



# Oracle Cloud Infrastructure Foundations

Activity Guide

S105665GC20

Learn more from Oracle University at [education.oracle.com](https://education.oracle.com)





**Copyright © 2023, Oracle and/or its affiliates.**

## **Disclaimer**

This document contains proprietary information and is protected by copyright and other intellectual property laws. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

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**

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

## **Trademark Notice**

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

## **Third-Party Content, Products, and Services Disclaimer**

This documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

2005182023

## Table of Contents

---

<b>Identity and Access Management (IAM): Create IAM Components - With Identity Domains Enabled</b>	<b>5</b>
Get Started .....	6
Create a Compartment (With Identity Domains Enabled) .....	8
Create a User (With Identity Domains Enabled) .....	9
Create a Group, and Add a User to the Group (With Identity Domains Enabled) .....	10
Create a Policy (With Identity Domains Enabled) .....	11
Create a Dynamic Group (With Identity Domains Enabled) .....	12
<b>Identity and Access Management (IAM): Create IAM Components - Without Identity Domains Enabled</b>	<b>13</b>
Get Started .....	14
Create a Compartment (Without Identity Domains Enabled) .....	16
Create a User (Without Identity Domains Enabled) .....	17
Create a Group, and Add a User to the Group (Without Identity Domains Enabled) .....	18
Create a Policy (Without Identity Domains Enabled) .....	19
Create a Dynamic Group (Without Identity Domains Enabled) .....	20
<b>Networking—Virtual Cloud Network: Create and Configure a Virtual Cloud Network</b>	<b>21</b>
Get Started .....	22
Create a Virtual Cloud Network .....	24
<b>Networking: OCI Load Balancer</b>	<b>27</b>
Get Started .....	28
Create a Virtual Cloud Network .....	30
Create Two Compute Instances (Backend Servers) .....	31
Create a Load Balancer .....	34
<b>Compute: Create a Web Server on an OCI Compute Instance</b>	<b>37</b>
Get Started .....	38
Launch Cloud Shell .....	39
Generate SSH Keys .....	40
Create a Virtual Cloud Network and Its Components .....	42
Create a Compute Instance .....	45
Install an Apache HTTP Server on the Instance .....	47
<b>Object Storage: Create and Manage OCI Object Storage</b>	<b>49</b>
Get Started .....	50
Create an Object Storage Bucket .....	51
Upload an Object to a Bucket .....	53

<b>Block Storage: Create, and Attach a Block Volume .....</b>	<b>55</b>
Get Started .....	56
Create a Virtual Cloud Network and Its Components .....	58
Create a VM Instance .....	60
Create a Block Volume .....	63
Attach a Block Volume to a Compute Instance .....	64
<b>Security: Configure Security Zones Using Maximum Security Zones .....</b>	<b>67</b>
Get Started .....	68
Set Up Security Zone with Maximum Security Recipe .....	70
View the Security Zone Policies Attached with a Created Security Zone .....	71
Verify Creating a Bucket in an Assigned Compartment Using a Oracle-Managed Key .....	72

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# **Identity and Access Management (IAM): Create IAM Components - With Identity Domains Enabled**

## **Lab 1-1 Practices**

Paweł Domański (pawel@dexterteam.eu) data non-transferable  
license to use this content

# Get Started

---

## Overview

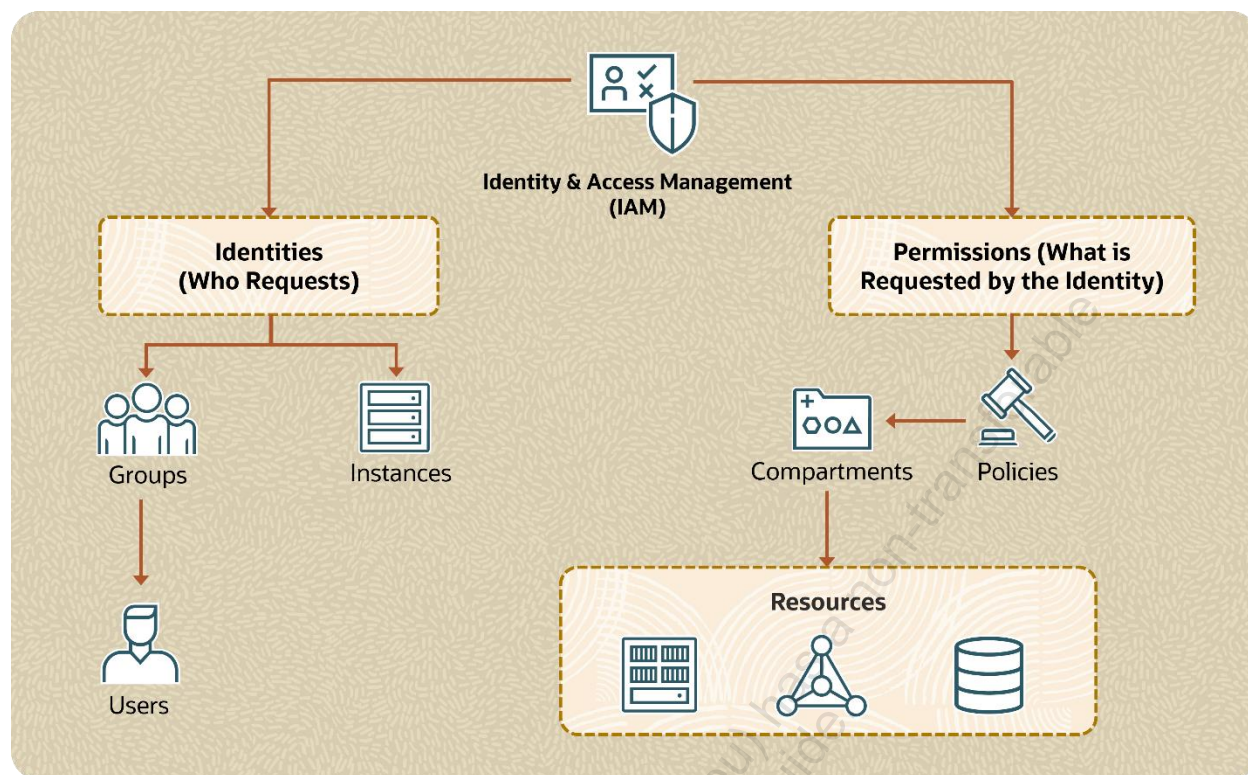
Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) lets you control who has access to your cloud resources.

