



ORACLE

Oracle Cloud Winter Camp

Security and Compliance in
Oracle Cloud
18 Febrero 2020

Speakers

David Nuñez Escobedo
Principal Security Solution Engineer, Oracle

Juan Carlos Díaz
Principal Security Solution Engineer, Oracle



Contents

1	INTRODUCTION.....	5
2	PRE-REQUISITE.....	6
3	OCI CONSOLE.....	7
4	IDENTITY ACCESS MANAGEMENT (IAM).....	9
4.1	Compartments.....	9
4.2	Groups.....	11
4.3	Users.....	12
4.3.1	Create Passwords.....	14
4.4	Assign Users to their Groups.....	15
4.5	Policies.....	16
4.5.1	Policy Syntax.....	16
4.5.2	Policies for Network Resources.....	17
4.5.3	Policies for Compute Resources.....	18
4.5.4	Policies for OCI Vault Resources.....	21
4.5.5	Policies for Object Storage Resources.....	22
4.6	Summary.....	23
5	OCI NETWORKING.....	24
5.1	Introduction.....	24
5.2	Access to OCI.....	24
5.3	Test User Permissions.....	26
5.4	Create VCN.....	26
5.5	Subnets.....	29
5.6	Virtual Routers in OCI.....	32
5.6.1	Internet Gateway.....	32
5.6.2	NAT Gateway.....	33
5.6.3	Service Gateway.....	33
5.7	Summary.....	34
6	OCI VAULT.....	35
6.1	Access to OCI.....	35
6.2	User Permissions.....	36
6.3	Create Vault.....	36

6.4	Create Key.....	37
7	CREATE VIRTUAL MACHINES.....	40
7.1	Access to OCI.....	40
7.2	User Permissions.....	40
7.3	Create SSH Key Pair.....	40
7.4	Create Instances.....	40
7.4.1	BastionVM.....	41
7.4.2	PrivateVM.....	44
7.5	Summary.....	49
8	Object Storage.....	50
8.1	Access to OCI.....	50
8.2	User Permissions.....	50
8.3	Create Bucket.....	50
9	Connect via SSH to the VM.....	52
9.1.1	Connect via PuTTY.....	52
9.1.2	Connect via OpenSSH.....	57
9.1.3	Block SSH Connection.....	58
9.2	Summary.....	60
10	Maximum Security Zone.....	61
10.1	Introduction.....	61
10.2	Create a Compartment.....	62
10.3	Create a policy for the newly created compartment.....	65
10.3.1	Create Network Policy.....	65
	66
10.3.2	Attach a network policy to root compartment.....	67
10.3.3	Create Instance Policy.....	69
10.3.4	Create Vault Policy.....	71
10.4	Create Vault and Key.....	74
10.5	Summary.....	76
10.6	Use cases.....	77
10.6.1	Scenario 1: Create a subnet that allows public IPs in a compartment UAT_Maximum_security_zone_cmp (Which is in Maximum security Zone).....	77

10.6.2	Scenario 2: Create an instance in a security zone compartment (UAT_Maximum_security_zone_cmp) with an associated subnet not in a security zone (Production)	80
10.6.3	Scenario 3: Create an instance in a security zone without sanctioned image (which is not an Oracle image)	83
11	Conclusions	89

Abbreviations

IAM – Identity Access Management

OCI – Oracle Cloud Infrastructure

VM – Virtual Machine

VCN – Virtual Cloud Network

AD – Availability Domain

IG – Internet Gateway

NG – NAT Gateway

SG – Service Gateway

1 INTRODUCTION

Oracle's mission is to build cloud infrastructure and platform services for your business to have effective and manageable security to run your mission-critical workloads and store your data with confidence.

In this Lab we will use several OCI Services to build secure infrastructure and store your data with confidence following Oracle's best practices.

Oracle Cloud Infrastructure Identity and Access Management Service (OCI IAM) lets you control who has access to your cloud resources. You control the types of access a group of users has and to which specific resources.

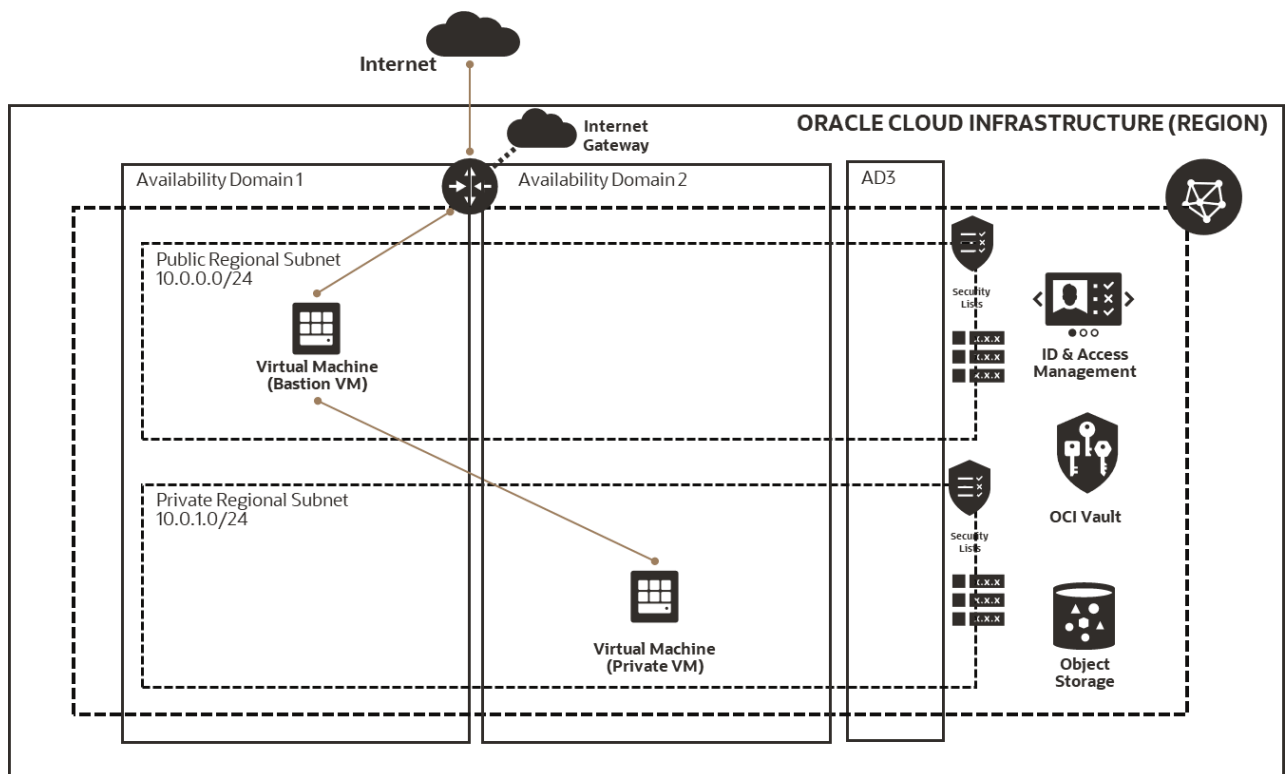
The purpose of the first part of lab is to give you an overview of the IAM Service components and an example scenario to help you understand how they work together.

We will also create VMs in a public and in a private subnet following Oracle's best practices, like creating Bastion hosts, which will secure the private hosts behind them, and in the same time allowing secure client connections to them. We will test the Security Lists rules and understand better their role in OCI.

Moreover, we will learn how to encrypt block volumes and buckets in Object Storage, by simply using master encryption keys from OCI Vault.

Therefore, understanding how security in OCI is compliant and can fulfill any customer's requirements.

Below you can see the cloud topology which will be used in this lab:



2 PRE-REQUISITE

We assume that you've already activated your Oracle Cloud Free Tier account in region Germany Central (Frankfurt) eu-frankfurt-1.

You can activate Oracle Cloud Free Tier account at the following link:

<https://signup.oraclecloud.com/>

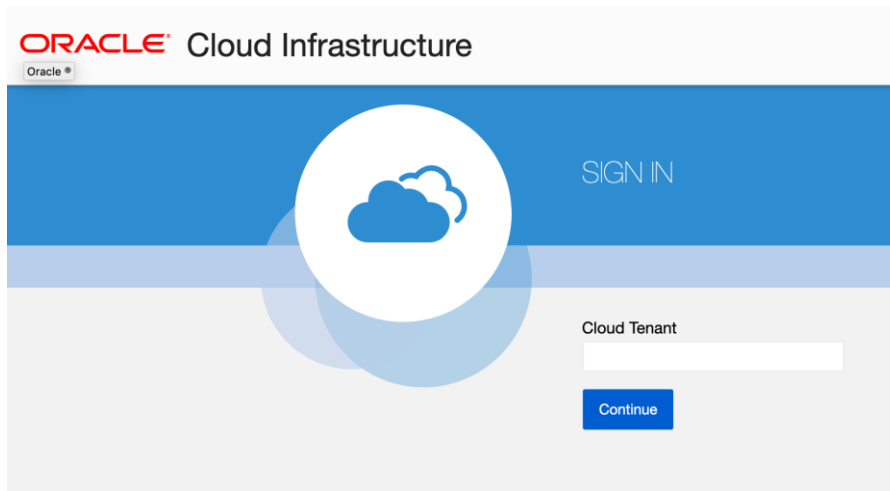
Once activated, you will have a default administrator user (your email at sign up to OCI Console) which have administrative rights in your tenant.

This user will be used in this lab, until it will be requested explicitly to log in with other users that you will create in this lab.

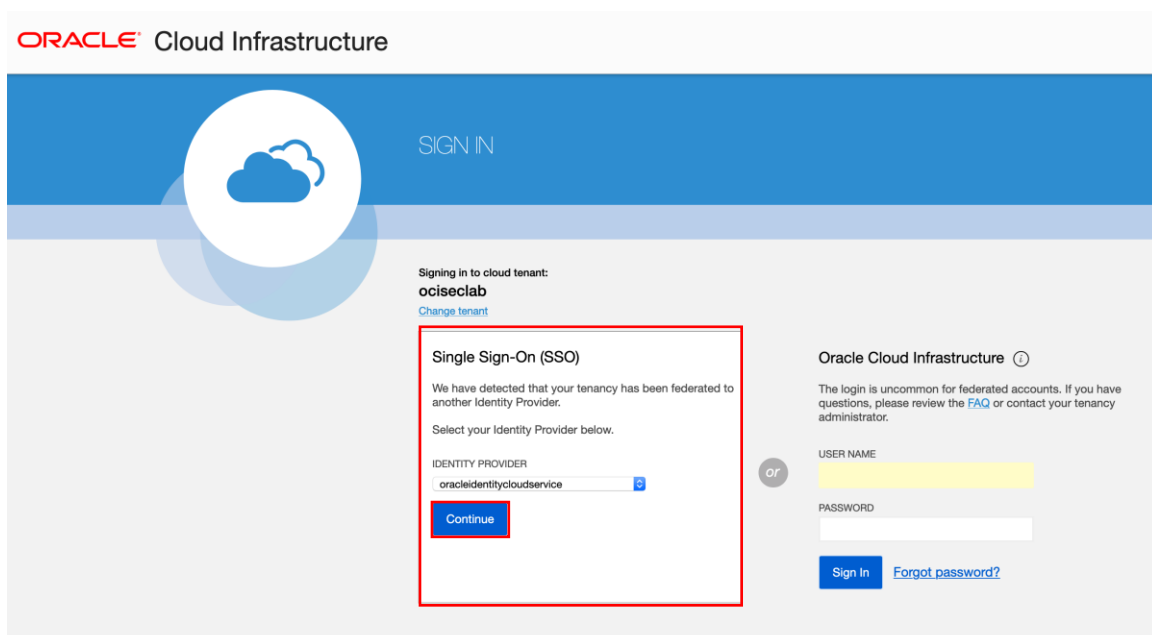
3 OCI CONSOLE

For the lab, you need to access to OCI console with default administrator user.

1. Access to URL: <https://console.eu-frankfurt-1.oraclecloud.com/>
2. Add cloud tenant selected during Oracle Cloud Free Tier account registration



3. Click Continue into Single Sign-On (SSO)



4. Add username and password of default administrator user and click Sign-in

ORACLE Cloud

ociseclab

Oracle Cloud Account Sign In

User Name

User name or email

Password

Password

Sign In

Need help signing in? [Click here](#)

5. You will access to OCI Console with default administrator capabilities

ORACLE Cloud

Search for resources and services

Germany Central (Frankfurt)

Quick Actions

Collapse ^

COMPUTE

Create a VM instance

2-6 mins

Always Free Eligible

AUTONOMOUS TRANSACTION PROCESSING

Create an ATP database

3-5 mins

Always Free Eligible

AUTONOMOUS DATA WAREHOUSE

Create an ADW database

3-5 mins

Always Free Eligible

NETWORKING

Set up a network with a wizard

2-3 mins

NETWORKING

Set up a load balancer

5 mins

Always Free Eligible

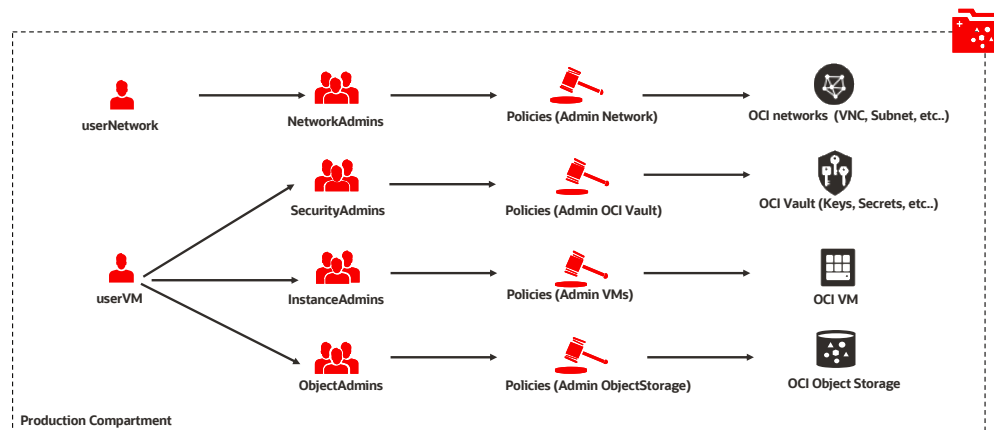
SEARCH

View all my resources

4 IDENTITY ACCESS MANAGEMENT (IAM)

Oracle Cloud Infrastructure Identity and Access Management (IAM) Service lets you control who has access to your cloud resources. You control the types of access a group of users has and to which specific resources.

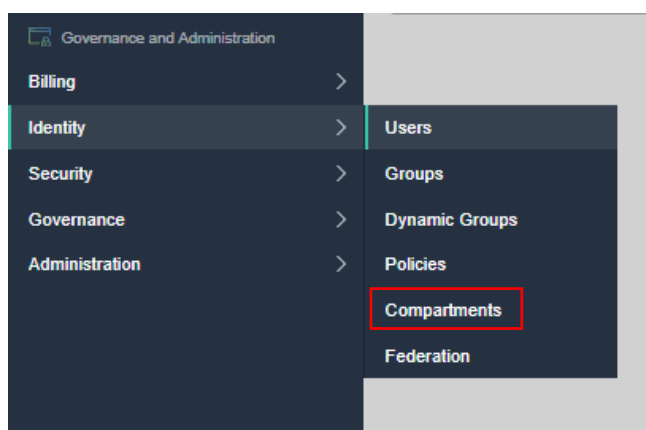
In this Chapter we will create the following example scenario:



4.1 Compartments

A collection of related resources. Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating your cloud resources. You can use them to clearly separate resources for the purposes of measuring usage and billing, access (through the use of policies), and isolation (separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of your organization.

1. In the OCI Console, on the left side click Menu - Identity – Compartments:



2. Click Create Compartment:

The screenshot shows the Oracle Cloud Identity and Access Management console. On the left, the 'Identity' sidebar is visible with options like Users, Groups, Dynamic Groups, Network Sources, Policies, Compartments (selected), Federation, and Authentication Settings. The main area is titled 'Compartments' and contains a table with columns: Name, Status, OCID, Authorized, and Subcompartments. The table lists three compartments: 'ociseclab (root)', 'ManagedCompartmentForPaaS', and 'Production'. A red box highlights the 'Create Compartment' button at the top left of the table.

Name	Status	OCID	Authorized	Subcompartments
ociseclab (root)	Active	...7ms5nq	Yes	3
ManagedCompartmentForPaaS	Active	...w42o6a	Yes	0
Production	Active	...kzfjoq	Yes	0

3. We will create 2 compartments with *Name*: Production and Test.
 - Fill in the *Name* of the compartment
 - Add a friendly *Description*.
 - Choose the *Parent Compartment* - select <Cloud Tenant> (root) ex: ociseclab (root)
 - Click Create Compartment.

The screenshot shows the 'Create Compartment' form. It has fields for NAME, DESCRIPTION, and PARENT COMPARTMENT. The NAME field contains 'Production', the DESCRIPTION field contains 'Compartment for Production', and the PARENT COMPARTMENT dropdown is set to 'ociseclab (root)'. Below these fields is a section for Tagging, which includes a 'TAG NAMESPACE' dropdown set to 'None (add a free-form tag)', and empty 'TAG KEY' and 'VALUE' input fields. A '+ Additional Tag' button is also present. At the bottom, the 'Create Compartment' button is highlighted with a red box.

Compartments

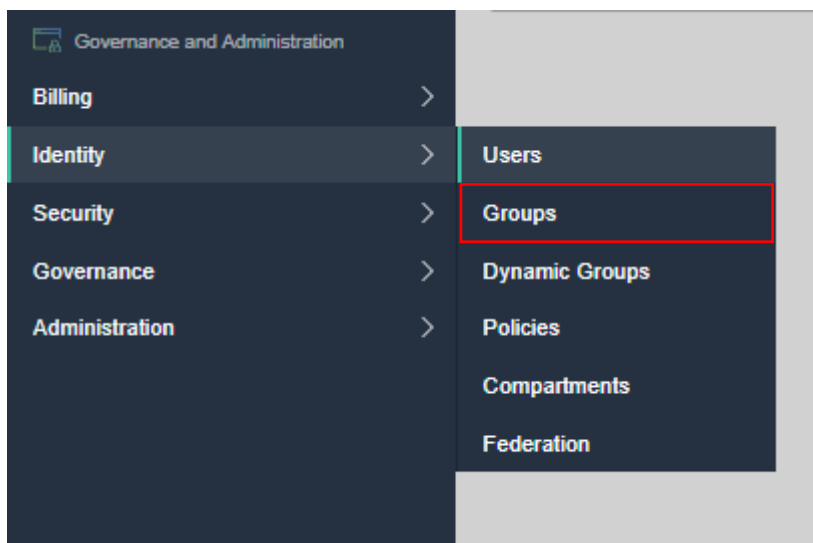
Create Compartment					
Name	Status	OCID	Authorized	Subcompartments	Created
ociseclab (root)	● Active	...7ms5nq	Yes	4	-
ManagedCompartmentForPaaS	● Active	...w42o6a	Yes	0	Mon, Apr 27, 2020, 21:39:18 UTC
Production	● Active	...kzfjjoq	Yes	0	Tue, Apr 28, 2020, 09:16:01 UTC
Test	● Active	...ee7w5a	Yes	0	Wed, May 6, 2020, 10:24:23 UTC
Showing 4 Items < Page 1 >					

4.2 Groups

A user's permissions to access services comes from the *groups* to which they belong.

We can define a *group* as a collection of users that need the same type of access to a particular set of resources or compartment.

1. In the OCI Console, on the left side click Menu - Identity – Groups:



2. Click Create Group:

Groups

i Create or manage federated groups instead?
 This tenancy has a federation with one or more identity providers (IdP). This page creates local groups and manages the membersh manage groups for federated users, go to the [Federation page](#) to find the appropriate IdP Details page.

[Create Group](#)

Name	OCID	Description	Created
Administrators	...aflihq	Administrators	Mon, Apr 27, 2020, 20:59:21 UTC

3. We will create 4 groups with Name: NetworkAdmins, InstanceAdmins, SecurityAdmins, ObjectAdmins:
 - Fill in the name of the *Group*
 - Add a friendly *Description*
 - Click Create.

Repeat the following steps for all the groups.

Groups

Create Group [Help](#) [Cancel](#)

NAME
NetworkAdmins
No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION
Group for network administrators

TAGS
Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.
[Learn more about tagging](#)

TAG NAMESPACE **TAG KEY** **VALUE**

None (add a free-form tag) [] [] X

+ Additional Tag

Create [Cancel](#)

Groups

Create or manage federated groups instead?

