **Networking**, select **Load Balancers**.
2. Click **Create Load Balancer**.
3. Select **Load Balancer Type** as **Load Balancer** and click **Create Load Balancer.**
4. In the **Add Details** section, populate the following information:
   - **Load Balancer Name:** `FRA-AA-LAB09-1-LB-01`
   - **Choose visibility type:** Public
   - **Assign a public IP address:** Ephemeral IP Address
   - **Shapes:** Flexible Shapes
   - **Choose the minimum bandwidth:** `10`
   - **Choose the maximum bandwidth:** `20`
   - **Virtual Cloud Network in <*your compartment*>:** FRA-AA-LAB09-1-VCN-01
   - **Subnet in <*your compartment*>:** FRA-AA-LAB09-1-SNET-01 (regional)
5. Click **Next**.
6. In the **Choose Backends** section, select **Weighted Round Robin** in the **Specify a Load Balancing Policy** field.

   Note: Do not click **Add Backends** and keep the **Specify Health Check Policy** field default.
7. Click **Show Advanced Options** and enter `FRA-AA-LAB09-1-LB-BS-01` in the **Backend Set Name** field.

8. Click **Next**.

9. In the **Configure Listener** section, populate the following information:

    - **Listener Name:** `FRA-AA-LAB09-1-LB-LS-01`
    - **Specify the type of traffic your listener handles:** HTTP
    - **Specify the port your listener monitors for ingress traffic:** `80`

10. Click **Next**.

11. In the **Manage Logging** section, disable **Error Logs** and **Access Logs**.

12. Click **Submit.**

Create a Compute Instance and a Custom Image

In this practice, you will create SSH keys, launch a compute instance, install Apache HTTP server, and create a custom image.

Tasks

1. Click the **Cloud Shell** icon in the console header next to the Region icon.

2. After the Cloud Shell has started, run the following command:

   ```
   $ mkdir .ssh
   ```

   Important: In case you get an error that says, "cannot create director: File exists", you can skip running the first command.

   ```
   $ cd .ssh
   $ ssh-keygen -b 2048 -t rsa -f <<sshkeyname>>
   ```

   Replace `<<sshkeyname>>` with **ociaalab9key**. Select the key name you can remember. This will be the key name you will use to connect to the compute instance you create.

   Remember:

   - After entering the third command, press **Enter** twice for no passphrase.
   - Do not include the angle brackets «» and `$` symbol when pasting code into Cloud Shell.

3. Examine the two files that you just created by running the following command:

   ```
   $ ls
   ```

   Note: In the output there are two files, a private key: <*sshkeyname*> and a public key: <*sshkeyname*>.pub. Keep the private key safe and don't share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems as well as copied and pasted to facilitate secure communications in the cloud.

4. To list the contents of the public key, run the following command:

   ```
   $ cat <<sshkeyname>>.pub
   ```

   Replace `<<sshkeyname>>` with **ociaalab9key**.

5. Copy the contents of the public key as you will need this in a subsequent step. Make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

6. From the navigation menu, under **Compute**, click **Instances**.

7. Click **Create instance** and populate the following information:

   - **Name**: `FRA-AA-LAB09-1-VM-01`
   - **Create in compartment**: <*your compartment*>
   - **Availability Domain**: AD 1

     Click **Show advanced options** and select **On-demand capacity** under Capacity type.
   - **Image**: Oracle Linux 8
   - **Shape**: Select VM.Standard.A1.Flex (1 OCPU, 6GB Memory) [Shape series: Ampere]
   - **Primary Network**: Select existing virtual cloud network.
   - **Virtual cloud network in <*your compartment*>**: FRA-AA-LAB09-1-VCN-01
   - **Subnet**: Select existing subnet.
   - **Subnet in <*your compartment*>**: FRA-AA-LAB09-1-SNET-01 (regional)
   - **Public IP address**: Assign a public IPv4 address.
   - **Add SSH keys**: Paste public keys.
   - **SSH Keys**: <*contents of the public key*> (which is copied in Step 5 of this practice)

8. Keep the **Boot Volume** default and click **Create**.

   Note: In a couple of minutes, you will see that the Instance is created successfully, and the state is Running.

9. Open **Cloud Shell** and log in to your instance by running the following command:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address>
   ```

   Remember:

   - <*private_key_file*> is the full path and name of the file that contains the private key associated with the instance you want to access.
   - <*username*> is the default user `opc`.

- <*public-ip-address*> is the public IP address of the instance.

Note: Enter `yes` in response to "Are you sure you want to continue connecting (yes/no)?".

10. While connected to your Compute instance via SSH, run the following commands:

    - Install Apache http:
      ```
      $ sudo yum install httpd -y
      ```
    - Start the Apache server and configure it to start after system:
      ```
      $ sudo apachectl start
      $ sudo systemctl enable httpd
      ```
    - Run a quick check on Apache configurations:
      ```
      $ sudo apachectl configtest
      ```
    - Create firewall rules to allow access to the ports on which the HTTP server listens:
      ```
      $ sudo firewall-cmd --permanent --zone=public --add-service=http
      $ sudo firewall-cmd --reload
      ```
    - Create an index file for your web server:
      ```
      $ sudo bash -c 'echo $(hostname) >> /var/www/html/index.html'
      ```

11. Now that you have a compute instance and Apache web server installed, you need to create a custom image from it.

12. From the navigation menu, under **Compute**, select **Instances**.

13. Click the **FRA-AA-LAB09-1-VM-01** instance.

14. From the **More Actions** drop-down list, select **Create custom image**.

15. In the **Create custom image** dialog box, populate the following information:

    - **Create in compartment**: <*your compartment*>
    - **Name**: `FRA-AA-LAB09-1-CIM-01`

16. Click **Create custom image**.

    Note: Now, you need to create a new compute instance based on the custom image. Once the custom image has been successfully created, you have to delete the instance **FRA-AA-LAB09-1-VM-01** as it is no longer required. (If you don't delete this instance, you might face quota issues and your lab will not work correctly.)

17. From the navigation menu, under **Compute**, select **Instances**.

18. Click **Create instance** and populate the following information:

    - **Name**: `FRA-AA-LAB09-1-VM-02`
    - **Create in compartment**: <*your compartment*>
    - **Availability Domain**: AD 1

      Click **Show advanced options** and select **On-demand capacity** under Capacity type.

    - **Image**: FRA-AA-LAB09-1-CIM-01

      Note: To select the custom image, click **Change image** and select **Custom images** in the **Image source** field. Select **<*your compartment*>** in the **Compartment** field. Then, select the custom image you just created from the list.

    - **Shape**: Select VM.Standard.A1.Flex (1 OCPU, 6GB Memory) [Shape series: Ampere]
    - **Primary Network**: Select existing virtual cloud network.
    - **Virtual cloud network in <*your compartment*>**: FRA-AA-LAB09-1-VCN-01
    - **Subnet**: Select an existing subnet.
    - **Subnet in <*your compartment*>**: FRA-AA-LAB09-1-SNET-01 (regional)
    - **Public IP address**: Assign a public IPv4 address.
    - **Add SSH keys**: Paste public keys.
    - **SSH Keys**: <*contents of the public key*> (which is copied in Step 5 of this practice)

19. Keep the Boot Volume default and click **Create**.

Create an Instance Configuration

The instance configurations let you define the settings to use when creating compute instances.

In this practice, you will create an instance configuration and subsequently use it to create one or more instances in an instance pool.

Tasks

1. From the navigation menu, under **Compute**, select **Instances**.
2. Click **FRA-AA-LAB09-1-VM-02** (the instance of an image you want to use as a template to create the instance configuration).
3. From the **More Actions** drop-down list, select **Create instance configuration**.
4. In the **Create instance configuration** dialog box, populate the following information:
   - **Create in compartment**: <*your compartment*>
   - **Name**: `FRA-AA-LAB09-1-INST-CF-01`
5. Click **Create instance configuration.**

   Note: You will see that the instance configuration is created successfully.

Create an Instance Pool

The instance pools let you create and manage multiple compute instances within the same region as a group. Before you create an instance pool, you need an instance configuration and optionally a load balancer and back-end set.

In this practice, you will create an instance pool.

Tasks

1. From the navigation menu, under **Compute**, select **Instance Pools**.
2. Click **Create instance pool**.
3. In the **Add basic details** section, populate the following information:
   - **Name**: `FRA-AA-LAB09-1-INST-PL-01`
   - **Create in compartment**: <*your compartment*>
   - **Instance configuration in <*your compartment*>**: FRA-AA-LAB09-1-INST-CF-01
   - **Number of instances**: 2
4. Click **Next**.
5. In the **Configure pool placement** section, you will select the location where you want to place the instances. Populate the following information:
   - **Availability domain:** AD 1
   - **Select a virtual cloud network in <*your compartment*>**: FRA-AA-LAB09-1-VCN-01
   - **Select a subnet in <*your compartment*>**: FRA-AA-LAB09-1-SNET-01

     Note: You can leave the Fault domains field blank.
6. To create instances in more than one availability domain, click **+ Another availability domain** and populate the following information:
   - **Availability domain:** AD 2
   - **Select a virtual cloud network in <your compartment>**: FRA-AA-LAB09-1-VCN-01

- **Select a subnet in <your compartment>**: FRA-AA-LAB09-1-SNET-01

  Note: You can leave the Fault domains field blank.

7. Select the **Attach a load balancer** check box and populate the following information:

   - **Load balancer type**: Load Balancer
   - **Load balancer in <*your compartment*>**: FRA-AA-LAB09-1-LB-01
   - **Backend set**: `FRA-AA-LAB09-1-LB-BS-01`
   - **Port**: `80`

     Note: This field is the server port on the instances to which the load balancer must direct traffic.

   - **VNIC**: Primary VNIC

8. Click **Next**.

9. Review the instance pool details and click **Create**.

   Note: You will see that the instance pool creation is successful.

10. Under **Resources** in the left navigation panel, click **Attached instances**. You should see two instances in the Running state.

Create a Metric-Based Autoscaling Configuration

In metric-based autoscaling, you select a performance metric to monitor, and set thresholds that the performance metric must reach to trigger an autoscaling event. When system usage meets a threshold, autoscaling dynamically resizes the instance pool in near-real time. As load increases, the pool scales out. As load decreases, the pool scales in.

In this practice, you will create a metric-based autoscaling configuration.

Tasks

1. From the navigation menu, under **Compute**, click **Autoscaling Configurations**.
2. Click **Create autoscaling configuration**.
3. In the **Add basic details** section, populate the following information:
    - **Name**: `FRA-AA-LAB09-1-AS-CF-01`
    - **Create in compartment**: <*your compartment*>
    - **Instance Pool**: FRA-AA-LAB09-1-INST-PL-01
4. Click **Next**.
5. In the **Configure autoscaling policy** section, select **Metric-based autoscaling**. Then populate the following information:
    - **Autoscaling policy name**: `FRA-AA-LAB09-1-AS-POL-01`
    - **Cooldown in seconds**: `300`
    - **Performance metric**: CPU utilization
6. In the **Scale-out rule** subsection, populate the following information:
    - **Scale-out operator**: Greater than (>)
    - **Threshold percentage**: `70`
    - **Number of instances to add**: `1`

7. In the **Scale-in rule** subsection, populate the following information:

    - **Scale-in operator**: Less than (<)
    - **Threshold percentage**: `20`
    - **Number of instances to remove**: `1`

8. In the **Scaling limits** subsection, populate the following information:

    - **Minimum number of instances**: `1`
    - **Maximum number of instances**: `3`
    - **Initial number of instances**: `2`

9. Click **Next**.

10. Review the autoscaling configuration and click **Create**.

    Note: You will see that the autoscaling configuration is created successfully and the state is Enabled.

Test Autoscaling

In the metric-based autoscaling, you choose a performance metric to monitor, and set thresholds that the performance metric must reach to trigger an autoscaling event. When system usage meets a threshold, autoscaling dynamically resizes the instance pool in near-real time. As load increases, the pool scales out. As load decreases, the pool scales in.

In this practice, you will test a metric-based autoscaling configuration.

Tasks

1. From the navigation menu, under **Compute**, select **Instance Pools**.
2. Click **FRA-AA-LAB09-1-INST-PL-01**.
3. Under **Resources** in the left navigation panel, click **Attached instances**.

   Note: After a few minutes, you will notice that one of the instances is terminated due to the scale-in rule you defined. Please note that initially two instances were in Running state.

   Note: You might have to wait for a couple of minutes before the scale in occurs.
4. Click the instance. (You will see only one instance here.)
5. Open Cloud Shell and use SSH to log in to your instance by running the following command:

   ```
   $ ssh -i <private_key_file> <username>@<public-ip-address>
   ```

   Remember:

   - *<private_key_file>* is the full path and name of the file that contains the private key associated with the instance you want to access.
   - *<username>* is the default user `opc`.
   - *<public-ip-address>* is the public IP address of the instance.

   Note: Enter `yes` in response to "Are you sure you want to continue connecting (yes/no)?"
6. To install the stress package, run the following command:

   ```
   $ sudo dnf makecache
   $ sudo dnf install stress-ng-0.14.00-1.el8.aarch64
   ```

7. To generate stress, run the following command:

```
$ stress-ng --cpu 2 -t 5m
```

8. From the navigation menu, under **Compute**, select **Instance Pools**.

9. Click **FRA-AA-LAB09-1-INST-PL-01**.

10. Under **Resources** in the left navigation panel, click **Attached instances**.

    Note: After a few minutes, you will notice that one of the instances will be added to the instance pool due to the scale-out rule you defined.

Object Storage: Create and Manage OCI Object Storage

Lab 10-1 Practices

Get Started

Overview

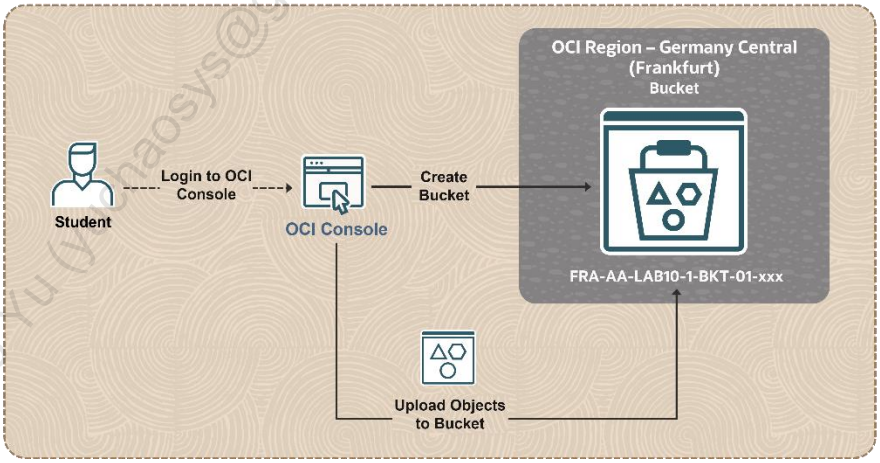
The Oracle Cloud Infrastructure (OCI) Object Storage provides unlimited capacity with high durability and scalability. It is highly reliable and cost efficient. The object storage resources include namespace, bucket, and object.

The Object Storage is characterized with strong consistency and security with encryption. By creating unlimited buckets, you can add as many objects as required with a maximum of 10TiB per object. In this lab, you will work on buckets, object versioning, object lifecycle management, replication policy, and retention rule.

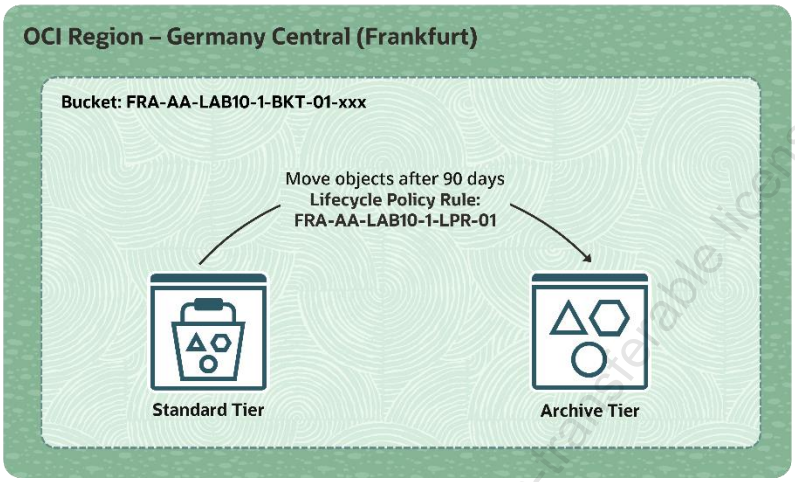
In this lab, you will:

- Create an object storage bucket
- Upload an object to a bucket
- Configure a lifecycle policy rule for the bucket
- Create a replication policy for the bucket
- Create a retention rule for the bucket

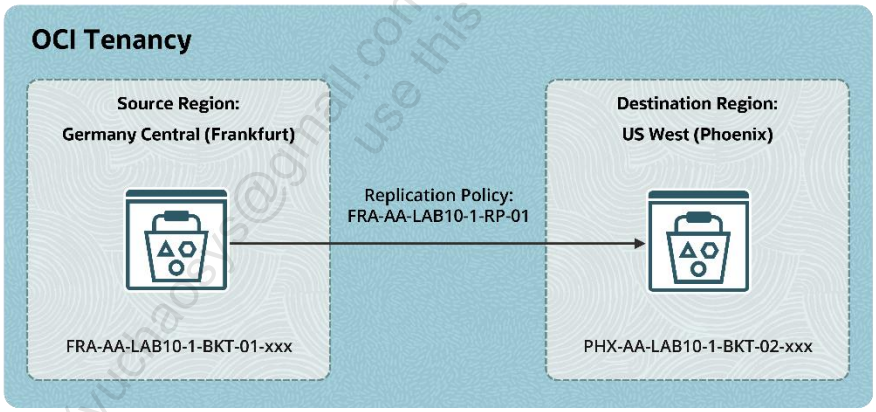
Create a Bucket and Upload an Object



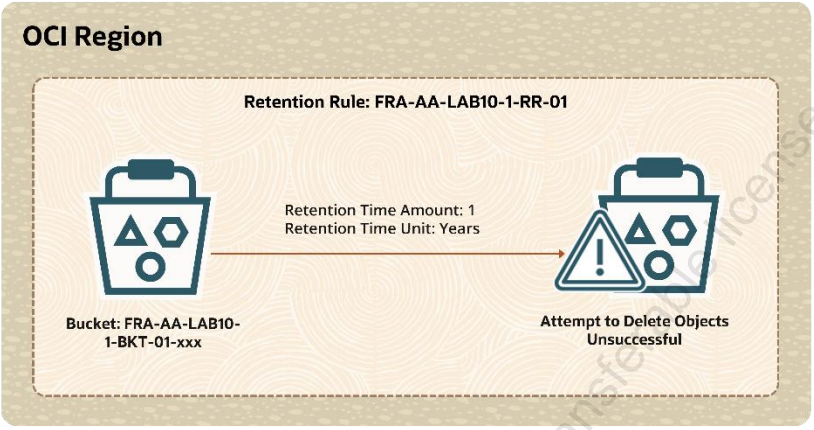
Configure a Lifecycle Policy Rules for the Bucket



Create a Replication Policy for the Bucket



Create a Retention Rule for the Bucket



Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Create an Object Storage Bucket

In this practice, you will create an Object Storage bucket.

Select the region available in the tenancy allotted to you. In this lab, we will use Germany Central (Frankfurt) as our region.

If you are not in the Germany Central (Frankfurt) region, specify the correct region key corresponding to your region in place of **FRA**. Visit Regions and Availability Domains (oracle.com) for information about the region key.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. From the **Main Menu**, select **Storage.**
3. Under **Object Storage and Archive Storage**, click **Buckets**.
4. From the left navigation panel, select the compartment in which you have permission to work. Then the page updates to display only the resources in that compartment.
5. Click **Create Bucket**.
6. In the **Create Bucket** dialog box, specify the following attributes of the bucket:
   - **Bucket Name**: Enter **`FRA-AA-LAB10-1-BKT-01-xxx`** as the name for the bucket. Specify a random number in place of xxx to make it unique.
   - **Default Storage Tier**: Select the default tier in which you want to store the data. After it is set, you cannot change the default storage tier of a bucket. When you upload objects, this tier will be selected by default. You can, however, select a different tier. In this case, select **Standard**, which is the primary and default storage tier used for the Object Storage.
   - **Enable Auto-Tiering**: Auto-Tiering helps you automatically move objects between Standard and Infrequent Access tiers based on their access patterns. Do not enable this field now.
   - **Enable Object Versioning**: Versioning directs object storage to automatically create an object version each time a new object is uploaded, an existing object is overwritten, or when an object is deleted. You can enable it while creating a bucket or later. Do not enable this field now.

- **Emit Object Events**: Emit Object Events lets the bucket to emit events for object state changes. Do not select this field now.
- **Encryption**: Buckets are encrypted with keys managed by Oracle by default, but you can optionally encrypt the data in this bucket using your own vault encryption key. Select the **Encrypt using Oracle managed keys** option.
- **Tags**: If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. Skip this option. You can always apply tags later.

7. Click **Create**.

   The bucket is created immediately, and you can add objects to it.

Upload an Object to a Bucket

In this practice, you will upload an object to your bucket. Object Storage supports uploading individual files up to 10 TiB.

Before you upload an object to a bucket, you must have a bucket. In this case, you will use the bucket that is created from the previous practice.

Tasks

1. In the **Main Menu**, navigate to **Storage**, and then select **Buckets**.
2. Click the bucket **FRA-AA-LAB10-1-BKT-01-*xxx*** to view its details.
3. Under **Objects**, click **Upload**.
4. In the **Object Name Prefix** field, enter the file name prefix `oci/` for the files you plan to upload. This step is optional.
5. The **Storage Tier** field is populated as **Standard**. You can optionally change the storage tier (to Infrequent Access or Archive) to upload objects. In this case, keep it as **Standard**.
6. Select the objects to upload (browse any object from your local machine) by using one of the following options:
   - Drag files from your computer into the **Drop files here...** section.
   - Click the **Select Files** link to display a file selection dialog box.

     As you select files to upload, they are displayed in a scrolling list. If you decide that you do not want to upload a file that you have selected, click **X** to the right of the file name.

     If selected files to upload and files already stored in the bucket have the same name, warning messages to overwrite are displayed.
7. Click **Upload**.

   The selected objects are uploaded. Click **Close** to return to the bucket.

Configure a Lifecycle Policy Rules for the Bucket

In this practice, you will use Object Lifecycle Management to manage the object storage data. You will define a rule that automatically moves standard tier objects to the archive tier 90 days after creation or last update.

Before you configure a lifecycle policy rule for the bucket, you must have a bucket.

Tasks

1. In the **Main Menu**, navigate to **Storage**, then **Buckets**.
2. Click the bucket **FRA-AA-LAB10-1-BKT-01-*xxx*** to view its details.
3. Under **Resources** in the left navigation panel, click **Lifecycle Policy Rules** to access the lifecycle policy rule list.
4. Click **Create Rule**.

   The Console checks the IAM policies that are in place to ensure policy rule creation success.
5. Provide the following information:

   - **Name**: The system generates a default rule name that reflects the current year, month, day, and time. In this case, enter **`FRA-AA-LAB10-1-LPR-01`** as the name.
   - **Target**: Select the target to which the lifecycle rule applies. In this case, select **Objects**.
   - **Lifecycle Action**: If the rule target is Objects, you will get three options: Move to Archive, Move to Infrequent Access, and Delete. In this case, select **Move to Archive**.
   - **Number of Days**: This field implies the number of days until the specified action is taken. In this case, enter **`90`** days.

     Note: Values in the **Name** and **Target** fields are required.

6. Use **Object Name Filters** to specify the object where the lifecycle rule applies.

   You can choose objects using prefixes and pattern matching. If no name filter is specified, the rule applies to all objects in the bucket.

   To create an object name filter:

   - Click **Add Filter**.
   - Select the **Filter Type** - **Include by prefix**.
   - Enter the **Filter Value** - `oci/`.

7. Select whether the rule is enabled or disabled upon creation using the **State** selector. In this case, ensure that the State is **Enabled**.

8. Click **Create**.

The lifecycle policy rule is successfully configured for this bucket.

Create a Replication Policy for the Bucket

In this practice, you will create a replication policy to replicate objects in one bucket to another in a different region.

Before you configure a replication policy for the bucket, you must have two buckets in two different regions.

Please note that in our case Germany Central (Frankfurt) is the source region and we have selected US West (Phoenix) as the target region. This might change for you depending on the region available in the tenancy allotted to you.

Tasks

1. As a first step, you will create a destination bucket in the destination region. To do this:
   - In the console ribbon at the top of the screen, click the Region icon to expand the menu and select destination region **US West (Phoenix)** - PHX.
   - Create a destination bucket named **PHX-AA-LAB10-1-BKT-02-*xxx*** (specify a random number in place of xxx to make it unique) using the **Create an Object Storage bucket** practice instructions.
2. In the console ribbon at the top of the screen, click the Region icon to expand the menu. Select **Germany Central (Frankfurt)**.
3. In the **Main Menu**, navigate to **Storage**, then **Buckets**.
4. On the **Buckets** screen, click the bucket name **FRA-AA-LAB10-1-BKT-01-*xxx*** to view its details.
5. Under **Resources** in the left navigation panel, click **Replication Policy** to access the replication policy list.
6. Click **Create Policy**.

   The Console checks the IAM policies that are in place to ensure replication policy creation success.

7. In the **Create Replication Policy** dialog box, enter the following:

   - **Name**: The system generates a default policy name that reflects the current year, month, day, and time. Enter **`FRA-AA-LAB10-1-RP-01`** as the name.
   - **Destination Region**: This refers to the OCI region containing the destination bucket that you want to replicate to. Your tenancy must be subscribed to a region for you to replicate to that region. In this case, select **US West (Phoenix)**.
   - **Destination Bucket**: This refers to the name of the destination bucket for replication. Select the **PHX-AA-LAB10-1-BKT-02-*xxx*** bucket that is created in the destination region. Please note that the replication cannot automatically create the bucket.

     Note: Entry in the **Name** and **Destination Region** fields are required.

8. Click **Create**.

   After the policy is created, **Replication: Source** is added to the **Bucket Information** tab. The objects uploaded to the source bucket after policy creation are asynchronously replicated to the destination bucket.

9. Navigate back to the **Buckets** screen and click the bucket **FRA-AA-LAB10-1-BKT-01-*xxx***. Upload another object using **Upload Objects to a Bucket** practice instruction.

10. Navigate to the destination region using the region menu. In this case, it's **Phoenix** and click the bucket name **PHX-AA-LAB10-1-BKT-02-*xxx***.

11. Validate that the uploaded object to the source bucket **FRA-AA-LAB10-1-BKT-01-*xxx*** is asynchronously replicated to the destination bucket **PHX-AA-LAB10-1-BKT-02-*xxx***.

Create a Retention Rule for the Bucket

In this practice, you will create a time-bound retention rule to protect your data from accidental or malicious update, overwrite, or deletion.

Before you configure a retention rule for the bucket, you must have a bucket.

Tasks

1. In the **Main Menu**, navigate to **Storage**, then **Buckets**.
2. In the Console ribbon at the top of the screen, ensure you are in the correct region, Germany Central (Frankfurt).
3. Click the bucket name **FRA-AA-LAB10-1-BKT-01-*xxx*** created earlier to view its details.
4. Under **Resources** in the left navigation panel, click **Retention Rules** to access the retention rule list.
5. Click **Create Rule**.
6. In the **Create Retention Rule** dialog box, enter **`FRA-AA-LAB10-1-RR-01`** as the name.
7. Select **Retention Rule Type** that you want to create:
   - **Time-Bound**: These rules have a user-defined duration. The object modification is prevented for the duration specified. The duration is applied to each object individually and is based on the object's Last Modified timestamp.
   - **Indefinite**: These rules have no duration or expiration. The object modification is prevented until an indefinite rule is deleted.

   In this case, select **Time-Bound** retention rule type.
8. Enter the following retention rule duration attributes:
   - **Retention Time Amount**: 1
   - **Retention Time Unit**: Years

   The retention duration that you specify is applied to each object individually and is based on the object's Last Modified timestamp.

9. Do not select **Enable Retention Rule Lock**. When a rule is locked, only an increase in the retention duration is allowed and the rule can be deleted only by deleting the bucket. A bucket must be empty to be deleted.

10. Click **Create**.

11. Under **Resources** in the left navigation panel, click **Objects**.

12. Next, try deleting one of the objects uploaded in the earlier steps. To do this, click the ellipsis icon corresponding to an object and click **Delete**.

13. Click **Delete**.

    You will notice that the delete was unsuccessful. This is because if you have active retention rules, the actions that you can perform on a bucket are limited. You cannot update, overwrite, or delete objects or object metadata, or delete the bucket until the retention duration expires or the retention rule is deleted.

14. Click **Cancel.**

Object Storage: Perform Multipart Upload Using CLI (Using Cloud Shell)

Lab 11-1 Practices

Get Started

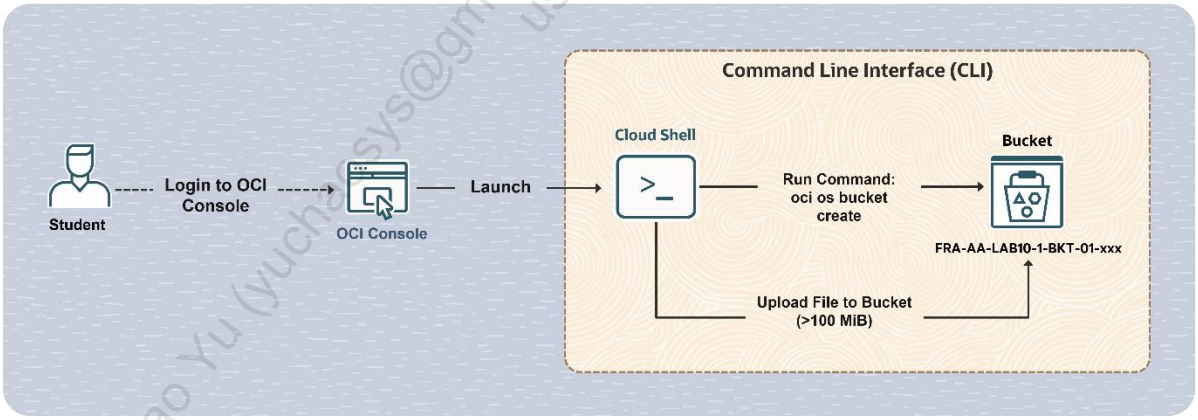
Overview

The Oracle Cloud Infrastructure (OCI) Object Storage supports multipart uploads for more efficient and resilient uploads, especially for large objects. With multipart uploads, the individual parts of an object can be uploaded in parallel to reduce the amount of time you spend uploading. In this lab, you will perform a multipart upload on the Command Line Interface (CLI) using Cloud Shell.

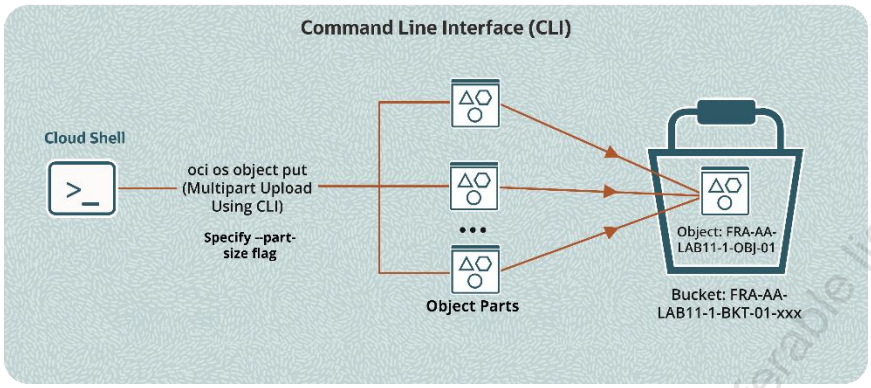
In this lab, you will:

- Access Cloud Shell via the Console
- Create a standard default storage tier bucket using CLI (Cloud Shell)
- Upload a file (larger than 100 MiB) to Cloud Shell
- Perform a multipart upload using the CLI (Cloud Shell)

Create a Standard default storage tier bucket using CLI (Cloud Shell) and Upload a File



Perform a multipart upload using the CLI (Cloud Shell)



Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Access Cloud Shell via the Console

The OCI Cloud Shell is a web browser–based terminal accessible from the Console. It provides access to a Linux shell, with a pre-authenticated OCI CLI.

In this practice, you will access Cloud Shell via the OCI Console.

Tasks

1. Sign in to your Oracle Cloud Infrastructure (OCI) Console.
2. In the console ribbon at the top of the screen, click the Region icon to expand the menu. Select **Germany Central (Frankfurt)** as the region.
3. Click the **Cloud Shell** icon next to the Region selection menu in the console header.

   Note: The OCI CLI running in the Cloud Shell will execute commands against the region selected when the Cloud Shell starts.
4. Now, the Cloud Shell is displayed in a "drawer" at the bottom of the Console.
5. You can use the icons in the upper-right corner of the Cloud Shell window to minimize, maximize, and close your Cloud Shell session.

Create a Standard Default Storage Tier Bucket Using CLI (Cloud Shell)

In the OCI Object Storage, a bucket is a container for storing objects in a compartment within an object storage namespace.

In this practice, you will create a standard default storage tier bucket using the CLI.

Tasks

1. Ensure that the Cloud Shell session is running.
2. Run the following command to get your object storage namespace:

   ```
   $ oci os ns get
   ```

   Reminder: Do not include the $ symbol when pasting code into Cloud Shell.

   Your object storage namespace is returned. Please make a note of it as you will be using it in the subsequent task.

3. Run the following command to get the OCID of the compartment. Replace *<compartment-name>* with the compartment name assigned to you.

   ```
   $ oci iam compartment list --name <compartment-name>
   ```

   Make note of the value corresponding to the "**id**" (without the ditto/quotation mark). You will use this in the subsequent task. The following is an example of how it looks:

   ```
   "id": "ocid1.compartment.oc1..xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
   ```

4. Create a bucket by using the following command.

   ```
   $ oci os bucket create --namespace <object_storage_namespace> --
   name <bucket_name> --compartment-id <target_compartment_id>
   ```

   - Replace <*object_storage_namespace*> with the name returned in Step 2.
   - Replace <*bucket_name*> with **FRA-AA-LAB11-1-BKT-01-*xxx***. Specify a random number in place of xxx to make it unique.
   - Replace <*target_compartment_id*> with the compartment ID returned in Step 3.

   A standard tier bucket is created immediately.

Upload a File (Larger than 100 MiB) to Cloud Shell

In this practice, you will transfer a file larger than 100 MiB (~105 MB) from your local machine to the Cloud Shell.

Tasks

1. Click the **Cloud Shell** icon next to the Region selection menu in the Console header.
2. In the Cloud Shell window, click the **Cloud Shell Menu** icon at the top-right corner and select **Upload**. The **File Upload to your Home Directory** dialog box appears.
3. Drag and drop a file or click **Select from your computer**.

   Note: The File Transfer dialog box supports selecting only one file at a time to transfer. Select any file larger than 100 MiB.

   Tip: You can optionally download a sample file which is around 247 MB from the following link.

   https://yum.oracle.com/ISOS/OracleLinux/OL6/u8/x86_64/x86_64-boot-uek.iso
4. Click **Upload**.
5. Wait for the file transfer to finish. The file transfers that are in-process are shown with a progress bar and the completed file transfers are shown with a green check mark.
6. After the file transfer is complete, you can hide the File Transfer dialog box by clicking **Hide.**

Perform a Multipart Upload Using the CLI (Cloud Shell)

In this practice, you will perform a multipart upload by using the CLI (Cloud Shell).

Tasks

1. Click the **Cloud Shell** icon next to the Region selection menu in the Console header.
2. To perform a multipart upload of an object, run the following command in Cloud Shell:

```
$ oci os object put --namespace <object_storage_namespace> --
bucket-name <bucket_name> --file <file_location> --name
<object_name> --part-size <upload_part_size_in_MB> --parallel-
upload-count <maximum_number_parallel_uploads>
```

   - Replace <*object_storage_namespace*> with the name returned in Step 2 of **Create a Standard default storage tier bucket using CLI (Cloud Shell)**.
   - Replace <*bucket_name*> with **FRA-AA-LAB11-1-BKT-01-*xxx*** that was created earlier.
   - Replace <*file_location*> with the path to the downloaded file that you uploaded to the Cloud Shell.
   - Replace <*object_name*> with **FRA-AA-LAB11-1-OBJ-01**.
   - The `--part-size` value represents the size of each part in mebibytes (MiBs). It must be an integer. Replace <*upload part size in MB*> with **20**.
   - Optionally, you can use the `--parallel-upload-count` flag to set the maximum number of parallel uploads allowed. By default, the CLI limits the number of parts that can be uploaded in parallel to three. In this case, replace <*maximum_number_parallel_uploads*> with **5**.
3. You specify the part size of your choice, and the object storage splits the object into parts and performs the upload of all parts automatically. You will see that the uploading object operation is 100% complete. When using the CLI, you do not have to perform a commit when the upload is complete.
4. From the **Main Menu**, select **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.
5. From the **Buckets** screen, click the bucket name **FRA-AA-LAB11-1-BKT-01-*xxx*** to view its details.
6. Under **Objects**, validate that the object **FRA-AA-LAB11-1-OBJ-01** is present.

Block Storage: Create, Attach, Detach, and Resize a Block Volume

Lab 12-1 Practices

Get Started

Overview

The Oracle Cloud Infrastructure (OCI) Block Volume service lets you dynamically provision and manage block storage volumes. You can create, attach, connect, and move volumes, as well as change volume performance, as needed, to meet your storage, performance, and application requirements.

In this lab, you'll:

a. Create a Virtual Cloud Network and its components

b. Create a VM instance

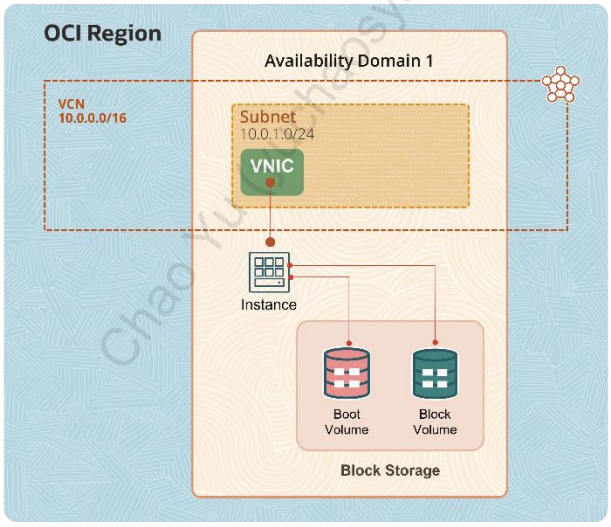
c. Create a block volume

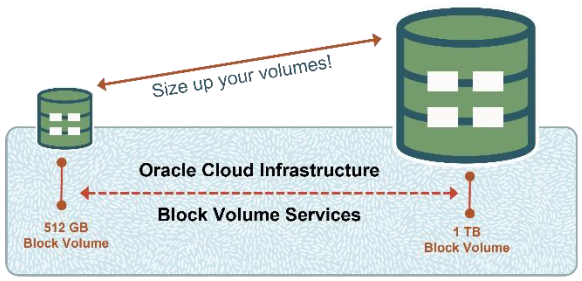
d. Attach a block volume to a compute instance

e. Resize a block volume

f. Detach a block volume

Create and Attach Block Volume and Online Resize of Block Volume





Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- You will select the region available in the tenancy allotted to you. In this lab, we consider Germany Central (Frankfurt) as your region.

Create a Virtual Cloud Network and Its Components

In this practice, you will learn how to create a Virtual Cloud Network (VCN), Subnet, and Internet Gateway, and add route rules in the Route Table.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks.**
3. Click **Create VCN.**
4. Enter the following:
   a. **Name:** Enter **`FRA-AA-LAB12-1-VCN-01`**.
   b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
   c. **IPv4 CIDR Blocks:** Type **`10.0.0.0/16`** and press **Enter** on your keyboard to add.

   Note: You can leave all the other options as default.
5. Click **Create VCN**. The VCN is now created successfully.
6. Click **Create Subnet**.
7. In the Create Subnet dialog box, enter the following:
   a. **Name:** Enter **`FRA-AA-LAB12-1-SNET-01`**.
   b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
   c. **Subnet Type:** Select **Regional**.
   d. **IPv4 CIDR Blocks:** Enter **`10.0.1.0/24`**.
   e. **Subnet Access:** Select **Public Subnet.**

   Note: You can leave all the other options as default.
8. Click **Create Subnet.** The subnet is now created successfully, and the state is Available.
9. In the left navigation pane, under **Resources**, click **Internet Gateways.**
10. Click **Create Internet Gateway.**

11. Enter the following:

    a. **Name:** Enter **`FRA-AA-LAB12-1-IG-01`**.

    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.

12. Click **Create Internet Gateway.** The Internet Gateway is now created successfully, and the state is Available.

13. In the left navigation pane, under **Resources**, click **Route Tables.**

14. Click **Default Route Table for FRA-AA-LAB12-1-VCN-01**.

15. Click **Add Route Rules** and enter the following:

    a. **Target Type:** Select **Internet Gateway** from the drop-down list.

    b. **Destination CIDR Block:** Enter **`0.0.0.0/0`**.

    c. **Target Internet Gateway:** Select **FRA-AA-LAB12-1-IG-01** from the drop-down list.

16. Click **Add Route Rules**. The route rule is now successfully added to the default Route Table.

Create a VM Instance

In this practice, you will learn how to create SSH keys using Cloud Shell and how to launch an instance.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. In the console ribbon at the top of the screen, click the **Cloud Shell** icon next to the Region selection menu.
3. Once the Cloud Shell is ready, enter the following commands:

   ```
   $ mkdir .ssh
   ```

   - **Important:** In case you get an error "Cannot create directory: File exists," you can skip running this first command.

   ```
   $ cd .ssh
   ```

   ```
   $ ssh-keygen -b 2048 -t rsa -f <<sshkeyname>>
   ```

   - **Remember:** After entering this third command, press **Enter** twice for no passphrase.

   Note: Replace `<<sshkeyname>>` with `cloudshellkey`. Choose the key name you can remember. This will be the key name you will use to connect to the compute instance you create.

   Reminder: The angle brackets «» should not appear in your code.

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

4. Examine the two files that you just created by running the following command:

   ```
   $ ls
   ```

   Note: In the output, there are two files, a private key: *<<sshkeyname>>* and a public key: *<<sshkeyname>>.pub*. Keep the private key safe and don't share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems, as well as copied and pasted to facilitate secure communications in the cloud.

5. To list the contents of the public key, use the following command:

```
$ cat <<sshkeyname>>.pub
```

Note: Replace `<<sshkeyname>>` with `cloudshellkey`.

Reminder: The angle brackets «» should not appear in your code.

6. Copy the contents of the public key as you will need this in a subsequent step. Make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

7. From the **Main Menu**, select **Compute**. Under **Compute**, click **Instances.**

8. Click **Create instance** and enter the following:

   a. **Name:** Enter **`FRA-AA-LAB12-1-VM-01`**.

   b. **Create in compartment:** Select the <*compartment name*> assigned to you.

   c. **Placement:** Select Availability Domain **AD1**. Click **Show advanced options** and select **On-demand capacity** from the **Capacity type** menu.

   d. **Image and shape**: Choose the image **Oracle Linux 8** and shape **VM.Standard.A1.Flex** (1 OCPU, 6GB Memory) [Shape series: Ampere].

   e. **Networking**: Select the existing virtual cloud network **FRA-AA-LAB12-1-VCN-01** and existing subnet **FRA-AA-LAB12-1-SNET-01 (regional)** . Under **Public IP address,** select **Assign a public IPv4 address.**

   f. **Add SSH keys**: Select **Paste public keys** and paste the contents of the public key, which you copied in Step 6, in the box.

   g. **Boot volume:** Keep the default selection.

9. Click **Create**.

   Note: After a couple of minutes, you see that the Instance is successfully created and the state is Running.

10. Under **Instance access**, copy the **Public IP address**.

11. Click the **Cloud Shell** icon to open Cloud Shell, and use SSH to connect to your instance by using the following command:

    Note: Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

    ```
    $ ssh -i <private_key_file> <username>@<public-ip-address>
    ```

    Reminders:

    - `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
    - `<username>` is the default user **opc**.
    - `<public-ip-address>` is the Public IP address of the instance.

12. You are now connected to the Instance FRA-AA-LAB12-1-VM-01. Run the following command to display information about the block devices:

    ```
    $ lsblk
    ```

    Note: You will only see the boot disk **sda**.

Create a Block Volume

The Oracle Cloud Infrastructure (OCI) Block Volume service lets you dynamically provision and manage block storage volumes.

In this practice, you will learn how to create a block volume.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. Open the **Main Menu** and click **Storage**. Under **Block Storage**, click **Block Volumes**.
3. Click **Create Block Volume.**
4. Fill in the required volume information:
    a. **Name**: Enter **`FRA-AA-LAB12-1-BV-01`**.
    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    c. **Availability Domain:** Select the first availability domain.
    d. **Volume Size and Performance:** Select **Custom** and specify the following:
        1) **Volume Size (in GB):** Enter **`512`**.
        2) **Target Volume Performance**: Drag the VPUs/GB slider to the left to make the performance **Lower Cost** .
    e. **Backup Policies:** Do not specify any policy.
    f. **Cross Region Replication:** Keep the **OFF** default selection.
    g. **Encryption:** Keep the default **Encrypt using Oracle-managed keys** selection.
5. Click **Create Block Volume**. You now see that the Block Volume state becomes Available.

Attach a Block Volume to a Compute Instance

You can create, attach, connect, and move volumes. You can also change volume performance, as needed, to meet your storage, performance, and application requirements. After you attach and connect a volume to an instance, you can use the volume like a regular hard drive.

In this practice, you'll learn how to attach a block volume to a compute instance and perform various configuration tasks on the attached volume.

Tasks

1. Open the **Main Menu** and click **Compute**. Under **Compute**, click **Instances**.
2. In the **Instances** list, click the instance **FRA-AA-LAB12-1-VM-01**.
3. In the left navigation pane, under **Resources**, click **Attached block volumes**.
4. Click **Attach block volume**.
5. Specify the volume you want to attach to. For example, to use the volume name, choose **Select volume**, and then select the volume **FRA-AA-LAB12-1-BV-01** from the **Volume** drop-down list.
6. If the instance supports consistent device paths, and the volume you are attaching is not a boot volume, select the path **/dev/oracleoci/oraclevdb** from the **Device path** drop-down list. This enables you to specify a device path for the volume attachment that remains consistent between instance reboots.
7. In the **Attachment type** section, select **Paravirtualized.**

   Note: After you attach a volume using the Paravirtualized attachment type, it is ready to use, and you do not need to run any additional commands.
8. In the **Access** section, select **Read/Write.**

   Note: This is the default option for volume attachments and, with this option, an instance can read and write data to the volume.
9. Click **Attach**. You now see the state as Attached and, since the attachment type is Paravirtualized, you can use the volume without running any additional commands.

10. Ensure that you are connected to the Instance **FRA-AA-LAB12-1-VM-01**.

    Note: For help with this, refer to Step 11 in the **Create a VM Instance** practice.

11. Run the following command to display information about the block devices:

    ```
    $ lsblk
    ```

    Note: You now see that the system recognizes a new disk device, and the size is 512 GB.

12. To verify that the volume is attached to the instance, run the following command:

    ```
    $ ll /dev/oracleoci/oraclevd*
    ```

13. To partition the disk using `fdisk`, run the following command:

    ```
    $ sudo fdisk /dev/oracleoci/oraclevdb
    ```

    Note: Enter the following responses as seen in the Cloud Shell:

    a. `Command (m for help):` Enter **`n`** to create a new partition.

    b. `Select (default p):` Enter **`p`**.

    c. `Partition number (1,4, default 1):` Press **Enter**.

    d. `First sector:` Press **Enter**.

    e. `Last sector:` Press **Enter**.

    f. `Command (m for help):` Enter **w** to write the new partition.

14. To format the partition, run the following command:

    ```
    $ sudo mkfs -t ext4 /dev/oracleoci/oraclevdb1
    ```

15. To mount the partition, run the following commands:

    ```
    $ sudo mkdir -p /mnt/volume1
    ```

    ```
    $ sudo mount /dev/oracleoci/oraclevdb1 /mnt/volume1
    ```

    Note: On Linux instances, if you want to automatically mount volumes on an instance boot, you need to set some specific options in the `/etc/fstab` file.

16. To display information about the block devices, run the following command:

```
$ lsblk
```

Note: You now see the partition and the mountpoint `/mnt/volume1`.

Resize a Block Volume

With online resizing, you can expand the volume size without detaching the volume from an instance.

In this practice, you will resize a block volume.

Tasks

1. From the **Main Menu,** select **Storage**. Under **Block Storage**, click **Block Volumes**.
2. In the **Block Volumes** list, select the block volume **FRA-AA-LAB12-1-BV-01**.
3. Click **Edit**.
4. Under **Volume Size and Performance,** enter the new size `1024` in the **Volume Size (in GB)** field.

   Note: You must specify a larger value than the block volume's current size.
5. Click **Save Changes**.

   Note: A window appears with a list of commands. The commands are required to rescan the disk after the volume is provisioned. You need to run these commands so that the operating system identifies the expanded volume size. Click the **Copy** link to copy the commands, and then click **Close** to close the window.
6. Connect to your instance **FRA-AA-LAB12-1-VM-01.**

   Note: For help with this, refer to Step 11 in the **Create a VM Instance** practice.
7. Paste and run the rescan commands you copied in the previous step into your instance session window:

   ```
   $ sudo dd iflag=direct if=/dev/oracleoci/oraclevdb of=/dev/null
   count=1

   $ echo "1" | sudo tee /sys/class/block/`readlink
   /dev/oracleoci/oraclevdb | cut -d'/' -f 2`/device/rescan
   ```

   Note: After you've run the volume rescan commands, you need to extend the partition and grow the file system; however, this is beyond the scope of this lab activity. For more details on this topic, see Extending the Partition for a Block Volume (oracle.com) at:

https://docs.oracle.com/en-us/iaas/Content/Block/Tasks/extendingblockpartition.htm#Extending_the_Partition_for_a_Block_Volume

Detach a Block Volume

When an instance no longer needs access to a volume, you can detach the volume from the instance without affecting the volume's data.

In this practice, you will detach a block volume.

Tasks

1. From the **Main Menu**, select **Compute**. Under **Compute**, click **Instances**.
2. In the **Instance** list, click the instance **FRA-AA-LAB12-1-VM-01** to display the instance details.
3. In the left navigation pane, under **Resources,** click **Attached block volumes.**
4. From the **Attached block volumes** list, click the three dots on the right to open the Actions menu, then click **Detach**.
5. Click **OK** to confirm detachment. You now see that there are no block volumes attached to the instance **FRA-AA-LAB12-1-VM-01** .

Block Storage: Create a Volume Group and Enable Cross Region Replication

Lab 13-1 Practices

Get Started

Overview

The Oracle Cloud Infrastructure (OCI) Block Volume service provides you with the capability to group together multiple volumes in a volume group. A volume group can include both types of volumes, boot volumes, which are the system disks for your compute instances, and block volumes, which are for data storage.

In this lab, you'll work with volume groups. You will:

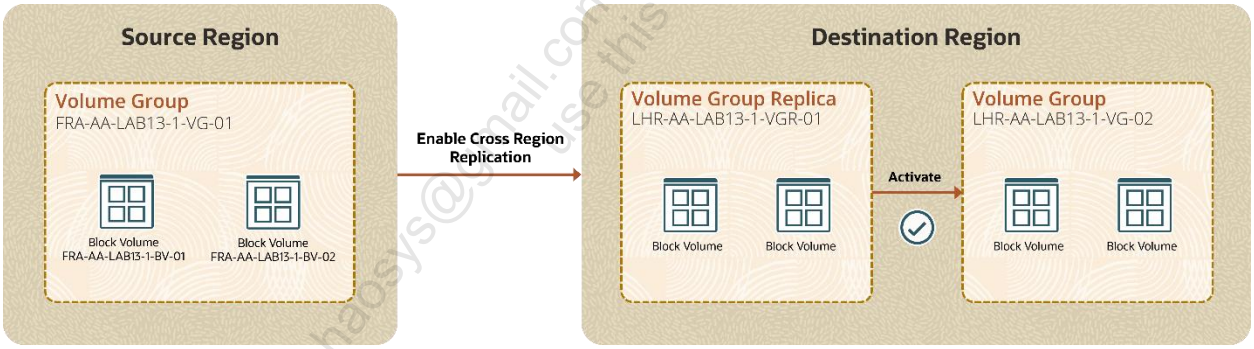
a. Create two block volumes

b. Create a volume group

c. Enable Cross-Region Replication for the volume group

d. Activate the Volume Group replica

e. Disable replication for a volume group



Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.
- Enabling Cross-Region Replication for the Volume Group requires access to a destination region. See Replicating a Volume (oracle.com) for the list of region mappings for cross-region replication.

Create Two Block Volumes

The Oracle Cloud Infrastructure Block Volume service lets you dynamically provision and manage block storage volumes.

In this practice, you will learn how to create two block volumes, which will subsequently be part of a volume group.

Tasks

1. Use the console to sign in to your Oracle Cloud Infrastructure (OCI) account.
2. Select the region available in the tenancy allotted to you. In this lab, consider Germany Central (Frankfurt) as your region.
3. From the **Main Menu**, select **Storage**. Under **Block Storage**, click **Block Volumes**.
4. Click **Create Block Volume.**
5. Fill in the required volume information:
    a. **Name:** Enter **`FRA-AA-LAB13-1-BV-01.`**
    b. **Create In Compartment:** Select the compartment assigned to you.
    c. **Availability Domain:** Select the first availability domain.
    d. **Volume Size and Performance:** Select the **Custom** option and enter `512` in the **Volume Size** field.
    e. **Target Volume Performance:** Drag the VPUs/GB slider to the left to make it **Lower Cost.**
    f. **Backup Policies:** Do not specify any policy.
    g. **Cross Region Replication:** Select the **OFF** radio button.
    h. **Encryption:** Select the **Encrypt using Oracle-managed keys** radio button.
6. Click **Create Block Volume**.

    Note: The Block Volume state is now Available.

7. Repeat steps 3-6 to create a second block volume. Name this volume **FRA-AA-LAB13-1-BV-02**.

   Note: You now have two block volumes where the state is Available.

Create a Volume Group

The Oracle Cloud Infrastructure (OCI) Block Volume service provides you with the capability to group together multiple volumes in a volume group.

In this practice, you'll learn how to create a volume group.

Tasks

1. From the **Main Menu**, select **Storage**. Under **Block Storage**, click **Volume Groups**.
2. Click Create **Volume Group.**
3. Fill in the required fields on the **Basic Information** page:
    a. **Name:** Enter **`FRA-AA-LAB13-1-VG-01`**.
    b. **Compartment:** Select the compartment assigned to you.
    c. **Availability Domain:** Select the first availability domain. (This must be the same Availability Domain, which you selected while creating the two block volumes in the previous exercise.)
4. Click **Next** to go to the next page.
5. On the **Add Volumes** page, for each volume you want to add:
    a. Select the compartment containing the volume from the **Compartment** drop-down list.
    b. Select the volume **FRA-AA-LAB13-1-BV-01** from the **Volume** drop-down list.
    c. Click **+ Additional Volume** to add more volumes.
        1) Select the compartment containing the volume from the **Compartment** drop-down list.
        2) Select the volume **FRA-AA-LAB13-1-BV-02** from the **Volume** drop-down list.
6. After you've added all the volumes you want to include when creating the volume group, click **Next.**

7. On the **Cross Region Replication** page, you can optionally enable asynchronous cross region volume replication for the volume group. You will be enabling this option in the subsequent steps. For now, leave the **OFF** option selected and click **Next.**

8. On the **Backup Policies** page, you can optionally configure scheduled backups for the volume group by selecting a backup policy to use for scheduled backups. You will not configure any Backup Policies at this time. Click **Next.**

9. On the **Summary** page, review the information. To edit any information, click **Edit** in the right corner.

10. Once everything looks correct, click **Create** to create the volume group. You can see that the Volume Group is created successfully, and it includes two block volumes.

Enable Cross-Region Replication for the Volume Group

The Block Volume service provides you with the capability to perform ongoing automatic asynchronous replication of volume groups to other regions.

In this practice, you'll learn how to enable replication for a volume group.

Tasks

1. Open the **Main Menu** and click **Storage**. Under **Block Storage**, click **Volume Groups**.
2. Click the volume group **FRA-AA-LAB13-1-VG-01**.
3. Click **Edit.**
4. Click **Cross Region Replication** on the left of the screen and select the **ON** option.
5. Enter the following information into the data fields:
   a. **Target Region:** Select the UK South (London) region to replicate the volume group.

      Note: See Replicating a Volume (oracle.com) for the list of region mappings for cross-region replication.

   b. **Availability Domain:** Select the first availability domain to place the volume group replica in.

   c. **Volume Group Replica Name:** Enter `LHR-AA-LAB13-1-VGR-01` for the volume group replica name.

   Note: In this lab, we used Germany Central (Frankfurt) as the source region and UK South (London) as the target region. This might change depending on the region available in the tenancy allotted to you.
6. Select the **Confirm** check box to acknowledge the cost warning and click **Next.**
7. Click **Summary** on the left of the screen.
8. Click **Save Changes.**

   Note: The Volume Group state changes to Updating. After a couple of seconds, the state becomes Available.
9. Under **Resources** in the left navigation pane**,** click **Volume Group Replicas**. The replica **LHR-AA-LAB13-1-VGR-01** is now created in the target region, UK South (London).

10. In the console ribbon at the top of the screen, click the Region icon to expand the menu. Select the target region, **UK South (London).**

11. Under **Block Storage** in the left navigation menu, click **Volume Group Replicas.**

    Note: You can now see the replica **LHR-AA-LAB13-1-VGR-01** and its details such as OCID, Source Region, Last Sync, and Created.

Activate the Volume Group Replica

To create a new volume group from a volume group replica, you need to activate the replica. The activation process creates a new volume group by cloning the replica.

In this practice, you'll learn how to activate a volume group replica.

Tasks

1. Make sure that you are in the correct destination region that contains the volume group replica you want to activate.
2. Open the **Main Menu** and click **Storage**. Under **Block Storage**, click **Volume Group Replicas**.
3. Click the replica **LHR-AA-LAB13-1-VGR-01**.
4. Click **Activate**.
5. Click **Confirm** to acknowledge that there may be a delay in the initial replication sync of the volume group.
6. In the **Activate Volume Group Replica** window, select the compartment assigned to you and specify the name for the new volume group as **LHR-AA-LAB13-1-VG-02**.
7. Click **Activate.**

   Notes

   - Activating a volume group from the replica creates a clone of the source volume group.
   - In the left navigation pane, under **Resources**, you can see and access the **Activated Volume Groups** and **Block Volume Replicas.**
8. From the **Main Menu**, select **Storage**. Under **Block Storage**, click **Volume Groups**.

   Note: You can now see the volume group **LHR-AA-LAB13-1-VG-02** in the volume groups list along with details such as Number of Volumes and Total Size of the volume groups.
9. In the left navigation pane, under **Block Storage**, click **Block Volumes** to see both activated Block Volumes.

Disable Replication for a Volume Group

When you turn off replication for a volume group, by default, all volumes continue to replicate. However, as separate Volume Replicas, they are no longer part of a Volume Group Replica. At this point, you can turn off individual volume replication for all volumes.

In this practice, you'll learn how to disable replication for a volume group.

Tasks

1. Select the source region where you created your volume group, **Germany Central (Frankfurt)**.
2. From the **Main Menu**, select **Storage**. Under **Block Storage**, click **Volume Groups.**
3. Select the volume group **FRA-AA-LAB13-1-VG-01**.
4. Click **Edit**.
5. Click **Cross Region Replication** on the left of the screen and select the **OFF** option.
6. Select the **Check here to confirm** check box to acknowledge that the volume group replica will be deleted.
7. Select the **Volume replication off** check box to turn off replication for individual volumes.
8. Click **Summary** on the left of the screen.
9. Click **Save Changes.**

   Note: The Volume Group state changes to Updating. After a couple of seconds, the state becomes Available.

10. In the console ribbon at the top of the screen, click the Region icon to expand the menu. Ensure that you are in the correct destination region, **UK South (London).**
11. Open the **Main Menu** and click **Storage**. Under **Block Storage**, click **Volume Group Replicas**.

    Note: The **LHR-AA-LAB13-1-VGR-01** Volume Group Replica will be in a Terminating state. After a couple of minutes, it will be terminated.

File Storage: Create and Mount a File System

Lab 14-1 Practices

Get Started

Overview

The Oracle Cloud Infrastructure (OCI) File Storage service provides robust and shareable file systems. Network access to your file system is provided through a mount target, which is an NFS endpoint that lives in a subnet and connects NFS clients to file systems.

In this lab, you'll learn how to create a file system within the OCI console.

In this lab, you'll:

a. Create a Virtual Cloud Network (VCN) and its components

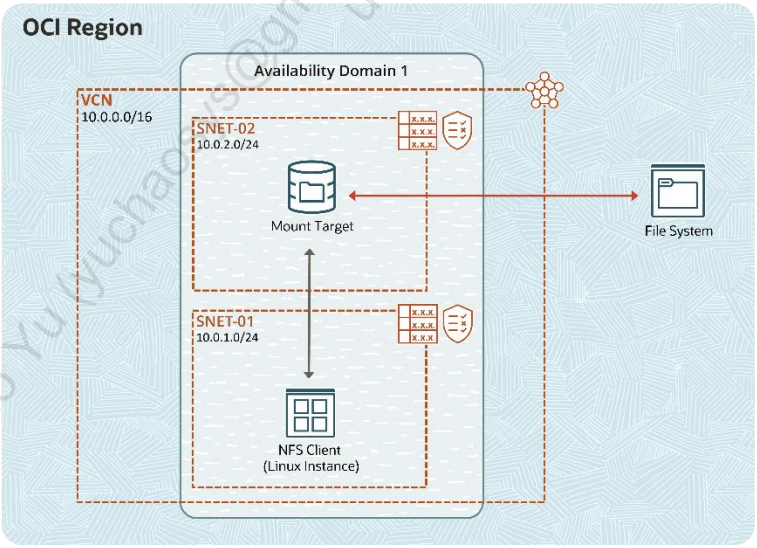
b. Create a VM instance

c. Create a file system

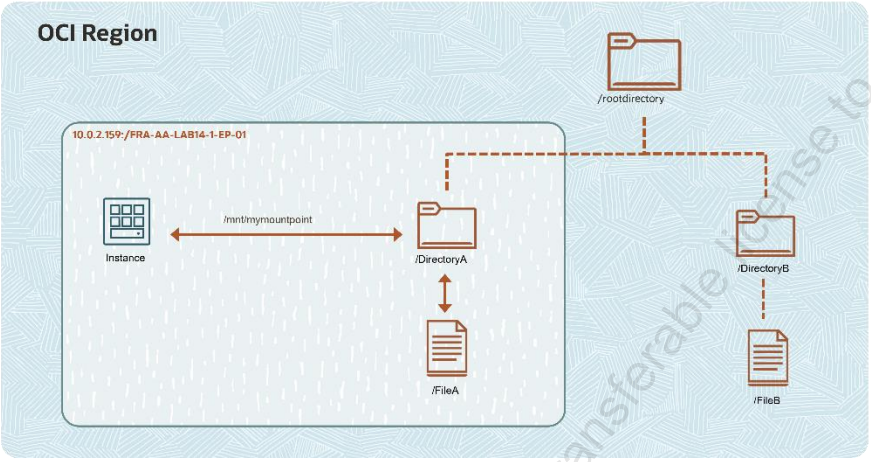
d. Configure VCN Security Rules for file storage

e. Mount the file system from an instance

Create and Mount a File System



Mount a File System



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- You must be familiar with navigating the OCI Console.
- Select the region that's available in the tenancy allotted to you. In this lab, we are considering Germany Central (Frankfurt) as your region.

Create a Virtual Cloud Network and Its Components

In this practice, you will learn how to create a Virtual Cloud Network, Subnet, Internet Gateway, and Security List, and add route rules in the Route Table.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks.**
3. Click **Create VCN.**
4. Enter the following:
   a. **Name:** Enter **`FRA-AA-LAB14-1-VCN-01`**.
   b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
   c. **IPv4 CIDR Blocks:** Enter **10.0.0.0/16**. Press **Enter** to add.

   Note: Leave all the other options in their default setting.
5. Click **Create VCN**. You now see that the VCN is created successfully and in the Available state.
6. Click **Create Subnet**.
7. In the Create Subnet dialog box, enter the following:
   a. **Name:** Enter **`FRA-AA-LAB14-1-SNET-01`**.
   b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
   c. **Subnet Type:** Select **Regional**.
   d. **IPv4 CIDR Block:** Enter **`10.0.1.0/24`**.
   e. **Subnet Access:** Select **Public Subnet.**

   Note: Leave all the other options in their default setting.
8. Click **Create Subnet.** You now see that the subnet is created successfully and in the Available state.

9. Click **Create Subnet** to create another Subnet. In the Create Subnet dialog box, enter the following:

    a. **Name:** Enter **`FRA-AA-LAB14-1-SNET-02`**.

    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.

    c. **Subnet Type:** Select **Regional**.

    d. **IPv4 CIDR Block:** Enter **`10.0.2.0/24`**.

    e. **Subnet Access:** Select **Public Subnet**.

    f. **DNS Label:** Enter **`FRAAALAB141SNE2`**.

    Note: Leave all the other options in their default setting.

10. Click **Create Subnet.**

11. In the left navigation pane, under **Resources**, click **Internet Gateways.**

12. Click **Create Internet Gateway.**

13. Enter the following:

    a. **Name:** Enter **`FRA-AA-LAB14-1-IG-01`.**

    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.

14. Click **Create Internet Gateway.** You now see that the Internet Gateway is created successfully and in the Available state.

15. In the left navigation pane, under **Resources**, click **Route Tables.**

16. Click to open **Default Route Table for FRA-AA-LAB14-1-VCN-01**.

17. Click **Add Route Rules** and enter the following:

    a. **Target Type**: Select **Internet Gateway**.

    b. **Destination CIDR Block:** Enter **`0.0.0.0/0`**.

    c. **Target Internet Gateway:** Select **FRA-AA-LAB14-1-IG-01**.

18. Click **Add Route Rules**. You now see that the route rule is successfully added in the default Route Table.

19. Using the breadcrumb trail at the top of the screen, return to your VCN page.

20. In the left navigation pane, under **Resources**, click **Security Lists**.

21. Click **Create Security List.**

22. Enter the following:

    a. **Name:** Enter **`FRA-AA-LAB14-1-SL-01`**.

    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.

    c. Do not add any Ingress or Egress rules.

23. Click **Create Security List.** You now see that the security list is created and displayed on the **Security Lists** page.

    Note: As of now, both Subnets FRA-AA-LAB14-1-SNET-01 and FRA-AA-LAB14-1-SNET-02 are using the Default Security List.

24. Leave Subnet FRA-AA-LAB14-1-SNET-01 as is with the Default Security List. Change the Security List for Subnet FRA-AA-LAB14-1-SNET-02 by doing the following:

    a. Click **Subnets**.

    b. Click the subnet **FRA-AA-LAB14-1-SNET-02**.

    c. In the left navigation pane, under **Resources**, click **Security Lists**.

    d. To add a security list, click **Add Security List**, and select **FRA-AA-LAB14-1-SL-01**.

    e. Click **Add Security List**.

    f. To remove the default security list, **Default Security List for FRA-AA-LAB14-1-VCN-01**, click the three dots on the right to open the Actions menu, then click **Remove**.

    g. Click **Remove** when prompted to confirm removal.

    Note: The changes take effect within a few seconds.

Create a VM Instance

In this practice, you will learn how to create SSH keys using Cloud Shell and launch an Instance.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. In the console ribbon at the top of the screen, click the **Cloud Shell** icon next to the Region selection menu.
3. Once the Cloud Shell is ready, enter the following commands:

   ```
   $ mkdir .ssh
   ```

   - **Important:** In case you get an error message that says "Cannot create director: File exists," you can skip running this first command.

   ```
   $ cd .ssh
   ```

   ```
   $ ssh-keygen -b 2048 -t rsa -f <<sshkeyname>>
   ```

   - **Remember:** After entering this third command, press **Enter** twice for no passphrase.

   Note: Replace `<<sshkeyname>>` with `ociaalabkey`. Choose the key name you can remember. This will be the key name you will use to connect to the compute instance you create.

   Reminder: The angle brackets «» should not appear in your code.

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

4. Examine the two files that you just created by running the following command:

   ```
   $ ls
   ```

   Note: In the output, there are two files, a private key: *<<sshkeyname>>* and a public key: *<<sshkeyname>>.pub*, keep the private key safe and don't share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems as well as copied and pasted to facilitate secure communications in the cloud.

5. To list the contents of the public key, use the following command:

   ```
   $ cat <<sshkeyname>>.pub
   ```

   Note: Replace `<<sshkeyname>>` with `ociaalabkey`.

   Reminder: The angle brackets «» should not appear in your code.

6. Copy the contents of the public key as you will need this in a subsequent step. Make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

7. From the **Main Menu**, select **Compute**. Under **Compute**, click **Instances.**

8. Click **Create instance** and enter the following:

   a. **Name:** Enter **`FRA-AA-LAB14-1-VM-01`**.

   b. **Create in compartment:** Select the <*compartment name*> assigned to you.

   c. **Placement:** Select Availability Domain **AD1**. Click **Show advanced options** and select **On-demand capacity** from the **Capacity type** menu.

   d. **Image and shape:** Choose the image **Oracle Linux 8** and shape **VM.Standard.A1.Flex** (1 OCPU, 6GB Memory) [Shape series: Ampere].

   e. **Networking:** Select the existing virtual cloud network **FRA-AA-LAB14-1-VCN-01** and existing subnet **FRA-AA-LAB14-1-SNET-01 (regional)** . Under **Public IP address,** select **Assign a public IPv4 address**.

   f. **Add SSH keys:** Select **Paste public keys** and paste the contents of the public key, which you copied in Step 6, in the box.

   g. **Boot volume:** Keep the default selections.

9. Click **Create**.

   Note: After a couple of minutes, you can see that the Instance is successfully created and the state is Running.

10. Under **Instance access**, copy the **Public IP address**.

11. Click the **Cloud Shell** icon to open Cloud Shell, and use SSH to connect to your instance by using the following command:

    Note: Enter **yes** in response to "Are you sure you want to continue connecting (yes/no)?"