In this lab, we will help you create a compartment, group, user, and policy. We will also provide the steps to create a dynamic group.

**Note:** Below instructions are for accounts with Identity Domains enabled.

In this lab, you'll:

- a. Create a compartment
- b. Create a user
- c. Create a group, and add a user to the group
- d. Create a policy
- e. Create a dynamic group



## Create a Compartment (With Identity Domains Enabled)

---

A compartment is a collection of related resources. Compartments are fundamental components of OCI and are used for organizing and isolating your cloud resources.

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

### Tasks

1. Sign in to the OCI Console.
2. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Compartments**. A list of the compartments to which you have access appears.
3. Click **Create Compartment**.
4. Do the following:
  - a. **Name:** Enter a unique name for the compartment. The name must be unique across all the compartments in your tenancy.
  - b. **Description:** Enter a compartment-related description.
  - c. **Parent Compartment:** The compartment you are in appears by default.
5. Click **Create Compartment**. The Child Compartment now appears in the list of compartments.



## Create a User (With Identity Domains Enabled)

---

A user is an individual employee or system that needs to manage or use your company's OCI resources.

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

### Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Domains**. A list of domains in your tenancy appears.
2. Select the Domain that is allotted to you. Otherwise, you can click on the **Default** domain.
3. Under **Identity domain**, click **Users**. A list of the users in your domain appears.
4. Click **Create User**.
5. Enter the following:
  - a. **First Name:** Enter first name of user.
  - b. **Last Name:** Enter last name of user.
  - c. **Username/Email:** Enter an email address for the user.
  - d. Check the **Use the same email address as the username**. Do not select the **Assign cloud account administrator role** check box.
6. Click **Create**. The user now appears in the list of users.

# Create a Group, and Add a User to the Group (With Identity Domains Enabled)

---

A group is a collection of users who need the same type of access to a particular compartment or set of resources.

In this practice, you'll learn how to create a group, and add a user to a group.

## Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Domains**. A list of domains in your tenancy appears.
2. Click on the **Default** domain.
3. Under **Identity domain**, click **Groups**. A list of the groups in your domain appears.
4. Select the **Administrators** group.
5. Click **Assign User to Groups**.
6. Select the user created earlier from the **Users** drop-down list, and then click **Add**. The user now appears in the group.
7. Use the breadcrumb trail to go back to the **Groups** page and click **Create Group**.
8. Enter the following:
  - a. **Name:** Enter a unique name for the group.
  - b. **Description:** Enter a group-related description.
9. Click **Create**. The group now appears in the list of groups.

## Create a Policy (With Identity Domains Enabled)

---

A policy is a document that specifies who can access which resources, and how.

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

### Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Policies**.
2. Click **Create Policy**.
3. Enter the following:
  - a. **Name:** Enter a unique name for the policy.
  - b. **Description:** Enter a policy-related description.
  - c. **Compartment:** If you want to attach the policy to a compartment other than the one you're viewing, select it from the drop-down list. Remember, where the policy is attached controls who can later modify or delete it.
4. In the **Policy Builder** section, click **Show manual editor** and enter the policy statement.

**Note:** A sample statement would look like the following:

```
allow group <group_name> to manage virtual-network-family in
compartment <compartment_name>
```

5. Click **Create**. The policy now appears in the list of policies.

## Create a Dynamic Group (With Identity Domains Enabled)

---

A dynamic group is a special type of group that contains resources, such as compute instances, which match rules that you define. This means that group membership can change dynamically as matching resources are created or deleted. These instances serve as “principal” actors and can make API calls to services according to policies that you write for the dynamic group.

In this practice, you’ll learn how to create a dynamic group.

### Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Domains**. A list of domains in your tenancy appears.
2. Click on the **Default** domain.
3. Under **Identity domain**, click **Dynamic Groups**.
4. Click **Create Dynamic Group**.
5. Enter the following:
  - a. **Name:** Enter a unique name for the group. The name must be unique across all groups in your tenancy, including dynamic groups and user groups.
  - b. **Description:** Enter a friendly description.
6. Enter the **Matching Rules**. Resources that meet the rule criteria are members of the dynamic group.
  - a. **Rule 1:** Enter a rule by following the guidelines in <https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm#Writing>  
<https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm>.  
**Note:** You can manually enter the rule in the text box or launch the rule builder.
    - For example, to include all instances that are in a specific compartment, add a rule with the following syntax:  

```
instance.compartment.id = '<compartment_ocid>'
```
  - b. Enter additional rules as needed. To add a rule, click **+Additional Rule**.
7. Click **Create**. The dynamic group now appears in the list of dynamic groups.



# **Identity and Access Management (IAM): Create IAM Components - Without Identity Domains Enabled**

## **Lab 1-2 Practices**

Paweł Domański (pawel@dexterteam.pl) data non-transferable  
license to use this content