This tenancy has a federation with one or more identity providers (IdP). This page creates local groups and manages the memberships of local users. To create and manage groups for federated users, go to the [Federation page](#) to find the appropriate IdP Details page.

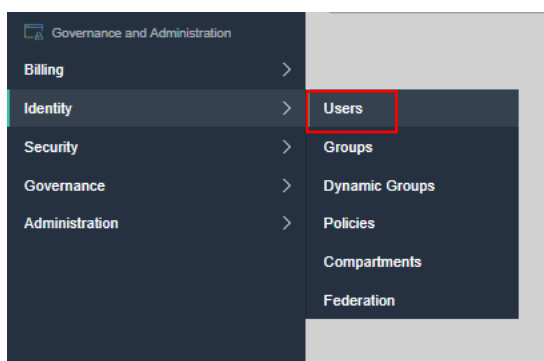
[Create Group](#)

Name	OCID	Description	Created
Administrators	...8fllhq	Administrators	Mon, Apr 27, 2020, 20:59:21 UTC
InstanceAdmins	...5flhsa	Group for Instances/VMs Administrators	Wed, May 6, 2020, 10:30:09 UTC
NetworkAdmins	...sheziq	Group for Network Administrators	Wed, May 6, 2020, 10:27:42 UTC
ObjectAdmins	...gde37q	Group for Object Storages Administrators	Wed, May 6, 2020, 10:30:53 UTC
SecurityAdmins	...bua7lq	Group for OCI Vault/Key Management Administrators	Wed, May 6, 2020, 10:29:20 UTC

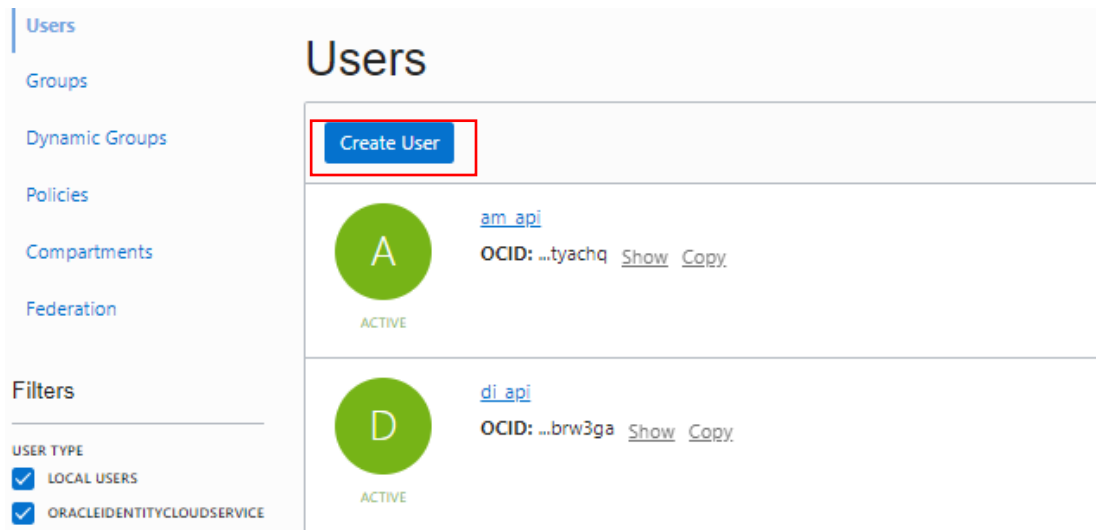
Showing 5 Items < Page 1 >

4.3 Users

1. In the OCI Console, on the left side click Menu – Identity – Users:



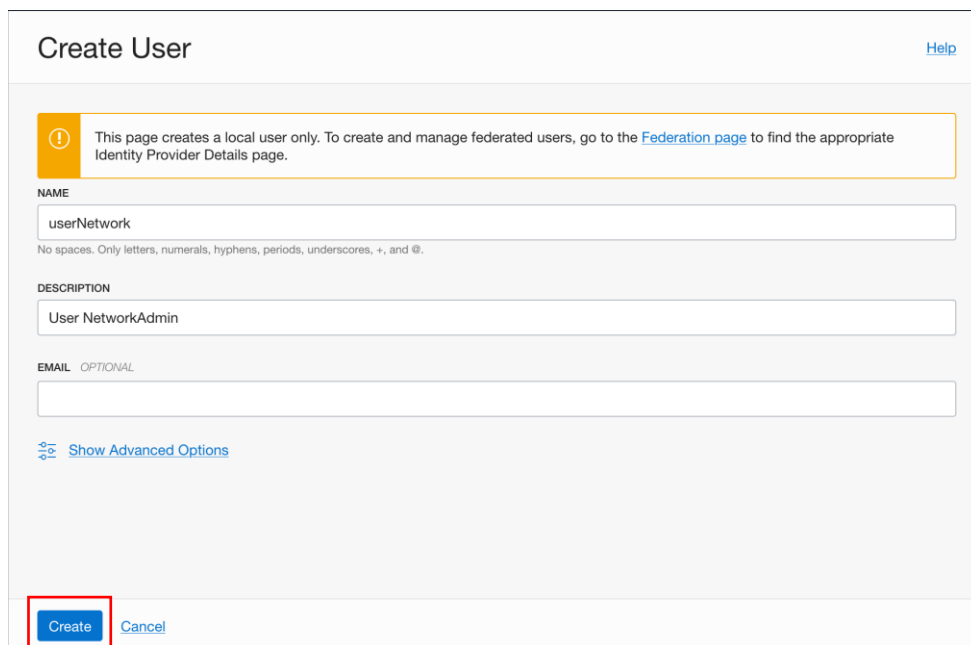
2. Click Create Users:



The screenshot shows the 'Users' management interface. On the left is a navigation menu with options: Users, Groups, Dynamic Groups, Policies, Compartments, and Federation. Below this is a 'Filters' section with 'USER TYPE' and checkboxes for 'LOCAL USERS' and 'ORACLEIDENTITYCLOUDSERVICE'. The main area is titled 'Users' and contains a 'Create User' button (highlighted with a red box). Below the button is a list of two users:

Name	OCID	Status
am_api	...tyachq	ACTIVE
di_api	...brw3ga	ACTIVE

3. We will create 2 users with *Name* (Username): userNetwork and userVM
 - o Fill in the *Name* of the user (it must be unique across all users in the tenancy)
 - o Add a friendly *Description*
 - o Click Create.




The 'Create User' form is shown with the following fields and values:

- NAME:** userNetwork
- DESCRIPTION:** User NetworkAdmin
- EMAIL (OPTIONAL):** (empty)

At the bottom, the 'Create' button is highlighted with a red box, and a 'Cancel' button is also visible.

Create User [Help](#)


 This page creates a local user only. To create and manage federated users, go to the [Federation page](#) to find the appropriate Identity Provider Details page.

NAME





No spaces. Only letters, numerals, hyphens, periods, underscores, +, and @.

DESCRIPTION

EMAIL OPTIONAL

 [Show Advanced Options](#)

[Create](#) [Cancel](#)


userNetwork	 Active	-	User NetworkAdmin	No	Wed, May 6, 2020, 10:38:52 UTC	
userVM	 Active	-	User VMs and Vault Admin	No	Wed, May 6, 2020, 10:40:53 UTC	


Showing 8 Items < Page 1 >

4.3.1 Create Passwords


The last step to perform here is to *Create Passwords* for these users.

1. In the OCI Console, on the left side click Menu – Identity – Users:
2. In the user list, select userNetwork
Click the tab Create/Reset Password

 ORACLE Cloud

Germany Central (Frankfurt) 

[Identity](#) » [Users](#) » [User Details](#) » [API Keys](#)

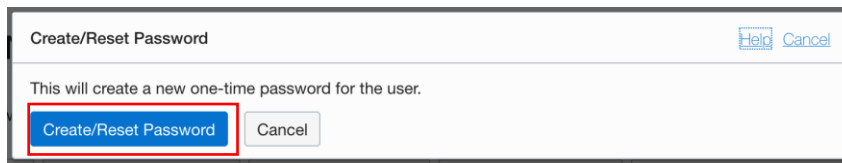


userNetwork

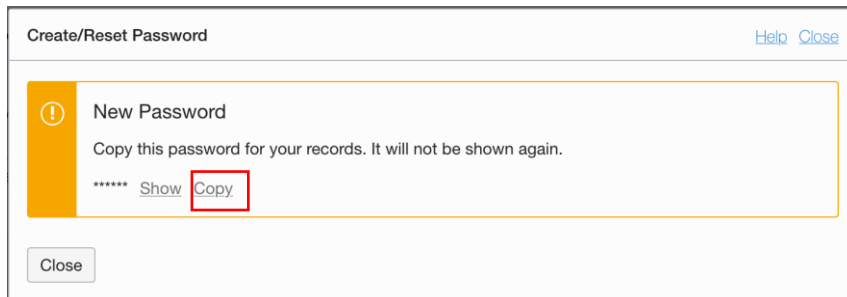
User belonging to CompTestNetwork

[Edit User](#)
[Create/Reset Password](#)
[Edit User Capabilities](#)
[Enable Multi-Factor Authentication](#)
[Add Tags](#)
[Delete](#)

3. Click Create/Reset Password in the pop-up window



4. Click in Copy and Paste the password in notepad.



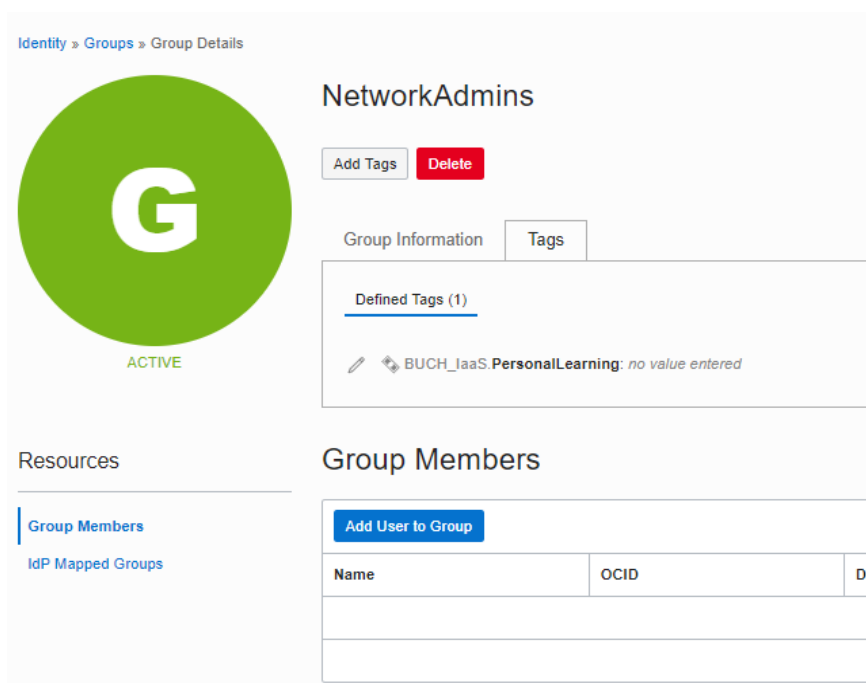
5. Perform the same steps for userVM.

4.4 Assign Users to their Groups

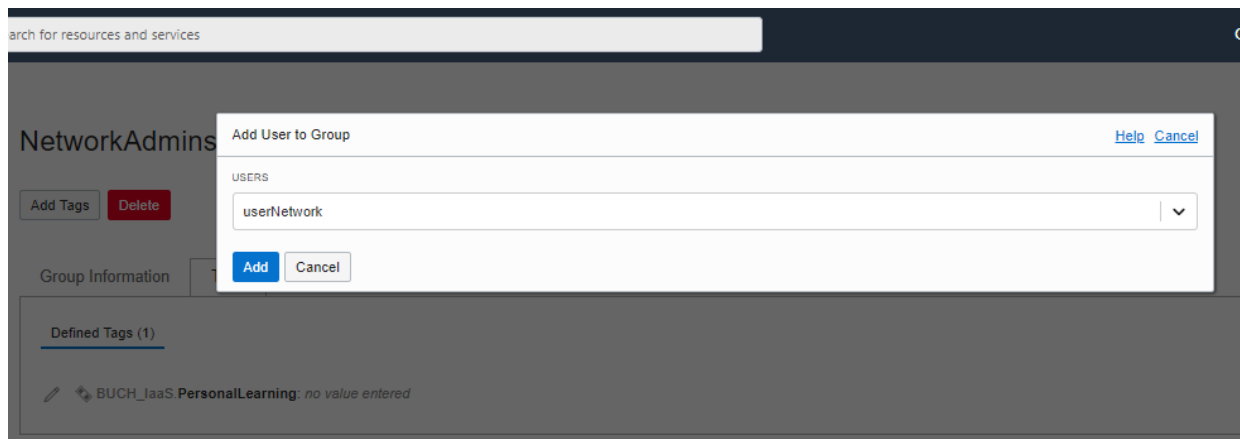
In this stage we will assign the above created users: userNetwork and userVM to their groups.

Therefore, we will assign userNetwork to the group NetworkAdmins and userVM to the groups InstanceAdmins, SecurityAdmins and ObjectAdmins.

1. In the OCI Console, on the left side click Menu - Identity – Groups and select the group: NetworkAdmins. You will be redirected to this Groups' Console:



- Click Add User to Group and select from the drop-down list the user: userNetwork



Repeat the same steps to add userVM to the groups: InstanceAdmins, SecurityAdmins and ObjectAdmins.

4.5 Policies

Specifies who can access which resources, and how. Access is granted by an administrator at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy.

4.5.1 Policy Syntax

Allow **<subject>** to **<verb>** **<resource-type>** in **<location>** where **<conditions>**

Verb	Type of access
inspect	Ability to list resources
read	Includes inspect + ability to get user-specified metadata/actual resource
use	Includes read + ability to work with existing resources (the actions vary by resource type)*
manage	Includes all permissions for the resource

* In general, this verb does not include the ability to create or delete that type of resource

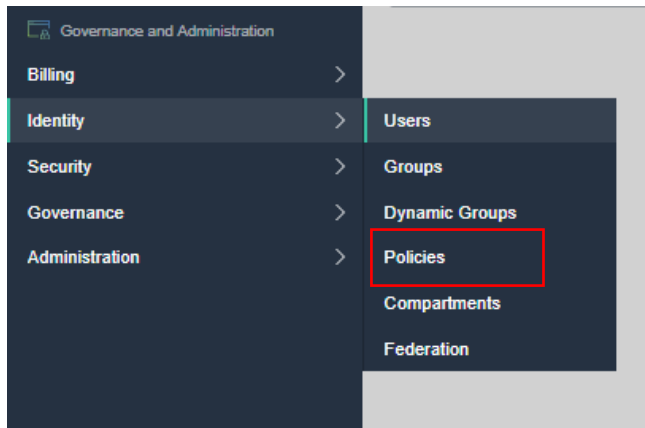
Aggregate resource-type	Individual resource type
all-resources	
database-family	db-systems, db-nodes, db-homes, databases
instance-family	instances, instance-images, volume-attachments, console-histories
object-family	buckets, objects
virtual-network-family	vcn, subnet, route-tables, security-lists, dhcp-options, and many more resources (link)
volume-family	volumes, volume-attachments, volume-backups
Cluster-family	clusters, cluster-node-pool, cluster-work-requests
File-family	file-systems, mount-targets, export-sets
dns	dns-zones, dns-records, dns-traffic,...

The IAM Service has no family resource-type, only individual ones

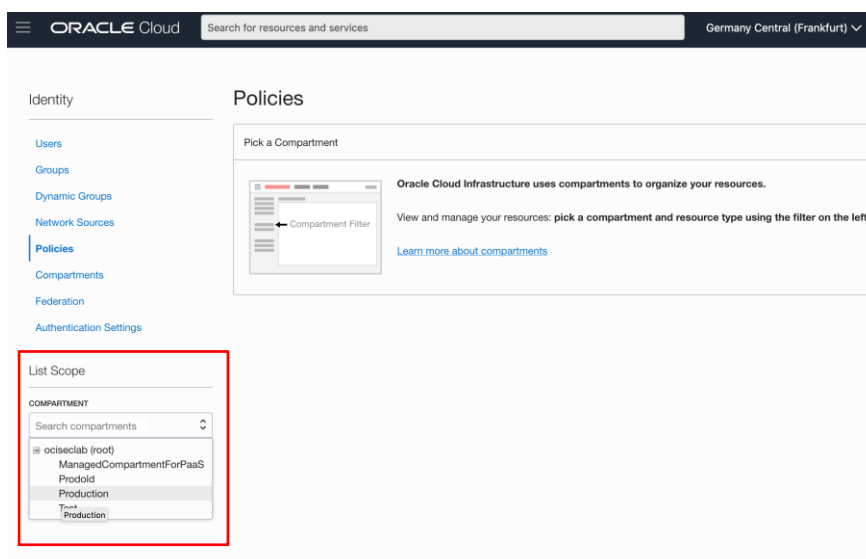
4.5.2 Policies for Network Resources

In this section we will provide permission to the group NetworkAdmins to manage network resources in the compartment Production.

1. In the OCI Console, on the left side click Menu – Identity – Policies:



2. In List Scope select *Production* Compartment, if not already selected



3. Click Create Policy and fill in the following fields:
 - o *Name* for the policy – Network_Policy
 - o A friendly *Description* - Allow the group NetworkAdmins to manage Network Components in compartment Production
 - o The *Policy Statement*:
 Allow **group NetworkAdmins** to **manage virtual-network-family** in **compartment Production**
 - o Click Create.

ORACLE Cloud Search for resources and services Germany Central (Frankfurt) ✓
Germany Central (Frankfurt)

Identity

Users
Groups
Dynamic Groups
Network Sources
Policies
Compartments
Federation
Authentication Settings

List Scope

COMPARTMENT
Production
ociseclab (root)/Production

Tag Filters [add](#) | [clear](#)
no tag filters applied

Policies in Production Compartment

Create Policy

Name	Description	Statements	Created
No items found.			

Create Policy [Help](#)

NAME
Network_Policy
No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION
Allow the group NetworkAdmins to manage Nwtwork Components in compartment Production

☒ KEEP POLICY CURRENT ☐ USE VERSION DATE

COMPARTMENT
Production
ociseclab (root)/Production

Policy Statements

STATEMENT 1
⋮ ^ v Allow group NetworkAdmins to manage virtual-network-family in compartment Production
[+ Another Statement](#)

[Show Advanced Options](#)

Create Cancel

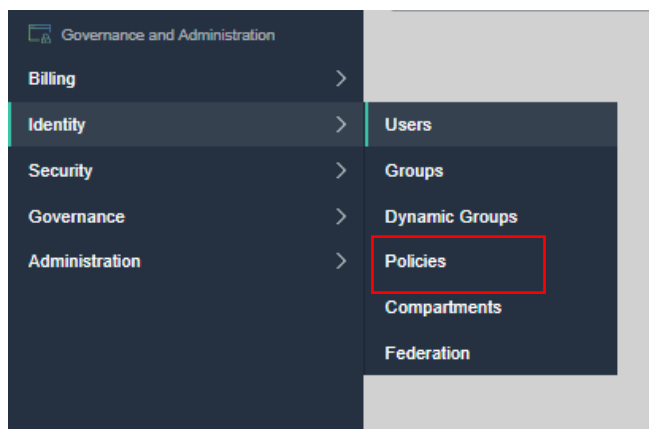
4.5.3 Policies for Compute Resources

Since we will create compute instances in OCI, we need to provide permissions for it.

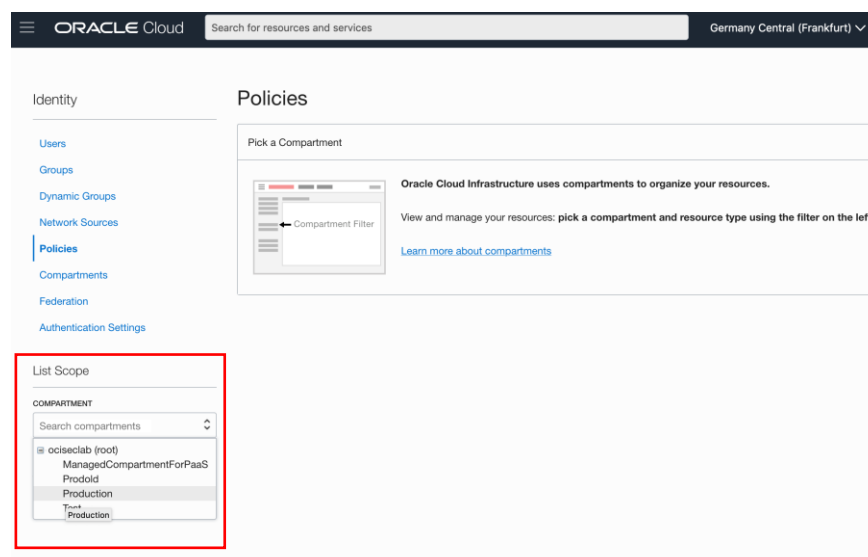
Hence, we will provide policies for the group InstanceAdmins to *manage* the *instance-family*.