```
$ ssh -i <private_key_file> <username>@<public-ip-address>
```

Reminders:

- `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
- `<username>` is the default user **opc**.
- `<public-ip-address>` is the Public IP address of the instance.

Note: You are now connected to the Instance FRA-AA-LAB14-1-VM-01.

Create a File System

You can create a shared file system in the cloud by using the File Storage service. Network access to your file system is provided through a mount target. Exports control how NFS clients access file systems when they connect to a mount target. When you use the OCI console to create your file system, the workflow also creates a mount target and export for it.

In this practice, you will learn how to create a file system.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. From the **Main Menu**, select **Storage**. Under **File Storage**, click **File Systems**.
3. In the left navigation pane, in the **List Scope** section, under **Compartment**, select the <*compartment name*> assigned to you.
4. Click **Create File System**.
5. In the **File System Information** section**,** click **Edit Details** and enter the following:
    a. **Name:** Enter **`FRA-AA-LAB14-1-FS-01`**.
    b. **Availability Domain:** Select the first availability domain.
    c. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    d. **Encryption:** Keep the default **Encrypt using Oracle-managed keys** selection.
6. In the **Export Information** section, click **Edit Details** and enter the following:
    a. **Export Path:** Enter **`/FRA-AA-LAB14-1-EP-01`**.
    b. Do not select the **Use Secure Export Options** check box.
7. In the **Mount Target Information** section, click **Edit Details** and specify the following:
    a. Select the **Create New Mount Target** option.
    b. Enter **`FRA-AA-LAB14-1-MNT-01`** in the **New Mount Target Name** field.
    c. Select **FRA-AA-LAB14-1-VCN-01** from the **Virtual Cloud Network** drop-down list.

d. Select **FRA-AA-LAB14-1-SNET-02** from the Subnet drop-down list.

e. Do not select the **Use network security groups to control traffic** check box.

8. Click **Create.**

Note: The File Storage service typically creates the file system and mount target within a few seconds.

Configure VCN Security Rules for File Storage

Before you can mount a file system, you must configure security rules to allow traffic to the mount target's VNIC using specific protocols and ports. Security rules enable traffic for the following:

- Open Network Computing Remote Procedure Call (ONC RPC) `rpcbind` utility protocol
- Network File System (NFS) protocol
- Network File System (MOUNT) protocol
- Network Lock Manager (NLM) protocol

In this practice, you'll learn how to configure security rules for both the mount target and the instance in a security list.

Note

In this lab scenario, the mount target that exports the file system is in a different subnet (FRA-AA-LAB14-1-SNET-02） than the instance you want to mount the file system to (FRA-AA-LAB14-1-SNET-01) .

You need to set up the following security rules in **FRA-AA-LAB14-1-SL-01** for the mount target. You also need to specify the instance IP address or CIDR block 10.0.1.0/24 as the source for ingress rules and the destination for egress rules:

- Stateful ingress from ALL ports in the source instance CIDR block to TCP ports 111, 2048, 2049, and 2050
- Stateful ingress from ALL ports in the source instance CIDR block to UDP ports 111 and 2048
- Stateful egress from TCP ports 111, 2048, 2049, and 2050 to ALL ports in the destination instance CIDR block
- Stateful egress from UDP port 111 to ALL ports in the destination instance CIDR block

Next, you need to set up the following security rules in **Default Security List for FRA-AA-LAB14-1-VCN-01** for the instance. You also need to specify the mount target IP address or CIDR block 10.0.2.0/24 as the source for ingress rules and the destination for egress rules:

- Stateful ingress from source mount target CIDR block TCP ports 111, 2048, 2049, and 2050 to ALL ports
- Stateful ingress from source mount target CIDR block UDP port 111 to ALL ports
- Stateful egress from ALL ports to destination mount target CIDR block TCP ports 111, 2048, 2049, and 2050
- Stateful egress from ALL ports to destination mount target CIDR block UDP ports 111 and 2048.

Tasks

1. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks.**
2. Select **FRA-AA-LAB14-1-VCN-01** from the list of VCNs.
3. In the left navigation pane, under **Resources**, click **Security Lists**.
4. Select **FRA-AA-LAB14-1-SL-01** from the list of security lists.
5. In the left navigation pane, under **Resources**, click **Ingress Rules**.
6. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR**.
    c. **Source CIDR:** Enter `10.0.1.0/24.`
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `111`.
7. Click **Add Ingress Rules**.

8. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR**.

    c. **Source CIDR:** Enter `10.0.1.0/24`.

    d. **IP Protocol:** Select **TCP**.

    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `2048-2050`.

9. Click **Add Ingress Rules**.

10. Click **Add Ingress Rule** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR**.

    c. **Source CIDR:** Enter `10.0.1.0/24.`

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `111`.

11. Click **Add Ingress Rules**.

12. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR**.

    c. **Source CIDR:** Enter `10.0.1.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `2048`.

13. Click **Add Ingress Rules**.
14. In the left navigation pane, under **Resources**, click **Egress Rules**.
15. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: Enter `111`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
16. Click **Add Egress Rules**.
17. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: Enter `2048-2050`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
18. Click **Add Egress Rules**.
19. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **UDP**.

e. **Source Port Range**: Enter `111`.

f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.

20. Click **Add Egress Rules**.
21. Using the breadcrumb trail at the top of the screen, click back to go to the VCN **FRA-AA-LAB14-1-VCN-01**.
22. In the left navigation pane, under **Resources**, click **Security Lists**.
23. Click to open **Default Security List for FRA-AA-LAB14-1-VCN-01**.
24. In the left navigation pane, under **Resources**, click **Ingress Rules**.
25. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR**.

    c. **Source CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **TCP**.

    e. **Source Port Range:** Enter `2048-2050`.

    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.

26. Click **Add Ingress Rules.**
27. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR**.

    c. **Source CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **TCP**.

    e. **Source Port Range:** Enter `111`.

    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.

28. Click **Add Ingress Rules.**

29. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR**.
    c. **Source CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **UDP**.
    e. **Source Port Range:** Enter `111`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
30. Click **Add Ingress Rules.**
31. In the left navigation pane, under **Resources**, click **Egress Rules**.
32. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `2048-2050`.
33. Click **Add Egress Rules.**
34. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter **111**.

35. Click **Add Egress Rules.**

36. Click **Add Egress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Destination Type:** Select **CIDR**.

    c. **Destination CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `111`.

37. Click **Add Egress Rules.**

38. Click **Add Egress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Destination Type:** Select **CIDR**.

    c. **Destination CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `2048`.

39. Click **Add Egress Rules.**

Mount the File System from an Instance

In this practice, you will learn how to mount a file system from an instance.

Tasks

1. From the **Main Menu**, **Storage**. Under **File Storage**, click **File Systems**.
2. In the **File Systems** list, click the **FRA-AA-LAB14-1-FS-01** file system.
3. In the left navigation pane, under **Resources**, click **Exports.**
4. Locate /FRA-AA-LAB14-1-EP-01 and click the three dots to the right to open the Actions menu. Then select **Mount Commands.**
5. In **Image**, choose **Oracle Linux** from the drop-down list.
6. Click the **Copy** links to copy the three commands listed.
7. Connect to your instance **FRA-AA-LAB14-1-VM-01**.

   Note: For help with this, refer to Step 11 in the **Create a VM Instance** practice.

8. Paste and run the commands that you copied in the previous step into your instance session window.

   Important: Please run the commands that you copied and not the following commands which are just for reference:

   ```
   $ sudo yum install nfs-utils

   $ sudo mkdir -p /mnt/FRA-AA-LAB14-1-EP-01

   $ sudo mount 10.0.2.159:/FRA-AA-LAB14-1-EP-01 /mnt/FRA-AA-LAB14-1-
   EP-01
   ```

9. View the file system by entering the following:

   ```
   $ df -h
   ```

10. Write a file to the file system by entering the following:

    ```
    $ sudo touch /mnt/yourmountpoint/helloworld
    ```

    Note: Replace `yourmountpoint` with the path to the local mount point. For example:

    ```
    $ sudo touch /mnt/FRA-AA-LAB14-1-EP-01/helloworld
    ```

11. Verify that you can view the file by entering the following:

```
$ cd /mnt/yourmountpoint
```

Note: Replace `yourmountpoint` with the path to the local mount point. For example:

```
$ cd /mnt/FRA-AA-LAB14-1-EP-01
$ ls
```

File Storage: Configure NFS Export Options

Lab 15-1 Practices

Get Started

Overview

NFS export options enable you to create more granular access control to limit VCN access. You can use NFS export options to specify access levels for IP addresses or CIDR blocks connecting to file systems through exports in a mount target. Doing this provides better security controls in multi-tenant environments.

Additionally, by using NFS export option access controls, you can limit the clients' ability to connect to the file system and view or write data.

In this lab, you'll learn how to allow read-only access to the file system from one instance and read/write access from the other instance.

In this lab, you'll:

a. Create a Virtual Cloud Network and its components

b. Create two VM instances

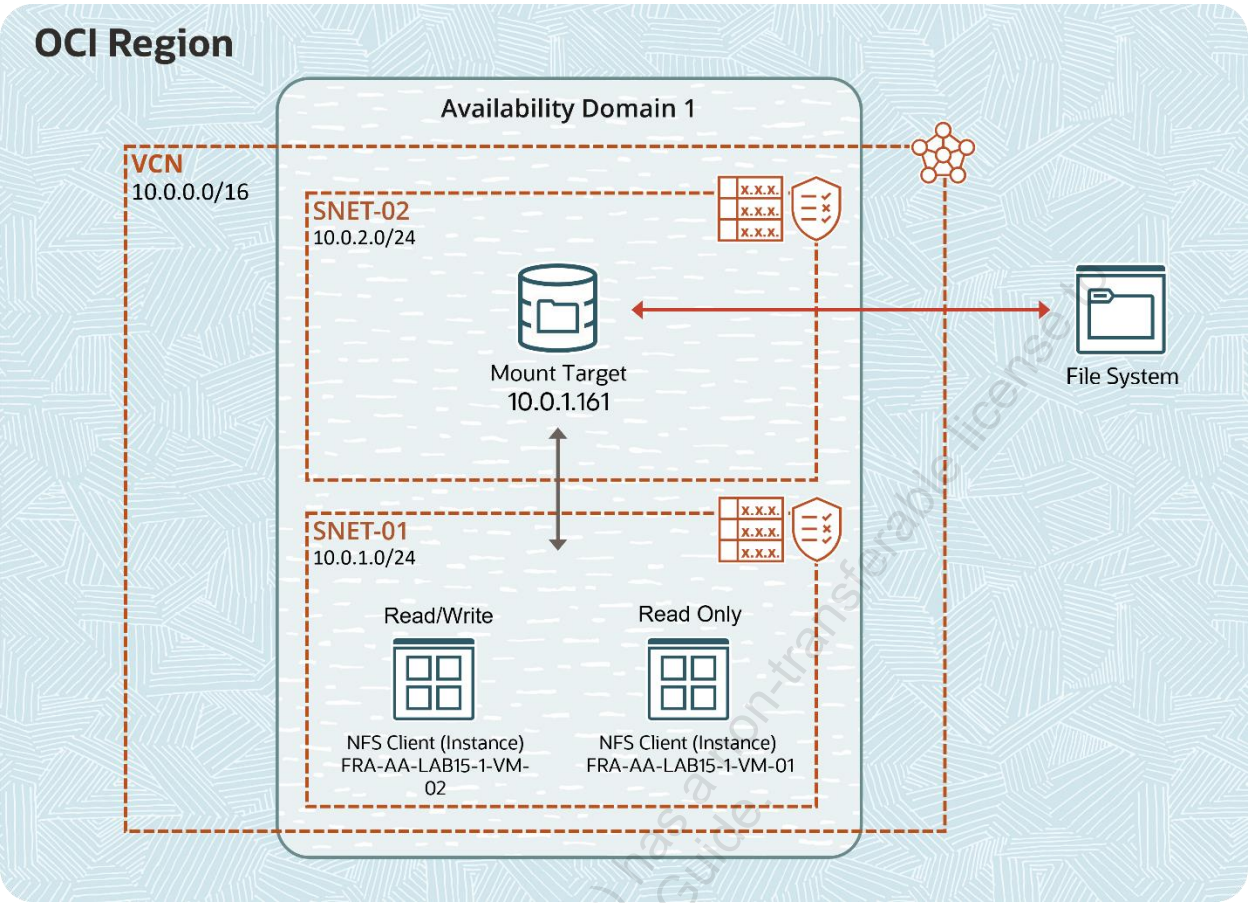
c. Create a file system

d. Configure VCN Security Rules for file storage

e. Set Export Options for the file system

f. Mount the file system from both the Instances

g. Perform testing



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Assumptions

- You must be familiar with navigating the OCI Console.
- You will select the region available in the tenancy allotted to you. In this lab, we are considering Germany Central (Frankfurt) as your region.

Create a Virtual Cloud Network and Its Components

In this practice, you will learn how to create a Virtual Cloud Network (VCN), Subnet, Internet Gateway, and Security List, and add route rules in the Route Table.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. Open the **Main Menu**, click **Networking**, and then click **Virtual Cloud Networks.**
3. Click **Create VCN.**
4. Enter the following:
    a. **Name:** Enter **`FRA-AA-LAB15-1-VCN-01`**.
    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    c. **IPv4 CIDR Block:** Enter **10.0.0.0/16**. Press **Enter** to add.

    Note: You can leave all the other options as default.
5. Click **Create VCN**. The VCN is now created successfully.
6. Click **Create Subnet**.
7. In the Create Subnet dialog box, enter the following:
    a. **Name**: Enter **`FRA-AA-LAB15-1-SNET-01`**.
    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    c. **Subnet Type:** Select **Regional**.
    d. **IPv4 CIDR Block:** Enter **`10.0.1.0/24`**.
    e. **Subnet Access:** Select **Public Subnet.**

    Note: You can leave all the other options as default.
8. Click **Create Subnet.** The subnet is now created successfully and the state is Available.

9. Click **Create Subnet** to create another subnet. In the Create Subnet dialog box, enter the following:
    a. **Name**: Enter **`FRA-AA-LAB15-1-SNET-02`**.
    b. **Create in Compartment**: Select the <*compartment name*> assigned to you.
    c. **Subnet Type**: Select **Regional.**
    d. **IPv4 CIDR Blocks:** Enter `10.0.2.0/24`.
    e. **Subnet Access**: Select **Public Subnet.**
    f. **DNS Label**: Enter **`FRAAALAB151SNE2.`**
    g. **Note:** Leave all the other options in their default setting.
10. Click **Create Subnet**.
11. In the left navigation pane, under **Resources**, click **Internet Gateways**.
12. Click **Create Internet Gateway.**
13. Enter the following:
    a. **Name**: Enter **`FRA-AA-LAB15-1-IG-01`**.
    b. **Create in Compartment**: Select the <*compartment name*> assigned to you.
14. Click **Create Internet Gateway.** The Internet Gateway is now created successfully, and the state is Available.
15. In the left navigation pane, under **Resources**, click **Route Tables.**
16. Click **Default Route Table for FRA-AA-LAB15-1-VCN-01**.
17. Click **Add Route Rules** and enter the following:
    a. **Target Type**: Select **Internet Gateway**.
    b. **Destination CIDR Block:** Enter `0.0.0.0/0`.
    c. **Target Internet Gateway:** Select **FRA-AA-LAB15-1-IG-01**.
18. Click **Add Route Rules**. The route rule is successfully added in the default Route Table.

19. Using the breadcrumb trail at the top of the screen, return to your VCN page.

20. In the left navigation pane, under **Resources**, click **Security Lists**.

21. Click **Create Security List.**

22. Enter the following:

    a. **Name:** Enter **`FRA-AA-LAB15-1-SL-01`**.

    b. **Create in Compartment:** Select the <*compartment name*> assigned to you.

    c. Do not add any Ingress or Egress rules.

23. Click **Create Security List.** The security list is created and displayed on the **Security Lists** page.

    Note: As of now, both the Subnets FRA-AA-LAB15-1-SNET-01 and FRA-AA-LAB15-1-SNET-02 are using the Default Security List.

24. Leave Subnet FRA-AA-LAB15-1-SNET-01 as is with the Default Security List. Change the Security List for Subnet FRA-AA-LAB15-1-SNET-02 by doing the following:

    a. Click **Subnets**.

    b. Click the subnet **FRA-AA-LAB15-1-SNET-02**.

    c. In the left navigation pane, under **Resources**, click **Security Lists**.

    d. To add a security list, click **Add Security List**, and select **FRA-AA-LAB15-1-SL-01**.

    e. To remove the default security list **Default Security List for FRA-AA-LAB15-1-VCN-01**, click the three dots on the right to open the Actions menu, and then select **Remove**.

    f. Click **Remove** when prompted to confirm removal.

    Note: The changes take effect within a few seconds.

Create a VM Instance

In this practice, you will learn how to create SSH keys using Cloud Shell and launch an instance.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. In the console ribbon at the top of the screen, click the **Cloud Shell** icon next to the Region selection menu.
3. After the Cloud Shell is ready, enter the following commands:

   ```
   $ mkdir .ssh
   ```

   - **Important:** In case you get an error message that says "Cannot create director: File exists," you can skip running this first command.

   ```
   $ cd .ssh
   ```

   ```
   $ ssh-keygen -b 2048 -t rsa –f <<sshkeyname>>
   ```

   - **Remember:** After entering this third command, press **Enter** twice for no passphrase.

   Note: Replace `<<sshkeyname>>` with `ociaalab15key`. Choose the key name you can remember. This will be the key name you will use to connect to the compute instance you create.

   Reminder: The angle brackets «» should not appear in your code.

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

4. Examine the two files that you just created by running the following command:

   ```
   $ ls
   ```

   Note: In the output, there are two files, a private key: *<<sshkeyname>>* and a public key: *<<sshkeyname>>.pub*, keep the private key safe and don't share its content with anyone. The public key will be needed for various activities and can be uploaded to certain systems as well as copied and pasted to facilitate secure communications in the cloud.

5. To list the contents of the public key, use the following command:

   ```
   $ cat <<sshkeyname>>.pub
   ```

   Note: Replace `<<sshkeyname>>` with `ociaalabkey`.

   Reminder: The angle brackets «» should not appear in your code.

6. Copy the contents of the public key as you will need this in a subsequent step. Make sure that you remove any hard returns that may have been added when copying. The `.pub` key should be one line.

7. Open the **Main Menu** and click **Compute**. Under **Compute**, click **Instances.**

8. Click **Create instance** and enter the following:

   a. **Name:** Enter **`FRA-AA-LAB15-1-VM-01`**.

   b. **Create in compartment:** Select the <*compartment name*> assigned to you.

   c. **Placement:** Select Availability Domain **AD1**. Click **Show advanced options** and select **On-demand capacity** under the **Capacity type** menu.

   d. **Image and shape**: Choose the image **Oracle Linux 8** and shape **VM.Standard.A1.Flex** (1 OCPU, 6GB Memory) [Shape series: Ampere].

   e. **Networking**: Select the existing virtual cloud network **FRA-AA-LAB15-1-VCN-01** and existing subnet **FRA-AA-LAB15-1-SNET-01 (regional)**. Under **Public IP address** select **Assign a public IPv4 address.**

   f. **Add SSH keys**: Select **Paste public keys** and paste the contents of the public key, which you copied in Step 6, in the box.

   g. **Boot volume:** Keep the default selections.

9. Click **Create**.

10. To create a second Instance, repeat steps 7–9. Keep all settings the same except enter the **Name** as **FRA-AA-LAB15-1-VM-02**.

    Note: Once finished, you see that the both the instances are created successfully and in the Running state.

11. To connect to the instances, on the **Instance information** tab and under **Instance access**, copy the **Public IP address**.

12. Open **Cloud Shell** and use SSH to connect to your instance by using the following commands:

    Note: Enter **`yes`** in response to "Are you sure you want to continue connecting (yes/no)?"

    ```
    $ ssh -i <private_key_file> <username>@<public-ip-address>
    ```

    Reminders:

    - `<private_key_file>` is the full path and name of the file that contains the private key associated with the instance you want to access.
    - `<username>` is the default user `opc`.
    - `<public-ip-address>` is the Public IP address of the instance.

Create a File System

You can create a shared file system in the cloud using the File Storage service. Network access to your file system is provided through a mount target. Exports control how NFS clients access file systems when they connect to a mount target. When you use the console to create your file system, the workflow also creates a mount target and an export for it.

In this practice, you will learn how to create a file system.

Tasks

1. Sign in to the Oracle Cloud Infrastructure (OCI) Console.
2. Open the **Main Menu** and click **Storage**. Under **File Storage**, click **File Systems**.
3. In the left navigation pane, in the **List Scope** section, under **Compartment**, select the <*compartment name*> assigned to you.
4. Click **Create File System**.
5. In **File System Information**, click **Edit Details** and enter the following:
    a. **Name:** Enter **`FRA-AA-LAB15-1-FS-01.`**
    b. **Availability Domain:** Select the first availability domain.
    c. **Create in Compartment:** Select the <*compartment name*> assigned to you.
    d. **Encryption:** Keep the default **Encrypt using Oracle-managed keys** selection.
6. In the **Export Information** click **Edit Details** and enter the following:
    a. **Export Path**: Enter **`/FRA-AA-LAB15-1-EP-01.`**
    b. Do not select **Use Secure Export Options**.
7. In the **Mount Target Information**, click **Edit Details** and specify the following:
    a. Select the **Create New Mount Target** option.
    b. Enter **`FRA-AA-LAB15-1-MNT-01`** in the **New Mount Target Name** field.
    c. Select **FRA-AA-LAB15-1-VCN-01** from the **Virtual Cloud Network** drop-down list.

d. Select **FRA-AA-LAB15-1-SNET-02 (regional)** from the **Subnet** drop-down list.

e. Do not select the **Use network security groups to control traffic** check box.

8. Click **Create.**

Note: The File Storage service typically creates the file system and mount target within a few seconds.

Configure VCN Security Rules for File Storage

Before you can mount a file system, you must configure security rules to allow traffic to the mount target's VNIC using specific protocols and ports. Security rules enable traffic for the following:

- Open Network Computing Remote Procedure Call (ONC RPC) rpcbind utility protocol
- Network File System (NFS) protocol
- Network File System (MOUNT) protocol
- Network Lock Manager (NLM) protocol

In this practice, you'll learn how to configure security rules for both the mount target and the instance in a security list.

Note

In this lab scenario, the mount target that exports the file system is in a different subnet (FRA-AA-LAB15-1-SNET-02) than the instance on which you want to mount the file system (FRA-AA-LAB15-1-SNET-01) .

You need to set up the following security rules in **FRA-AA-LAB15-1-SL-01** for the mount target. You also need to specify the instance IP address or CIDR block 10.0.1.0/24 as the source for ingress rules and the destination for egress rules:

- Stateful ingress from ALL ports in the source instance CIDR block to TCP ports 111, 2048, 2049, and 2050
- Stateful ingress from ALL ports in the source instance CIDR block to UDP ports 111 and 2048
- Stateful egress from TCP ports 111, 2048, 2049, and 2050 to ALL ports in the destination instance CIDR block
- Stateful egress from UDP port 111 to ALL ports in the destination instance CIDR block

Next, you need to set up the following security rules in **Default Security List for FRA-AA-LAB15-1-VCN-01** for the instance. You also need to specify the mount target IP address or CIDR block 10.0.2.0/24 as the source for ingress rules and the destination for egress rules:

- Stateful ingress from source mount target CIDR block TCP ports 111, 2048, 2049, and 2050 to ALL ports
- Stateful ingress from source mount target CIDR block UDP port 111 to ALL ports
- Stateful egress from ALL ports to destination mount target CIDR block TCP ports 111, 2048, 2049, and 2050.
- Stateful egress from ALL ports to destination mount target CIDR block UDP ports 111 and 2048.

Tasks

1. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks.**
2. Click **FRA-AA-LAB15-1-VCN-01** from the list of VCNs.
3. In the left navigation pane, under **Resources**, click **Security Lists**.
4. Click **FRA-AA-LAB15-1-SL-01**.
5. In the left navigation pane, under **Resources**, click **Ingress Rules**.
6. Click **Add Ingress Rule** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR**.
    c. **Source CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP.**
    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `111`.
7. Click **Add Ingress Rules**.

8. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR.**

    c. **Source CIDR:** Enter `10.0.1.0/24`.

    d. **IP Protocol:** Select **TCP.**

    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `2048-2050`.

9. Click **Add Ingress Rules**.

10. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR.**

    c. **Source CIDR:** Enter `10.0.1.0/24`.

    d. **IP Protocol:** Select **UDP.**

    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `111`.

11. Click **Add Ingress Rules**.

12. Click **Add Ingress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Source Type:** Select **CIDR.**

    c. **Source CIDR:** Enter `10.0.1.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range:** By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `2048`.

13. Click **Add Ingress Rules**.
14. In the left navigation pane, under **Resources**, click **Egress Rules**.
15. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP.**
    e. **Source Port Range**: Enter `111`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
16. Click **Add Egress Rules**.
17. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: Enter `2048-2050`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
18. Click **Add Egress Rules**.
19. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.1.0/24`.
    d. **IP Protocol:** Select **UDP**.

e. **Source Port Range**: Enter `111`.

f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.

20. Click **Add Egress Rules**.
21. Click the VCN **FRA-AA-LAB15-1-VCN-01**.
22. In the left navigation pane, under **Resources**, click **Security Lists**.
23. Click **Default Security List for FRA-AA-LAB15-1-VCN-01**.
24. In the left navigation pane, under **Resources**, click **Ingress Rules**.
25. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR.**
    c. **Source CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP.**
    e. **Source Port Range:** Enter `2048-2050`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank).
26. Click **Add Ingress Rules.**
27. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR.**
    c. **Source CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP.**
    e. **Source Port Range:** Enter `111`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
28. Click **Add Ingress Rules**.

29. Click **Add Ingress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Source Type:** Select **CIDR**.
    c. **Source CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **UDP.**
    e. **Source Port Range:** Enter `111`.
    f. **Destination Port Range:** By default, it will be All, even if you leave the field blank.
30. Click **Add Ingress Rules**.
31. In the left navigation pane, under **Resources**, click **Egress Rules**.
32. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `2048-2050`.
33. Click **Add Egress Rules.**
34. Click **Add Egress Rules** and enter the following:
    a. Do not select the **Stateless** check box.
    b. **Destination Type:** Select **CIDR**.
    c. **Destination CIDR:** Enter `10.0.2.0/24`.
    d. **IP Protocol:** Select **TCP**.
    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.
    f. **Destination Port Range:** Enter `111`.

35. Click **Add Egress Rules**.

36. Click **Add Egress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Destination Type:** Select **CIDR**.

    c. **Destination CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `111`.

37. Click **Add Egress Rules**.

38. Click **Add Egress Rules** and enter the following:

    a. Do not select the **Stateless** check box.

    b. **Destination Type:** Select **CIDR**.

    c. **Destination CIDR:** Enter `10.0.2.0/24`.

    d. **IP Protocol:** Select **UDP**.

    e. **Source Port Range**: By default, it will be All, even if you leave the field blank.

    f. **Destination Port Range:** Enter `2048`.

39. Click **Add Egress Rules.**

Set Export Options for the File System

In this practice, you'll learn how to allow read-only access to the file system FRA-AA-LAB15-1-FS-01 from the Instance FRA-AA-LAB15-1-VM-01 and read/write access from the Instance FRA-AA-LAB15-1-VM-02.

Tasks

1. From the **Main Menu**, select **Compute**. Under **Compute**, click **Instances.**
2. Make a note of the Private IP addresses of both the instances FRA-AA-LAB15-1-VM-01 and FRA-AA-LAB15-1-VM-02.

   Note: In this lab, the Private IP addresses are as follows:

   - 10.0.1.15 for instance FRA-AA-LAB15-1-VM-01
   - 10.0.1.161 for instance FRA-AA-LAB15-1-VM-02

   Reminder: In your case, the Private IP address can be different.
3. From the **Main Menu**, click **Storage**. Under **File Storage**, click **File Systems**.
4. Click the file system **FRA-AA-LAB15-1-FS-01**.
5. From the **Exports** list, select the Export Path **/FRA-AA-LAB15-1-EP-01**.
6. Click **Edit NFS Export Options.**
7. In the existing Export Options window, make the following changes:

   a. **Source:** Enter `10.0.1.15/32`.

      Reminder: The Private IP address of FRA-AA-LAB15-1-VM-01 is **10.0.1.15**. However, when you perform the lab, it might be a different IP address.

   b. **Ports:** Select **Any.**

   c. **Access:** Select **Read Only.**

   d. **Squash:** Select **None.**
8. Click **+ Another Option** to create a new export option entry.

9. In the new entry boxes, specify the following information:

    a. **Source:** Enter `10.0.1.161/32`.

    Reminder: The Private IP address of FRA-AA-LAB15-1-VM-02 is **10.0.1.161**. However, when you perform the lab, it might be a different IP address.

    b. **Ports:** Select **Any**.

    c. **Access:** Select **Read/Write**.

    d. **Squash:** Select **None**.

10. When you're finished with your entries, click **Update**.

Mount the File System from Both the Instances

In this practice, you will learn how to mount a file system from two instances.

Tasks

1. From the **Main Menu**, select **Storage**. Under **File Storage**, click **File Systems**.
2. In the **File Systems** list, click the file system **FRA-AA-LAB15-1-FS-01**.
3. In the left navigation pane, under **Resources**, click **Exports**.
4. Locate /FRA-AA-LAB15-1-EP-01 and click the three dots on the right to open the Actions menu, and then select **Mount Commands.**
5. In **Image**, choose **Oracle Linux** from the drop-down menu.
6. Click the **Copy** links to copy the three commands listed.
7. Connect to your instance **FRA-AA-LAB15-1-VM-01**.

   Note: For help with this, refer to Steps 11–12 in the **Create a VM Instance** practice.

8. Paste and run the commands that you copied in the previous step into your instance session window.

   Important: Please run the commands that you copied and not the following commands which are just for reference:

   ```
   $ sudo yum install nfs-utils