# Get Started

---

## Overview

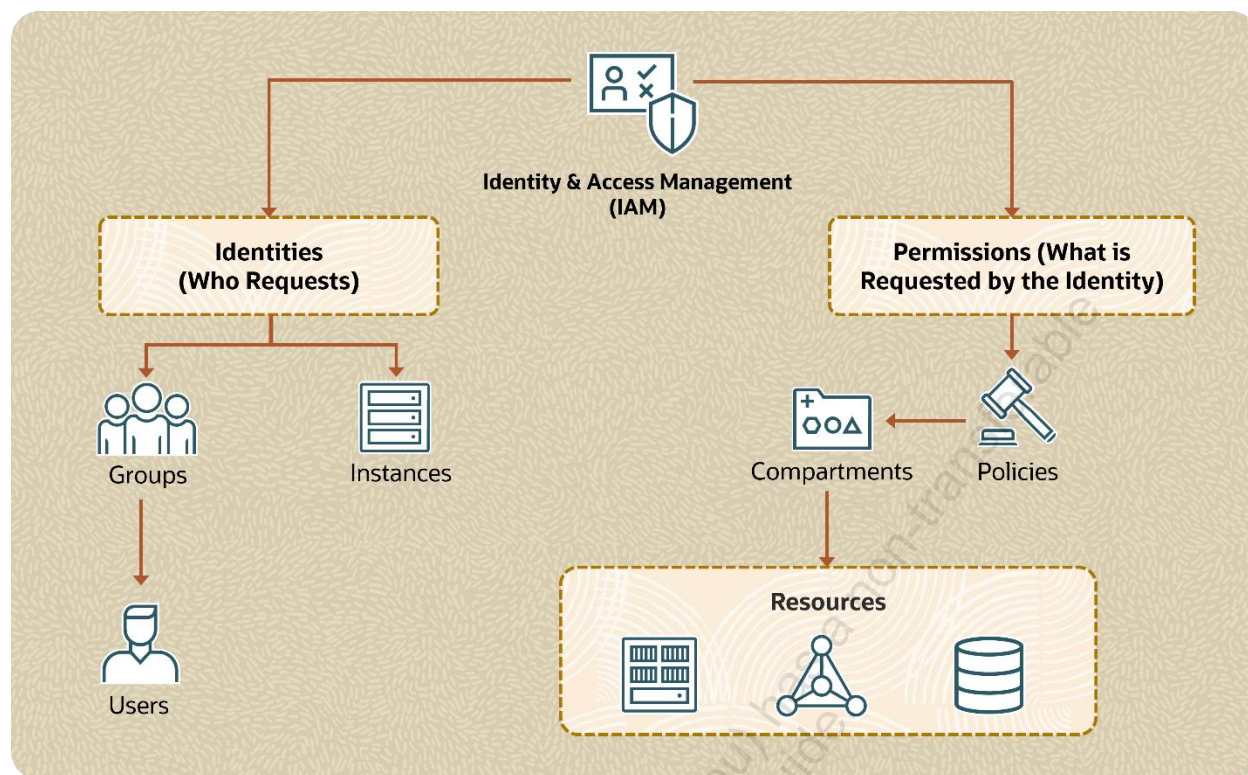
Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) lets you control who has access to your cloud resources.

In this lab, we will help you create a compartment, group, user, and policy. We will also provide the steps to create a dynamic group.

**Note:** Below instructions are for accounts without Identity Domains enabled.

In this lab, you'll:

- a. Create a compartment
- b. Create a user
- c. Create a group, and add a user to the group
- d. Create a policy
- e. Create a dynamic group



## Create a Compartment (Without Identity Domains Enabled)

---

A compartment is a collection of related resources. Compartments are fundamental components of OCI and are used for organizing and isolating your cloud resources.

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

### Tasks

1. Sign in to the OCI Console.
2. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Compartments**. A list of the compartments to which you have access appears.
3. Under **Child Compartment**, click **Create Compartment**.
4. Do the following:
  - a. **Name:** Enter a unique name for the compartment. The name must be unique across all the compartments in your tenancy.
  - b. **Description:** Enter a compartment-related description.
  - c. **Parent Compartment:** The compartment you are in appears by default. To choose another compartment in which to create this compartment, select from the drop-down list.
5. Click **Create Compartment**. The Child Compartment now appears in the list of compartments.



## Create a User (Without Identity Domains Enabled)

---

A user is an individual employee or system that needs to manage or use your company's OCI resources.

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

### Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Users**. A list of users in your tenancy appears.
2. Click **Create User**.
3. Enter the following:
  - a. **Name:** Enter a unique name or email address for the user.
  - b. **Description:** This value could be the user's full name, a nickname, or any other descriptive information.
  - c. **Email:** Enter an email address for the user. This email address is used for password recovery.
4. Click **Create**. The user now appears in the list of users.

# Create a Group, and Add a User to the Group (Without Identity Domains Enabled)

---

A group is a collection of users who need the same type of access to a particular compartment or set of resources.

In this practice, you'll learn how to create a group, and add a user to a group.

## Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Groups**. A list of the groups in your tenancy appears.
2. Click on the **Administrators** group.
3. Click **Add User to Group**.
4. Select the user created earlier from the **Users** drop-down list, and then click **Add**. The user now appears in the group.
5. Use the breadcrumb trail to go back to the **Groups** page and click **Create Group**.
6. Enter the following:
  - a. **Name:** Enter a unique name for the group.
  - b. **Description:** Enter a group-related description.
7. Click **Create**. The group now appears in the list of groups.

## Create a Policy (Without Identity Domains Enabled)

---

A policy is a document that specifies who can access which resources, and how.

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

### Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Policies**.
2. Choose a compartment.
3. A list of the policies in the compartment you're currently viewing appears.
4. Click **Create Policy**.
5. Enter the following:
  - a. **Name:** Enter a unique name for the policy.
  - b. **Description:** Enter a policy-related description.
  - c. **Compartment:** If you want to attach the policy to a compartment other than the one you're viewing, select it from the drop-down list. Remember, where the policy is attached controls who can later modify or delete it.
6. In the **Policy Builder** section, click **Show manual editor** and enter the policy statement.

**Note:** A sample statement would look like the following:

```
allow group <group_name> to manage virtual-network-family in
compartment <compartment_name>
```
7. Click **Create**. The policy now appears in the list of policies.

# Create a Dynamic Group (Without Identity Domains Enabled)

---

A dynamic group is a special type of group that contains resources, such as compute instances, which match rules that you define. This means that group membership can change dynamically as matching resources are created or deleted. These instances serve as “principal” actors and can make API calls to services according to policies that you write for the dynamic group.

In this practice, you’ll learn how to create a dynamic group.

## Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Dynamic Groups**.
2. Click **Create Dynamic Group**.
3. Enter the following:
  - a. **Name:** Enter a unique name for the group. The name must be unique across all groups in your tenancy, including dynamic groups and user groups.
  - b. **Description:** Enter a friendly description.
4. Enter the **Matching Rules**. Resources that meet the rule criteria are members of the dynamic group.
  - a. **Rule 1:** Enter a rule by following the guidelines in <https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm#Writing>  
<https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm>.  
**Note:** You can manually enter the rule in the text box or launch the rule builder.
    - For example, to include all instances that are in a specific compartment, add a rule with the following syntax:  
`instance.compartment.id = '<compartment_ocid>'`
  - b. Enter additional rules as needed. To add a rule, click **+Additional Rule**.
5. Click **Create**. The dynamic group now appears in the list of dynamic groups.