Moreover, when creating the instances we will also need to choose the subnet where we will deploy them. For this purpose, we need to provide *inspect* rights for the group InstanceAdmins to the *virtual-network-family* resource type.

1. In the OCI Console, on the left side click Menu – Identity – Policies:



2. In List Scope select *Production* Compartment, if not already selected



3. Click Create Policy and fill in the following fields:
 - o *Name* for the policy – Instance_Policy
 - o A friendly *Description* - Allow the group InstanceAdmins to manage Instances Compute in compartment Production
 - o The *Policy Statement* – click in Another Statement for add second Policy Statement:

Allow **group InstanceAdmins** to **manage instance-family** in **compartment Production**

Allow **group InstanceAdmins** to **use virtual-network-family** in **compartment Production**

- Click Create.

ORACLE Cloud Search for resources and services Germany Central (Frankfurt) Germany Central (Frankfurt)

Identity

Users Groups Dynamic Groups Network Sources **Policies** Compartments Federation Authentication Settings

Create Policy

Name	Description	Statements	Created
No items found.			

List Scope

COMPARTMENT

Production

ociseclab (root)/Production

Tag Filters add | clear

no tag filters applied

Create Policy [Help](#)

NAME

Instance_Policy

No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION

Allow the group InstanceAdmins to manage Instances Compute in compartment Production

☒ KEEP POLICY CURRENT ☐ USE VERSION DATE

COMPARTMENT

Production

ociseclab (root)/Production

Policy Statements

STATEMENT 1

⋮ ^ v Allow group InstanceAdmins to manage instance-family in compartment Production

+ Another Statement

[Show Advanced Options](#)

Create [Cancel](#)

Create Policy [Help](#)

NAME
 Instance_Policy
No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION
 Allow the group InstanceAdmins to manage Instances Compute in compartment Production

☒ KEEP POLICY CURRENT ☐ USE VERSION DATE

COMPARTMENT
 Production
oci:seclab (root)/Production

Policy Statements

STATEMENT 1
 Allow group InstanceAdmins to manage instance-family in compartment Production

STATEMENT 2
 Allow group InstanceAdmins to use virtual-network-family in compartment Production

[+ Another Statement](#)

[Create](#) [Cancel](#)

4.5.4 Policies for OCI Vault Resources

In this section we will provide OCI Vault permissions to the group SecurityAdmins in the compartment Production.

Moreover, we will need to provide permissions to delegate key usage for the Block Volume service (during block volume encryption, Section [4.2](#)) and for the Object Storage service (Section [5.1](#))

1. Access as in the previous section Menu – Identity – Policies and Create Policy
2. In List Scope select *Production* Compartment, if not already selected
3. Provide a *Name* for the policy: Vault_Policy and eventually a description - Allow the group SecurityAdmins to manage Vaults, Keys in compartment Production
4. Fill in the following statements to provide permissions to create Vaults and Keys for the group SecurityAdmins:

```
Allow group SecurityAdmins to manage vaults in compartment
Production
Allow group SecurityAdmins to manage keys in compartment
Production
Allow group SecurityAdmins to use key-delegate in compartment
Production
Allow service blockstorage, objectstorage-eu-frankfurt-1 to
use keys in compartment Production
```

5. Click Create

Create Policy [Help](#)

COMPARTMENT
 Production
 ociseclab (root)/Production

Policy Statements

STATEMENT 1
 Allow group SecurityAdmins to manage vaults in compartment Production

STATEMENT 2
 Allow group SecurityAdmins to manage keys in compartment Production

STATEMENT 3
 Allow group SecurityAdmins to use key-delegate in compartment Production

STATEMENT 4
 Allow service blockstorage, objectstorage-eu-frankfurt-1 to use keys in compartment Production

[+ Another Statement](#)

[Show Advanced Options](#)

Create [Cancel](#)

4.5.5 Policies for Object Storage Resources

1. As in the previous sections, access Menu – Identity – Policies and Create Policy
2. In List Scope select *Production* Compartment, if not already selected
3. Provide a *Name* for the policy: Object_Policy and eventually a friendly *Description* - Allow the group ObjectAdmins to manage ObjectStorage in compartment Production
4. Fill in the following statement to provide permission to the Object Storage resources for the group ObjectAdmins in the compartment Production:

Allow **group ObjectAdmins** to **manage object-family** in **compartment Production**

The screenshot shows the 'Create Policy' interface in the Oracle Cloud console. At the top, there's a title 'Create Policy' and a 'Help' link. The form is divided into several sections: 'NAME' with a text input containing 'Object_Policy' and a note 'No spaces. Only letters, numerals, hyphens, periods, or underscores.'; 'DESCRIPTION' with a text area containing 'Allow the group ObjectAdmins to manage ObjectStorage in compartment Production'; a section for policy versioning with two radio buttons, 'KEEP POLICY CURRENT' (selected) and 'USE VERSION DATE'; a 'COMPARTMENT' dropdown menu showing 'Production' with a path 'oci.seclab (root)/Production' below it; a 'Policy Statements' section with a list containing 'STATEMENT 1' and a text input 'Allow group ObjectAdmins to manage object-family in compartment Production', along with a '+ Another Statement' button; and a 'Show Advanced Options' link. At the bottom are 'Create' and 'Cancel' buttons.

Create Policy [Help](#)

NAME
Object_Policy
No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION
Allow the group ObjectAdmins to manage ObjectStorage in compartment Production

☒ KEEP POLICY CURRENT ☐ USE VERSION DATE

COMPARTMENT
Production
oci.seclab (root)/Production

Policy Statements

STATEMENT 1
⋮ ^ v Allow group ObjectAdmins to manage object-family in compartment Production

+ Another Statement

[Show Advanced Options](#)

Create Cancel

4.6 Summary

So far we have created 2 users (userVM and userNetwork) and 4 groups (NetworkAdmins, InstanceAdmins, SecurityAdmins, ObjectAdmins).

Afterwards we have assigned these users to their corresponding groups, where will be applied certain type of policies that will *allow* or implicitly *deny* access to specific cloud resources. The goal here is to simulate a real-life configuration in the cloud.

Good job so far, and let's proceed now to the Networking part.

5 OCI NETWORKING

When you work with Oracle Cloud Infrastructure, one of the first steps is to set up a virtual cloud network (VCN) for your cloud resources. This topic gives you an overview of Oracle Cloud Infrastructure Networking components and typical scenarios for using a VCN.

5.1 Introduction

A Virtual Cloud Network (VCN) is a virtual version of a traditional network—including subnets, route tables, and gateways—on which your instances run. A cloud network resides within a single region but can cross multiple Availability Domains.

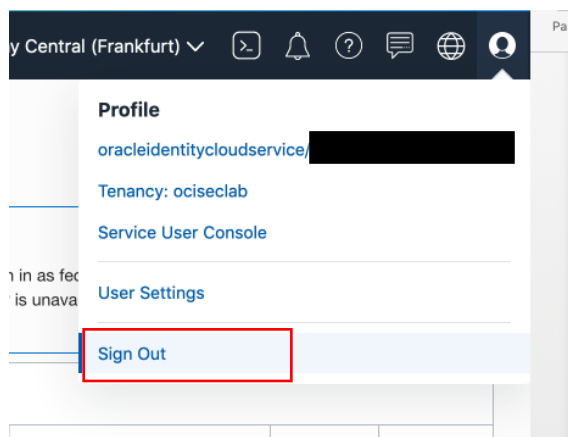
You can configure the cloud network with an optional Internet Gateway to handle public traffic, and an optional IPSec VPN connection to securely extend your on-premises network.

In the previous chapter we have defined the user – userNetwork and assign it to the group NetworkAdmins. Therefore, we can now test if the policies applied for this group are functional and also learn more about OCI Networking.

5.2 Access to OCI

Access the OCI Console using the user – userNetwork.

1. Sign out with your current user (default administrator user) and log in with userNetwork and the password paste in notepad from the previous step (Par. 4.3.1)



❗ You are now logged out of the Oracle Cloud Infrastructure Console.

Signing in to cloud tenant:
ociseclab
[Change tenant](#)

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

IDENTITY PROVIDER

[Continue](#)

or

Oracle Cloud Infrastructure **❗**

The login is uncommon for federated accounts. If you have questions, please review the [FAQ](#) or contact your tenancy administrator.


USER NAME

PASSWORD

[Sign In](#) [Forgot password?](#)

- At your first sign in with this user, a password change will be required. Please follow the instructions:

ORACLE Cloud Infrastructure



CHANGE PASSWORD

Change Your Password

You must change your password either because this is your first time signing in, your password was reset, or you opted to change it.

Current Password

New Password

Confirm New Password

[Save New Password](#)

Password requirements:

- 12 or more characters
- at least one lowercase letter
- at least one uppercase letter
- at least one number
- at least one special character
- must not contain your username

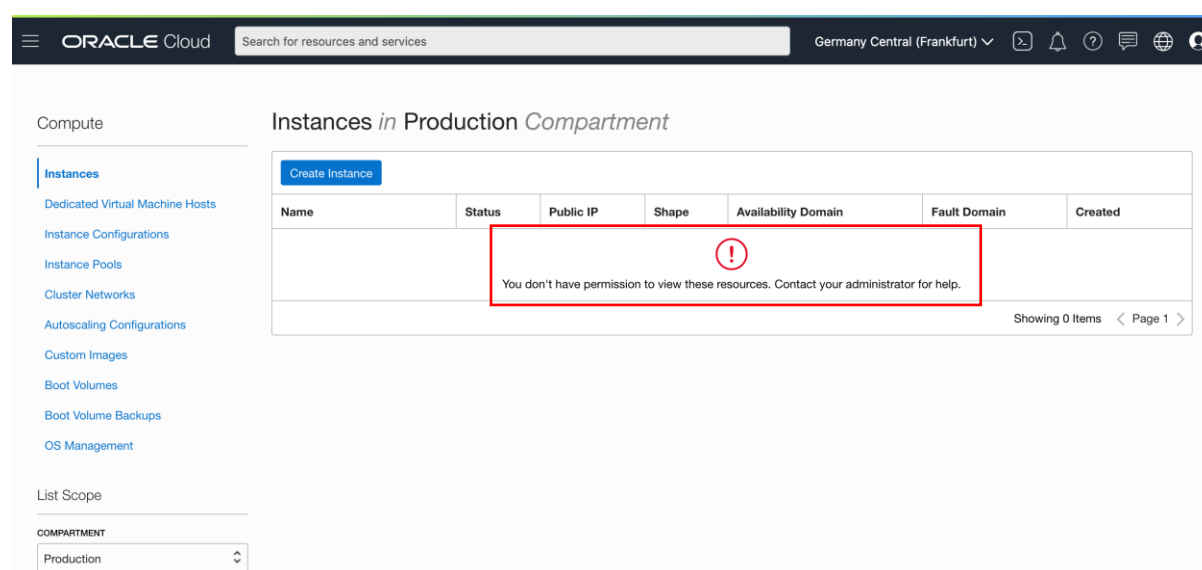
- After a successful log in, the OCI Console will be displayed

5.3 Test User Permissions

Since we have provided permissions to access networking resources to the group NetworkAdmins in the compartment Production, to which userNetwork belongs, at this point we are able to create only Network Components (ex. VCN).

For test permissions, we will try to create Compute Instance in OCI Console

1. In the OCI Console, on the left side click Menu – Compute – Instances.
2. On the left choose the compartment Production
3. User don't have permission to access to Compute Instance.



5.4 Create VCN

For this purpose, we will use the *VCN Wizard*:

What this wizard does:

- Creates a VCN.
- Creates an Internet Gateway, NAT Gateway, and Service Gateway for the VCN.
- Creates a regional public subnet with routing to the internet gateway. Instances in a public subnet may optionally have public IP addresses.
- Creates a regional private subnet with routing to the NAT gateway and service gateway (and therefore the Oracle Services Network). Instances in a private subnet cannot have public IP addresses.
- Sets up basic security list rules for the two subnets, including SSH access

1. In the OCI Console, on the left side click Menu – Networking – Virtual Cloud Networks
2. On the left choose the compartment Production (as in the image below)

- Click the tab Start VCN Wizard

Networking

Overview

Virtual Cloud Networks

Dynamic Routing Gateways

Customer-Premises Equipment

IPSec Connections

Load Balancers

FastConnect

Public IPs

DNS Zone Management

TSIG Keys

Traffic Management Steering Policies

HTTP Redirects

List Scope

COMPARTMENT

Production

ociseclab (root)/Production

Virtual Cloud Networks *in Production Compartment*

Create VCN Start VCN Wizard

Name	State	CIDR Block

- In the Wizard click Start VCN Wizard and select VCN with Internet Connectivity.
 - In the dialog box click Start VCN Wizard

Start VCN Wizard

Help Cancel

VCN with Internet Connectivity

VCN with Internet Connectivity and Site-to-Site VPN Connect

VCN

Public Subnet

Private Subnet

IG

NAT

SG

Internet

Oracle Services Network

Creates a VCN with a public subnet that can be reached from the internet. Also creates a private subnet that can connect to the internet through a NAT gateway, and also privately connect to the Oracle Services Network.

Includes: VCN, public subnet, private subnet, internet gateway (IG), NAT gateway (NAT), service gateway (SG).

Start VCN Wizard Cancel

- Fill in the fields with:
 - VCN NAME: Choose a name for your VCN (ex.: VCN-add your initials)

- Choose the compartment Production
- Leave the default values for VCN, PUBLIC SUBNET and PRIVATE SUBNET CIDR BLOCK
- Click Next

Basic Information

VCN NAME ⓘ
VCN-VBA

COMPARTMENT ⓘ
Production
ociseclab (root)/Production

Configure VCN and Subnets

VCN CIDR BLOCK ⓘ
10.0.0.0/16
If you plan to peer this VCN with another VCN, the VCNs must not have overlapping CIDRs. [Learn more.](#)

PUBLIC SUBNET CIDR BLOCK ⓘ
10.0.0.0/24
The subnet CIDR blocks must not overlap.

PRIVATE SUBNET CIDR BLOCK ⓘ
10.0.1.0/24
The subnet CIDR blocks must not overlap.

DNS RESOLUTION
☒ USE DNS HOSTNAMES IN THIS VCN
Required for instance hostname assignment if you plan to use VCN DNS or a third-party DNS. This choice cannot be changed after the VCN is created. [Learn more.](#)

6. You will see the Review and Create page with all the info of your VCN and its related resources. Click Create
7. In the end you will see the progress of the VCN creation:

Create a VCN with Internet Connectivity

1 Configuration
2 **Review and Create**

Virtual Cloud Network creation complete

▶ Create Virtual Cloud Network (1 resolved)	Done
▶ Create Subnets (2 resolved)	Done
▶ Create Internet Gateway (1 resolved)	Done
▶ Create NAT Gateway (1 resolved)	Done
▶ Create Service Gateway (1 resolved)	Done
▶ Create Route Table for Private Subnet (1 resolved)	Done
▶ Create Security List for Private Subnet (1 resolved)	Done
▶ Update Route Tables (2 resolved)	Done
▶ Update Private Subnet (1 resolved)	Done

[View Virtual Cloud Network](#)

- Click View Virtual Cloud Network and you will be redirected to the VCN Console, where you can see on the left side all resources associated to your VCN.
Let's go through all of them in order to understand better their purpose.

The screenshot shows the Oracle Cloud VCN Console interface. At the top, there's a navigation bar with the Oracle Cloud logo and a search bar. Below the navigation bar, the breadcrumb trail reads: Networking » Virtual Cloud Networks » Virtual Cloud Network Details.

The main content area is titled "VCN-VBA". On the left, there's a large green hexagon with "VCN" inside, and below it, the status "AVAILABLE". To the right of the hexagon, there are three buttons: "Move Resource", "Add Tags", and "Terminate".

Below the buttons, there's a tabbed interface with "VCN Information" and "Tags". The "VCN Information" tab is active, showing the following details:

- CIDR Block: 10.0.0.0/16
- Compartment: Production
- Created: Tue, Apr 28, 2020, 13:08:13 UTC

On the left side of the console, there's a "Resources" section with a list of resource types and their counts:

- Subnets (2)
- Route Tables (2)
- Internet Gateways (1)
- Dynamic Routing Gateways (0)
- Network Security Groups (0)
- Security Lists (2)
- DHCP Options (1)
- Local Peering Gateways (0)
- NAT Gateways (1)
- Service Gateways (1)

The "Subnets" section is expanded, showing a table of subnets in the "Production" compartment. The table has columns for Name, State, and CIDR Block. There are two subnets listed:

Name	State	CIDR Block
Private Subnet-VCN-VBA	Available	10.0.1.0/24
Public Subnet-VCN-VBA	Available	10.0.0.0/24

5.5 Subnets

Each subnet in a VCN consists of a contiguous range of IPv4 addresses that do not overlap with other subnets in the VCN.

Subnets act as a unit of configuration: all instances in a given subnet use the same route table, security lists, and DHCP options.

Subnets can be either public or private, therefore in a private subnet all instances will have private IPv4 addresses and those in a public subnet can also have public IPv4 addresses, but it's up to the user if he wants to assign to it a public address.

- In the [VCN Console](#), on the left click Subnets:

Resources

Subnets (2)

Route Tables (2)

Internet Gateways (1)

Dynamic Routing Gateways (0)

Network Security Groups (0)

Security Lists (2)

DHCP Options (1)

Local Peering Gateways (0)

NAT Gateways (1)

Service Gateways (1)

You can notice that we have 2 subnets: *Private* and *Public*

Subnets *in* Production *Compartment*


Create Subnet			
Name	State	CIDR Block	Subnet Access
Private Subnet-VCN-VBA	● Available	10.0.1.0/24	Private (Regional)
Public Subnet-VCN-VBA	● Available	10.0.0.0/24	Public (Regional)

2. Select the Private Subnet, where you can see all the details associated to this subnet.
3. On the bottom you can see the *Security List* associated to this subnet. They act as a virtual firewall, where we can define which protocols may be allowed in this subnet.
In the *Security Lists* section, click the Security List associated with your subnet (in this case it's *Security List for Private Subnet-VCN-VBA*)

Networking > Virtual Cloud Networks > VCN-VBA > Subnet Details

Private Subnet-VCN-VBA

[Edit](#)
[Move Resource](#)
[Add Tags](#)
[Terminate](#)



Subnet Information Tags

OCID: ...377nha [Show](#) [Copy](#)
 CIDR Block: 10.0.1.0/24
 Virtual Router Mac Address: 00:00:17:4B:82:BA
 Subnet Type: Regional

Compartment: Production
 DNS Domain Name: sub04281306591... [Show](#) [Copy](#)
 Subnet Access: Private Subnet
 DHCP Options: [Default DHCP Options for VCN-VBA](#)
 Route Table: [Route Table for Private Subnet-VCN-VBA](#)

Resources

Security Lists (1)

Tag Filters [add](#) / [clear](#)
no tag filters applied

Add Security List

Name	State	Compartment
Security List for Private Subnet-VCN-VBA	● Available	Production

4. In this console we can observe the default Security Rules which have been created to allow certain type of protocols.

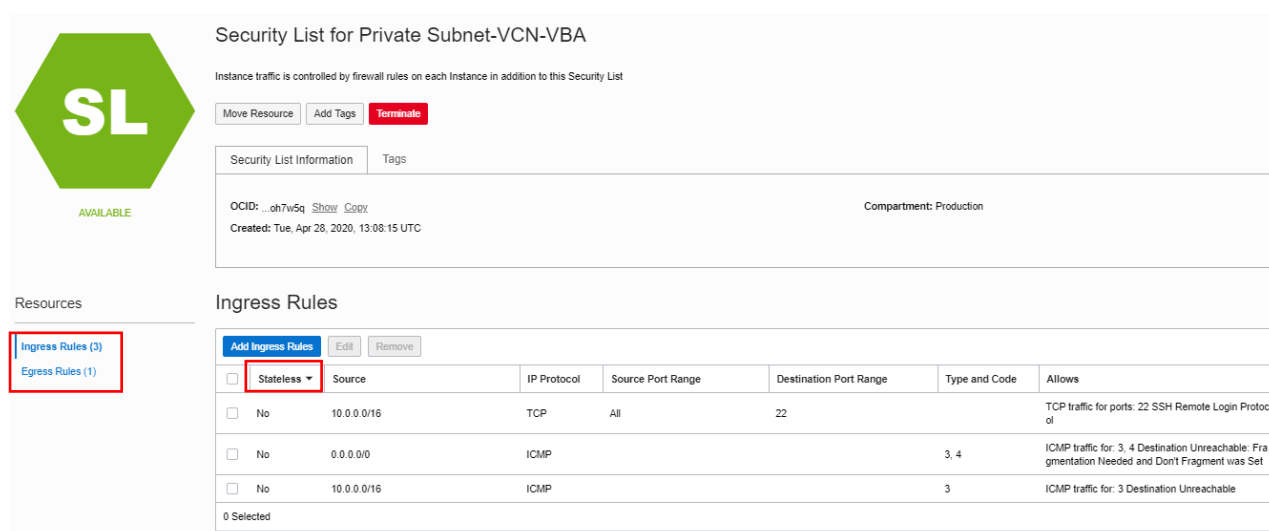
On the left are the Ingress and Egress Rules. Hence, they refer to the incoming traffic to the subnets (*Ingress Rules*) and the outgoing traffic from the subnets (*Egress Rules*).