   $ sudo mkdir -p /mnt/FRA-AA-LAB15-1-EP-01

   $ sudo mount 10.0.2.227:/FRA-AA-LAB15-1-EP-01 /mnt/FRA-AA-LAB15-1-
   EP-01
   ```

9. View the file system by entering the following:

   ```
   $ df -h
   ```

10. To mount the file system from the second instance FRA-AA-LAB15-1-VM-02, perform the following steps:

    a. Open a new duplicate tab in your browser.

    b. Repeat steps 7–8 of this practice.

    Note: The file system is now mounted from both instances, FRA-AA-LAB15-1-VM-01 and FRA-AA-LAB15-1-VM-02.

Perform Testing

In this practice, you will validate that you have read-only access to the file system FRA-AA-LAB15-1-FS-01 from the Instance FRA-AA-LAB15-1-VM-01, and read/write access from the Instance FRA-AA-LAB15-1-VM-02.

Tasks

1. Connect to your instance **FRA-AA-LAB15-1-VM-01**.

   Note: For help with this, refer to Steps 11-12 in the **Create a VM Instance** practice.

2. Try to write a file to the file system by entering the following:

   ```
   $ sudo touch /mnt/yourmountpoint/helloworld
   ```

   Note: Replace `yourmountpoint` with the path to the local mount point.

   For example:

   ```
   $ sudo touch /mnt/FRA-AA-LAB15-1-EP-01/helloworld
   ```

   Important: You will receive an error that validates that the instance FRA-AA-LAB15-1-VM-01 does not have write access to the file system.

3. Connect to your instance **FRA-AA-LAB15-1-VM-02.**

   Reminder: For help with this, refer to Steps 11–12 in the **Create a VM Instance** practice.

4. Try to write a file to the file system by entering the following:

   ```
   $ sudo touch /mnt/yourmountpoint/helloworld
   ```

   Note: Replace `yourmountpoint` with the path to the local mount point.

   For example:

   ```
   $ sudo touch /mnt/FRA-AA-LAB15-1-EP-01/helloworld
   ```

5. Once the file is successfully written, verify that you can view the file by entering the following.

   ```
   $ cd /mnt/yourmountpoint
   ```

   Note: Replace `yourmountpoint` with the path to the local mount point.

For example:

```
$ cd /mnt/FRA-AA-LAB15-1-EP-01

$ ls
```

6. Verify that you can view the file by enter the Step 5 commands from the instance **FRA-AA-LAB15-1-VM-01.**

   Note: You now see that the instance FRA-AA-LAB15-1-VM-01 has read-only access to the file system.

Security: Enable Cloud Guard

Lab 16-1 Practices

Get Started

Overview

Cloud Guard examines your Oracle Cloud Infrastructure resources for security weakness related to configuration, and your operators and users for risky activities. Upon detection, Cloud Guard can suggest, assist, or take corrective actions, based on your configuration.

In this lab, you will:

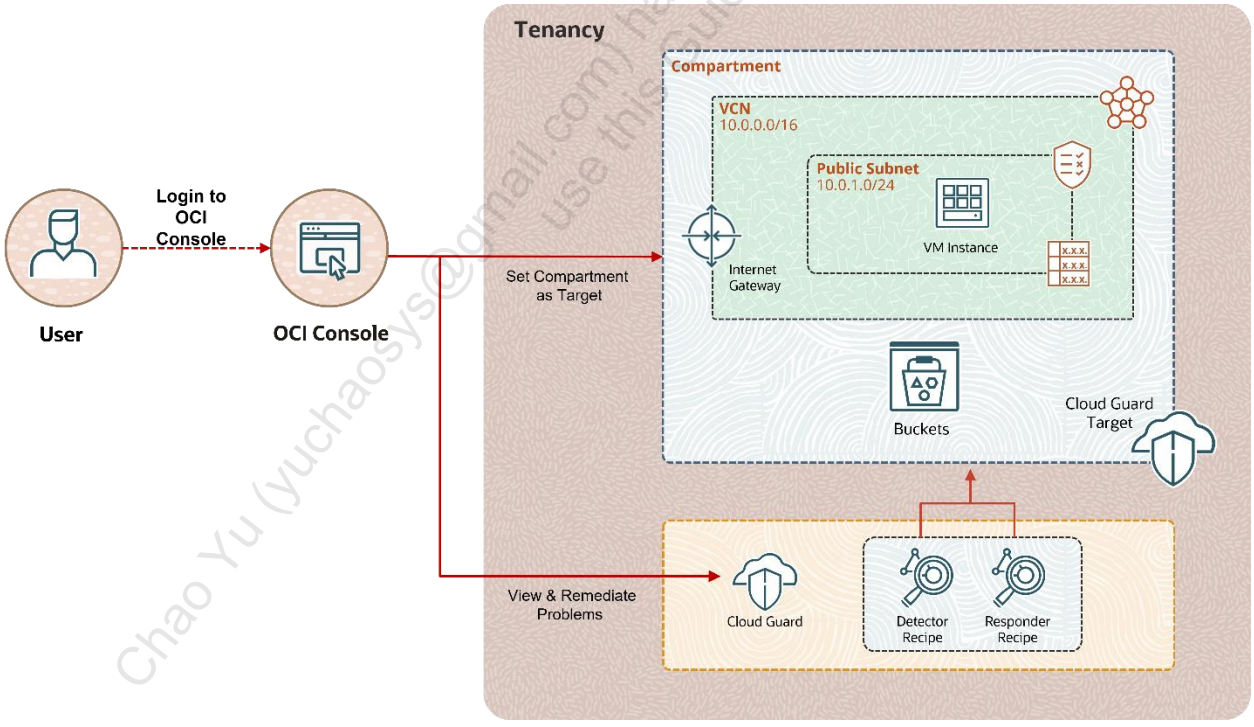
a. Create a Virtual Cloud Network

b. Explore Cloud Guard

c. Create a Cloud Guard target

d. Create a scenario to verify Cloud Guard monitoring

e. Remediate problems identified by Cloud Guard



Prerequisites

- You must have access to the OCI Console.
- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.

Create a Virtual Cloud Network

In this section, you will create a VCN by using the Start VCN Wizard tool.

Tasks

1. In the console ribbon at the top of the screen, click the **Regions menu** and select **UK South (London).**
2. Click the navigation menu, click **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:** `LHR-AA-LAB16-1-VCN-01`
   - **Compartment:** Select your assigned <*compartment name*>.
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**.

Explore Cloud Guard

In this practice, you will explore Cloud Guard to obtain a unified view of your tenancy's cloud security posture. You will also explore detector recipes for monitoring targets and responder recipes for responding with any problems that occur.

Tasks

1. In the console ribbon at the top of the screen, from the **Regions menu**, select **US East (Ashburn).**
2. From the navigation menu, select **Identity & Security**, and then click **Cloud Guard**.

   Note: A dashboard with the current Cloud Guard observations is displayed. If the Guided Tour is displayed, go through the same to explore the various features. You can also click **Stop tour** if you are not interested in the tour. Once you are done with the tour, the dashboard with various options under Cloud Guard on the left side in the browser window is displayed.
3. In the left navigation pane, under **Cloud Guard**, click **Detector Recipes.**
4. In the left navigation pane, under **Scope**, select ***<Tenancy Name>*** **(root).**
5. Click **OCI Configuration Detector Recipe (Oracle managed)** and view the detector rules that are included in this recipe.
6. To view the details of a particular rule, click the **disclosure triangle,** a downward arrow located next to the three dots the right of the rule.
7. Click **Risk level** to organize rules by their risk level.
8. Click **Detector Recipes** from the breadcrumb list at the top left.
9. Click **OCI Activity Detector Recipe (Oracle managed)** and explore the rules that are within activity detector recipe. You also see that for the built-in, Oracle-Managed detector recipes, you can clone the recipe. You may clone an existing recipe and customize it to your needs.
10. Click **Detector recipes** from the breadcrumb list at the top left.
11. In the left navigation pane, under **Cloud Guard**, click **Responder Recipes.**

12. Click **OCI Responder Recipe (Oracle Managed)**.

    View the responder rules that are included in this recipe.

13. To view the details of a particular rule, click the **disclosure trx1iangle,** a downward arrow located next to the three dots to the right of the rule.

14. Click **Responder recipes** from the breadcrumb at the top left.

15. In the left navigation pane, under **Cloud Guard**, click **Managed lists**.

16. Click the **Oracle Cloud Guard CIDR Managed List**.

    Note: A managed list is a reusable list of parameters that makes it easier to set the scope for detector and responder rules. A managed list is a tool that can be used to apply certain configurations to detectors.

    Under **Entries,** observe the predefined list of trusted IP address ranges used by Oracle Cloud Infrastructure (OCI). Cloud Guard also lets you define your own managed lists as needed.

    For example, you can define lists of states or provinces, ZIP codes, OCIDs, or whatever else you may define. Click the **Managed Lists** breadcrumbs and you will see an option to create your own managed list.

17. In the left navigation pane, under **Cloud Guard**, click **Settings**.

    Note: Observe the reporting region listed. If you are in the home region of your tenancy, you will also see the option to **Disable Cloud Guard** (if it is already enabled). If you are in any other region, this button will be disabled.

Create a Cloud Guard Target

In this practice, you will learn to add target to set scope of resources that Cloud Guard monitors.

Note: Cloud Guard is enabled in your practice tenancy.

Tasks

1. In the console ribbon at the top of the screen, click the **Regions menu** and select **UK South (London).**
2. Click the navigation menu, click **Identity & Security**, and then click **Cloud Guard**.
3. In the left navigation pane, under **Cloud Guard**, click **Targets.**
4. In the left navigation pane, under **List Scope**, and select your assigned <*compartment name*>.

   Note: If you already have a specific target set for your compartment, delete it.
5. Click **Create New Target**.
6. Enter the following:
   - **Target Name:** `LHR-AA-LAB16-1-CG-01`
   - **Description:** Enter a description.
   - **Compartment:** Select your assigned <*compartment name*>
   - **Configuration detector recipe:** OCI Configuration Detector Recipe (Oracle managed)
   - **Threat detector recipe:** OCI Threat Detector Recipe (Oracle managed)
   - **Activity Detector Recipe:** Oracle Activity Detector Recipe (Oracle managed)
   - **Responder recipe:** OCI Responder Recipe (Oracle managed)
7. Click **Create**.

   Note: The detail page for the new target will be displayed.
8. In the left navigation pane, under **Resources**, click **Detector recipes** and view the detector recipes associated with the created target.

Create a Scenario to Verify Cloud Guard Monitoring

To identify a problem in the set target, you will create a bucket and make its visibility public.

1. In the console ribbon at the top of the screen, click the **Regions menu** and select **UK South (London).**

2. Click the navigation menu and click **Storage**. Under Object Storage, click **Buckets**.

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

4. Click **Create Bucket**.

5. In the **Create Bucket** dialog box, specify the attributes of the bucket:
   - **Bucket Name:** `LHR-AA-LAB16-1-BKT-01-<user-id>`
     Please specify your user ID in place of `<user-id>` to make it unique.
   - **Default Storage Tier:** Select Standard.

   Note: Leave all the other options in their default settings.

6. Click **Create**.

7. Click the three dots on the right to open the Actions menu and select **Edit Visibility**. Select **Public** and click **Save Changes**.

   Note: You have now created a bucket with public visibility in the assigned compartment. To assure cloud security posture, the detector recipe includes a configuration rule for **Bucket with a public visibility**.

   As a result, you must wait for Cloud Guard to evaluate your allocated detector configuration and list its observations on the set target. Wait 30-60 minutes before checking the Cloud Guard Dashboard to see if the problem has been identified and resolving it.

Remediate the Problems Identified by Cloud Guard

1. From the navigation menu, select **Identity & Security**. Click **Cloud Guard**.
2. In the left navigation pane, under **Cloud Guard**, click **Problems.**
3. In the left navigation pane, under **List Scope**, select your assigned <*compartment name*>.
4. View the list of problems Cloud Guard has identified with the resources in your assigned compartment based on your previous practices. The Problems page displays information about each problem, including:
   - Problem Name
   - Risk Level
   - Detector Type
   - Resource affected
   - Target
   - Region
   - Labels
   - First Detected
   - Last Detected

Follow this process to remediate the problem **Bucket is Public.**

1. In the breadcrumbs at the top left, click **Problems.**
2. In the left navigation pane, under **Resource type,** select **Bucket**.
3. Select "**Bucket is Public**" from the problem list.
4. Check problem details and problem history, before the actions are taken.

   Note: As per the problem details, you have the option to remediate (if there are any responder suggestions) or mark it as resolved or dismiss the problem.

   The problem specifies that Bucket has a public visibility, it is recommended to carefully assess whether public visibility is required for the mentioned resource and to act if it does not.
5. Click **Remediate** and confirm that you want to execute the responder to remediate the problem.

Note: After a couple of minutes, you will see that the problem is successfully resolved, and the problem icon turns green.

6. To verify, click **Buckets** under **Object storage**. Click the bucket **LHR-AA-LAB16-1-BKT-01-<User_Id>** . You will now see that the visibility is now Private.

   Similarly, Cloud Guard can remediate or resolve identified problems in your OCI tenancy, ensuring security posture.

Security: Create a Vault and Encryption Key and Perform Encryption/Decryption of Data

Lab 17-1 Practices

Get Started

Overview

OCI Vault is a cloud native service that allows customers to securely store and manage their master encryption keys and configuration information. The OCI Vault service supports several key encryption algorithms such as the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA).

This lab enables you to encrypt or decrypt sensitive information (such as credit card details, salary information, and so on) by using the master encryption key stored in OCI Vault.

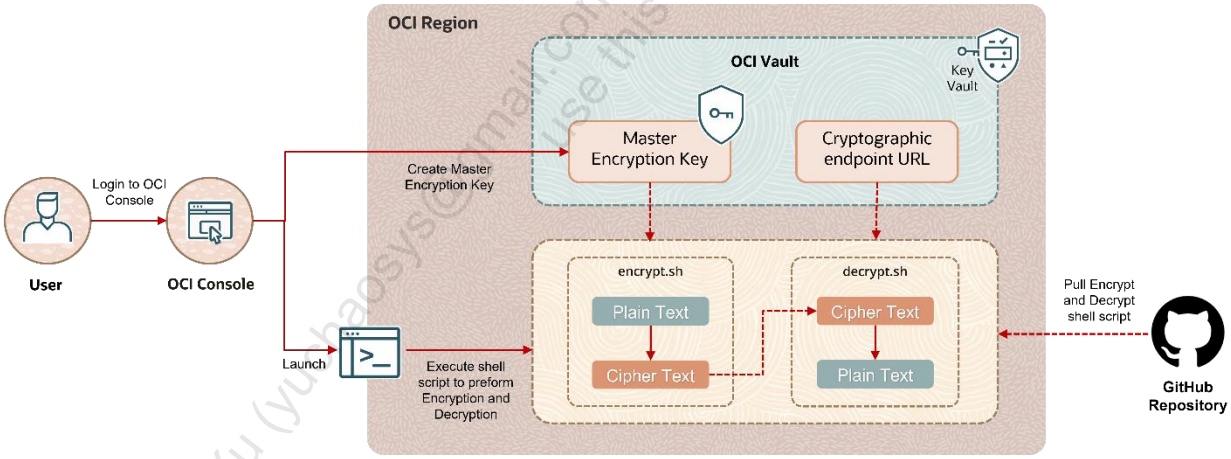
In this lab, you'll:

a. Create a master encryption key

b. Perform basic encryption and decryption by using the master encryption key

Prerequisites

- A precreated Vault console setting configured to leverage a Hardware Security Module (HSM)
- URL of a precreated encryption script located at a predetermined location git
- URL of a precreated decryption script located at a predetermined location git



Create a Master Encryption Key

You'll use an existing Vault that is at the root-level compartment, and will create a master encryption key required to perform cryptographic operations.

Tasks

1. Log in to the Oracle Cloud Infrastructure (OCI) console.
2. From the Main Menu, select **Identity & Security,** and then click **Vault**.
3. In the left navigation pane, under **List Scope**, select the **(root)** compartment from the **Compartment** drop-down list.
4. Select **ARCHITECT-ASS-VAULT** from the list of vaults in the root compartment. This resource has been precreated for you and is configured to leverage a Hardware Security Module (HSM).
5. Locate the **Cryptographic Endpoint** URL on the Vault Information tab. Copy the URL to your clipboard and save it somewhere to use later during encryption process.
    a. Example: https://xxxxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
6. From the left navigation pane under **Resources**, click **Master Encryption Keys**, and then click **Create Key**.
7. In the Create Key dialog box, enter the following values for your key:
    a. **Create in Compartment:** <Select your *assigned compartment*>

    Note: Do not choose the (root) compartment.
    b. Protection Mode: HSM
    c. **Name:** FRA-AA-LAB17-VK-01
    d. Leave everything else to default values and click **Create Key**. It will take about a minute to create the master encryption key. The keys will go through the **Creating** state to the **Enabled** state.
8. Select your assigned compartment from the **Compartment** drop-down list in the left column under List Scope. To the right, you will see the key that you created. Click your Master Encrypted Key.
9. On the Key Details page, locate the OCID value on the Key Information tab. Click the **Copy** link located to the right of the OCID value. Save the OCID value somewhere to use later during the encryption process.

    Sample: ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Perform Encryption

You will now run the provided shell script, which will take as input the OCI Vault cryptographic endpoint, the OCID of the master encryption key you created, and plain text to encrypt. The provided shell script invokes `oci kms crypto encrypt` to perform data encryption.

Tasks

1. Click the **Cloud Shell** icon in the Console header to launch your Cloud Shell.
   a. Go to your home directory.
      ```
      $ cd ~
      ```
   b. Get the shell script to encrypt the plain text.
      ```
      $ wget https://raw.githubusercontent.com/ou-developers/oci-vaultoperations/main/ocivault-encrypt.sh
      ```
   c. Make the downloaded shell script executable.
      ```
      $ chmod +x ocivault-encrypt.sh
      ```
   d. Run the shell script.
      ```
      $ ./ocivault-encrypt.sh
      ```
   Note: This command will execute the downloaded interactive script, which will prompt you for the following values. When prompted, locate, and enter the values that you saved in the previous section.
2. Provide the required parameters as input.
   a. **`Please enter the OCI Vault Cryptographic Endpoint URL`**
      < OCI Vault Cryptographic Endpoint URL>
      Example: https://xxxxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
   b. **`Please enter your Master Encryption Key OCID`**
      < Master Encryption Key OCID>
      Example: ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

c. **Please enter the text you wish to encrypt**

<Plain text to be encrypted>

Example: HelloWorld

3. The Shell script will invoke `oci kms crypto encrypt` and perform a cryptographic operation. The following is a sample output of the script:

```
Please enter the OCI Vault Cryptographic Endpoint URL
https://xxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
Please enter your Master Encryption Key OCID
ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxx
Please enter the text you wish to encrypt
HelloWorld
{
"data": {
    "ciphertext":
"QRu3Y6UBExxxxxaSCNyAKuhqRsxxxxxuk/shqzs4iimhWgyyAA==",
    "encryption-algorithm": "AES_256_GCM",
    "key-id": "ocid1.key.oc1.xxx.xxxxxxxxxxbbbbbbbbbxxxx",
    "key-version-id": "ocid1.keyversion.oc1.xxx.aaaabbbbb"
  }
}
---------- Encrypted Text ----------
QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==
```

4. Copy and save the **Encrypted Text** somewhere to use later during the decryption process.

Perform Decryption

You will now run the provided shell script, which will take as input the OCI Vault cryptographic endpoint, the OCID of the master encryption key you created, and the encrypted text to decrypt. The provided shell script invokes `oci kms crypto decrypt` to perform data decryption.

Tasks

1. Click the **Cloud Shell** icon in the Console header to launch your Cloud Shell.
   a. Go to your home directory.
      ```
      $ cd ~
      ```
   b. Get the shell script to decrypt the encrypted text.
      ```
      $ wget https://raw.githubusercontent.com/ou-developers/oci-vaultoperations/main/ocivault-decrypt.sh
      ```
   c. Make the downloaded shell script executable.
      ```
      $ chmod +x ocivault-decrypt.sh
      ```
   d. Run the shell script.
      ```
      $ ./ocivault-decrypt.sh
      ```
2. Provide the required parameters as input.
   a. **`Please enter the OCI Vault Cryptographic Endpoint URL`**
      < OCI Vault Cryptographic Endpoint URL>
      Example: https://xxxxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
   b. **`Please enter your Master Encryption Key OCID`**
      < Master Encryption Key OCID>
      Example: ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      `ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`
   c. **`Please enter the Encrypted Text (Generated Above)`**
      `<Encrypted_Text_from_above_step>`
      `Example:`
      `QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==`
3. The Shell script will invoke `oci kms crypto decrypt` and perform a cryptographic operation. The following is a sample output of the script:

   ```
   Please enter the OCI Vault Cryptographic Endpoint URL
   https://xxxx-crypto.kms.eu-frankfurt-1.oraclecloud.com
   Please enter your Master Encryption Key OCID
   ```

```
ocid1.key.oc1.xxx.xxxxxxxxxxxxxxxxxxxxxxxxx
Please enter the Encrypted Text (Generated Above)
QYcEncB2aSYnAC7QkpXd589LxN8XdddFWJzHyFg2gTKCaCcht97rAAAA==

{
"data": {
          ....
    "key-id": "ocid1.key.oc1.xxx.xxxxxxxxxxbbbbbbbbbxxxx",
    "key-version-id": "ocid1.keyversion.oc1.xxx.aaaabbbbb"
    "plaintext": "ampqanNzc3NzCg==",
"plaintext-checksum": "2060560141"
  }
}
---------- Plain Text ----------
HelloWorld
------------------------------
```

Observability and Management: Configure Alarms with Notifications and Create Monitoring Queries

Lab 18-1 Practices

Get Started

Overview

Oracle Cloud Infrastructure (OCI) Observability and Management provides visibility and actionable insights derived using Machine Learning Algorithms. This platform is open and extensible, and provides cloud-based monitoring and analytics.

Some of the Observability and Management services include Monitoring, Logging, Event Services, Logging Analytics, and Application Performance Monitoring. In this lab, you will create alarms and queries, and trigger alarms.

In this lab, you will:

a. Create a Virtual Cloud Network (VCN)

b. Launch three Compute Virtual Machine instances

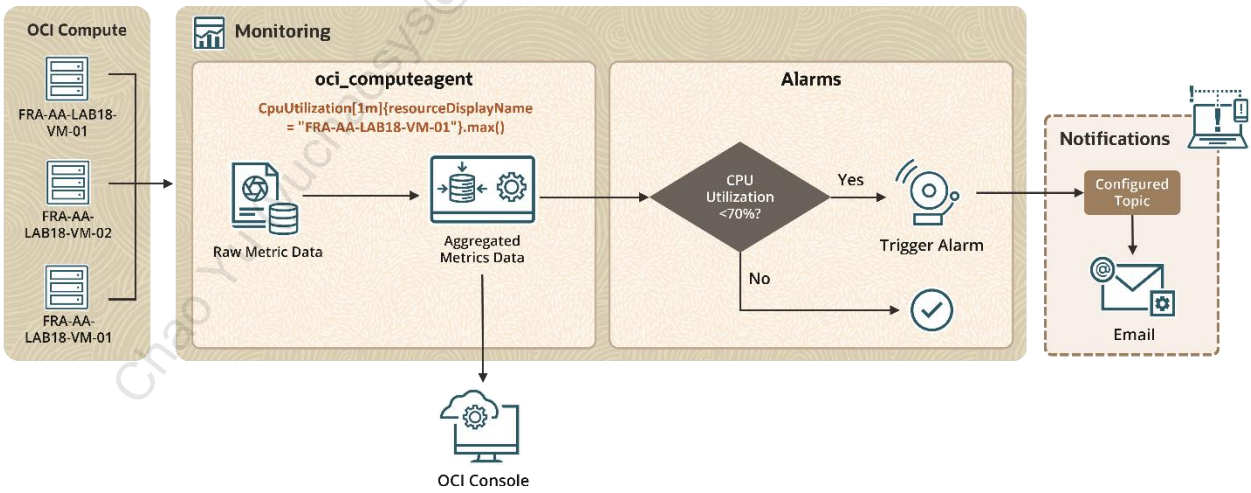
c. Create alarms and view service metrics

d. Create CPU stress and fire alarms

e. Create queries

Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.



Assumptions

- You must be familiar with navigating the OCI Console.
- Select the region available in the tenancy allotted to you. In this lab, **Germany Central (Frankfurt)** is considered as your region.

Set Up the Environment

In this practice, you will configure the cloud environment, create a virtual network, and compute instances. The resources created in this practice will help you complete the rest of the lab.

Task 1: Create a VCN

A Virtual Cloud Network (VCN) defines a private network in the cloud environment where you can specify networking parameters such as CIDR block and route tables, along with security controls like access control lists and virtual firewalls. You can also allow connectivity to the public Internet. In this task, you will create a VCN.

Note: For a production VCN environment, it is recommended to further restrict network access controls to meet your security requirements.

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. In the console ribbon at the top of the screen, click the Region icon to expand the menu and select **Germany Central (Frankfurt)**.
3. From the navigation menu, under **Networking**, select **Virtual Cloud Networks**.
4. From the left navigation panel, ensure you are in the compartment allotted to you. Click **Create VCN**.
5. In the **Create a Virtual Cloud Network** dialog box, populate the following information:
   - **Name**: FRA-AA-LAB18-1-VCN-01
   - **Create In Compartment**: <*your compartment*>.
   - **IPv4 CIDR Block**: 10.0.0.0/16 (Press **Enter** to add the IP block.)
6. Leave other fields as default. Click **Create VCN**.
7. After the VCN is created, click **FRA-AA-LAB18-1-VCN-01** VCN to view the details page. Under **Resources** in the left navigation panel, click **Internet Gateways**.
8. Click **Create Internet Gateway**.

9. In the **Create Internet Gateway** dialog box, populate the following information:
    - **Name**: FRA-AA-LAB18-1-IG-01
    - **Create In Compartment**: <*your compartment*>
10. Click **Create Internet Gateway**.
11. Next, make a quick update to the VCN route table to make use of the Internet Gateway created in the previous step. Under **Resources** in the left navigation panel, click **Route Tables**.
12. Click **Default Route Table for FRA-AA-LAB18-1-VCN-01** and then, click **Add Route Rules**.
13. In the **Add Route Rules** dialog box, populate the following information:
    - **Target Type:** Internet Gateway
    - **Destination CIDR Block**: 0.0.0.0/0
    - **Target Internet Gateway**: FRA-AA-LAB18-1-IG-01
14. Click **Add Route Rules** to complete the process.
15. Finally, create a subnet in the VCN to identify IP space and deploy a VM. Return to the VCN details page by clicking **FRA-AA-LAB18-1-VCN-01** in the breadcrumb list at the top of the page.
16. Under **Resources** in the left navigation panel, click **Subnets**. Then, click **Create Subnet**.
17. In the Create Subnet dialog box, populate the following information:
    - **Name**: FRA-AA-LAB18-1-SNET-01
    - **Create In Compartment**: <*your compartment*>.
    - **Subnet Type**: Regional (Recommended)
    - **IPv6 CIDR Block**: 10.0.0.0/24
    - **Route Table Compartment in <*your compartment*>**: Default Route Table
    - **Subnet Access**: Public Subnet
18. Leave other fields as default. Click **Create Subnet**.

Task 2: Set Up SSH Keys for Virtual Machine Instance

Before launching a Virtual Machine instance, you will create SSH keys to authenticate the Instance using Oracle Cloud Shell.

1. In the OCI Console ribbon at the top of the screen, ensure that the correct Region is selected. In this case, the region is **Germany Central (Frankfurt)**.
2. Click **Cloud Shell** icon next to the region.
3. In the Cloud Shell, ensure that you are in the home directory of your account. To check, run the following command:

   ```
   $ pwd
   ```

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

   If you are in your home directory, the value will be `/home/<user_name>`.
4. To change the directory to `.ssh` directory, run the following command:

   ```
   $ cd .ssh/
   ```
5. If the previous step shows an error as "No such file or directory," then run the following command:

   ```
   $ mkdir .ssh/
   ```
6. Now, change directory to `.ssh/` by running the following command:

   ```
   $ cd .ssh/
   ```
7. To create ssh keys, run the following command:

   ```
   $ ssh-keygen -b 2048 -t rsa -f sshkeys
   ```
8. Do not enter a password when prompted, press **Enter**.

   Note: There are two files saved into the `.ssh` directory: **sshkeys.pub** (public key) and **sshkeys** (private key). **sshkeys.pub** will be used while creating compute instances, and **sshkeys** will be used to authenticate.
9. Run the following command to view the contents of the **sshkeys.pub** public key.

```
$ cat /home/<user_name>/.ssh/sshkeys.pub
```

Note: Replace <user_name> with your username as noted in step 3.

10. Copy and paste the content of **sshkeys.pub** public key into a Notepad file. You will use this content while creating compute instance.

11. Close the Cloud Shell by clicking **X** at the top-right corner. Then, click **Exit**.

Task 3: Launch Compute Virtual Machine Instance

Now, you will launch a Virtual Machine in your newly created VCN. For this lab, you will create three instances.

1. In the OCI Console ribbon at the top of the screen, ensure that you have selected the same region where you created the VCN.

2. From the navigation menu, under **Compute**, click **Instances**.

3. From the left navigation panel, ensure that you are in the compartment allotted to you. To create the first instance, click **Create instance**.

4. In the **Create compute instance** dialog box, enter **FRA-AA-LAB18-1-VM-01** in the **Name** field.

5. In the **Create in compartment** field, select <*your compartment*>.

6. The **Availability Domain** will be pre-populated to match the subnet you created earlier.

7. Ensure that the **Image** is selected as **Oracle Linux 8**. If not, click **Change Image** and select **Oracle Linux 8**.

8. In the **Shape** field, click **Change Shape**. Then select **VM.Standard.A1.Flex** (1 OCPU, 6GB Memory) [Shape series: Ampere].

   Note: Your options and naming conventions may not match exactly as given here, so select an appropriate shape if it is shown different for your region.

9. In the **Primary network** field, select **Select Existing Virtual Cloud Network** and ensure **FRA-AA-LAB18-1-VCN-01** is specified in the **Virtual cloud network** field.

10. In the **Subnet** field, select **Select Existing Subnet**. Ensure the **Subnet** is specified as **FRA-AA-LAB18-1-SNET-01**.

    If not, double-check the compartment is set to <*your compartment*>. You may have to switch to a different Availability Domain (see above – the Availability Domain of your subnet and compute instance must match) to allow the selection of your existing subnet, if not already selected.

11. In the **Public IP address** field, select **Assign a public IPv4 address**.

12. In the **Add SSH keys** field, select **Paste public keys**. Then copy the sshkeys.pub public key from the Notepad (copied earlier in previous task) and paste it in the **SSH keys** field.

13. Keep the other options default and click **Create**. The first compute instance is successfully created.

14. Navigate back to the **Instances** page from the navigation menu. Ensure that the **State** of the instance you just created is **Running**.

15. Copy the Public IP corresponding to the **FRA-AA-LAB18-1-VM-01** instance and paste it in the Notepad.

16. Now, click the **Cloud Shell** icon next to the Region at the top of the screen.

17. Run the following command with pasting the sshkeys - private key and Public IP:

    ```
    $ ssh -i /home/<user_name>/.ssh/sshkeys opc@X.X.X.X
    ```

    - Replace `<user_name>` with your username.
    - Replace *X.X.X.X* with the public IP address copied in step 15.

    Note: The SSH Key is the private key created in the previous task. It is used to authenticate.

18. Enter **Yes** when prompted to connect and ensure you are connected to the instance.

19. Enter **exit** to close the connection.

20. To create a second instance, repeat steps 2 through 7. Keep all settings the same except the **Name** of the instance. Enter the **Name** of the second instance as **FRA-AA-LAB18-1-VM-02**.

21. In the **Shape** field, click **Change Shape**. Then select **VM.Standard.A1.Flex** (1 OCPU, 6GB Memory) [Shape series: Ampere].

22. In the **Public IP address** field, select **Do not assign a public IPv4 address**. In the **Add SSH keys** field, select **No SSH keys**.

    Note: The instance is not required to be accessed; therefore, assigning a Public IP address and SSH keys for this instance can be skipped.

23. Keep the other options default and click **Create**. The second compute instance is successfully created.

24. Navigate back to the **Instances** page from the navigation menu. Ensure that the State of the second instance created is **Running**.

25. To create a third instance, repeat steps 2 through 7. Keep all settings the same except the **Name** of the instance. Enter the **Name** of the second instance as **`FRA-AA-LAB18-1-VM-03`**.

26. In the **Shape** field, click **Change Shape**. Then select **VM.Standard.A1.Flex** (1 OCPU, 6GB Memory) [Shape series: Ampere].

27. In the **Public IP address** field, select **Do not assign a public IPv4 address**. In the **Add SSH keys** field, select **No SSH keys**.

    Note: The instance is not required to be accessed; therefore, assigning a Public IP address and SSH keys for this instance can be skipped.

28. Click **Create**. The third compute instance is successfully created.

29. Navigate back to the **Instances** page from the navigation menu. Ensure that the State of the third instance created is **Running**.

Create Alarms and View Service Metrics

In this practice, you will view the service metrics for your instances, confirm that the required monitoring plug-in is enabled, and set up alarm notifications.

Task 1: Confirm that Compute Instance Monitoring Plug-In Is Enabled

To view the service metrics available in the OCI Console, the compute instance monitoring plug-in must be enabled. This plug-in emits metrics about the instance's health, capacity, and performance—such as CPU and memory utilization.

Note: The plug-in will be enabled by default, but it should be confirmed.

1. From the OCI Console navigation menu, under **Compute**, select **Instances**.
2. Click the instance **FRA-AA-LAB18-1-VM-01**.
3. Click **Oracle Cloud Agent** tab.
4. Scroll down to find the **Compute Instance Monitoring** plug-in and ensure that it is running and enabled.
5. Navigate back to the **Instances** page and repeat steps 1-4 for the instance **FRA-AA-LAB18-1-VM-02**.
6. Repeat steps 1-4 for the instance **FRA-AA-LAB18-1-VM-03**.

Task 2: Create a Topic and a Subscription Inside a Topic

Now that you have confirmed that Monitoring is enabled, you will create an alarm that is triggered when the service metrics reach a designated threshold. You will see this alarm gets triggered later in the practice when you perform a CPU stress test.

To create an alarm, you must first create a notification so that the alarm has a way to notify the relevant parties. For example, an alarm can email an administrator when a CPU usage threshold has been breached.

1. From the OCI Console navigation menu, select **Developer Services**. Under **Application Integration**, select **Notifications**.
2. From the left navigation panel, ensure you are in the compartment assigned to you.

3. Click **Create Topic**.

4. In the **Create Topic** dialog box, enter **FRA-AA-LAB18-1-TOP-01** in the **Name** field and enter **Description** if required as its optional.

5. Click **Create**.

6. Once the topic state changes to **Active**, click the topic to view the details.

7. Under **Resources**, click **Create Subscription**.

8. In the **Create Subscription** dialog box, select **Email** in the **Protocol** field.

9. In the **Email** field, enter your email address.

10. Click **Create**.

11. Click the subscription that you just created.

12. The Subscription Information will be displayed with the status as **Pending Confirmation**.

13. Check the email account you specified and click the "Confirm subscription" verification link in it. A pop-up browser window will tell you that the subscription has been confirmed.

14. Navigate back to the **Subscriptions** page and verify that the subscription status has changed to **Active**.

    Note: You may need to refresh your browser if the status is not updated.

A topic and a subscription inside a topic are successfully created.

Task 3: Create an Alarm for CPU Utilization

Now that you've created the topic and subscription for a notification, you will create your alarm. This alarm will be activated when the CPU utilization reaches a threshold that you designate.

1. From the OCI Console navigation menu, select **Observability & Management**. Under **Monitoring**, click **Alarm Definitions**.

2. From the left navigation panel, ensure that you are in the compartment assigned to you.

3. Click **Create Alarm**.

4. In the **Create Alarm** dialog box, populate the following information in the **Create alarm** section:

   - **Alarm name**: FRA-AA-LAB18-1-ALA-01
   - **Alarm severity**: Critical
   - **Alarm body**: High Usage of CPU

5. The **Tags** section is optional. Therefore, keep the default selections.

6. Populate the following information in the **Metric description** section:

   - **Compartment**: <*your compartment*>
   - **Metric namespace**: oci_computeagent
   - **Metric name**: CpuUtilization
   - **Interval**: 1m
   - **Statistic**: Max

   Note: The **Resource Group** field is optional. Therefore, you can skip it for now.

7. Populate the following information in the **Metric dimensions** section:

   - **Dimension name**: resourceDisplayName
   - **Dimension value**: FRA-AA-LAB18-1-VM-01

8. Populate the following information in the **Trigger rule** section:

   - **operator**: greater than
   - **Value**: 70
   - **Trigger delay minutes**: 1

9. Populate the following information in the **Define alarm notifications** section:

   - **Destination service**: Notifications
   - **Compartment**: <*your compartment*>
   - **Topic**: FRA-AA-LAB18-1-TOP-01

You have created the topic earlier and recall that the topic is the communication channel, such as email. When the alarm is triggered, a notification is sent to the subscribed email addresses.

10. Select the option **Split notifications per metric stream** in the **Message grouping** section.

    With this setting, you are configuring the Alarm to send a message for the specific instance when it reaches the CPU threshold. The UI shows a message which is just a reference- **Consider limits when the alarm contains a high number of metric streams.**

11. You can select the message format, which is generally the first option, **Send formatted messages**.

12. You can also choose to have a notification repeated at certain frequencies if an alarm continues. Keep the **Repeat notification** option deselected.

13. You have the option to suppress the notification. Keep the **Suppress notifications** option deselected.

14. Select **Enable this alarm** and click **Save Alarm**.

You should now be able to see the alarm's details.

Create CPU Stress and Fire Alarm

In this practice, you will create a CPU Stress on the first instance (FRA-AA-LAB18-1-VM-01), monitor the effect of CPU stress on the instance, and see an event triggered when the CPU utilization is greater than the threshold, which causes the alarm to fire.

Task 1: Create CPU Stress for an Instance

Now that you have created an alarm, Observability and Management monitors the working of instances and sends a notification when the alarm is triggered. For this purpose, the CPU is subjected to stress and forced to run to its maximum capacity. When the CPU Utilization metric is greater than the threshold value, the alarm gets triggered.

This is simulated by means of a CPUStress generator. The following steps are with respect to a Linux OS.

1. From the OCI Console navigation menu, under **Compute**, click **Instances.**
2. Click the instance **FRA-AA-LAB18-1-VM-01.** Copy the Public IP address.
3. Click the **Cloud Shell** icon from the Console ribbon at the top of the page.
4. Connect to the instance by running the following command:

   ```
   $ ssh -i /home/<user_name>/.ssh/sshkeys opc@<X.X.X.X>
   ```

   - Replace `<user_name>` with your username.
   - Replace *X.X.X.X* with the public IP address.
5. You should get a message that the FIPS mode is initialized.
6. Run the following command to install the EPEL (Extra Packages for Enterprise Linux) repository on Linux distributions to install additional standard open-source software packages by using YUM and DNF package manager. If you are asked if it is OK, enter **Y**.

   ```
   $ sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```
7. Enter **Y**. You will see **Complete!** when it is complete.