# **Networking—Virtual Cloud Network: Create and Configure a Virtual Cloud Network**

## **Lab 2-1 Practice**

Paweł Domański (pawel@dexterteam.eu)  
license to use this content is non-transferable

# Get Started

---

## Overview

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

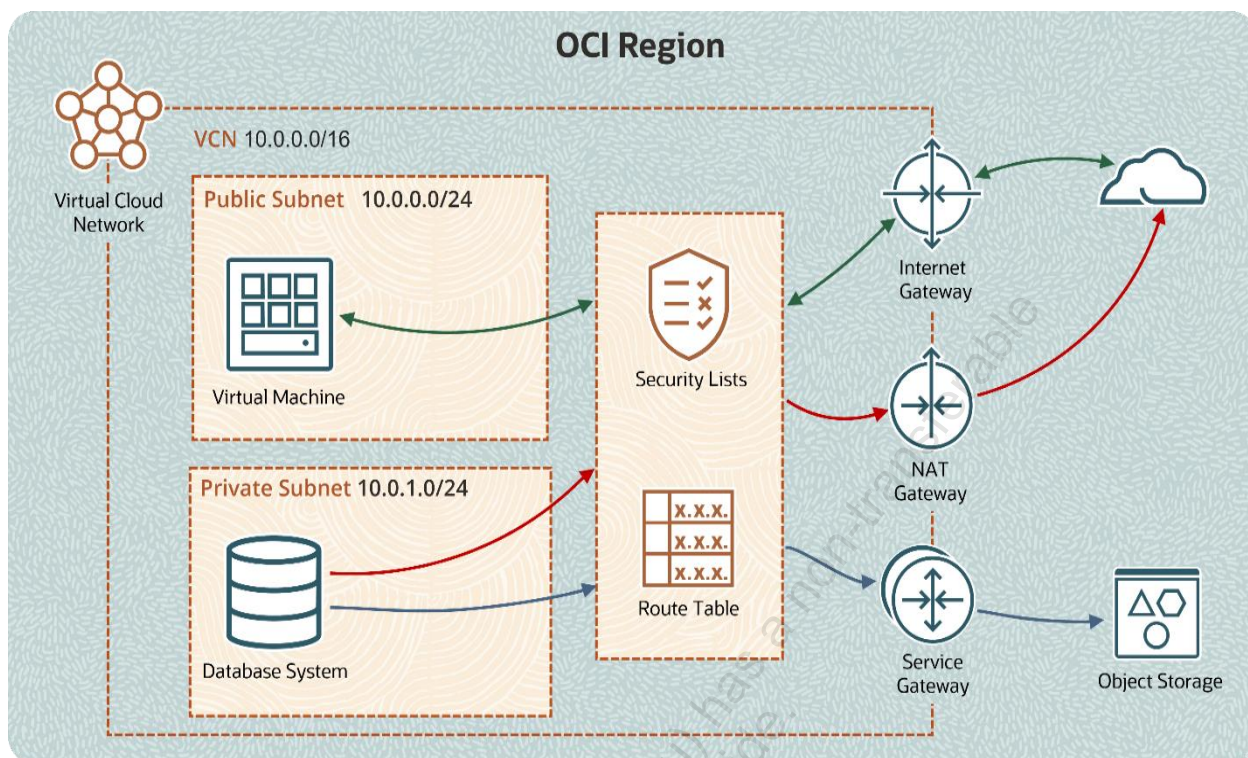
A VCN is a software-defined network specific to your OCI tenancy or a compartment in a specified region.

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)
- One CIDR Blocks/Prefixes
- One DHCP Option

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



## Prerequisites

- You have access to the OCI Console.

## Assumptions

- In this lab, we are considering US East (Ashburn, Region Key – IAD) as your region.
- You must be familiar with navigating the OCI Console.

# Create a Virtual Cloud Network

---

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

## Tasks

1. Log in to the 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, **US East (Ashburn)**.
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:** IAD-FA-LAB02-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** to start creating the VCN and its resources and wait for the VCN Wizard to successfully complete the VCN creation.
10. Click **View Virtual Cloud Network** to verify the creation of the VCN and its resources.

You can see that the VCN is successfully created with the following components:

- VCN
- Public Subnet
- Private Subnet
- CIDR Blocks/Prefixes
- Route Tables
- Internet Gateway
- Security Lists
- DHCP Options
- NAT Gateway
- Service Gateway

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.



Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# **Networking: OCI Load Balancer**

## **Lab 3-1 Practice**

Paweł Domański (pawel@dexterteam.eu) - data non-transferable  
license to use this Guide.

# Get Started

---

## Overview

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

## Load Balancer

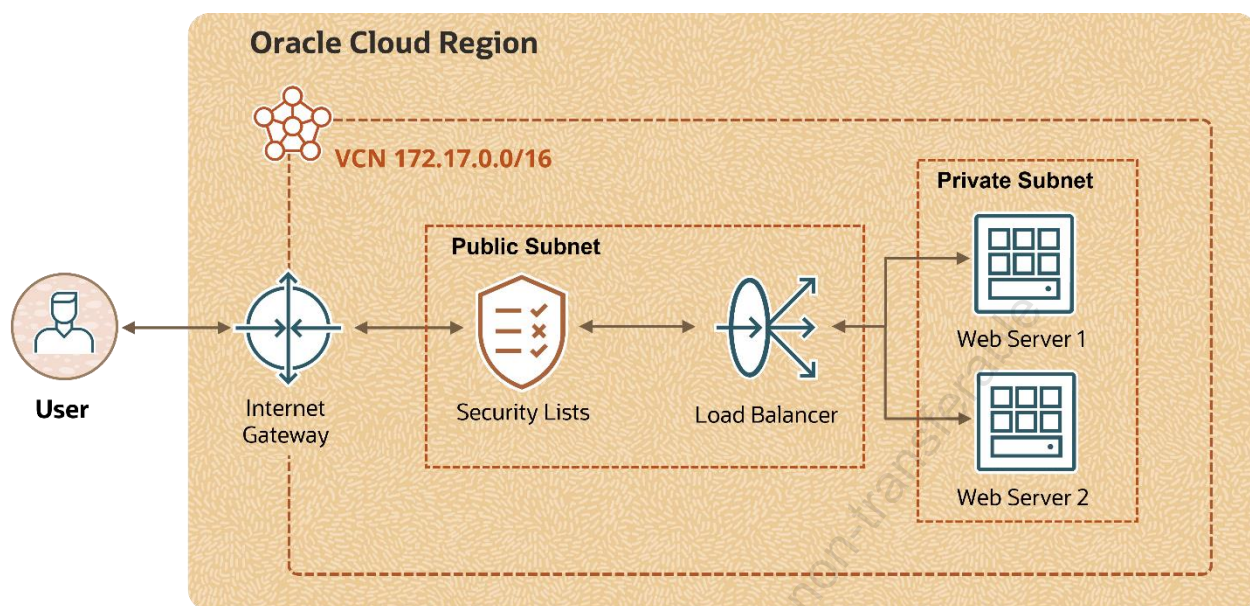
The OCI Load Balancer provides automated traffic distribution from one entry point to multiple backend servers in your VCN. It operates at the connection level and balances incoming client connections to healthy backend servers. The service offers a load balancer with your choice of a regional public 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
- **Backend server:** An application server responsible for generating content in reply to the incoming traffic
- **Backend set:** A logical entity defined by a list of backend servers
- **Load-balancing policy:** Tells the load balancer how to distribute incoming traffic to the backend servers
- **Health check:** A test to confirm the availability of backend 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

- You have access to the OCI Console.