The rules can also be stateful (for any traffic matching a rule, will also be allowed by default the response to the originating host) and stateless (the response traffic is not automatically allowed). For more info please visit [Stateful vs Stateless](#).

We can also observe the *Source IPv4 address* in these rules, which is the origin IPv4 address block from which we expect the traffic to come (0.0.0.0/0 will allow all sources).

Also, we can see the *type of IP Protocol* allowed: *TCP*, *ICMP*.

The *source and destination port range* which represent the source port from which the traffic will come and to which destination port (i.e. the destination protocol)



Security List for Private Subnet-VCN-VBA

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

Move Resource Add Tags Terminate

Security List Information Tags

OCID: ...oh7w5q Show Copy Compartment: Production

Created: Tue, Apr 28, 2020, 13:08:15 UTC

Resources

Ingress Rules (3)
Egress Rules (1)

Ingress Rules

Add Ingress Rules Edit Remove

<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows
<input type="checkbox"/>	No	10.0.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable

0 Selected

- Ingress Rule: The first rule has the *Destination Port Range*= 22 (for TCP it's the SSH Protocol), hence all the incoming SSH connections from the 10.0.0.0/16 network (which is our public subnet in the VCN) with any source range ports will be allowed to our subnets.

<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	10.0.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	

This rule is used by default, because the only way to access instances, using SSH, in our private network is through instances in our public subnet.

Therefore, we have opened this type of traffic. We will perform some tests in the next chapters with this rule, to show you how we can block the SSH traffic to our private subnet.

- Egress Rule: This rule allows all outgoing traffic from the subnet to all the destinations (0.0.0.0/0 is the any IPv4 address)

Egress Rules

Add Egress Rules Edit Remove							
<input type="checkbox"/>	Stateless	Destination	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows
<input type="checkbox"/>	No	0.0.0.0/0	All Protocols				All traffic for all ports
0 Selected							

- The same steps can be performed for the Public Subnet in our VCN.
Go back to the [subnet](#) list and select our Public Subnet-VCN then select the Default Security List for VCN:

Resources		Ingress Rules					
Ingress Rules (3) Egress Rules (1)		Add Ingress Rules Edit Remove					
<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	22		
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	
0 Selected							

Here, we also have the Ingress and Egress Rules. The concepts are the same as in the previous case: *allow traffic in and out for certain type of protocols*.

5.6 Virtual Routers in OCI

5.6.1 Internet Gateway

An Internet Gateway is a virtual router that connects the edge of the VCN with the Internet.

For example, it will allow us to connect to our compute instances in OCI via SSH, from our local PC (in the next chapters).

In the [VCN Console](#) select Internet Gateways, where you will see the IG of your VCN:

Resources		Internet Gateways <i>in Production Compartment</i>	
Subnets (2) Route Tables (2) Internet Gateways (1) Dynamic Routing Gateways (0) Network Security Groups (0) Security Lists (2) DHCP Options (1) Local Peering Gateways (0)		Create Internet Gateway	
		Name	State
		Internet Gateway-VCN-VBA	● Available

On the left, under Resources, select Route Tables – Default Route Table for VCN:

Resources

Route Rules

Route Rules (1)

Add Route Rules Edit Remove

<input type="checkbox"/>	Destination	Target Type	Target
<input type="checkbox"/>	0.0.0.0/0	Internet Gateway	Internet Gateway-VCN-VBA

0 Selected

The route rules from the Route Tables, look and act like the traditional network route rules, where you have a *Destination CIDR Block* and the *Next Hop (Target)*.

Each subnet has a single route table.

In this specific case, all the traffic from the public subnet will go through the IG and then to all IP addresses matching the Destination (in this case it's the *All IPv4 Address: 0.0.0.0/0*)

5.6.2 NAT Gateway

You can add a NAT gateway to your VCN to give instances in a private subnet access to the internet.

Instances in a private subnet don't have public IP addresses. With the NAT gateway, they can initiate connections to the internet and receive responses, but not receive inbound connections initiated from the internet.

In the [VCN Console](#), on the left under Resources, select Route Tables – Route Table for Private Subnet VCN:

Resources

Route Rules

Route Rules (2)

Add Route Rules Edit Remove

<input type="checkbox"/>	Destination	Target Type	Target
<input type="checkbox"/>	0.0.0.0/0	NAT Gateway	NAT Gateway-VCN-VBA

As in the previous case, with the [IG](#), here all traffic from the private subnet will be routed through the NAT Gateway (*Next Hop*) to the Internet (*Destination*) using the *All IPv4 address: 0.0.0.0/0*

5.6.3 Service Gateway

A Service Gateway (SG) lets your VCN privately access specific Oracle services without exposing the data to the public internet.

No IG or NAT is required to reach those specific services. The resources in the VCN can be in a private subnet and use only private IP addresses. The traffic from the VCN to the Oracle service travels over the Oracle network fabric and never traverses the internet.

In the [VCN Console](#), on the left under Resources, select Route Tables – Route Table for Private Subnet VCN:

<input type="checkbox"/>	Destination	Target Type	Target
<input type="checkbox"/>	0.0.0.0/0	NAT Gateway	NAT Gateway-VCN-VBA
<input type="checkbox"/>	All FRA Services In Oracle Services Network	Service Gateway	Service Gateway-VCN-VBA

0 Selected

As in the previous cases, all traffic from the private subnet will go through the SG (*Next Hop*) to the *All FRA Services in Oracle Services Network* (*Destination*), which is a *service CIDR label* to represent all regional cloud services in the region Frankfurt (If you choose another region it will be the services from that specific region)

5.7 Summary

In this chapter we have created a VCN with its related resources: *Public Subnet*, *Private Subnet*, *Internet Gateway*, *Service Gateway*, *NAT Gateway*, *Route Rules*, *Security Lists*, etc.

We have analysed the function of each one of them and their similarities with traditional networking concepts.

6 OCI VAULT

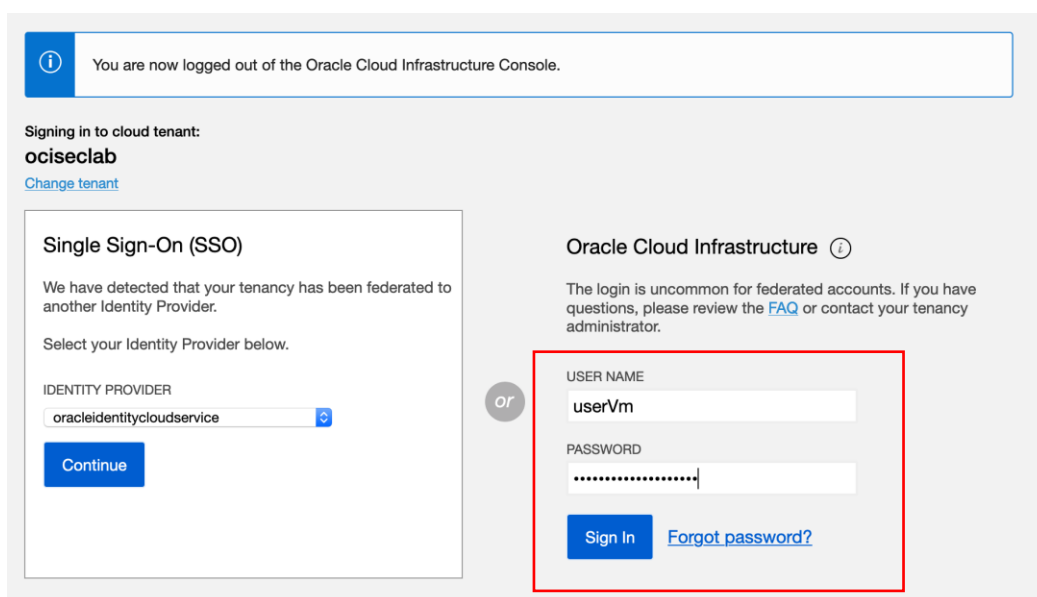
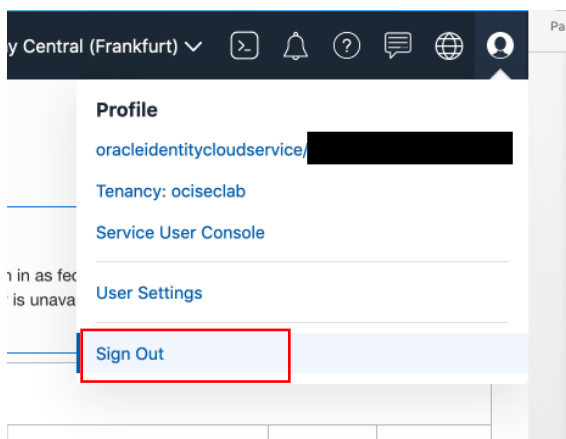
The Vault service lets you create vaults in your tenancy as containers for encryption keys and secrets. If needed, a virtual private vault provides you with a dedicated partition in a hardware security module (HSM), offering a level of storage isolation for encryption keys that's effectively equivalent to a virtual independent HSM.

At this point we will use userVM since we have provided privileges to this user to create vaults and keys.

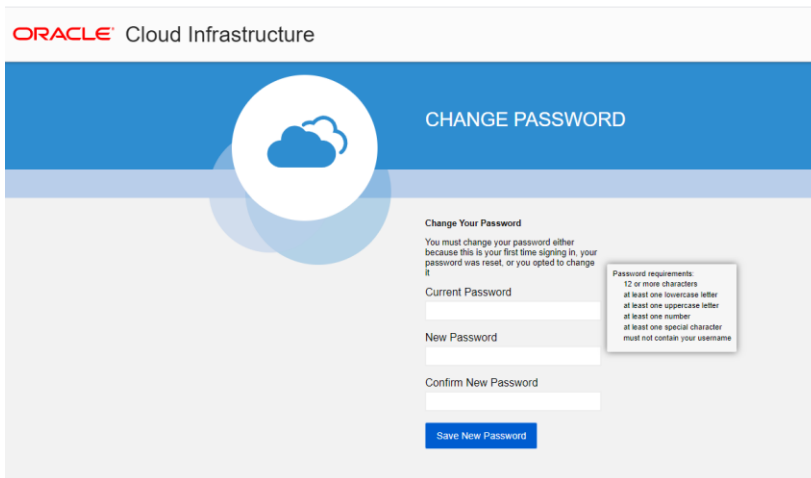
6.1 Access to OCI

Access the OCI Console using the user – userVM.

4. Sign out with your current user (default administrator user) and log in with userVM and the password paste in notepad from the previous step (Par. 4.3.1)



- At your first sign in with this user, a password change will be required. Please follow the instructions:



ORACLE Cloud Infrastructure

CHANGE PASSWORD

Change Your Password
You must change your password either because this is your first time signing in, your password was reset, or you opted to change it.

Current Password

New Password

Confirm New Password

[Save New Password](#)

Password requirements:
12 or more characters
at least one lowercase letter
at least one uppercase letter
at least one number
at least one special character
must not contain your username

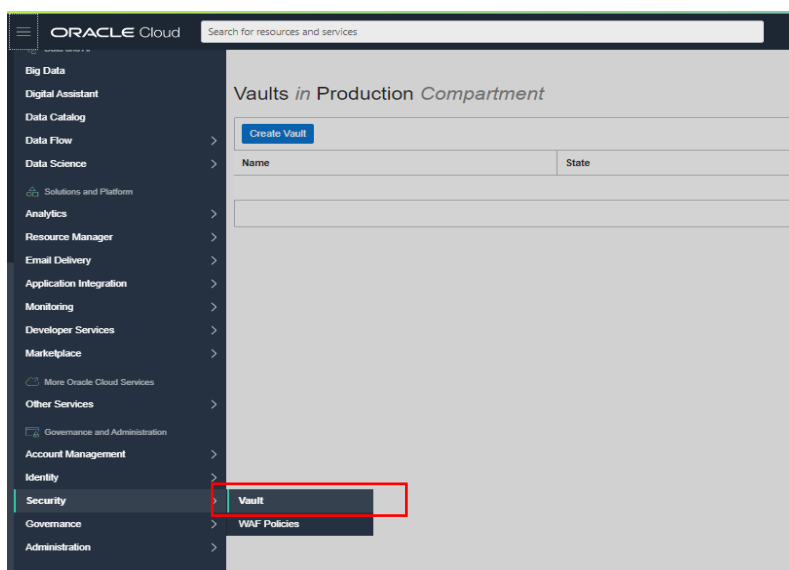
- After a successful log in, the OCI Console will be displayed

6.2 User Permissions

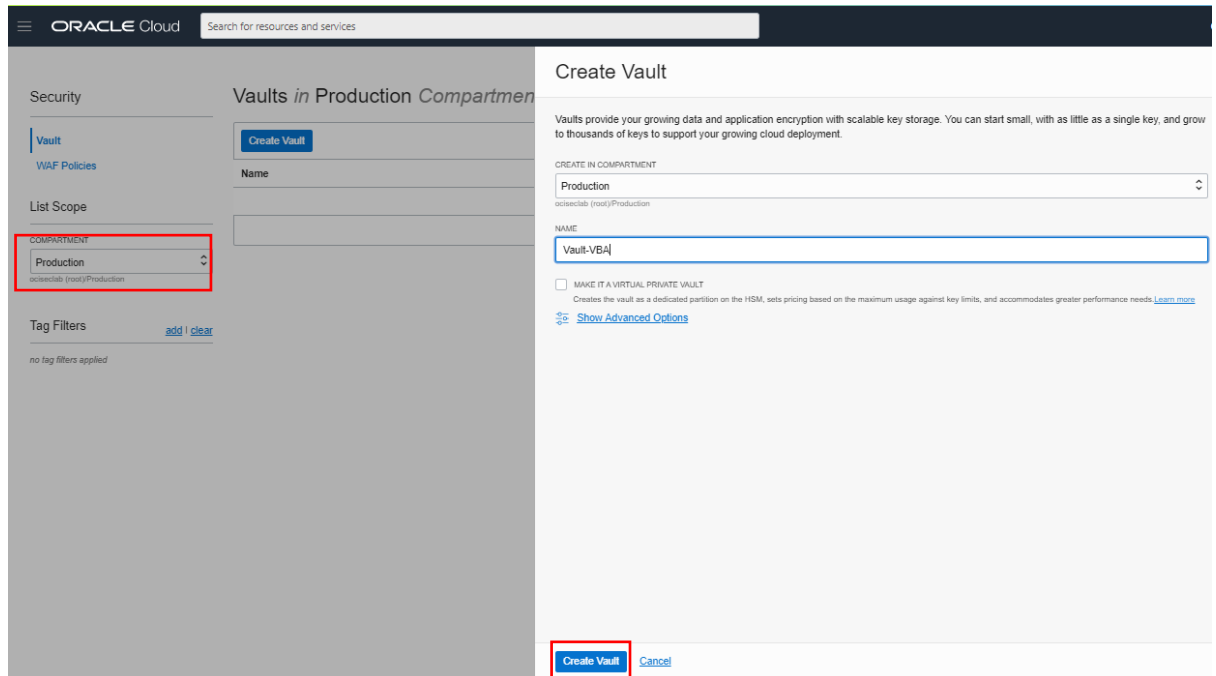
Since we have provided permissions to access OCI Vault to the group SecurityAdmins in the compartment Production, to which userVM belongs, at this point we are able to manage OCI Vault

6.3 Create Vault

- In the OCI Console, on the left side click Menu – Security – Vault:



2. On the left choose the compartment Production and click Create Vault:
 - NAME: Select a name for your vault (ex.: Vault_Your initials)
 - Click Create Vault



6.4 Create Key

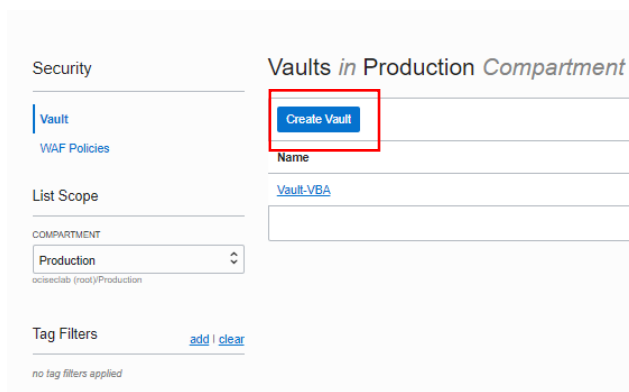
Keys are logical entities that represent one or more key versions that contain the cryptographic material used to encrypt and decrypt data, protecting the data where it is stored.

After the creation of the Vault (as described in [Section 3.2](#)), now we can access it and create Keys. For our purpose we will need 2 keys:

- One key for encrypting the Block Volume of our VM
- Another key for encrypting the buckets in Object Storage

These steps will be described in the next chapters.

Click the Vault that we've just created:



You will be redirected to the Vault console, where you can see the Vault Information and at the bottom the resources associated to this Vault.

1. Click Create Key

Security > Vaults > Vault Details

Vault-VBA

ACTIVE

Edit Name Move Resource Add Tags Delete Vault

Vault Information Tags

General Information

Compartment: ociseclab (root)/Production
 OCID: ...fk3biq [Show](#) [Copy](#)
 Created: Thu, Apr 30, 2020, 11:39:55 UTC
 Total HSM Keys: 1
 Total HSM Key Versions: 1

Wrapping Key Information

Public Wrapping Key: ...PUBLIC KEY—
 OCID: ...72t5qq [Show](#) [Copy](#)
 Type: RSA
 Date Modified: Thu, Apr 30, 2020, 11:40:03 UTC

Resources

Keys Secrets

Keys in Production *Compartment*

Create Key

Name	State
------	-------

2. Fill in the required fields:

- In *Create Compartment* choose Production
- Click Name, and then enter a name to identify the key: VM-Key
- Leave the *Key Shape Length* to 128 bits
- Click Create Key

Create Key

CREATE IN COMPARTMENT

Production

NAME

VM-Key

KEY SHAPE: ALGORITHM

AES

KEY SHAPE: LENGTH

128 bits

☐ IMPORT EXTERNAL KEY

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

[Show Advanced Options](#)

Create Key Cancel

- Repeat the same steps to create the second key (*Object-Key*) for Object Storage:

Create Key

CREATE IN COMPARTMENT

Production

ociseclab (root)/Production

NAME

Object-Key

KEY SHAPE: ALGORITHM

AES

KEY SHAPE: LENGTH

128 bits

☐ IMPORT EXTERNAL KEY

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

[Show Advanced Options](#)

Create Key [Cancel](#)

At this point we have created 2 keys: VM-Key and Object-Key, which will be used in the next chapters for our encryption purposes.

Resources	Keys in Production <i>Compartment</i>	
Keys	Create Key	
Secrets		
List Scope		
COMPARTMENT		
	Name	State
	Object-Key	● Enabled
	VM-Key	● Enabled

For more info about Vaults and Keys, please visit:

<https://docs.cloud.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm>

7 CREATE VIRTUAL MACHINES

VM instances offer compute resources in many shapes. A shape is a template that determines the number of CPUs (in OCI we call them OCPUs), amount of memory, and other resources allocated to a newly created instance.

Our purpose is to create 1 VM in the public subnet and 1 VM in the private subnet.