8. Install the stress package. Stress is a generator tool, devised to subject your system to configurable measure of CPU, memory, I/O, disk stress. To install, run the following command:

```
$ sudo yum install stress
```

Note: If you are asked if it is OK, enter **`y`** again.

You will get a message when the installation is successful.

Task 2: Include Stress to the Compute Instance

Now, you need to induce stress to the instance. The stress on the compute instances increases on repeated use of the stress command. Run the following command:

```
$ uptime
$ stress --cpu 8 --timeout 300
```

Task 3: Trigger the Alarm

1. From the OCI Console navigation menu, select **Observability & Management**. Under **Monitoring**, click **Alarm Definitions**.
2. Click **FRA-AA-LAB18-1-ALA-01** alarm that you created earlier.
3. The icon in FRA-AA-LAB18-1-ALA-01 would have changed to Firing mode due to the stress induced. This happens when the load on the CPU Utilization crosses the threshold limits. Please wait for a minute if the status is not changed to Firing, and then refresh the page.
4. Scroll down to the **Alarm history** graph, which signifies that the CPU stress has surpassed the set threshold.
5. An email notification is sent to the configured subscription email of the Notifications Topic as Alarm status changes from OK to Firing.
6. The email provides details about Alarm OCID, Number of Metrics breaching threshold, and Dimensions.
7. Navigate back to the **Alarm Definitions** page and select the check box against the FRA-AA-LAB18-1-ALA-01 alarm.

8. Click **Actions** and select **Add suppressions** from the drop-down list.

9. In the **Suppress Alarms** Wizard, select the default **Start time** and **End time** and click **Apply suppressions** to confirm.

10. Click **Close** and verify that the column **Suppressed** shows the alarm is suppressed for the period.

11. Click the **Cloud Shell** icon to open Cloud Shell where the stress was initiated on the Instance. Press Ctrl + C to stop the stress.

12. Navigate back to the **Alarm Definitions** page and click the **FRA-AA-LAB18-1-ALA-01** alarm.

13. The CPU-usage-alarm icon would have changed to OK mode as the stress is now stopped.

14. Verify an email notification is not received by the configured subscription email for the status being changed from Firing to OK. This notification is not sent due to Alarm being suppressed for the period.

Create Queries

In this practice, you will create different types of queries and see how they are all represented graphically.

Task 1: Create Standard Queries

In this task, you will learn about query expressions and components, and you will execute sample queries that can be used with the Monitoring service. The Metrics Explorer creates queries that are used to search and aggregate metric data points collected from resources.

A standard query includes a metric namespace (the source or application being measured), metric (what is being measured), interval (over what period), and statistic (how it's being measured, e.g., a sum, rate, or max value).

1. From the OCI Console navigation menu, select **Observability & Management**. Under **Monitoring**, click **Metrics Explorer**.
2. To create a standard query, populate the following information in the **Query** section:
    - **Compartment**: <*your compartment*>
    - **Metric namespace**: oci-computeagent
    - **Metric name**: CpuUtilization
    - **Interval**: 5m
    - **Statistic**: Max
3. Click **Update Chart**.

The chart generated is the output of the query. It represents the CPU utilization (CpuUtilization) of all instances (oci_computeagent) in the past five minutes. The corresponding Monitoring Query Language (MQL) is displayed under Query 1.

Task 2: Create Standard Queries with a Filter

A filter condition is used along with a standard query to display the graphs that satisfy specific conditions. The filter condition is entered in the Metric Dimensions area and includes a name and (optional) a value.

1. From the navigation menu, select **Observability & Management**. Under **Monitoring**, click **Metrics Explorer**.
2. Populate the following information to create a grouping function using Basic mode in the **Query** section:
    - **Compartment**: <*your compartment*>
    - **Metric namespace**: oci-computeagent
    - **Metric name**: CpuUtilization
    - **Interval**: 5m
    - **Statistic**: Max
3. In the **Metric dimensions** section, populate the following information:
    - **Dimension name**: availabilityDomain
    - **Dimension value**: *Select an availability domain.*
4. Click **Update Chart**.

The chart displays the CPU utilization of the compute instances in an interval of five minute for the inputted availability domain.

Task 3: Create Aggregation Using Basic Queries

Simple aggregation (grouping) function queries return the combined value of all metric streams for the selected statistic. They can be written manually in the Query Code Editor pane by checking the Advanced mode option, or you can use the Standard Query mode used above.

1. From the navigation menu, select **Observability & Management**. Under **Monitoring**, click **Metrics Explorer**.

2. Populate the following information to create a grouping function using Basic mode in the **Query** section:

   - **Compartment**: <*your compartment*>
   - **Metric namespace**: oci-computeagent
   - **Metric name**: CpuUtilization
   - **Interval**: 5m
   - **Statistic**: Max

3. In the **Metric dimensions** section, populate the following information:

   - **Dimension name**: availabilityDomain
   - Select the **Aggregate metric streams** check box.

   Note: You can leave the **Dimension value** field blank for now.

4. Click **Update Chart**.

The graph displays the aggregation of CPU utilization of all availability domains, with an interval of five minutes, and a statistic option of the Max function.

The selection of **Aggregate metric streams** check box is referred to as **grouping** function while using Advanced mode. This query can be viewed with selecting **Advanced mode** check box.

Task 4: Create Advanced Queries

The nested queries are written as part of the Advanced mode in the **Query code editor**.

1. From the navigation menu, select **Observability & Management**. Under **Monitoring**, click **Metrics Explorer**.
2. Select the **Advanced mode** check box at the top right of the **Query 1** section.

3. Populate the following information to create a grouping function using Basic mode in the **Query** section:

   - **Compartment**: <*your compartment*>
   - **Metric namespace**: oci-computeagent

4. Enter the following code in the **Query code editor** field.

```
(CpuUtilization[1m].max() > 5).grouping().max()
```

5. Click **Update Chart**.

   The displayed output groups the compute instances and displays the ones whose CpuUtilization is more than 5 percent in the past minute.

GroupBy is a grouping function, which can be written using Advanced mode. It is another way to aggregate metric streams. For example, you can group by **shape** used by the Instance.

1. To group by shape, enter the following code into the **Query code editor**.

```
CpuUtilization[5m].groupBy(shape).max()
```

2. Click **Update Chart**.

   The displayed output groups compute instances by shape and displays the CpuUtilization with an interval of 5 mins and showing the maximum reported value in the graph.

Observability and Management: Configure Logging for a Resource

Lab 19-1 Practices

Get Started

Overview

Logs contain critical diagnostic information that tells you how your resources are performing and being accessed. With OCI Logging, you can enable built-in service or custom logging on core cloud infrastructure resources. The custom logs contain diagnostic information from custom applications, other cloud providers, or an on-premises environment.

In this lab, you will:

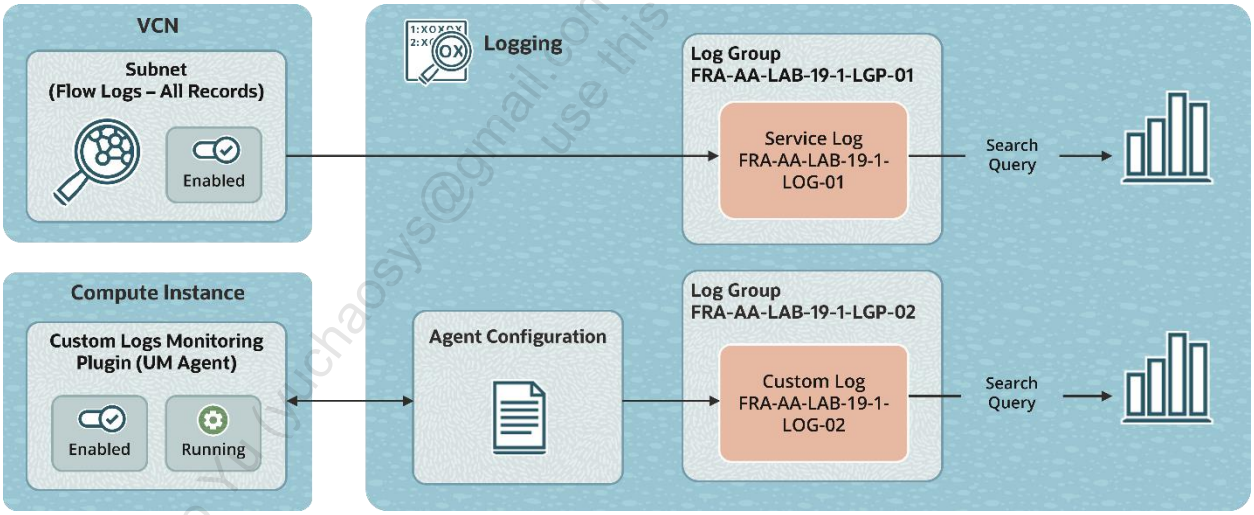
a. Create a Virtual Cloud Network (VCN)

b. Launch a compute Virtual Machine instance

c. Create a log group

d. Create a custom log agent configuration

e. Search the logs



Prerequisites

- The Oracle University lab team set up all the IAM policies required for you to complete this lab.

Assumptions

- You must be familiar with navigating the OCI Console.
- Select the region available in the tenancy allotted to you. In this lab, Germany Central (Frankfurt) is considered as your region.

Set Up the Environment

In this practice, you will configure the cloud environment, create a virtual network, and compute instances. The resources created in this practice will help you complete the rest of the lab.

Task 1: Create a VCN

A Virtual Cloud Network (VCN) defines a private network in the cloud environment where you can specify networking parameters such as CIDR block and route tables, along with security controls such as access control lists and virtual firewalls. You can also allow connectivity to the public Internet. In this task, you will create a VCN.

> **Note:** For a production VCN environment, it is recommended to further restrict network access controls to meet your security requirements.

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. In the console ribbon at the top of the screen, click the **Region** icon to expand the menu and select **Germany Central (Frankfurt)**.
3. From the navigation menu, under **Networking**, click **Virtual Cloud Networks**.
4. From the left navigation panel, ensure that you are in the compartment allotted to you. Click **Create VCN**.
5. In the **Create a Virtual Cloud Network** dialog box, populate the following information:
   - **Name**: `FRA-AA-LAB19-1-VCN-01`
   - **Create In Compartment**: The <*compartment name*> assigned to you
   - **IPv4 CIDR Block**: `10.0.0.0/16` (Press **Enter** to add the IP block)
6. Leave other fields as default. Click **Create VCN**.
7. After the VCN is created, click **FRA-AA-LAB19-1-VCN-01** VCN to view the details page. Under **Resources** in the left navigation panel, click **Internet Gateways**.
8. Click **Create Internet Gateway**.

9. In the **Create Internet Gateway** dialog box, enter the following information:
    - **Name**: `FRA-AA-LAB19-1-IG-01`
    - **Create In Compartment**: The <*compartment name*> assigned to you
10. Click **Create Internet Gateway**.
11. Next, make a quick update to the VCN route table to make use of the Internet Gateway created in the previous step. Under **Resources** in the left navigation panel, click **Route Tables**.
12. Click **Default Route Table for FRA-AA-LAB19-1-VCN-01** and then, click **Add Route Rules**.
13. In the **Add Route Rules** dialog box, populate the following information:
    - **Target Type:** Internet Gateway
    - **Destination CIDR Block**: `0.0.0.0/0`
    - **Target Internet Gateway**: `FRA-AA-LAB19-1-IG-01`
14. Click **Add Route Rules** to complete the process.
15. Finally, create a Subnet within the VCN to identify IP space and deploy a VM. Return to the VCN details page by clicking **FRA-AA-LAB19-1-VCN-01** in the breadcrumb list at the top of the page.
16. Under **Resources** in the left navigation panel, click **Subnets**. Then click **Create Subnet**.
17. In the **Create Subnet** dialog box, populate the following information:
    - **Name**: `FRA-AA-LAB19-1-SNET-01`
    - **Create In Compartment**: The <*compartment name*> assigned to you
    - **Subnet Type**: Regional (Recommended)
    - **IPv4 CIDR Block**: `10.0.0.0/24`
    - **Route Table Compartment in your <*compartment name*>**: Default Route Table
    - **Subnet Access**: Public Subnet
18. Leave other fields as default. Click **Create Subnet**.

Task 2: Set Up SSH Keys for Virtual Machine Instance

Before launching a Virtual Machine instance, you will create SSH keys to authenticate the instance using the Oracle Cloud Shell.

1. In the OCI Console ribbon at the top of the screen, ensure that the correct Region is selected. In this case, the region is **Germany Central (Frankfurt)**.

2. Click the **Cloud Shell** icon next to the region.

3. In the Cloud Shell, ensure you are in the home directory of your account. To check, run the following command:

   ```
   $ pwd
   ```

   Reminder: Do not include the `$` symbol when pasting code into Cloud Shell.

   If you are in your home directory, the value will be `/home/<user_name>`.

4. To change the directory to `.ssh` directory, run the following command:

   ```
   $ cd .ssh/
   ```

5. If the previous step shows an error as "No such file or directory," then run the following command to create a hidden directory:

   ```
   $ mkdir .ssh/
   ```

6. Now, change directory to `.ssh/` by running the following command:

   ```
   $ cd .ssh/
   ```

7. To create ssh keys, run the following command:

   ```
   $ ssh-keygen -b 2048 -t rsa -f sshkeysLAB19
   ```

8. Do not enter a password when prompted; press **Enter**.

   Note: There are two files saved into the `.ssh` directory: **sshkeysLAB19.pub** (public key) and **sshkeysLAB19** (private key). **sshkeysLAB19.pub** will be used while creating compute instances, and **sshkeysLAB19** will be used to authenticate.

9. Run the following command to view the contents of the **sshkeysLAB19.pub** public key:

   ```
   $ cat /home/<user_name>/.ssh/sshkeysLAB19.pub
   ```

   Note: Replace <user_name> with your username as mentioned in step 3.

10. Copy and paste the content of the **sshkeysLAB19.pub** public key into a Notepad file. You will use this content while creating the compute instance.

11. Close the Cloud Shell by clicking **X** at the top-right corner. Then, click **Exit**.

Task 3: Launch Compute Virtual Machine Instance

Now, you will launch a Virtual Machine in your newly created VCN.

1. In the OCI Console ribbon at the top of the screen, ensure that you have selected the same region where you created the VCN.

2. From the navigation menu, under **Compute**, select **Instances**.

3. From the left navigation panel, ensure that you are in the compartment allotted to you. To create an instance, click **Create instance**.

4. In the **Create compute instance** dialog box, enter the following information:
   - **Name**: FRA-AA-LAB19-1-VM-01
   - **Create in Compartment**: The <*compartment name*> assigned to you

   Note: The **Availability Domain** will be pre-populated to match the subnet you created earlier.

5. Ensure that the **Image** is selected as **Oracle Linux 8**. If not, click **Change Image** and select **Oracle Linux 8**.

6. In the **Shape** field, click **Change Shape**. Then select **VM.Standard.E4.Flex** (1 OCPU, 8GB Memory) [Shape series: AMD].

   Note: Your options and naming conventions may not match exactly as given here. Therefore, select an appropriate shape if it is shown different for your region.

7. In the **Primary network** field, select **Select Existing Virtual Cloud Network** and ensure that **FRA-AA-LAB19-1-VCN-01** is specified in the **Virtual cloud network** field.

8. In the **Subnet** field, select **Select Existing Subnet** and ensure that the **Subnet** is specified as **FRA-AA-LAB19-1-SNET-01 (regional)**.

   Note: If you do not find the required VCN or subnet, double-check whether the compartment is set to your <*compartment name*>. You may have to switch to a different Availability Domain (see above – the Availability Domain of your subnet and compute instance must match) to allow the selection of your existing subnet, if not already selected.

9. In the **Public IP address** field, select **Assign a public IPv4 address**.

10. In the **Add SSH keys** field, select **Paste public keys**. Then, copy the sshkeysLAB19.pub public key from Notepad (copied earlier in previous task) and paste it in the **SSH keys** field.

11. Keep the other options default and click **Create**. The compute instance is successfully created.

12. Navigate back to the **Instances** page from the navigation menu. Ensure that the **State** of the instance you just created is **Running**.

13. Copy the public IP corresponding to the **FRA-AA-LAB19-1-VM-01** instance and paste it in Notepad.

14. Click the **Cloud Shell** icon next to the Region at the top of the screen.

15. Run the following command by pasting the sshkeysLAB19 - private key and Public IP:

    ```
    $ ssh -i /home/<user_name>/.ssh/sshkeysLAB19 opc@X.X.X.X
    ```

    - Replace `<user_name>` with your username.
    - Replace *X.X.X.X* with the public IP address copied in step 15.

    Note: The SSH Key is the private key created in the previous task. It is used to authenticate.

16. Enter **Yes** when prompted to connect and ensure you are connected to the instance.

17. Enter **Exit** to close the connection.

Enable Service Logs

In this practice, you will enable automatic log collection for network activity in the VCN created earlier.

Task 1: Create a Log Group

The log groups are logical containers for organizing and managing logs. A log must always be inside a log group. You must first create a log group to enable or create logs. Fortunately, this is a fast and easy activity.

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure that you are in the compartment assigned to you.
3. Click **Create Log Group**.
4. In the **Create Log Group** dialog box, ensure that the **Compartment** field is populated with your <*compartment name*>.
5. In the **Name** field, enter **FRA-AA-LAB19-1-LGP-01**.
6. In the **Description** field, enter a brief description. For example, log group for service logs.
7. Click **Create**.

Task 2: Enable Network Flow Log

Many of the core cloud infrastructure services have built-in logging capabilities. Now that you have created a Log Group, select one of Oracle's core services and enable logging. In this task, you will enable logging on the VCN created earlier.

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure you are in the compartment assigned to you.
3. Click **FRA-AA-LAB19-1-LGP-01** Log Group.
4. From the left navigation panel, select **Logs**.

5. Click **Enable service Log**.

6. In the **Enable Resource Log** dialog box, populate the following information:

   - **Resource Compartment**: The <*compartment name*> assigned to you.
   - **Service**: Virtual Cloud Network - subnets
   - **Resource**: `FRA-AA-LAB19-1-SNET-01`
   - **Log Category**: Flow Logs – All records
   - **Log Name**: `FRA-AA-LAB19-1-SLOG-01`

7. Click **Enable Log**.

8. Review the log details page. It may take a couple minutes for the service to complete configurations. You may explore log content directly from this page.