## Assumptions

- In this lab, we are considering US East (Ashburn, Region Key – IAD) as your region.
- You must be familiar with navigating the OCI Console.

# 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, **US East (Ashburn)**.
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:** IAD-FA-LAB03-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 IAD-FA-LAB03-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 (Backend Servers)

---

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

### Task 1: 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, **US East (Ashburn)**.
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:** IAD-FA-LAB03-VM-01
  - **Compartment:** Your assigned *<compartment name>*
  - **Placement:** AD-1
  - **Image:** Oracle Linux 8
  - **Shape:** Click **Change Shape**.
    - **Instance Type:** Virtual Machine
    - **Shape Series:** Ampere
    - **Shape Name:** VM.Standard.A1.Flex
    - Leave **Number of OCPU** at one.
    - Leave **Amount of memory (GB)** at six.
    - Click **Select Shape**.
  - **Networking:**
    - **Primary network:** Select existing Virtual Cloud Network.
    - **Virtual Cloud Network in *<assigned compartment>*:** IAD-FA-LAB03-VCN-01
    - **Subnet in *<assigned compartment>*:** Private Subnet-IAD-FA-LAB03-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 IAD-FA-LAB03-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.

## Task 2: 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, **US East (Ashburn)**.
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:** IAD-FA-LAB03-VM-02
  - **Compartment:** Your assigned *<compartment name>*
  - **Placement:** AD-1
  - **Image:** Oracle Linux 8
  - **Shape:** Click **Change Shape**
    - **Instance Type:** Virtual Machine
    - **Shape Series:** Ampere

- **Shape Name:** VM.Standard.A1.Flex
- Leave **Number of OCPU** at one.
- Leave **Amount of memory (GB)** at six.
- Click **Select Shape**.
- **Networking:**
  - **Primary network:** Select existing Virtual Cloud Network.
  - **Virtual Cloud Network in <assigned compartment>:** IAD-FA-LAB03-VCN-01
  - **Subnet in <assigned compartment>:** Private Subnet-IAD-FA-LAB03-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 IAD-FA-LAB03-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 backend 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:** IAD-FA-LAB03-LB-01
  - **Choose visibility type:** Public
  - **Assign a public IP address:** Ephemeral IP Address
  - In the **Bandwidth** section, under **Shapes**, select **Flexible Shapes**.
  - Under **Choose Networking**, for the **Virtual Cloud Network in <compartment name>**, select IAD-FA-LAB03-VCN-01 and for the **Subnet in <compartment name>**, select Public Subnet-IAD-FA-LAB03\_VCN-01.
  - Click **Next**.
  - Under **Choose Backends**, select **Weighted Round Robin**.
  - Click **Add Backends**.
  - Select both IAD-FA-LAB03-VM-01 and IAD-FA-LAB03-VM-02.
  - Click **Add Selected Backends**.
  - Leave all values at defaults in the **Specify Health Check Policy** section.  
**Note:** The default values will add a TCP port 80 rule to the security list for your private subnet.
  - Click **Next**.
  - On the **Configure Listener** page, enter the following values:
    - **Listener Name:** IAD-FA-LAB03-LISTENER-01
    - **Specify the type of traffic your 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 IAD-FA-LAB03-WS-01** will appear.
10. Reload the page to see the other backend server has provided the message, **Hello World! My name is IAD-FA-LAB03-WS-02**.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.



Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# **Compute: Create a Web Server on an OCI Compute Instance**

## **Lab 4-1 Practices**

Paweł Domański (pawel@dexterfm.pl) - Oracle University non-transferable  
license to use this Guide

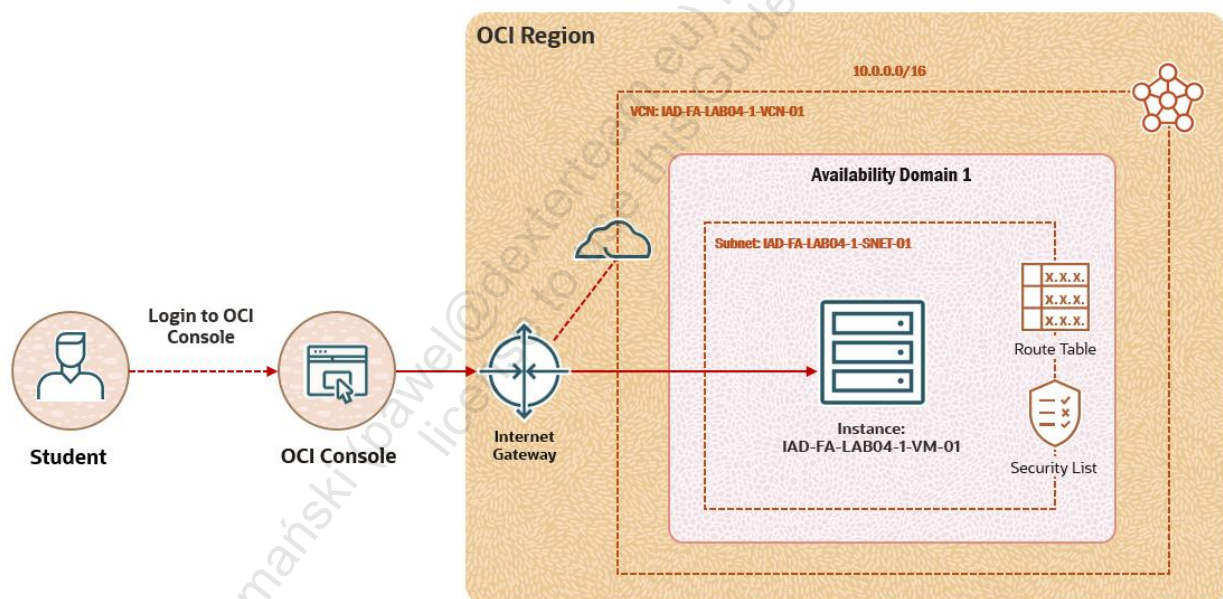
# Get Started

## 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 have access to the OCI Console.

## Assumptions

- In this lab, we are considering US East (Ashburn, Region Key – IAD) 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, **US East (Ashburn)**.
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 **ocifalab4key**. 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 contents 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 **ocifalab4key**.