The VM in the public subnet will have the role of a Bastion Host. Its purpose is to add a multi-tiered security approach to our network. It will act as a firewall for the resources in the private subnet, since it is the first host (with a public IPv4 address) through which the traffic from the Internet will pass.

7.1 Access to OCI

Access the OCI Console using the user – userVM.

7.2 User Permissions

Since we have provided permissions to access OCI Compute Instances to the group InstanceAdmins in the compartment Production, to which userVM belongs, at this point we are able to manage OCI Compute Instances.

7.3 Create SSH Key Pair

Instances use an SSH key pair instead of a password to authenticate a remote user. A key pair file contains a private key and a public key. You keep the private key on your computer and provide the public key when you create an instance.

To create key pairs, you can use a third-party tool such as OpenSSH on UNIX-style systems (including Linux, Solaris, BSD, and OS X) or PuTTY Key Generator on Windows.

Follow the instructions in the link below to create an SSH Key pair.

<https://docs.cloud.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingkeys.htm#>

If you have a UNIX-style OS, click the option: *Creating an SSH Key Pair on the Command Line*.

If you are using a Windows OS, click the option: *Creating an SSH Key Pair on Windows Using PuTTY Key Generator, but you'll need to download PuTTY before (download [here](#))* and use the PuTTYgen component of PuTTY.

In the end you will have a private and a public key which will be used to connect to our instances.

7.4 Create Instances

We will create two VMs:

- Bastion VM in public subnet with Public IP
- Internal VM in private subnet with Internal IP

7.4.1 BastionVM

In the OCI Console, on the left side click Menu – Compute – Instances.

1. On the left choose the compartment Production, and click Create Instance:

Compute

Instances

- Dedicated Virtual Machine Hosts
- Instance Configurations
- Instance Pools
- Cluster Networks
- Autoscaling Configurations
- Custom Images
- Boot Volumes
- Boot Volume Backups
- OS Management

Instances in Production Compartment

Create Instance

Name	Status

List Scope

COMPARTMENT

Production

ociseclab (root)/Production

- Enter a *Name* for the instance: *BastionVM*
- Leave the OS to Oracle Linux 7.8
- Click Show Shape, Network and Storage Options

Create Compute Instance

NAME

BastionVM

Image or operating system ⓘ

ORACLE Linux

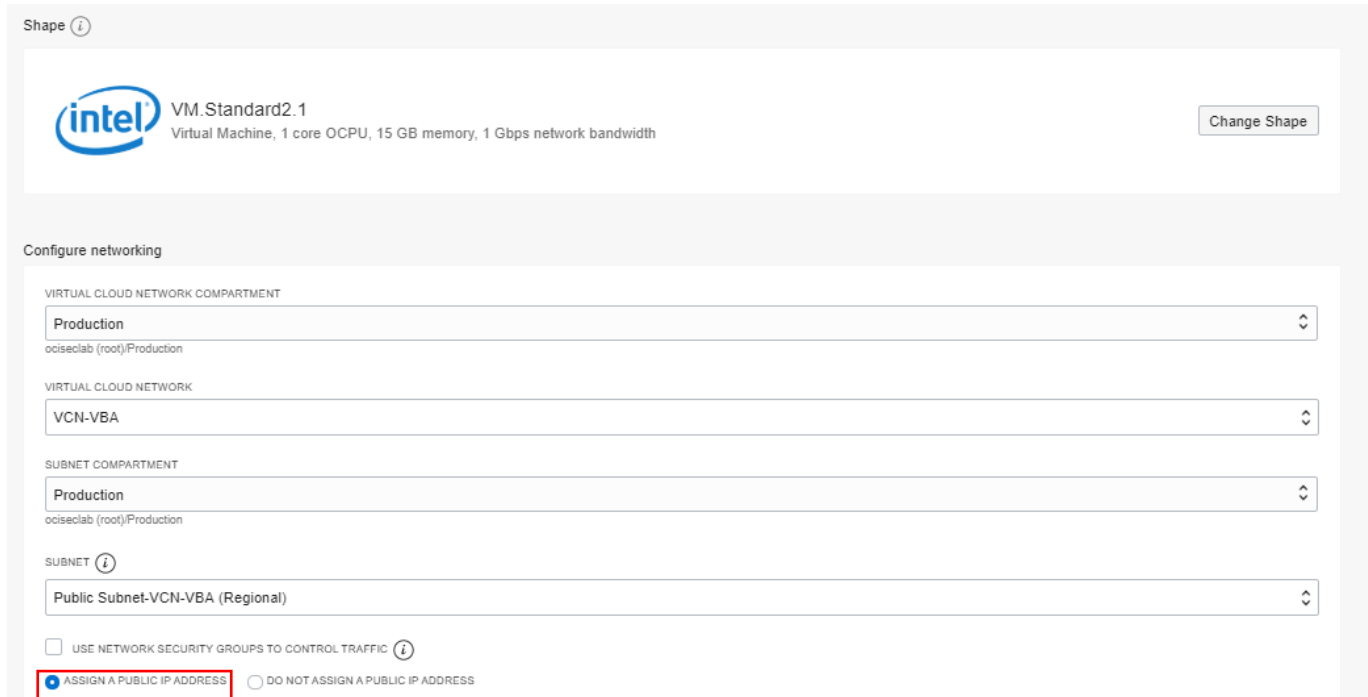
Oracle Linux 7.8
Image Build: 2020.04.17-0

Change Image

Show Shape, Network and Storage Options

4. Enter the following details:

- Shape: *VM.Standard2.1*
- Virtual Cloud Network Compartment: *Production*
- Virtual Cloud Network: *The VCN created in [Section](#)*
- Subnet Compartment: *Production*
- Subnet: *The Public Subnet in [Section](#)*
- Assign a Public IP Address: *Select this option (this instance requires a public IP)*



The screenshot shows the Oracle VM configuration interface. The 'Shape' section displays the 'VM.Standard2.1' shape with an Intel logo and a 'Change Shape' button. The 'Configure networking' section contains several dropdown menus: 'VIRTUAL CLOUD NETWORK COMPARTMENT' set to 'Production', 'VIRTUAL CLOUD NETWORK' set to 'VCN-VBA', 'SUBNET COMPARTMENT' set to 'Production', and 'SUBNET' set to 'Public Subnet-VCN-VBA (Regional)'. At the bottom, there are two radio buttons: 'ASSIGN A PUBLIC IP ADDRESS' (which is selected and highlighted with a red box) and 'DO NOT ASSIGN A PUBLIC IP ADDRESS'.

5. Encrypt the boot volume:

- Select the Use in-transit encryption check box: *Enable encryption between the VM and the block volume.*
- Select Encrypt This Volume With A Key That You Manage: *Boot volumes are encrypted by default, but you can optionally use your own Vault service encryption key to encrypt the data in this volume. If you enable this option, this key is used for both data at rest encryption and in-transit encryption (as explained in the previous operation)*
 - Vault Compartment: *Production*
 - Vault: *Choose the Vault created in [Section](#)*
 - Master Encryption Key Compartment: *Production*
 - Master Encryption Key: *Select the VM-Key created in [Section](#)*

Boot volume

☐ SPECIFY A CUSTOM BOOT VOLUME SIZE
[Volume performance](#) varies with volume size. Default boot volume size: 46.6 GB

☒ **USE IN-TRANSIT ENCRYPTION**
[Encrypts data](#) in transit between the instance and the boot volume

☒ **ENCRYPT THIS VOLUME WITH A KEY THAT YOU MANAGE**
 By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. [Learn more about managing your own encryption keys](#)

VAULT COMPARTMENT: **Production**
ociseclab (root)/Production

VAULT: **Vault-VBA**

MASTER ENCRYPTION KEY COMPARTMENT: **Production**
ociseclab (root)/Production

MASTER ENCRYPTION KEY: **VM-Key**

6. Upload the public SSH key created in [Section](#) or paste it (if you're using PuTTY) and click Create

Add SSH keys

Linux-based instances use an [SSH key pair](#) instead of a password to authenticate remote users. Upload the public key now. When you [connect to the instance](#), you will provide the associated private key.

☒ CHOOSE SSH KEY FILES ☐ PASTE SSH KEYS

SSH KEYS

Drop files here. [Or browse](#).
SSH public key (.pub) files only.

pub_key.pub x

[Show Advanced Options](#)


Create [Cancel](#)

7. After a short time (1-2 min), the state of the newly created instance will switch to RUNNING.

In the *General Information* of the instance, there is some info that will be useful for us in the next steps:

- Public IP Address: *We will use it to connect to BastionVM via SSH*
- Username: *The default user on any VM in OCI is opc, which we will use once connected via SSH to BastionVM*
- Verify other info in order to validate the correct creation of the VM (ex.: Compartment, Subnet, etc.)

Compute » Instances » Instance Details » Work Requests



BastionVM

[Start](#)
[Stop](#)
[Reboot](#)
[Change Shape](#)
[More Actions](#)

[Instance Information](#)
[Tags](#)

General Information

Availability Domain: AD-1
Fault Domain: FD-2
Region: eu-frankfurt-1
OCID: ...unkilq [Show](#) [Copy](#)
Launched: Sun, May 3, 2020, 17:56:25 UTC
Compartment: ociseclab (root)/Production
Oracle Cloud Agent Management: Enabled ⓘ

Instance Details

Virtual Cloud Network: [VCN-VBA](#)
Maintenance Reboot: -
Image: [Oracle-Linux-7.8-2020.04.17-0](#)
Launch Mode: NATIVE

Shape Configuration

Shape: VM.Standard2.1
OCPU Count: 1
Network Bandwidth (Gbps): 1
Memory (GB): 15
Local Disk: Block Storage Only

Instance Access

You [connect to a running Linux instance](#) using a [SSH client](#) to create the instance.

Public IP Address: 130.61.230.205 [Copy](#)
Username: opc

Primary VNIC

Private IP Address: 10.0.0.3
Network Security Groups: None [Edit](#) ⓘ
Internal FQDN: bastionvm... [Show](#) [Copy](#)
Subnet: [Public Subnet-VCN-VBA](#)

Launch Options

NIC Attachment Type: PARAVIRTUALIZED
Remote Data Volume: PARAVIRTUALIZED
Firmware: UEFI_64
Boot Volume Type: PARAVIRTUALIZED

7.4.2 PrivateVM

In this Section we will create a VM in the private subnet. As explained in the previous chapters, this VM is isolated from the Internet. However, we can connect to it using the BastionVM, created in the previous Section.

The steps are almost the same as in the previous Section, but we will need to choose the private subnet in the networking settings

In the OCI Console, on the left side click Menu – Compute – Instances.

1. On the left choose the compartment Production, and click Create Instance:

Compute

Instances *in Production Compartment*

Create Instance

Name	Status

List Scope

COMPARTMENT

Production

ociseclab (root)/Production

2. Enter a *Name* for the instance: *PrivateVM*
3. Leave the OS to Oracle Linux 7.8
4. Click Show Shape, Network and Storage Options

Create Compute Instance

NAME

PrivateVM

Image or operating system ⓘ

ORACLE Linux Oracle Linux 7.8
Image Build: 2020.04.17-0

Change Image

Show Shape, Network and Storage Options

5. We can select another AD, using the failure tolerance feature which OCI provides (for more info visit [here](#))
 - Select AD 2 and click Change Shape


Availability domain

AD 1
yTEz:EU-FRANKFURT-1-AD-1

AD 2
yTEz:EU-FRANKFURT-1-AD-2 ✓

AD 3
yTEz:EU-FRANKFURT-1-AD-3

Shape ⓘ



VM.Standard2.1
 Virtual Machine, 1 core OCPU, 15 GB memory, 1 Gbps network bandwidth

Change Shape

- Select Intel Skylake and the shape *VM.Standard2.1*. Click Select Shape

Browse All Shapes

A shape is a template that determines the number of CPUs, amount of memory, and other resources allocated to a newly created instance. See [Compute Shapes](#) for more information.

Don't see the shape you want?
To access all shapes, [upgrade](#). You'll pay only for what you use, no minimum terms and no prepayments.


Upgrade


Instance type

Virtual Machine Always Free Eligible
 A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓

Bare Metal Machine
 A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series


AMD Rome
 Customizable OCPU count. For general purpose workloads.


Intel Skylake
 Fixed OCPU count. Latest generation Intel Standard shapes. ✓

Specialty and Legacy
 Earlier generation AMD and Intel Standard shapes. Always Free, Dense I/O, GPU, and HPC shapes.

Shape Name	OCPU	Memory (GB)	Local Disk	Network Bandwidth (Gbps)	Max. Total VNICS
✓ VM.Standard2.1	1	15	Block Storage Only	1	2

1 Selected Showing 1 item


Select Shape

Cancel

6. Configure the Networking part:

- Virtual Cloud Network Compartment: *Production*
- Virtual Cloud Network: *The VCN created in [Section](#)*
- Subnet Compartment: *Production*
- Subnet: *The Private Subnet in [Section](#)*

Shape ⓘ



VM.Standard2.1
Virtual Machine, 1 core OCPU, 15 GB memory, 1 Gbps network bandwidth

Change Shape

Configure networking

VIRTUAL CLOUD NETWORK COMPARTMENT

Production ⓘ
ociseclab (root)/Production

VIRTUAL CLOUD NETWORK

VCN-VBA ⓘ

SUBNET COMPARTMENT

Production ⓘ
ociseclab (root)/Production

SUBNET ⓘ

Private Subnet-VCN-VBA (Regional) ⓘ

☐ USE NETWORK SECURITY GROUPS TO CONTROL TRAFFIC ⓘ

☐ ASSIGN A PUBLIC IP ADDRESS ☒ DO NOT ASSIGN A PUBLIC IP ADDRESS

7. Encrypt the boot volume:

- Select the Use in-transit encryption check box: *Enable encryption between the VM and the block volume.*
- Select Encrypt This Volume With A Key That You Manage:
 - Vault Compartment: *Production*
 - Vault: *Choose the Vault created in [Section](#)*
 - Master Encryption Key Compartment: *Production*
 - Master Encryption Key: *Select the VM-Key created in [Section](#)*

Boot volume

☐ SPECIFY A CUSTOM BOOT VOLUME SIZE
[Volume performance](#) varies with volume size. Default boot volume size: 48.8 GB

☒ USE IN-TRANSIT ENCRYPTION
[Encrypts data](#) in transit between the instance and the boot volume

☒ ENCRYPT THIS VOLUME WITH A KEY THAT YOU MANAGE
By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. [Learn more about managing your own encryption keys](#)

VAULT COMPARTMENT

Production ⓘ
ociseclab (root)/Production

VAULT

Vault-VBA ⓘ

MASTER ENCRYPTION KEY COMPARTMENT

Production ⓘ
ociseclab (root)/Production

MASTER ENCRYPTION KEY

VM-Key ⓘ

8. Upload the public SSH key (use the same key) created in [Section](#) or paste it (if you're using PuTTY) and click Create.

Add SSH keys

Linux-based instances use an [SSH key pair](#) instead of a password to authenticate remote users. Upload the public key now. When you [connect to the instance](#), you will provide the associated private key.

☒ CHOOSE SSH KEY FILES ☐ PASTE SSH KEYS

SSH KEYS


Drop files here. [Or browse.](#)
SSH public key (.pub) files only

pub_key.pub x

[Show Advanced Options](#)

Create Cancel

9. After a short time (1-2 min), the state of the newly created instance will switch to RUNNING.
 - Observe that we don't have any public IP address for this VM, since it is in a private subnet, hence it is isolated from the internet.



RUNNING

PrivateVM

Start Stop Reboot Change Shape More Actions

Instance Information Tags

General Information

Availability Domain: AD-2
 Fault Domain: FD-3
 Region: eu-frankfurt-1
 OCID: ...dtfnyq [Show](#) [Copy](#)
 Launched: Mon, May 4, 2020, 08:10:43 UTC
 Compartment: ociseclab (root)/Production
 Oracle Cloud Agent Management: Enabled ⓘ

Instance Details

Virtual Cloud Network: [VCN-VBA](#)
 Maintenance Reboot: -
 Image: [Oracle-Linux-7.8-2020.04.17-0](#)
 Launch Mode: NATIVE

Shape Configuration

Shape: VM.Standard2.1

Instance Access

The instance requires a public IP address to connect [public IP](#) or a [reserved public IP](#) to a private IP for the instance.

Public IP Address: -
 Username: **opc**

Primary VNIC

Private IP Address: **10.0.1.3**
 Network Security Groups: None [Edit](#) ⓘ
 Internal FQDN: privatevm-306940... [Show](#) [Copy](#)
 Subnet: **Private Subnet-VCN-VBA**

Launch Options

NIC Attachment Type: PARAVIRTUALIZED
 Remote Data Volume: PARAVIRTUALIZED
 Firmware: UEFI_64
 Boot Volume Type: PARAVIRTUALIZED

7.5 Summary

In this Chapter we have create 2 VMs – BastionVM and PrivateVM, the first one located in the public subnet and the second one in the private subnet.

We have created an SSH key pair (the key is the same for both VMs), private and public, which is required to access the VMs.

8 Object Storage

In this Chapter we will create a [bucket](#), which is a container for storing objects in a compartment within an Object Storage namespace.

Afterwards we will encrypt this bucket using the *Master Key (Object-Key)* which we have created previously in [Section](#).

8.1 Access to OCI

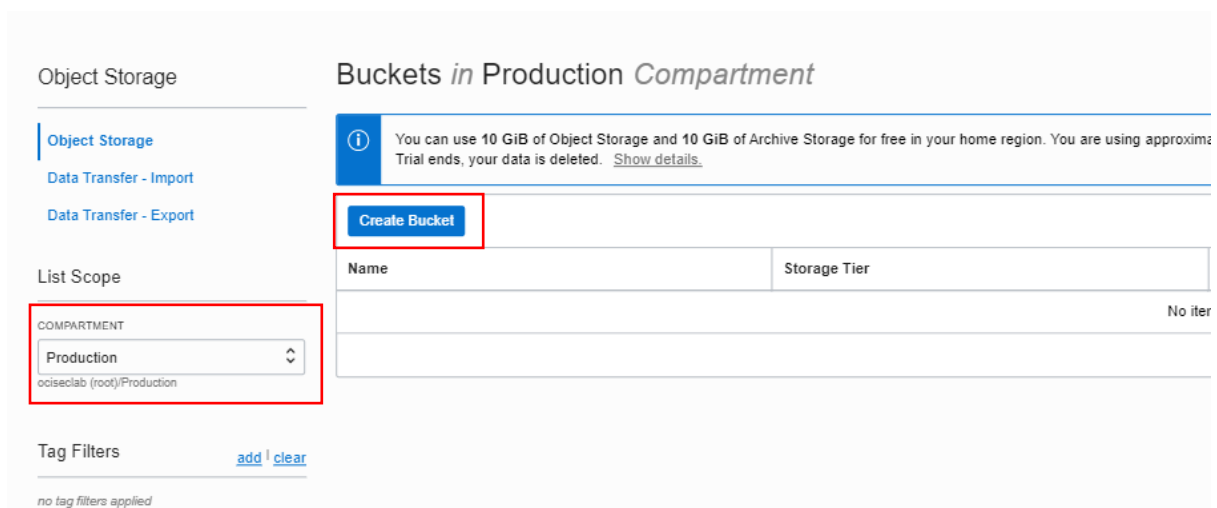
Access the OCI Console using the user – userVM.

8.2 User Permissions

Since we have provided permissions to access OCI ObjectStorage to the group ObjectAdmins in the compartment Production, to which userVM belongs, at this point we are able to manage OCI ObjectStorage components.

8.3 Create Bucket

1. In the OCI Console, on the left side click Menu – Object Storage and select the compartment Production.
2. Click Create Bucket.



3. Enter the following details:
 - Bucket Name: *bucket-your initials (ex.: bucket-VBA)*
 - Storage Tier: *Standard*
 - Object Versioning: *Create an object version each time the content changes or the object is deleted*
 - Encrypt Using Customer Managed Keys: *Select from our OCI Vault the Object-Key which we have created previously*
 - Click Create Bucket.