   Note: The full log search activities are covered later in this lab.

Create Custom Logs

In this practice, you will create a custom log and agent configuration. Then you will use it to import log content in real time from the virtual machine instance created earlier.

Logging makes it easy to ingest custom logs by providing an agent to extract, parse, and upload logs directly to OCI. The agent can be installed on many machines, and it pulls logs from local directories, where your apps or systems emit logs. The agent may be installed and configured on machines outside of OCI. However, to save time, in this practice you will use the virtual machine you recently created, since it is preconfigured with the agent already installed.

Task 1: Check if the Custom Log Plug-in Is Enabled

1. From the navigation menu, under **Compute**, click **Instances**.
2. Select the **FRA-AA-LAB19-1-VM-01** instance that you created earlier.
3. Click the **Oracle Cloud Agent** tab. You can see that the **Custom Logs Monitoring** plug-in is enabled, and the status is Running.

Task 2: Create a Log Group

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure that you are in the compartment assigned to you.
3. Click **Create Log Group**.
4. In the **Create Log Group** dialog box, ensure that the **Compartment** field is populated with your <*compartment name*>.
5. In the **Name** field, enter **FRA-AA-LAB19-1-LGP-02**.
6. In the **Description** field, enter a brief description, for example, log group for custom logs.
7. Click **Create**.

Task 3: Create a Custom Log

The custom log creation is a two-step process. You need to create a Custom Log first and then create an associated Custom Log Configuration Agent for it.

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure that you are in the compartment assigned to you.
3. Click **FRA-AA-LAB19-1-LGP-02**
4. In the left panel, click **Logs**
5. Click **Create custom Log**.
6. In the **Create custom log** dialog box, enter **FRA-AA-LAB19-1-CLOG-01** in the **Custom log name** field.
7. In the **Compartment** field, ensure your <*compartment name*> is selected.
8. In the **Log Group** field, select **FRA-AA-LAB19-1-LGP-02**.
9. Click **Create custom log**.

   The **Agent Configuration** page will be displayed with the following two options:
   - Create agent configuration
   - Add configuration later

   Note: In the next task, you will create a custom log agent configuration from the same page. Therefore, you can stay on the same page and continue to the next task.

Task 4: Create a Custom Log Agent Configuration

An agent configuration provides instructions for both the Logging services and a specific group of deployed agents to work together. It is required for custom logs. Follow these steps to create an agent configuration that will include importing syslog messages from our virtual machine instance created earlier.

The **Agent Configuration** page is currently displayed from previous Task, where you can create a new configuration. Select the **Create new configuration** option.

> **Note:** If the page is refreshed or changed, navigate to the navigation menu, and click **Agent Configuration** under **Observability & Management**.

1. In the **Configuration Name** field, enter **FRA-AA-LAB19-1-AGT-CONF-01**.
2. In the **Description** field, enter a brief description.
3. In the **Compartment** field, ensure that <*your compartment*> is selected.
4. In the **Group Type** field, select **Dynamic Group**.
5. In the **Group** field, select the **ARCHITECT-ASS-DYN-GRP** group.

   > **Note:** Do not click **Create** for option- **Create policy to allow instances in dynamic group to use logging service**. The required policies are already added.

6. In the **Input type** field, select **Log path**.
7. In the **Input Name** field, enter **messages**.
8. In the **File Paths** field, enter **`/var/log/messages`** and press the **Enter** key. Although you are instructing the agent to process system-generated logs, the same procedure may be used to select application log paths or entire log directories.
9. Verify the information in the **Select log destination** section. If the fields are shown read-only, validate the following information. If the fields are shown blank, enter the following information:
   - **Compartment**: The <*compartment name*> assigned to you
   - **Log Group**: `FRA-AA-LAB19-1-LGP-02`
   - **Log name**: `FRA-AA-LAB19-1-CLOG-01`
10. Click **Create Custom Log**.

Task 5: Verify the Creation of the Custom Log

1. From the navigation menu, under **Observability & Management** > **Logging**, select **Log Groups**.
2. Select the log group **FRA-AA-LAB19-1-LGP-02**.
3. Under **Resources** in the left navigation panel, click **Logs**. You can see that the Custom Log **FRA-AA-LAB19-1-CLOG-01** is listed with Active status.

Task 6: Review Log Data from Virtual Machine

It may take a few minutes for the configuration to propagate to local machine agents.

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. Click the **FRA-AA-LAB19-1-LGP-02** log group.
3. Under **Resources** in the left navigation panel, click **Logs**. Then select the **FRA-AA-LAB19-1-CLOG-01** custom log that you created earlier in this practice. This opens the details panel.
4. Review the log properties and note the options to edit the log and agent configuration.
5. Explore the log content if it's already flowing into the Logging service and available for viewing. If a graph is shown, this means the log data is flowing into the Logging service.

Search Your Logs

In this practice, you will explore the contents of your logs and become familiar with the built-in search capabilities provided by the Logging service.

Logging provides the tools to search any combination or scale of logs to identify events or patterns that may be difficult to observe via legacy methods. This is especially true when working in a distributed scale-out environment comprising several services and platforms.

Task 1: Select Custom Logs to Be Included in Search

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Search**. You're now going to create search criteria and look for logs pertaining to your instance, **FRA-AA-LAB19-1-VM-01.**

2. Click **Select logs to search** text field. The **Select logs to search** dialog box appears.

3. In the **Select logs to search** field, click **x** to remove your <*compartment name*> if selected by default.

4. Expand the **(root)** Compartment under the **Compartment** column and select <*your compartment*> from the Compartment list.

   Note: Do not click the plus (+) sign. Click the compartment name only.

   This will bring up the log groups in that compartment without including the compartment itself as part of the search criteria. You don't want the compartment itself included, because you don't want all the logs for that compartment in the search results.

5. In the **Log Groups** column, select **FRA-AA-LAB19-1-LGP-02** log group, but again, click the name only without clicking the plus sign. This will bring up the logs for that log group.

6. In the **Logs** column, select the **FRA-AA-LAB19-1-CLOG-01** log. This time, click the plus (+) sign to add it as the only search criteria. The **Select logs to search** field at the top of the dialog box will be updated.

7. Click **Continue** to execute the search.

   Note: Wait for a few minutes and click **Search**. If logs are not shown, click **Filter by time** and choose **Past hour**. Verify that log records are shown.

Task 2: Examine Search Results and Refine Search for Custom Logs

1. In continuation of the previous task, the log lines are shown under the graph. Click the down arrow to the right of each entry to expand the details. The details list in JSON format with the compartment's OCID, instance OCID, log message, tenant OCIDs (IDs), source (log), subject (log file path), and log type (custom log).
2. Click **Before & After** tab under the log entry. This shows what was going on before and after the log message was generated, which helps with troubleshooting.
3. In the **Custom filters** field at the top of the **Search** area, enter `data.message =`. You can then select from the list to further refine your search. Select one of the log records listed that contains the specific message.

   The graph and log section will be updated based on the data.message selection.

Task 3: Select Service Logs to Be Included in Search

Now that you've created the topic and subscription for a notification, you will create your alarm. This alarm will be activated when the CPU utilization reaches a threshold that you designate.

1. From the navigation menu, select **Observability & Management**, and then click **Search**. You're now going to create search criteria for Service Log **FRA-AA-LAB19-1-SLOG-01** that contains VCN flow logs**.**
2. Click inside the **Select logs to search** field. The **Select logs to search** dialog box appears.
3. In the **Select logs to search** field, click **x** to remove <*your compartment*> if selected by default.
4. Expand the **(root)** Compartment under the **Compartment** column and select your <*compartment name*> from the Compartment list.

   Note: Do not click the plus (+) sign. Click the compartment name only.

   This will bring up the log groups in that compartment without including the compartment itself as part of the search criteria. You don't want the compartment itself included, because you don't want all the logs for that compartment in the search results.

5. In the **Log Groups** column, select **FRA-AA-LAB19-1-LGP-01** log group, but again, click the name only without clicking the plus sign. This will bring up the logs for that log group.

6. In the **Logs** column, select the **FRA-AA-LAB19-1-SLOG-01** log. This time, click the plus (**+**) sign to add it as the only search criteria. **Select logs to search** will be updated in the top field.

7. Click **Continue** to execute the search.

Task 4: Examine Results and Refine Search for Service Logs

1. In continuation to the previous task, you are on the **Search** page under **Logging**.

2. In the **Custom filters** field at the top of the Search area, enter **`data.action = ACCEPT`**.

3. This will show the log records with connections that were accepted. If there are no log records displayed, select **Filter by time** by **Today**. This will return all log records matching the condition for the entire day.

4. Remove the Search filter by clicking the **x** icon under **Filters**.

5. In **Custom filters**, enter **`data.destinationPort=22`**.

6. Select **Filter by time** as **Past 5 minutes**.

7. Verify there is no recent log data. You may need to note the timestamp if there are log records.

8. Click **Save search**.

9. In the **Search Name** field, enter **`NewSearch`**, select your assigned *<compartment name>* and click **Save Search**.

10. Click **Reset Search** to reset the search filters.

11. Copy and paste the Public IP address of instance (FRA-AA-LAB19-1-VM-01) copied earlier into Notepad, and click the **Cloud Shell** icon on top of the screen next to region.

12. To access the instance, run the following `ssh` command in the Cloud Shell:

```
$ ssh -i <private_key_file> <username>@<public-ip-address>
```

    a. The *<private_key_file>* is the full path (*/home/<your_user>/.ssh/sshkey*) and name of the file that contains the private key associated with the instance you want to access.

    b. The *<username>* is the default the `opc` user.

    c. The *<public-ip-address>* is the public IP address of the instance.

    Once successfully authenticated, minimize the Cloud Shell window.

13. Click **Saved Searches** in the left navigation panel and click **NewSearch**.

14. Verify the log records to see the successful SSH connection.

    Note: It might take up to a minute to show the data.

15. Restore Cloud Shell window and click **X** to close the window.

Observability and Management: Configure Service Connectors

Lab 20-1 Practices

Get Started

Overview

A service connector specifies the source logs, optional filtering/processing, execution frequency, and the destination Object Storage bucket. In this lab, we will enable service logs for Object Storage events and export them into another Object Storage bucket.

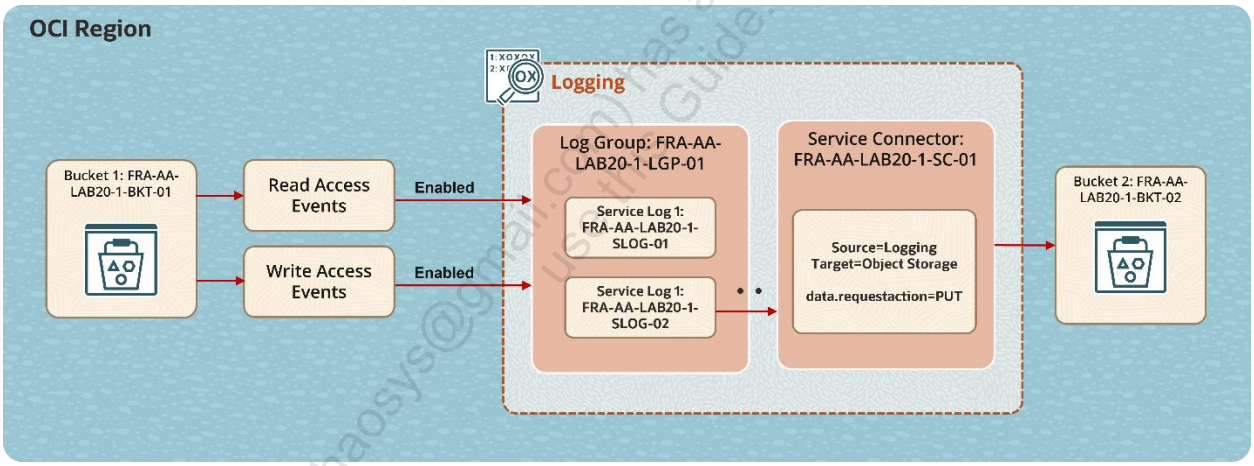
In this lab, you will:

a. Enable service logs

b. Export logs using service connectors

Prerequisites

- The Oracle University lab team has set up all the IAM policies required for you to complete this lab.



Assumptions

- You must be familiar with navigating the OCI Console.
- Select the region available in the tenancy allotted to you. In this lab, Germany Central (Frankfurt) is considered as your region.

Set Up the Environment

In this practice, you will create an automated job to export your log data into the Object Storage bucket for long-term storage and archive. The Oracle Cloud Infrastructure (OCI) makes this easy via service connectors, which provide a framework for creating jobs to filter, process, and move log data from Logging to Object Storage.

Task 1: Create Object Storage Buckets

An Object Storage bucket is a logical container for storing objects. A bucket is associated with a single compartment that has policies to determine what actions a user can perform on a bucket and on all the objects in the bucket. The objects can store any type of data regardless of the content type. In this task, you will create two buckets: one for enabling logging and another for archiving logs.

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. In the console ribbon at the top of the screen, click the Region icon to expand the menu and select **Germany Central (Frankfurt)**.
3. From the navigation menu, select **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.
4. Click **Create Bucket**.
5. In the **Create Bucket** dialog box, enter `FRA-AA-LAB20-1-BKT-01-xxx` in the **Name** field.

   Please specify a random number in place of xxx to make it unique.
6. In the **Default Storage Tier** field, select **Standard**.
7. In the **Encryption** field, select **Encrypt using Oracle managed keys**.
8. Keep the rest of the options as default and click **Create**.

   You will now create a second bucket, which will be used as the archive bucket to move logs generated for read events occurred for the first bucket.
9. Navigate back to the **Buckets** page from the navigation menu.
10. Click **Create Bucket**.

11. In the **Create Bucket** dialog box, enter `FRA-AA-LAB20-1-BKT-02-xxx` in the **Name** field.

    Please specify a random number in place of xxx to make it unique.

12. In the **Default Storage Tier** field, select **Standard.**

    Note: The Default Storage Tier can also be selected as Archive; however, in this lab, you will select Standard to immediately download the transitioned log. An object in Archive Storage Tier needs to be restored first before it can be downloaded.

13. Keep the rest of the options as default and click **Create**.

Enable Service Logs

In this practice, you will enable automatic log collection for Object Storage activity (read, write) for the bucket created earlier.

Task 1: Create a Log Group

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure that you are in the compartment assigned to you.
3. Click **Create Log Group**.
4. In the **Create Log Group** dialog box, ensure that the **Compartment** field is populated with *<your compartment>*.
5. In the **Name** field, enter `FRA-AA-LAB20-1-LGP-01`.
6. In the **Description** field, enter a brief description.
7. Click **Create**.

Task 2: Enable Object Storage Log

In this task, you will enable logging on the Object Storage bucket created earlier.

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure that you are in the compartment assigned to you.
3. Click the **FRA-AA-LAB20-1-LGP-01** log group.
4. From the left navigation panel, select **Logs**.
5. Click **Enable service log**.

6. In the **Enable Resource Log** dialog box, populate the following information:
    - **Resource Compartment**: <*your compartment*>
    - **Service**: Object Storage
    - **Resource**: `FRA-AA-LAB20-1-BKT-01-xxx`
    - **Log Category**: Read Access Events
    - **Log Name**: `FRA-AA-LAB20-1-SLOG-01`
7. Click **Enable Log**.
8. Review the log details page. It may take a couple minutes for the service to complete configurations. The Status under Log Information should be Active.
9. Navigate back to the **Logs** page and click **Enable service log**.
10. In the **Enable Resource Log** dialog box, populate the following information:
    - **Resource Compartment**: <*your compartment*>
    - **Service**: Object Storage
    - **Resource**: `FRA-AA-LAB20-1-BKT-01-xxx`
    - **Log Category**: Write Access Events
    - **Log Name**: `FRA-AA-LAB20-1-SLOG-02`
11. Click **Enable Log**.
12. Review the log details page. It may take a couple minutes for the service to complete configurations. The Status under Log Information should be **Active**.
13. From the navigation menu, select **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.
14. Click the **FRA-AA-LAB20-1-BKT-01-xxx bucket**.
15. Under **Resources** in the left navigation panel, click **Logs**.
16. Verify that the status of Read Access Events is Active and Enabled with Log Group FRA-AA-LAB20-1-LGP-01 and Log Name FRA-AA-LAB20-1-SLOG-01.

17. Verify that the status of Write Access Events is Active and Enabled with Log Group FRA-AA-LAB20-1-LGP-01 and Log Name FRA-AA-LAB20-1-SLOG-02.

18. Under **Resources** in the left navigation panel, click **Objects**.

19. Verify that the bucket is empty.

    Note: Leave the bucket empty for now. In a later task, you will upload a few objects into the bucket that generates write events and those logs (applied with a filter) will be transitioned into the second Object Storage bucket.

Export Logs Using Service Connectors

In this practice, you will explore the contents of your logs using the built-in search capabilities provided by the Logging service. This will validate that the logging is working for FRA-AA-LAB20-1-BKT-01.

In a later task, you will configure a service connector to export logs into second Bucket FRA-AA-LAB20-1-BKT-02.

Task 1: Validate Logs with Log Search

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Search**. You will now create search criteria and look for logs pertaining to your bucket, FRA-AA-LAB20-1-BKT-01-xxx.

2. Click **Select logs to search** text field.

3. In the **Select logs to search** field, click **x** to remove <*your compartment*> if selected by default.

4. Expand the **(root)** compartment under the **Compartment** column and select <*your compartment*> from the Compartment list.

   Note: Do not click the plus (+) sign. Click the compartment name only.

   This step will bring up the log groups in that compartment without including the compartment itself as part of the search criteria. You don't want the compartment itself included, because you don't want all the logs for that compartment in the search results.

5. In the **Log Groups** column, select the **FRA-AA-LAB20-1-LGP-01** log group, but again, click the name only without clicking the plus sign. This will bring up the logs for that log group.

6. In the **Logs** column, select **FRA-AA-LAB20-1-SLOG-01**.

7. This time, click the plus (+) sign to add it as the only search criteria. The **Select logs to search** field at the top of the dialog box will be updated.

8. Click **Continue** to execute the search.

9. Verify that the graph shows the corresponding log records. If the graph is not displayed, change the **Filter by time** field to **Past hour**.

10. In the **Custom filters** field at the top of the Search area, enter **`data.message =`**. You can then select from the list to further refine your search. Select one of the log records listed that contains the specific message.

    The graph and log section will be updated based on the selected `data.message`.

Task 2: Create a Service Connector

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Service Connectors**.
2. Click **Create Service Connectors**.
3. In the **Create service connectors** dialog box, populate the following information:
    - **Connector name**: `FRA-AA-LAB20-1-SC-01`
    - **Description**: <*description*>
    - **Resource compartment**: <*your compartment*>
    - **Source**: Logging
    - **Target**: Object Storage
4. In the **Configure source** section, ensure that the following information is populated:
    - **Compartment**: <*your compartment*>
    - **Log Group**: FRA-AA-LAB20-1-LGP-01
    - **Logs**: FRA-AA-LAB20-1-SLOG-02
5. Wait a few seconds for **Log filter task** section to load. Then in the **Property** field, enter **`data.requestAction`**.
6. In the **Operator** field, select **=**.
7. In the **Value** field, enter **`PUT`** and press the **Enter** key.

8. Keep the **Configure task** section as default. In the **Configure target** section, populate the following information:

   - **Compartment**: <*your compartment*>
   - **Bucket**: `FRA-AA-LAB20-1-BKT-02-xxx`

   Note: Do not click **Create** in the "Create default policy allowing this service connector to write to Object Storage in compartment <*your compartment*>" message box. The policies are already added to your compartment.

9. Click **Create**.

10. Navigate to the **Service Connectors** page using the breadcrumb list.

11. Verify that the Status column shows **Active** for FRA-AA-LAB20-1-SC-01, the Source column shows as **Logging**, and the Target column as **Object Storage**.

    Note: The service connector is created to move log data that contains the data.requestAction=PUT into the Object Storage bucket- **FRA-AA-LAB20-1-BKT-02-xxx**. The log message is generated when an object is uploaded in the bucket. To generate a specific log with PUT action, you will upload objects into the bucket using OCI CLI.

Task 3: Upload Objects into Object Storage Bucket

1. In the OCI Console header, click the **Cloud Shell** icon next to the Region icon.

2. Once the Cloud Shell launches, run the following commands:

```
$ echo "Object Storage Bucket Write Event 1" >> labobject1.txt
$ echo "Object Storage Bucket Write Event 2" >> labobject2.txt
$ echo "Object Storage Bucket Write Event 3" >> labobject3.txt
```

   Reminder: Do not include the $ symbol when pasting code into Cloud Shell.

3. Run the following command to verify if the files are created successfully:

```
$ ls
```

   The three files, `labobject1.txt`, `labobject2.txt`, and `labobject3.txt`, should be listed.

4. Run the following command to upload the **`labobject1.txt`** file into the bucket:

```
$ oci os object put --bucket-name="FRA-AA-LAB20-1-BKT-01-xxx" --
name labobject1.txt --file ./labobject1.txt
```

An output in JSON format should be returned with etag, last-modified, opc-content-md5 along with each of their values.

5. Run the following command to upload the `labobject2.txt` file:

```
$ oci os object put --bucket-name="FRA-AA-LAB20-1-BKT-01-
<User_Id>" --name labobject2.txt --file ./labobject2.txt
```

6. Run the following command to upload the `labobject3.txt` file:

```
$ oci os object put --bucket-name="FRA-AA-LAB20-1-BKT-01-xxx" --
name labobject3.txt --file ./labobject3.txt
```

7. Once done, close the Cloud Shell window.

Task 4: Verify the Logs Archived by Using Service Connector

The log content archived to Object Storage is aggregated via batches (default every seven minutes) and stored in `.gz` format. The timestamps allows easy retrieval by time ranges. In this task, you will locate the archived content and optionally download/extract/view to validate the storage integrity.

Note: This task needs to be run after 7 minutes, which is the rollover time for uploading files into the Object Storage bucket.

1. From the navigation menu, select **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.

2. Click the **FRA-AA-LAB20-1-BKT-01-xxx** bucket.

3. Verify that the new objects, `labobject1.txt`, `labobject2.txt`, and `labobject3.txt`, are uploaded and displayed.

4. Navigate back to the **Object Storage** page by using the breadcrumb list and click the **FRA-AA-LAB20-1-BKT-02-xxx** bucket.

5. Verify that there is a folder created for the service connector, and expand the bucket contents to view archive content in timestamped `log.gz` format.

   Note: It may take a few minutes after creating the connector for initial content to land in the bucket.

6. Select the content check box and click the three dots on the right to download, extract, and view the file.

7. User your preferred log or text viewer to verify the content.