**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.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# 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:** IAD-FA-LAB04-1-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 **IAD-FA-LAB04-1-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:** IAD-FA-LAB04-1-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:** IAD-FA-LAB04-1-IG-01
- b. **Create In Compartment:** *<your compartment>*

12. Click **Create Internet Gateway**.

You can see that the 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 IAD-FA-LAB04-1-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:** IAD-FA-LAB04-1-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 **IAD-FA-LAB04-1-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 IAD-FA-LAB04-1-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 route rule is successfully added.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# 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:** IAD-FA-LAB04-1-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:** Click **Change Shape** and select the following:
  - 1) **Instance Type:** Virtual Machine
  - 2) **Shape Series:** Ampere
  - 3) **Shape Name:** VM.Standard.A1.Flex
  - 4) Leave **Number of OCPU** at one.
  - 5) Leave **Amount of memory (GB)** at six.
  - 6) Click **Select Shape**.
- f. **Primary network:** Select an existing Virtual Cloud Network.
  - 1) **Virtual cloud network in *<your compartment>*:** IAD-FA-LAB04-1-VCN-01
  - 2) **Subnet:** Select an existing subnet.
  - 3) **Subnet in *<your compartment>*:** IAD-FA-LAB04-1-SNET-01 (regional)
  - 4) **Public IP address:** Assign a public IPv4 address.

- g. **Add SSH keys:** Paste public keys.
- h. **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 **IAD-FA-LAB04-1-VM-01** instance and paste it in the Notepad.
- 6. Click the **Cloud Shell** icon next to 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 */home/username/.ssh/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 IAD-FA-LAB04-1-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

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# **Object Storage: Create and Manage OCI Object Storage**

## **Lab 5-1 Practices**

Paweł Domański (pawel@dexterteam.eu) - data non-transferable  
license to use this Guided Learning Path

# Get Started

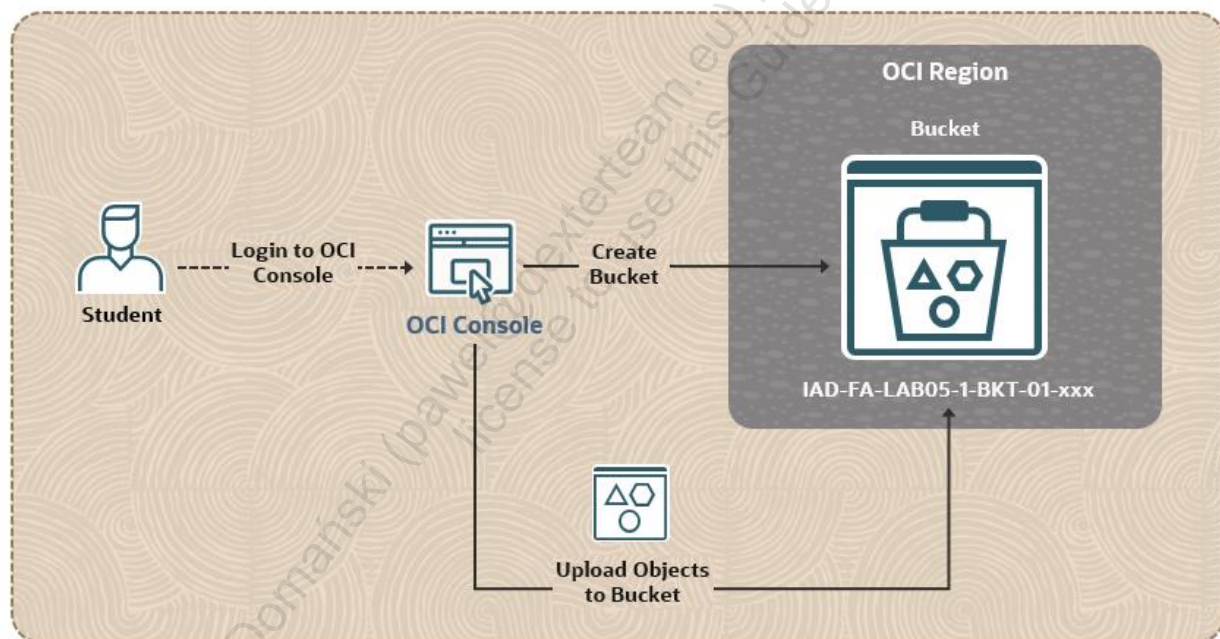
## Overview

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.

Object Storage is characterized by 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 life cycle management, replication policy, and retention rule.

In this lab, you will:

- Create an Object Storage bucket
- Upload an object to a bucket



## Prerequisites

- You have access to the OCI Console.

## Assumptions

- In this lab, we are considering US East (Ashburn, Region Key – IAD) as your region.
- You must be familiar with navigating the OCI Console.

# Create an Object Storage Bucket

---

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

## Tasks

1. Sign in to your 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 `IAD-FA-LAB05-1-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 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 emit events for object state changes. Do not select this field now.
  - **Uncommitted Multipart Uploads Cleanup:** Uncommitted Multipart Uploads Cleanup allows deletion of uncommitted or failed multipart uploads. 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.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.