Create Bucket [Help](#) [Cancel](#)

BUCKET NAME

STORAGE TIER
 Storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides.
☒ STANDARD
☐ ARCHIVE

OBJECT EVENTS ⓘ
☐ EMIT OBJECT EVENTS

OBJECT VERSIONING ⓘ
☒ ENABLE OBJECT VERSIONING

ENCRYPTION
☐ ENCRYPT USING ORACLE MANAGED KEYS
 Leaves all encryption-related matters to Oracle.
☒ ENCRYPT USING CUSTOMER-MANAGED KEYS
 Requires you to have access to a valid Key Management key. ([Learn More](#))

VAULT COMPARTMENT

 ociseclab (root)/Production

VAULT

MASTER ENCRYPTION KEY COMPARTMENT

 ociseclab (root)/Production

MASTER ENCRYPTION KEY

4. In the bucket console, we can notice several info relevant for us:

- Visibility: *Private* (means that it is not exposed publicly)
- Encryption Key: *The encryption key that we have assigned from our Vault and will encrypt our objects from this bucket.*

ORACLE Cloud Search for resources and services

bucket-VBA

[Edit Visibility](#) [Move Resource](#) [Re-encrypt](#) [Add Tags](#) [Delete](#)

Bucket Information Tags

Visibility: Private

Namespace: frvevqldpqus
 Storage Tier: Standard
 Approximate Count: 0 versioned objects ⓘ
 ETag: 4ff38b7a-5ea0-4089-8f31-7585c1074bb6
 OCID: ...a4rdidaa [Show](#) [Copy](#)

Encryption Key: Object-Key ...sb4qug [Edit](#) [Unassign](#)

Created: Mon, May 4, 2020, 12:54:06 UTC
 Compartment: [Production](#)
 Approximate Size: 0 bytes ⓘ
 Emit Object Events: ● Disabled [Edit](#) ⓘ
 Object Versioning: ● Enabled [Edit](#) ⓘ

Note: Encryption is enabled by default and cannot be turned off. By default, Oracle manages the master encryption key. However, in this case the purpose is to show that the customer can handle its own encryption keys, based on its own security requirements

9 Connect via SSH to the VM

In this Chapter we will connect to PrivateVM through the BastionVM, since the last one has been designated as the only host which is exposed to the internet.

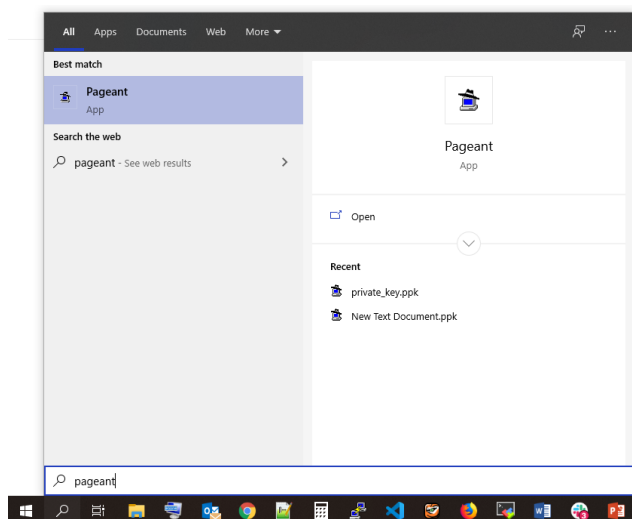
We will present 2 methods to access the VM, based on the OS on your local PC:

- Connection via PuTTY (Windows)
- Connection via OpenSSH (Unix-style OS)

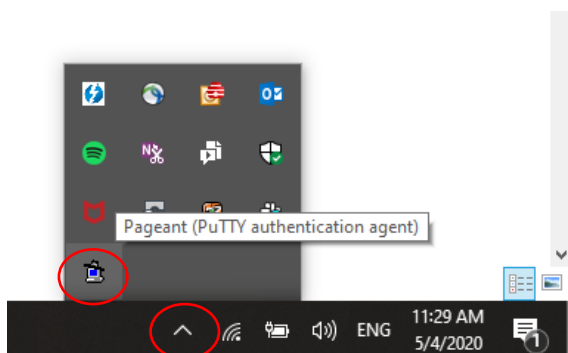
As explained in the previous Section, we have used the same SSH key pair for BastionVM and PrivateVM.

9.1.1 Connect via PuTTY

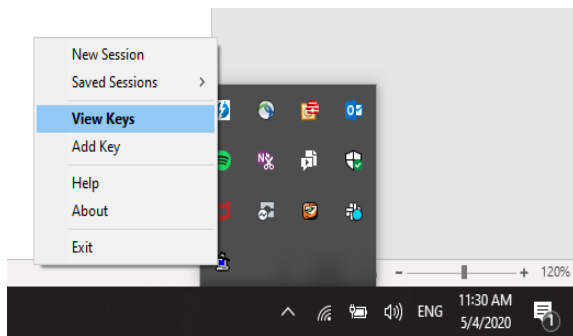
1. Open [Pageant.exe](#), which is a PuTTY SSH authentication agent.
 - Type *pageant* in the windows search box, and open the App.



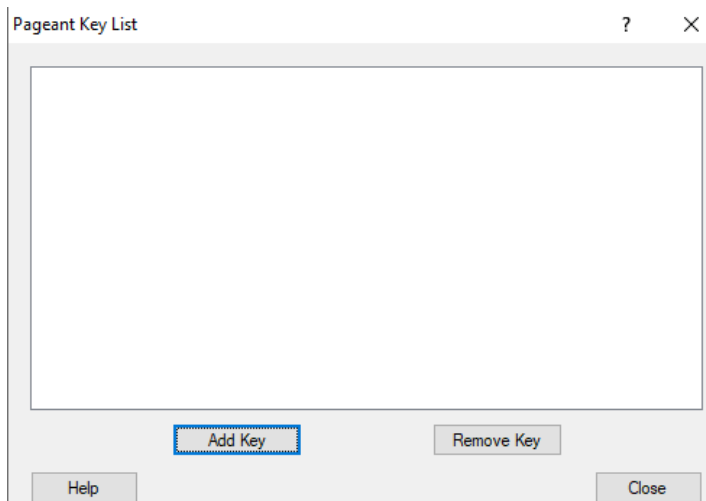
- In the bottom right hand corner, click the arrow “Show hidden icons”
- Right-click the icon of a computer wearing a hat



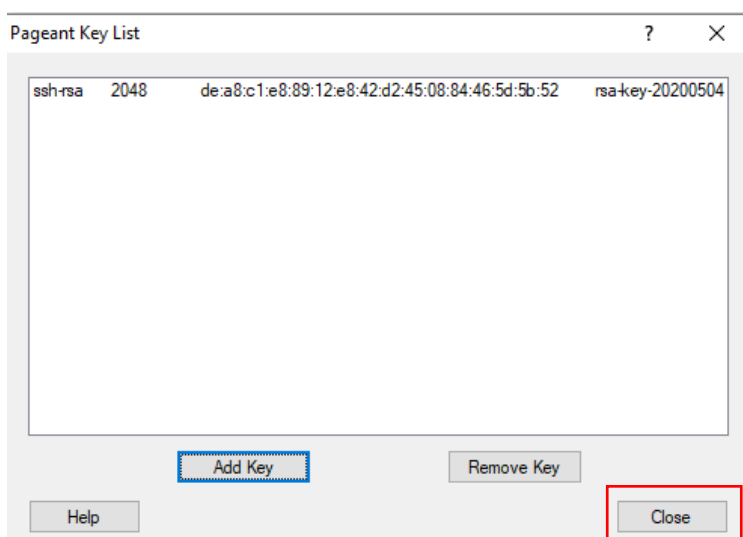
- Click View Keys



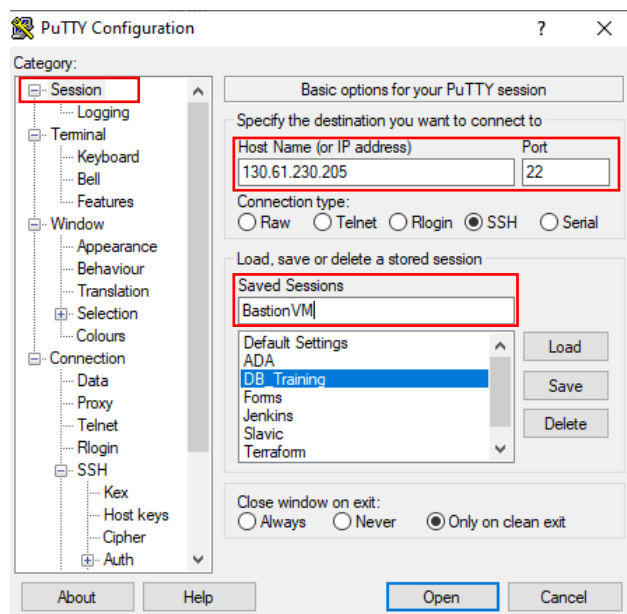
- A window will pop-up. Click Add Key to add your private SSH key



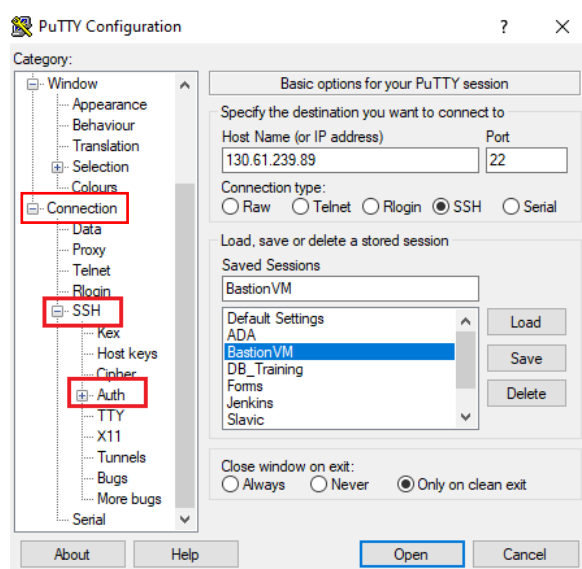
- After uploading your key, you will see it in the Pageant Key List. Click Close



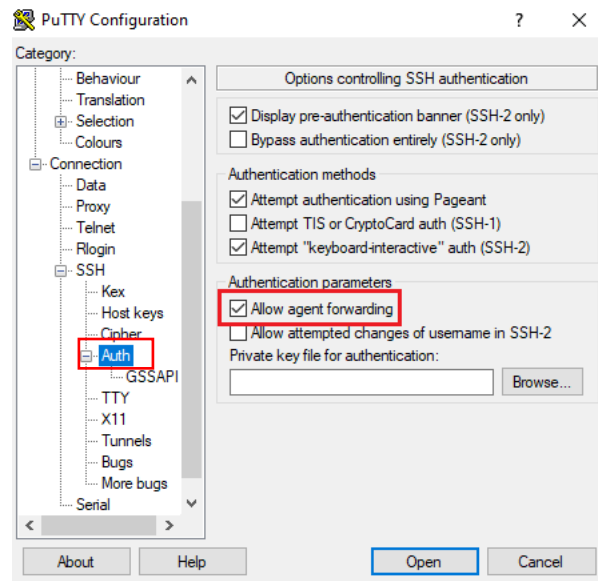
2. Open the PuTTY App
3. Enter the BastionVM connection details:
 - In the *Session* category, enter the public IP address of BastionVM
 - Enter a name for this Session



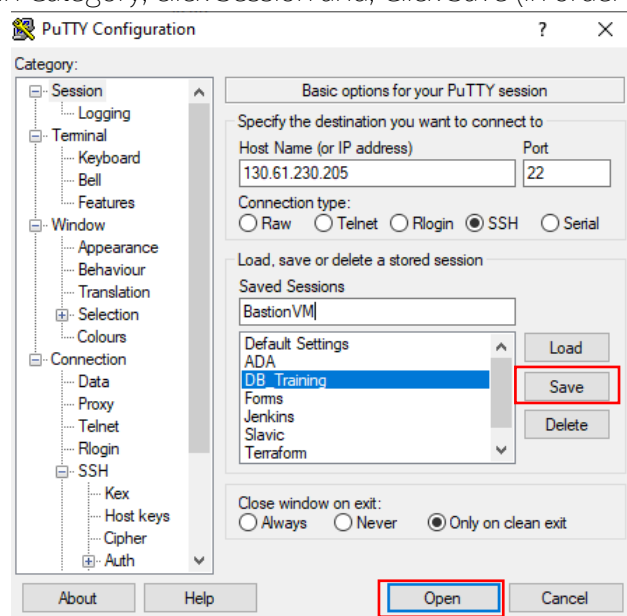
- In Category, open Connection, SSH, and click Auth



- In Auth select Allow agent forwarding option



- In Category, click Session and, Click Save (in order to use it in the future)



- Click Open

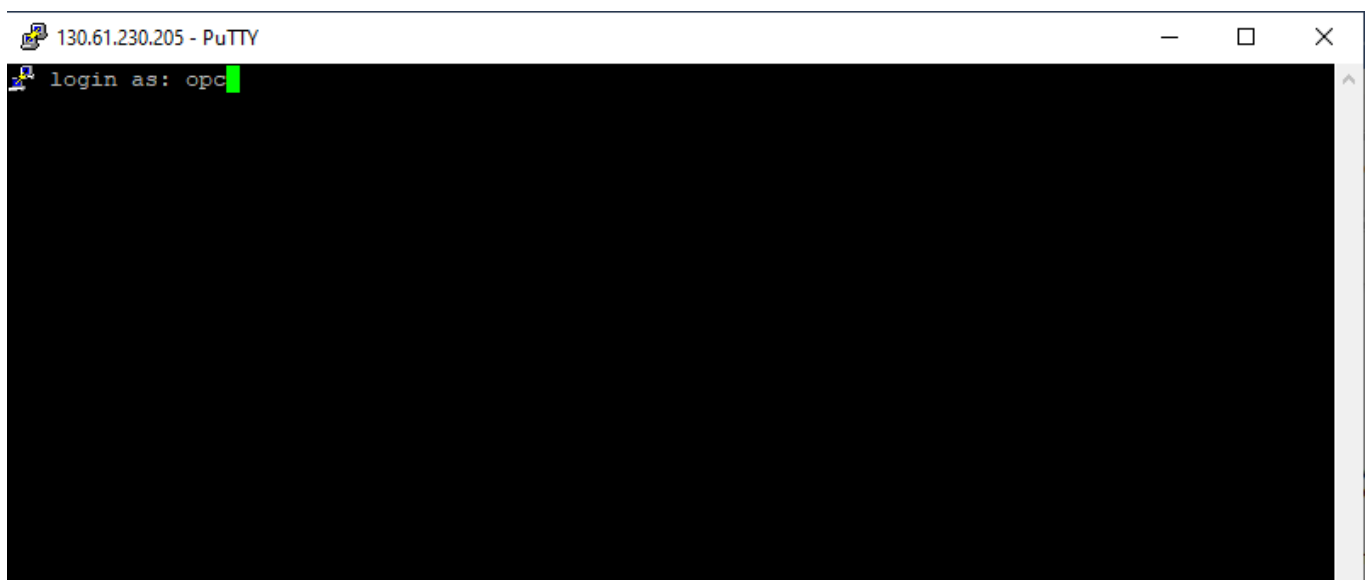
4. A dialog box will pop-up. Click Yes.

PuTTY Security Alert

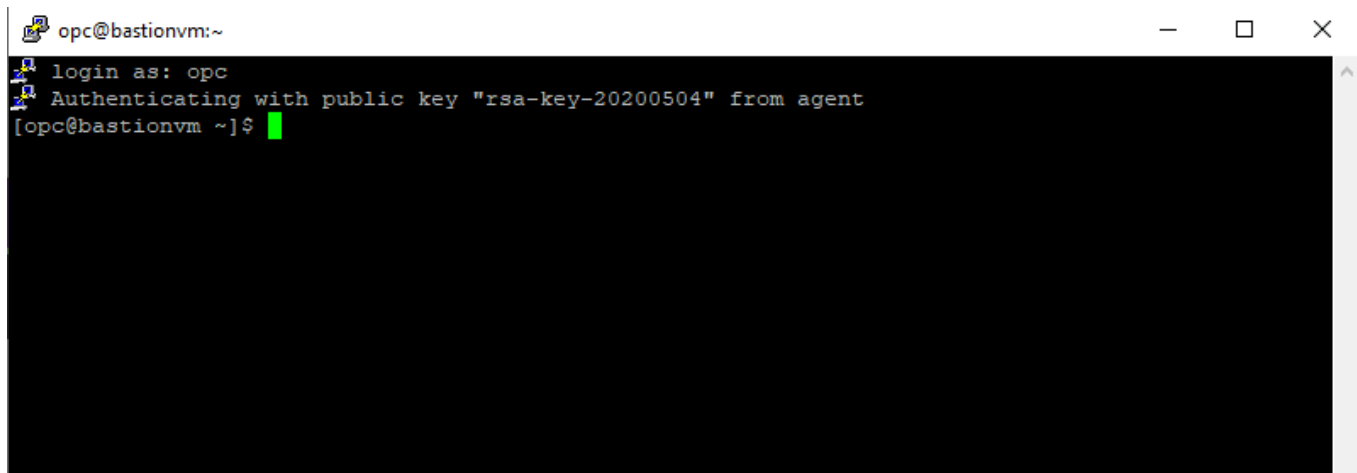


The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 4c34:ac52:21:8c88:29:76:40:af:fc38:60:cf:18
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

5. Log in with the user: opc



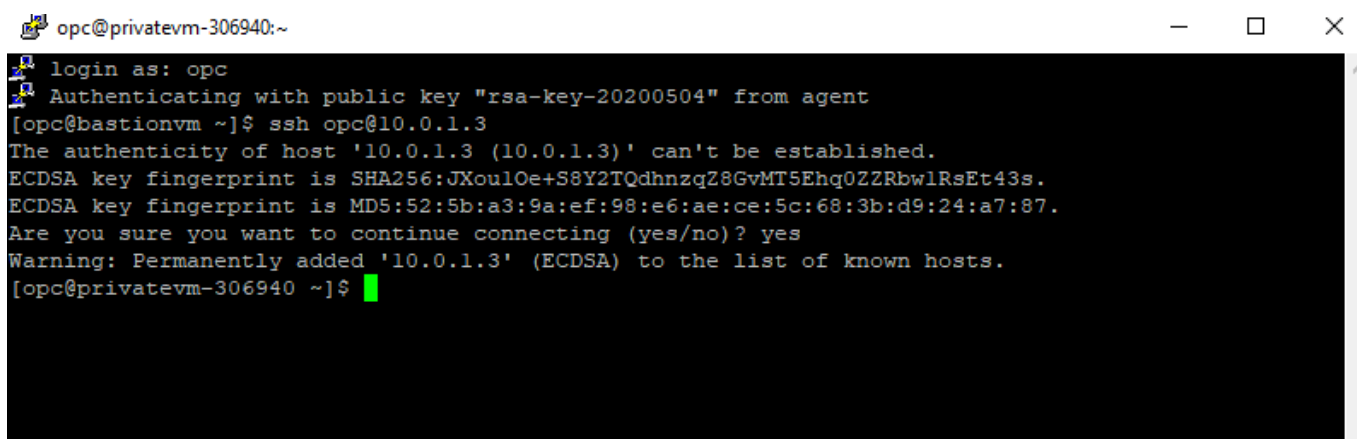
- If the Authentication is successful you will see the message with your public key and the *current_user@hostname*: opc@bastionvm



```
opc@bastionvm:~
login as: opc
Authenticating with public key "rsa-key-20200504" from agent
[opc@bastionvm ~]$
```

6. Connect to PrivateVM:

- Execute the command: **ssh opc@private_ip**
private_ip – The private IP address of PrivateVM
(ex.: ssh opc@10.0.1.3)
- In the yes/no dialog box, type – yes
- We are now connected to PrivateVM through BastionVM



```
opc@privatevm-306940:~
login as: opc
Authenticating with public key "rsa-key-20200504" from agent
[opc@bastionvm ~]$ ssh opc@10.0.1.3
The authenticity of host '10.0.1.3 (10.0.1.3)' can't be established.
ECDSA key fingerprint is SHA256:JXoulOe+S8Y2TQdhnzqZ8GvMT5Ehq0ZZRbwlRsEt43s.
ECDSA key fingerprint is MD5:52:5b:a3:9a:ef:98:e6:ae:ce:5c:68:3b:d9:24:a7:87.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.3' (ECDSA) to the list of known hosts.
[opc@privatevm-306940 ~]$
```

9.1.2 Connect via OpenSSH

1. From your local PC enter the following command in the Terminal Window:

```
ssh -J opc@public_ip opc@private_ip -i /key/directory/private_key
```

public_ip – IP address of BastionVM

private_ip – IP address of PrivateVM

/key/directory/private_key – the directory on your local PC where you keep your private key

Example:

```
ssh -J opc@130.61.239.89 opc@10.0.1.4 -i /home/opc/keys/private_key
```

2. In the two dialog boxes which will be prompted, type yes for both of them:

```
[opc@web-server-1 ~]$ ssh -J opc@130.61.239.89 opc@10.0.1.4 -i /home/opc/keys/FreeTier/private_key
The authenticity of host '130.61.239.89 (130.61.239.89)' can't be established.
ECDSA key fingerprint is SHA256:+mqnhklavmGZaf7xw6B0TbnVXeD3pMHyuE/JC+/W+2A.
ECDSA key fingerprint is MD5:3d:3b:c7:9f:69:ba:78:5e:e5:c1:f0:a8:fd:69:bf:29.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '130.61.239.89' (ECDSA) to the list of known hosts.
The authenticity of host '10.0.1.4 (<no hostip for proxy command>)' can't be established.
ECDSA key fingerprint is SHA256:d+2B9QwQAuzMXlTSVi/PirLZ8UUECU0ssT8TqR02Lps.
ECDSA key fingerprint is MD5:be:5a:1e:fe:73:8c:49:89:a5:3f:fe:9b:16:7f:4f:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.4' (ECDSA) to the list of known hosts.
[opc@privatevm-536946 ~]$
```

9.1.3 Block SSH Connection

At this point we can perform a test and understand better how *Security Lists* work.

Let's suppose that we would like to block all SSH connections to PrivateVM.

1. Access to OCI Console with user userNetwork
2. In the OCI Console, on the left side click Menu – Networking – Virtual Cloud Networks and select the VCN created in [Section](#)
3. In *Resources* go to Security Lists – Security List for Private Subnet VCN

The screenshot displays the OCI Console interface. On the left, the 'Resources' sidebar lists various networking components, with 'Security Lists (2)' selected and highlighted by a red box. The main panel, titled 'Security Lists in Production Compartment', features a 'Create Security List' button at the top. Below it, a table lists existing security lists. The first entry, 'Security List for Private Subnet-VCN-VBA', is highlighted with a red rectangular box. The second entry is 'Default Security List for VCN-VBA'.

- In *Ingress Rules* select the first rule, and on the right, click the 3 dots and select Remove. In this way we will remove all SSH connections from the public subnet to the private subnet.

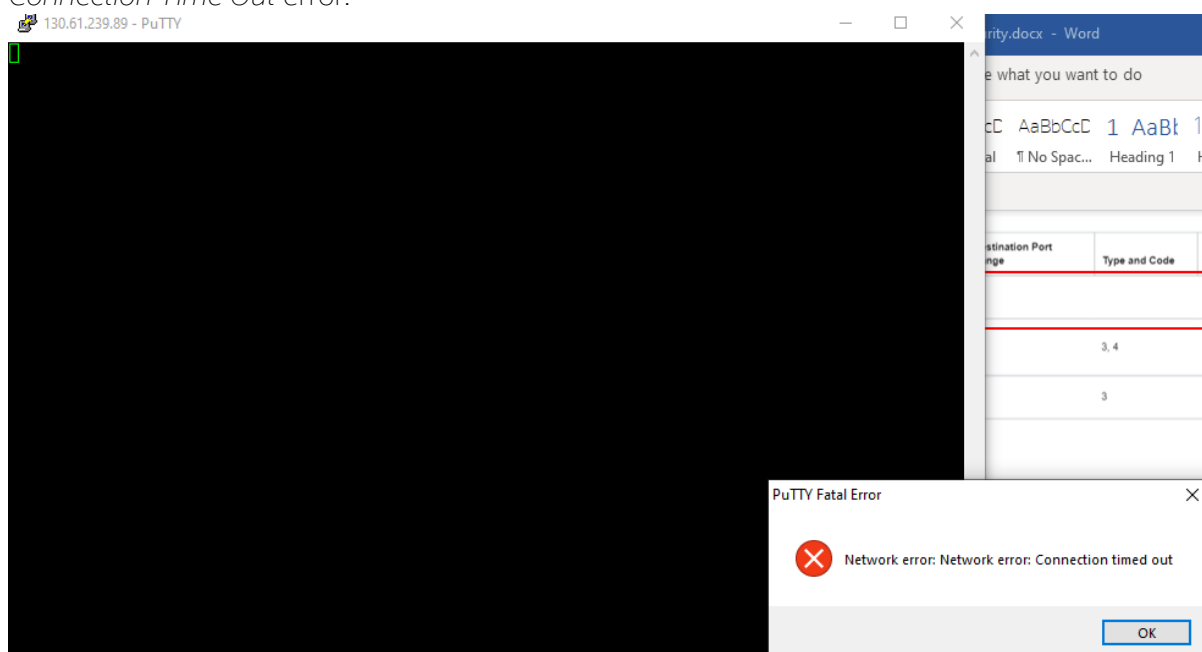
Ingress Rules

[Add Ingress Rules](#) [Edit](#) [Remove](#)

<input type="checkbox"/>	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description	
<input type="checkbox"/>	No	10.0.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol		Edit Remove
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set		
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable		

0 Selected Showing 3 Items < Page 1 >

- Connect via SSH to PrivateVM using the [methods](#) presented earlier, based on your OS
- You shouldn't be able to connect to PrivateVM, and in the end you should receive a *Connection Time Out* error.



- We'll re-establish the old SSH rule.
Go back to the OCI Console, and in the ingress rules for the same security list click Add Ingress Rules, and enter the following rule:
 - Source CIDR: *IPv4 network address of the public subnet (ex.: 10.0.0.0/16)*
 - IP Protocol: *TCP*
 - Source Port Range: *All*
 - Destination Port Range: *22*
 - Click Add Ingress Rule

Add Ingress Rules Cancel

Ingress Rule 1

Allows TCP traffic 22 SSH Remote Login Protocol

☐ STATELESS ⓘ

SOURCE TYPE: CIDR IP PROTOCOL ⓘ

SOURCE CIDR: 10.0.0.0/16 TCP

Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

SOURCE PORT RANGE OPTIONAL ⓘ: All DESTINATION PORT RANGE OPTIONAL ⓘ: 22

Examples: 80, 20-22 Examples: 80, 20-22

DESCRIPTION OPTIONAL: SSH Rule

Maximum 255 characters

+ Additional Ingress Rule

Add Ingress Rules Cancel

8. Retry connecting to PrivateVM via SSH. This time the connection should be successful.

9.2 Summary

In this chapter we have connected to PrivateVM through BastionVM, using the SSH key, while maintaining the PrivateVM isolated from the Internet.

In the end we have performed a test and experienced how security lists work. As mentioned earlier they act as virtual firewalls. Hence, we have blocked the SSH connection to the private subnet (where PrivateVM is located) by deleting the *Ingress Rule* for the SSH protocol in the *Security List* associated to the private subnet.

10 Maximum Security Zone

10.1 Introduction

Oracle Maximum Security Zones extends IaaS access management to restrict insecure actions or configurations using a new policy definition that applies to designated cloud compartments. This new Oracle Cloud Infrastructure service helps ensure resources are secure from inception by enforcing rigorous security best practices for highly sensitive workloads. It helps customers implement Oracle's security best practices by enforcing them from the start, thereby reducing the chance of someone violating them later. A Security Zone contains a firm set of policies that prevent certain behaviors. In a Security Zone, storage is encrypted at rest, networks are not open for connecting from the public Internet, and buckets are not public.

A security zone is associated with a compartment and a security zone recipe. When you create and update resources in a security zone, Oracle Cloud Infrastructure validates these operations against the list of policies defined in the security zone recipe. If any security zone policy is violated, then the operation is denied. Oracle Maximum Security Zones includes policies for several core Oracle Cloud Infrastructure Services, including Object Storage, Networking, Encryption, DBaaS, and File Storage.

For more information about maximum security zone please refer:

<https://docs.oracle.com/en-us/iaas/security-zone/using/security-zones.htm>

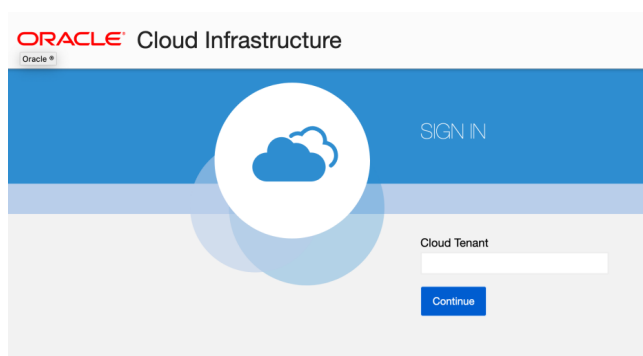
<https://www.oracle.com/security/cloud-security/security-zones/>

<https://docs.oracle.com/en/solutions/oci-security-zones/index.html#GUID-0A7E4C59-8A14-4C89-8D25-83474B82E381>

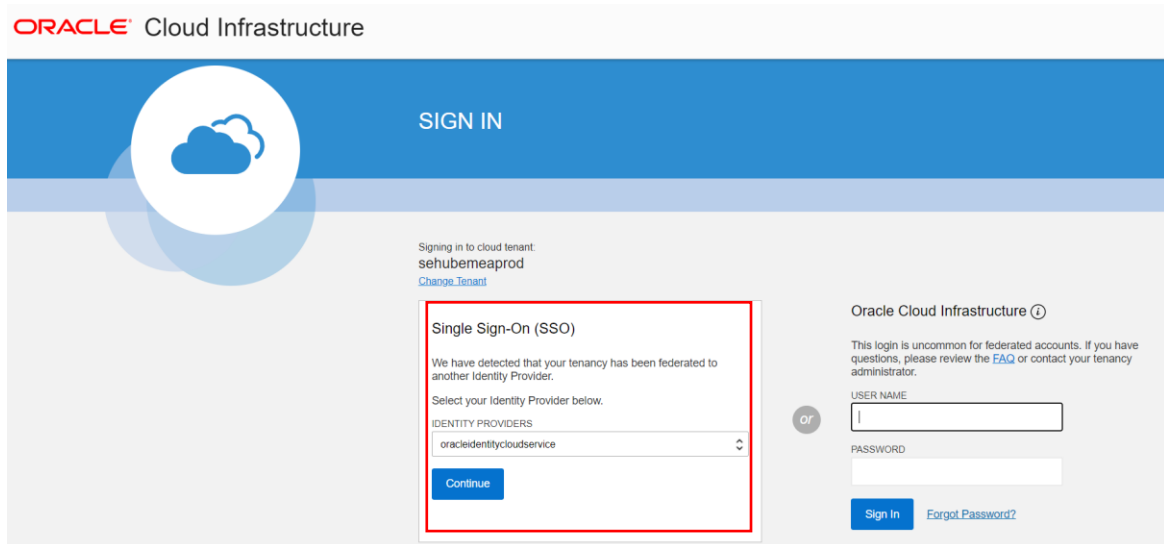
In this Lab we will see how maximum security zone recipes can help in securing the environment whenever the misconfiguration of resources is performed.

For the lab, you need to access to OCI console with default administrator user.

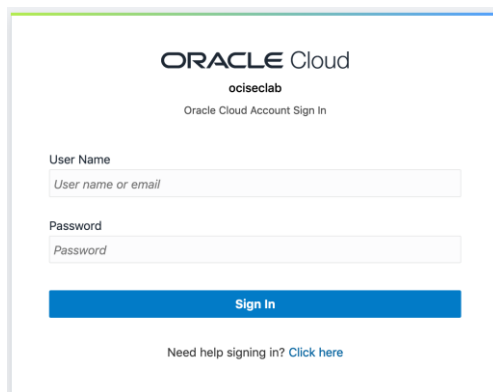
1. Access to URL: <https://console.eu-frankfurt-1.oraclecloud.com/>
2. Add cloud tenant selected during Oracle Cloud Free Tier account registration



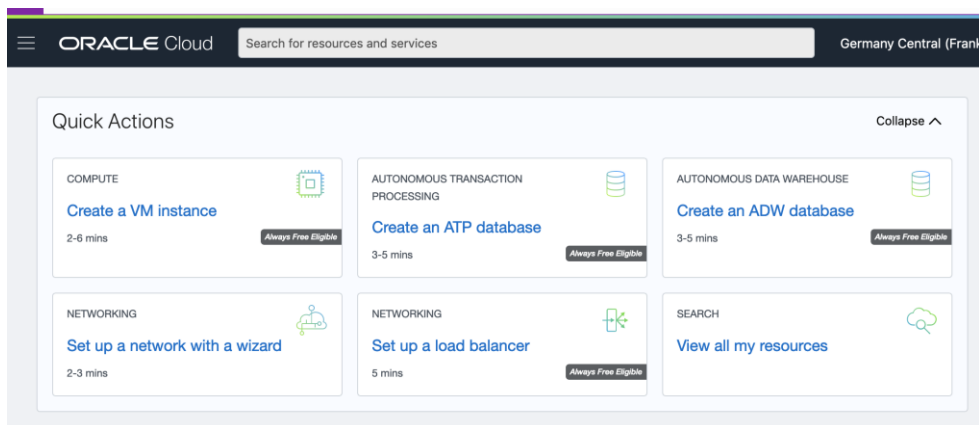
3. Click Continue into Single Sign-On (SSO)



4. Add username and password of default administrator user and click Sign-in

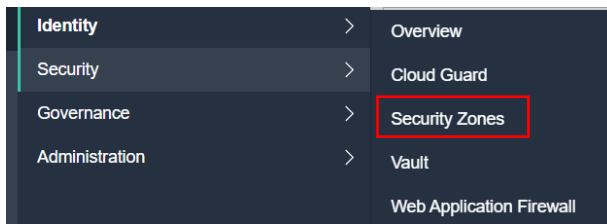


5. You will access to OCI Console with default administrator capabilities

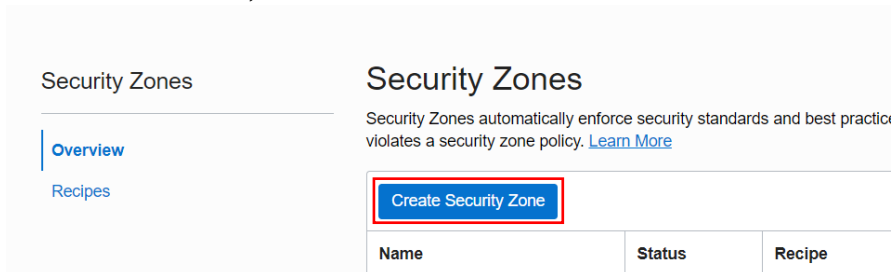


10.2 Create a Compartment

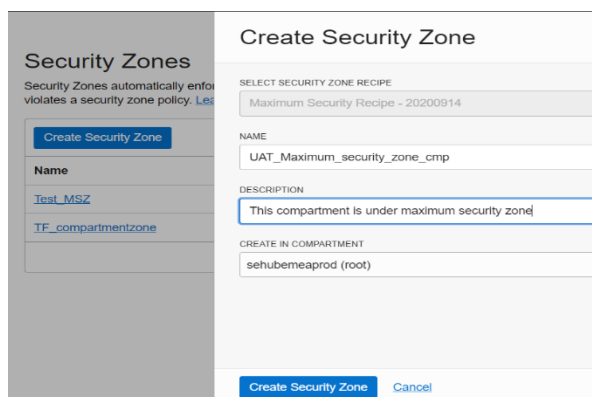
1. In the OCI Console, on the left side click Menu - Security – Security zones:



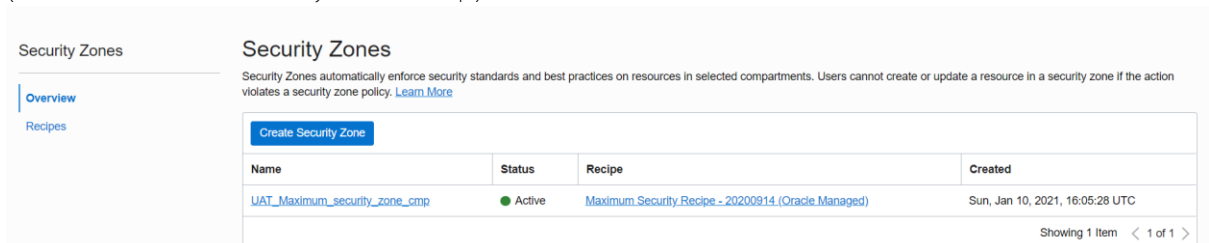
2. Click Create Security Zone:



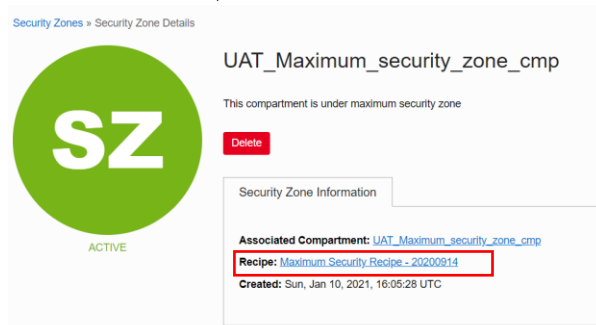
3. Give the name to the compartment and a friendly description
 - o Name: UAT_Maximum_security_zone_cmp
 - o Description: This compartment is under maximum security zone
 - o Create in compartment: Select the root compartment (The new compartment will be created under the root compartment)
 - o Click Create Security Zone



4. Click on the newly created Maximum security zone (UAT_Maximum_security_zone_cmp)



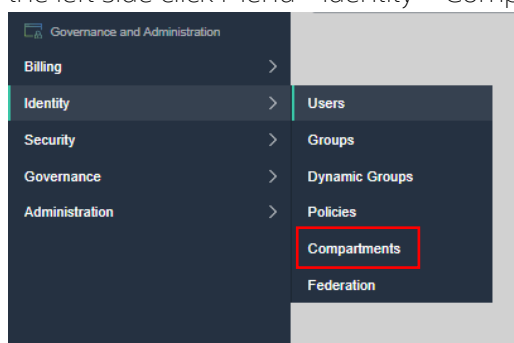
- Click on the Recipe.



- When you scroll down you can see there are 'n' number of policies which is in place by default whenever the zone is created.
Hence when the user performs any of the action against these policies, he will be denied to make changes to those resources which are in the security zone.


Policies		
Policy Statement		
DENY ATTACHED_BLOCK_VOLUME_NOT_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_IN_SECURITY_ZONE		⋮
DENY ATTACHED_BOOT_VOLUME_NOT_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_IN_SECURITY_ZONE		⋮
DENY BLOCK_VOLUME_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_NOT_IN_SECURITY_ZONE		⋮
DENY BLOCK_VOLUME_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_NOT_IN_SECURITY_ZONE		⋮
DENY BLOCK_VOLUME_NOT_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_IN_SECURITY_ZONE		⋮
DENY BLOCK_VOLUME_WITHOUT_VAULT_KEY		⋮
DENY BOOT_VOLUME_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_NOT_IN_SECURITY_ZONE		⋮
DENY BOOT_VOLUME_IN_SECURITY_ZONE_MOVE_TO_COMPARTMENT_NOT_IN_SECURITY_ZONE		⋮
DENY BOOT_VOLUME_NOT_IN_SECURITY_ZONE_ATTACH_TO_INSTANCE_IN_SECURITY_ZONE		⋮
DENY BOOT_VOLUME_WITHOUT_VAULT_KEY		⋮
Showing 10 Items < 1 of 4 >		

- In this Lab we will try to create the few of the resources against the policies and we will see how maximum security zone will help us in protecting the environment.
- Now let's check whether the new compartment is created or not. In the OCI Console, on the left side click Menu - Identity – Compartments:



- Search for the newly created compartment: UAT_Maximum_security_zone_cmp
- Click on UAT_Maximum_security_zone_cmp, Hence Compartment has been created

Identity » Compartments » Compartment details



ACTIVE

Information

Some actions are disabled because this compartment has a Security Zone.