## 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 **IAD-FA-LAB05-1-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.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# **Block Storage: Create, and Attach a Block Volume**

## **Lab 6-1 Practices**

Paweł Domański (pawel@dexterteam.eu) - data non-transferable  
license to use this Guided Path

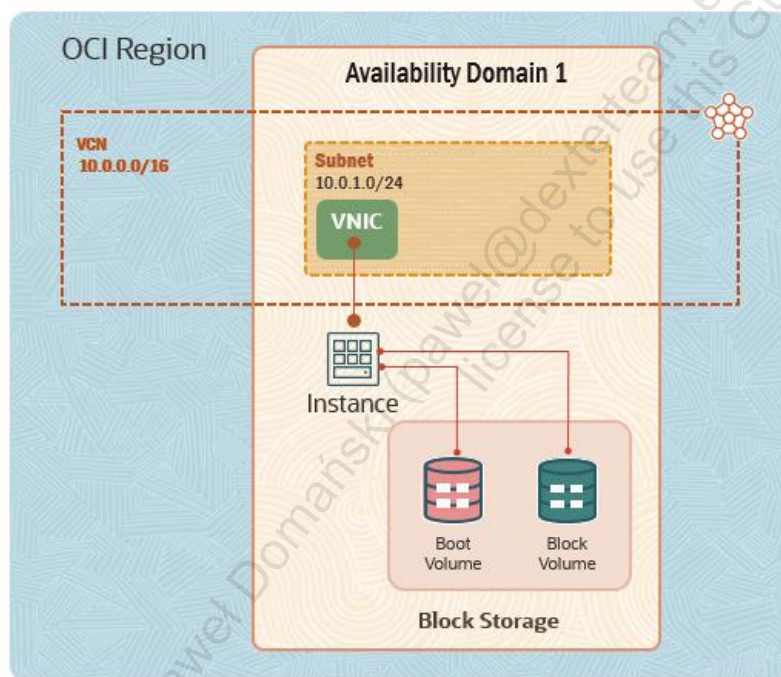
# Get Started

## 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 will:

- Create a Virtual Cloud Network and its components
- Create a VM instance
- Create a block volume
- Attach a block volume to a compute instance



## Prerequisites

- You have access to the OCI Console.

## Assumptions

- In this lab, we are considering US East (Ashburn, Region Key – IAD) as your region.
- You must be familiar with navigating the OCI Console.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# 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 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, **US East (Ashburn)**.
3. From the **Main Menu**, select **Networking**, and then click **Virtual Cloud Networks**.
4. Click **Create VCN**.
5. Enter the following:
  - a. **Name:** Enter IAD-FA-LAB06-1-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**.

**Note:** You can leave all the other options as default.
6. Click **Create VCN**. The VCN is now created successfully.
7. Click **Create Subnet**.
8. In the Create Subnet dialog box, do the following:
  - a. **Name:** Enter IAD-FA-LAB06-1-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.
9. Click **Create Subnet**. The subnet is now created successfully, and the state is **Available**.



10. In the left navigation pane, under **Resources**, click **Internet Gateways**.
11. Click **Create Internet Gateway**.
12. Do the following:
  - a. **Name:** Enter `IAD-FA-LAB06-1-IG-01`.
  - b. **Create in Compartment:** Select the *<compartment name>* assigned to you.
13. Click **Create Internet Gateway**. The Internet gateway is now created successfully, and the state is **Available**.
14. In the left navigation pane, under **Resources**, click **Route Tables**.
15. Click **Default Route Table for IAD-FA-LAB06-1-VCN-01**.
16. Click **Add Route Rules** and do 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 **IAD-FA-LAB06-1-IG-01** from the drop-down list.
17. 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 OCI Console.
2. 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, **US East (Ashburn)**.
3. In the Console ribbon at the top of the screen, click the **Cloud Shell** icon next to the Region selection menu.
4. 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 **ocifalab6key**. Choose a 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.

5. 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 contents 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.

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

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

**Note:** Replace <<sshkeyname>> with **ocifalab6key**.

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

7. 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.
8. From the **Main Menu**, select **Compute**. Under **Compute**, click **Instances**.
9. Click **Create instance** and do the following:
  - a. **Name:** Enter IAD-FA-LAB06-1-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:** Select Oracle Linux 8.
  - e. **Shape:** Click **Change Shape** and select the following:
    - 1) **Instance Type:** Virtual Machine
    - 2) **Shape Series:** Ampere
    - 3) **Shape Name:** VM.Standard.A1.Flex
    - 4) Leave **Number of OCPU** at one.
    - 5) Leave **Amount of memory (GB)** at six.
    - 6) Click **Select Shape**.
  - f. **Networking:** Select the existing VCN **IAD-FA-LAB06-1-VCN-01** and existing subnet **IAD-FA-LAB06-1-SNET-01 (regional)**. Under **Public IP address**, select **Assign a public IPv4 address**.
  - g. **Add SSH keys:** Select **Paste public keys** and paste the contents of the public key, which you copied in Step 6, in the box.

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

10. Click **Create**.

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

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

12. 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:**

- `/home/username/.ssh/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.

13. You are now connected to the instance IAD-FA-LAB06-1-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 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 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 IAD-FA-LAB06-1-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 50.
    - 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 **IAD-FA-LAB06-1-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 **IAD-FA-LAB06-1-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/oraclevd** 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 **IAD-FA-LAB06-1-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 50 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 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`.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# **Security: Configure Security Zones Using Maximum Security Zones**

## **Lab 7-1 Practices**

Paweł Domański (pawel@dexterfm.edu.pl) has a non-transferable license to use this Guide

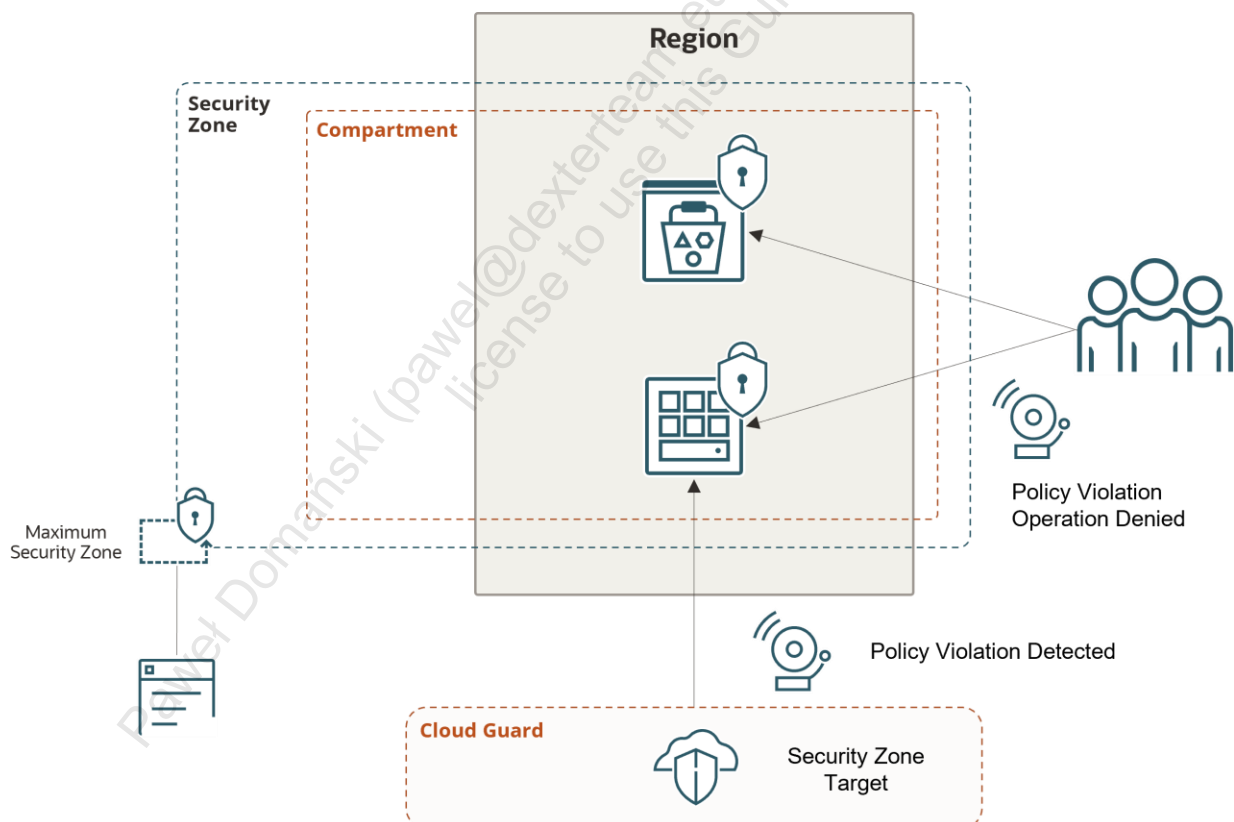
# Get Started

## Overview

Security zones enforce security posture on OCI cloud compartments and prevent actions that can compromise a customer's security posture. Security zone policies can be applied to various cloud infrastructure types (network, compute, storage, database, and so on) to guarantee cloud resources ensure security and to prevent potential misconfigurations.

In this lab, you will:

- Set up a security zone with Maximum Security Recipe
- View the security zone policies attached to a created security zone
- Test creating a bucket in an assigned compartment using an Oracle-managed key



## Prerequisites

- You have access to the OCI Console.
- Your tenancy should have Cloud Guard enabled.

## Assumptions

- In this lab, we are considering US East (Ashburn) (IAD) as your region.
- You must be familiar with navigating the OCI Console.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

# Set Up Security Zone with Maximum Security Recipe

---

You will create a security zone for an allocated compartment and check for any security zone policy violations.

## Tasks

1. Sign in to the 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, **US East (Ashburn)**.
3. From the navigation menu, select **Identity & Security**. Navigate to **Security Zones**, and then click **Overview**.
4. In the left navigation pane, under **Scope**, select *<your assigned compartment>* from the drop-down menu.

**Note:** The compartment should not be associated with a security zone. By default, all sub-compartments are also in the same security zone.

5. Click **Create Security Zone**.
6. On the Create Security Zone page, enter the following values:
  - a. **Security Zone Recipe:** Select **Oracle-managed** to use Maximum Security Recipe.
  - b. **Name:** IAD-FA-LAB07-1-SZ-01
  - c. **Description:** My Security Zone
  - d. **Create for compartment:** *<your assigned compartment>*

7. Click **Create Security Zone**.

**Note:** When you create a security zone for a compartment, Cloud Guard does the following:

- Deletes any existing Cloud Guard target for the compartment and for any child compartments
- Creates a security zone target for the compartment
- Adds the default Oracle-managed detector recipes to the security zone target



## View the Security Zone Policies Attached with a Created Security Zone

---

You will identify the recipe associated with the newly formed security zone, and then review its policies.

1. From the navigation menu, select **Identity & Security**. Navigate to **Security Zones**, and then click **Overview**.
2. In the left navigation pane, under Scope, select *<your assigned compartment>* from the drop-down menu.
3. Click the **IAD-FA-LAB07-1-SZ-01** security zone and view the Security Zone details page.
4. On the **Security Zone** information tab, locate the attached recipe and click the **Recipe** for this security zone: Maximum Security Recipe – 20200914.
5. View the Oracle-managed recipe attached to the Security Zone created on the **Recipe details** page.
6. View a few policy statements with associated Resource types:

```
deny public_subnets in VIRTUALNETWORK
deny public_buckets in OBJECTSTORAGE
deny buckets_without_vault_key in in OBJECTSTORAGE
```

Next, you will put a security zone to test by attempting to violate a few of its policies.

## Verify Creating a Bucket in an Assigned Compartment Using a Oracle-Managed Key

---

You will test the security zone. Create a bucket to check if it is restricted in the security zone. As a reference, the security zone recipe has a policy that prohibits bucket creation without a customer-managed vault key.

To create a bucket to observe the security zone violations:

1. Open the navigation menu and click **Storage**. Navigate Object Storage, click **Buckets**.
2. In the left navigation pane, under **List Scope**, select the assigned compartment from the drop-down menu.
3. Click **Create Bucket**.
4. In the **Create Bucket** dialog box, specify the attributes of the bucket:
  - a. **Bucket Name:** IAD-FA-LAB07-1-BKT-01-<user-id>  
Please specify your user ID in place of <user-id> to make it unique.
  - b. **Default Storage Tier:** Standard
  - c. **Encryption:** Encrypt using Oracle-managed keys.

**Note:** Leave all the other options in their default setting.
5. Click **Create**.  
You will receive an error indicating a security zone violation: "Encrypt the bucket with a customer-managed encryption key".
6. Click **Cancel**.

The security zone recipe created earlier has a policy that prohibits bucket creation without a customer-managed key. You will need to create an OCI Vault and a master encryption key, using which you can create a bucket. This way the security zone recipes enforce security posture on OCI cloud compartments and prevent actions that could compromise the security posture of a customer.

**Note:** Please purge the Security Zone created for this lab.

## Purge Security Zone

1. From the navigation menu, select **Identity & Security**. Navigate to **Security Zones** and click **Overview**.
2. Make sure you are in your given compartment.
3. From the list of Security Zones, locate your Security Zone and click its name: **IAD-FA-LAB07-1-SZ-01**.
4. Click **Delete**. Then click **Delete** in the Confirmation window.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.

Paweł Domański (pawel@dexterteam.eu) has a non-transferable license to use this Guide.