UAT_Maximum_security_zone_cmp

This compartment is under maximum security zone

[Rename Compartment](#)
[Edit Description](#)
[Move Resource](#)
[Delete](#)
[More Actions](#)

[Compartment Information](#)
[Tags](#)

Parent Compartment: [sehubemeaprod\(root\)](#)
Security Zone: [UAT_Maximum_security_zone_cmp](#)

OCID: ...s5w5oq [Show](#) [Copy](#)

Authorized: Yes

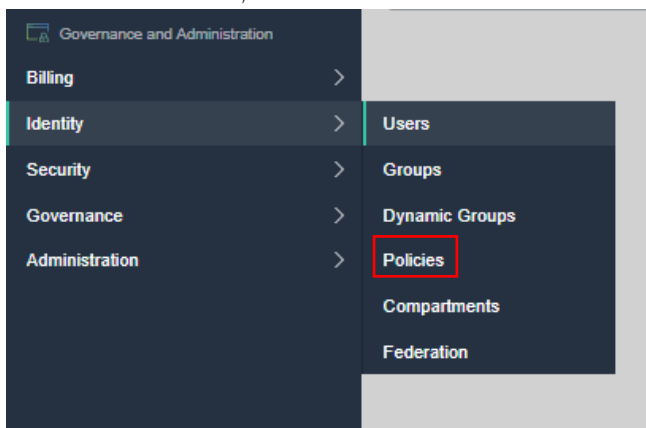
Created: Sun, Jan 10, 2021, 16:05:28 UTC

10.3 Create a policy for the newly created compartment

Let's create a network, instance & vault policies for compartment UAT_Maximum_security_zone_cmp

10.3.1 Create Network Policy

1. In the OCI Console, on the left side click Menu – Identity – Policies



2. In List Scope select UAT_Maximum_security_zone_cmp Compartment, if not already selected

Identity

Users

Groups

Dynamic Groups

Network Sources

Policies

Compartments

Federation

Authentication Settings

List Scope

COMPARTMENT

UAT_Maximum_security_zone_cm

setubemeaprod (root)UAT_Maximum_security_zo

nc_cmp

Policies in UAT_Max

Create Policy Delete

☐ Name

0 Selected

3. Click Create Policy and fill in the following fields and click Create
 - Name for the policy – Network_Policy
 - A friendly Description - Allow the group NetworkAdmins to manage Network Components in compartment UAT_Maximum_security_zone_cmp
 - Policy use cases – Network Management
 - Common policy templates – Let network admins manage a cloud network
 - Groups – NetworkAdmins
 - Location - UAT_Maximum_security_zone_cmp

Create Policy [Help](#)

NAME

Network_Policy

No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION

Allow the group NetworkAdmins to manage Network Components in compartment UAT_Maximum_security_zone_cmp

COMPARTMENT

UAT_Maximum_security_zone_cmp

setubemeaprod (root)UAT_Maximum_security_zone_cmp

Policy Builder [Customize \(Advanced\)](#)

Policy Options

POLICY USE CASES

Network Management

COMMON POLICY TEMPLATES

Let network admins manage a cloud network

Let network admins manage a cloud network

Ability to manage all components in Networking. This includes cloud networks, subnets, gateways, virtual circuits, security lists, route tables, and so on.

GROUPS

NetworkAdmins

LOCATION

UAT_Maximum_security_zone_cmp

Policy Statements

Allow NetworkAdmins to manage virtual-network-family in compartment UAT_Maximum_security_zone_cmp

[Show Advanced Options](#)

Create Cancel ☐ CREATE ANOTHER POLICY

4. In the policy page, click on newly created Network_policy


Create PolicyDelete

<input type="checkbox"/>	Name	Description	Statements
<input type="checkbox"/>	Network_Policy	Allow the group NetworkAdmins to manage Network Components in compartment UAT_Maximum_security_zone_cmp	1

0 Selected

5. Click on Edit Policy Statements

Identity » Policies » Policy Detail



Network_Policy

[Edit Policy](#) [Add Tags](#) [Delete](#)

Policy Information

OCID: ...k5eavrlq [Show](#) [Copy](#)

Compartment: sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Description: Allow the group NetworkAdmins to manage Network Components in compartment UAT_Maximum_security_zone_cmp

Created: Sun, Jan 10, 2021, 18:36:13 UTC

Resources

[Statements](#)

[Edit Policy Statements](#)

Allow group NetworkAdmins to manage virtual-network-family in compartment UAT_Maximum_security_zone_cmp

6. Click on add Another Statement

POLICY BUILDER

☒ BASIC ☐ ADVANCED

STATEMENT 1

Allow group NetworkAdmins to manage virtual-network-family in compartment UAT_Maximum_security_zone_cmp

[+ Another Statement](#)

7. Add the below Statement and click Save Changes
- Allow group NetworkAdmins to manage security-zone in compartment UAT_Maximum_security_zone_cmp

Edit Policy Statements [Help](#)

POLICY BUILDER

☒ BASIC ☐ ADVANCED

STATEMENT 1

Allow group NetworkAdmins to manage virtual-network-family in compartment UAT_Maximum_security_zone_cmp

STATEMENT 2

Allow group NetworkAdmins to manage security-zone in compartment UAT_Maximum_security_zone_cmp

[+ Another Statement](#)

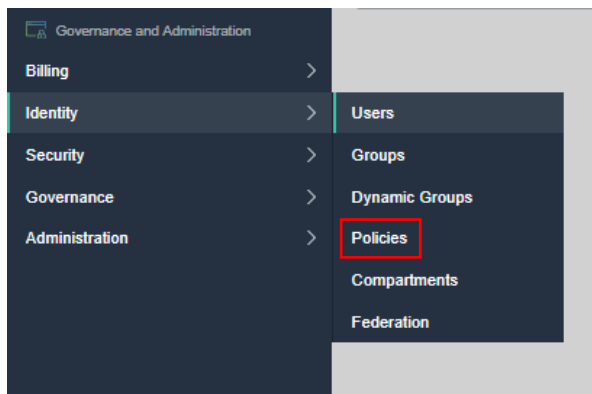
Example: Allow group [group_name] to [verb] [resource-type] in compartment [compartment_name] where [condition]

[Save Changes](#) [Cancel](#)

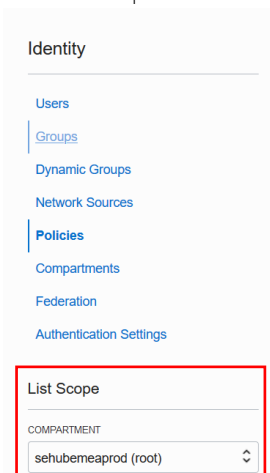
10.3.2 Attach a network policy to root compartment.

Later in one of the use cases we will use the subnet from the production compartment to create a VM in the UAT_Maximum_security_zone_cmp compartment.

1. In the OCI Console, on the left side click Menu – Identity – Policies



2. In List Scope select root compartment (eg: sehubemeaprod)



3. Click Create Policy and fill in the below details
 - o *Name* for the policy – Network_2_Policy
 - o A friendly *Description* – We will be using the subnet present in production compartment to create a compute instance in security zone UAT_Maximum_security_zone_cmp
 - o Policy use cases – Network Management
 - o Common policy templates – Let network admins manage a cloud network
 - o Groups – InstanceAdmins
 - o Location – Production
 - o Click create policy

NAME
Network_2_policy

No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION
we will be using the subnet present in production compartment to create a compute instance in security zone compartment (UAT_Maximum_security_zone_cmp)

COMPARTMENT
sehubemeaprod (root)

Policy Builder Customize (Advanced)

Policy Options

POLICY USE CASES
Network Management

COMMON POLICY TEMPLATES
Let network admins manage a cloud network

Let network admins manage a cloud network
Ability to manage all components in Networking. This includes cloud networks, subnets, gateways, virtual circuits, security lists, route tables, and so on.

GROUPS
InstanceAdmins

LOCATION
Production

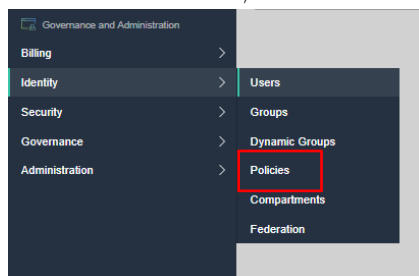
Policy Statements
Allow **InstanceAdmins** to manage virtual-network-family in **compartment Production**

[Show Advanced Options](#)

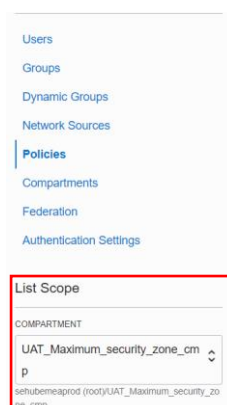
[Create](#) [Cancel](#) ☐ CREATE ANOTHER POLICY

10.3.3 Create Instance Policy

1. In the OCI Console, on the left side click Menu – Identity – Policies



2. In List Scope select UAT_Maximum_security_zone_cmp Compartment, if not already selected



3. Click Create Policy and fill in the following fields and click Create

- Name for the policy – Instance_Policy
- A friendly Description - Allow the group InstanceAdmins to manage Instances Compute in compartment UAT_Maximum_security_zone_cmp
- Policy use cases –Compute Instance Management
- Common policy templates – Let Users Launch Compute Instance
- Groups – InstanceAdmins
- Location - UAT_Maximum_security_zone_cmp

Create Policy

[Help](#)

NAME
Instance_policy
No spaces. Only letters, numerals, hyphens, periods, or underscores.

DESCRIPTION
- Allow the group InstanceAdmins to manage Instances Compute in compartment UAT_Maximum_security_zone_cmp

COMPARTMENT
UAT_Maximum_security_zone_cmp
sehubemeaprod (root)UAT_Maximum_security_zone_cmp

Policy Builder Customize (Advanced)

Policy Options

POLICY USE CASES
Compute Instances Management

COMMON POLICY TEMPLATES
Let users launch Compute instances

Let users launch Compute instances
Ability to do everything with instances launched into the cloud network and subnets in the selected location, and attach/detach any existing volumes that already exist in the selected location. The first statement also lets the group create and manage Instance Images in the selected location. If the group doesn't need to attach/detach volumes, you can delete the third statement. **Use the Advanced option to customize the policy.**

GROUPS
InstanceAdmins

LOCATION
UAT_Maximum_security_zone_cmp

Policy Statements

Allow InstanceAdmins to manage instance-family in compartment UAT_Maximum_security_zone_cmp

Allow InstanceAdmins to read app-catalog-listing in compartment UAT_Maximum_security_zone_cmp

Allow InstanceAdmins to use volume-family in compartment UAT_Maximum_security_zone_cmp

Allow InstanceAdmins to use virtual-network-family in compartment UAT_Maximum_security_zone_cmp

[Show Advanced Options](#)

Create [Cancel](#) ☐ CREATE ANOTHER POLICY


4. In the policy page, click on newly created Instance_policy

Policies in UAT_Maximum_security_zone_cmp Compartment

Create Policy		Delete			
<input type="checkbox"/>	Name	Description	Statements	Created	
<input type="checkbox"/>	Instance_policy	- Allow the group InstanceAdmins to manage Instances Compute in compartment UAT_Maximum_security_zone_cmp	4	Sun, Jan 10, 2021, 18:54:11 UTC	⋮
<input type="checkbox"/>	Network_Policy	Allow the group NetworkAdmins to manage Network Components in compartment UAT_Maximum_security_zone_cmp	1	Sun, Jan 10, 2021, 18:36:13 UTC	⋮
0 Selected			Displaying 2 Policies < Page 1 >		

5. Click on Edit Policy Statements

Identity » Policies » Policy Detail



Instance_policy

ACTIVE

[Edit Policy](#)
[Add Tags](#)
[Delete](#)

Policy Information Tags

OCID: ...ilrgbfqx [Show](#) [Copy](#)

Compartment: sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Description: - Allow the group InstanceAdmins to manage Instances Compute in compartment UAT_Maximum_security_zone_cmp

Created: Sun, Jan 10, 2021, 18:54:11 UTC

Resources

[Statements](#)

Statements

[Edit Policy Statements](#)

Allow group InstanceAdmins to manage instance-family in compartment UAT_Maximum_security_zone_cmp

6. Click on add Another Statement

Edit Policy Statements [Help](#)

POLICY BUILDER
☒ BASIC ☐ ADVANCED

STATEMENT 1
 Allow group InstanceAdmins to manage instance-family in compartment UAT_Maximum_security_zone_cmp

STATEMENT 2
 Allow group InstanceAdmins to read app-catalog-listing in compartment UAT_Maximum_security_zone_cmp

STATEMENT 3
 Allow group InstanceAdmins to use volume-family in compartment UAT_Maximum_security_zone_cmp

STATEMENT 4
 Allow group InstanceAdmins to use virtual-network-family in compartment UAT_Maximum_security_zone_cmp

[+ Another Statement](#)

7. Add the below Statement and click Save Changes

Allow group InstanceAdmins to manage security-zone in compartment UAT_Maximum_security_zone_cmp

Edit Policy Statements [Help](#)

☒ BASIC ☐ ADVANCED

STATEMENT 1
 Allow group InstanceAdmins to manage instance-family in compartment UAT_Maximum_security_zone_cmp

STATEMENT 2
 Allow group InstanceAdmins to read app-catalog-listing in compartment UAT_Maximum_security_zone_cmp

STATEMENT 3
 Allow group InstanceAdmins to use volume-family in compartment UAT_Maximum_security_zone_cmp

STATEMENT 4
 Allow group InstanceAdmins to use virtual-network-family in compartment UAT_Maximum_security_zone_cmp

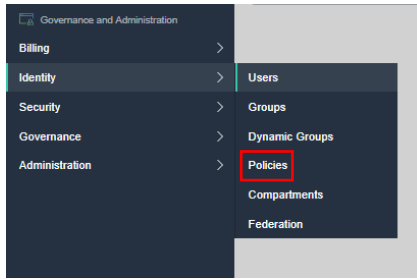
STATEMENT 5
 Allow group InstanceAdmins to manage security-zone in compartment UAT_Maximum_security_zone_cmp

[+ Another Statement](#)

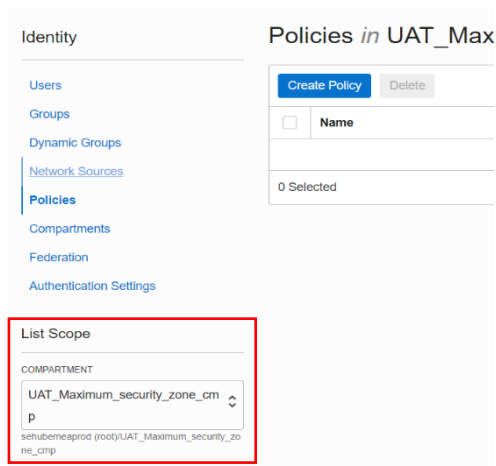
[Save Changes](#) [Cancel](#)

10.3.4 Create Vault Policy

1. In the OCI Console, on the left side click Menu – Identity – Policies



2. In List Scope select UAT_Maximum_security_zone_cmp Compartment, if not already selected



3. Click Create Policy and fill in the following fields and click Create
 - o *Name* for the policy – Vault_Policy
 - o A friendly *Description* - Allow the group SecurityAdmins to manage Vaults, Keys in compartment UAT_Maximum_security_zone_cmp
 - o Policy use cases – Key and Secret Management
 - o Common policy templates – Let security admins manage vaults, keys and secrets
 - o Groups –SecurityAdmins
 - o Location - UAT_Maximum_security_zone_cmp

Create Policy [Help](#)

NAME
Vault_policy
No spaces. Only letters, numerals, hyphens, periods, or underscores.

Let security admins manage vaults, keys, and secrets
Ability to do all things with the Vault service in the selected location. This makes sense if you want to have a single set of security admins manage all the vaults, keys, and secret components (including secrets, secret versions, and secret bundles) in the selected location.

GROUPS
SecurityAdmins

LOCATION
UAT_Maximum_security_zone_cmp

Policy Statements

Allow **SecurityAdmins** to manage vaults in compartment **UAT_Maximum_security_zone_cmp**

Allow **SecurityAdmins** to manage keys in compartment **UAT_Maximum_security_zone_cmp**

Allow **SecurityAdmins** to manage secret-family in compartment **UAT_Maximum_security_zone_cmp**

[Show Advanced Options](#)

[Create](#) [Cancel](#) ☐ CREATE ANOTHER POLICY


4. In the policy page, click on newly created Vault_policy.

Policies in UAT_Maximum_security_zone_cmp Compartment

Create Policy Delete					
<input type="checkbox"/>	Name	Description	Statements	Created	
<input type="checkbox"/>	Vault_policy	Allow the group SecurityAdmins to manage Vaults, Keys in compartment UAT_Maximum_security_zone_cmp	5	Mon, Jan 11, 2021, 05:54:51 UTC	⋮
<input type="checkbox"/>	Instance_policy	- Allow the group InstanceAdmins to manage Instances Compute in compartment UAT_Maximum_security_zone_cmp	6	Sun, Jan 10, 2021, 18:54:11 UTC	⋮
<input type="checkbox"/>	Network_Policy	Allow the group NetworkAdmins to manage Network Components in compartment UAT_Maximum_security_zone_cmp	2	Sun, Jan 10, 2021, 18:36:13 UTC	⋮
0 Selected			Displaying 3 Policies < Page 1 >		

5. Click on Edit Policy Statements

Identity » Policies » Policy Detail



Vault_policy

Edit Policy Add Tags Delete

Policy Information Tags

OCID: `..m7lprvsq` Show Copy

Compartment: sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Description: Allow the group SecurityAdmins to manage Vaults, Keys in compartment UAT_Maximum_security_zone_cmp

Created: Mon, Jan 11, 2021, 05:54:51 UTC

Resources

Statements Edit Policy Statements

6. Click on Add Another statement

Edit Policy Statements [Help](#)

POLICY BUILDER BASIC ADVANCED

STATEMENT 1: Allow group SecurityAdmins to manage vaults in compartment UAT_Maximum_security_zone_cmp

STATEMENT 2: Allow group SecurityAdmins to manage keys in compartment UAT_Maximum_security_zone_cmp

STATEMENT 3: Allow group SecurityAdmins to manage secret-family in compartment UAT_Maximum_security_zone_cmp

+ Another Statement

7. Add the below two Statements and click Save Changes
- Allow group SecurityAdmins to manage security-zone in compartment UAT_Maximum_security_zone_cmp
- Allow service blockstorage, objectstorage-eu-frankfurt-1 to use keys in compartment UAT_Maximum_security_zone_cmp

Edit Policy Statements

POLICY BUILDER
☒ BASIC ☐ ADVANCED

STATEMENT 1
 Allow group SecurityAdmins to manage vaults in compartment UAT_Maximum_security_zone_cmp

STATEMENT 2
 Allow group SecurityAdmins to manage keys in compartment UAT_Maximum_security_zone_cmp

STATEMENT 3
 Allow group SecurityAdmins to manage secret-family in compartment UAT_Maximum_security_zone_cmp

STATEMENT 4
 Allow group SecurityAdmins to manage security-zone in compartment UAT_Maximum_security_zone_cmp

STATEMENT 5
 Allow service blockstorage, objectstorage-eu-frankfurt-1 to use keys in compartment UAT_Maximum_security_zone_cmp

Save Changes [Cancel](#)

10.4 Create Vault and Key

1. Sign out with your current user (default administrator user) and log in with userVM

ORACLE Cloud Infrastructure

SIGN IN

Signing in to cloud tenant:
sehubemeaprod
[Change Tenant](#)

Single Sign-On (SSO)
 We have detected that your tenancy has been federated to another identity Provider.
 Select your Identity Provider below.

IDENTITY PROVIDERS
 oracleidentitycloudservice

[Continue](#)

OR

Oracle Cloud Infrastructure ⓘ

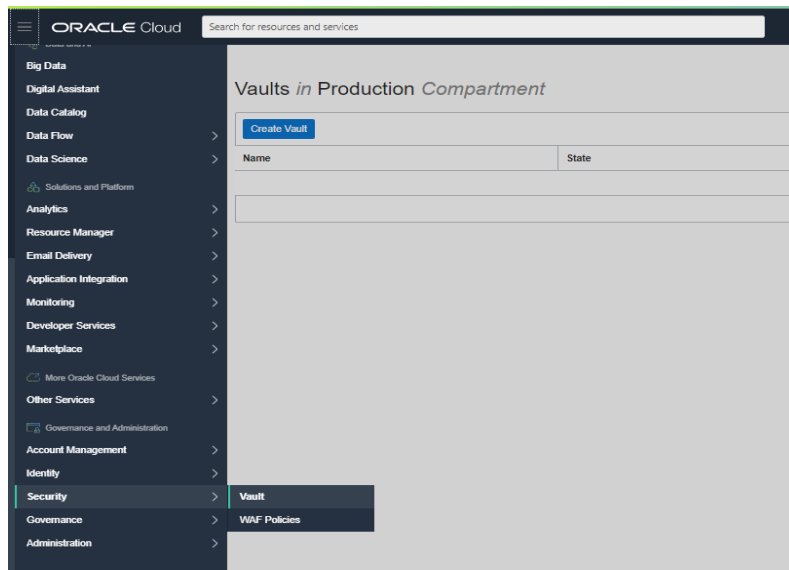
This login is uncommon for federated accounts. If you have questions, please review the [FAQ](#) or contact your tenancy administrator.

USER NAME
 userVM

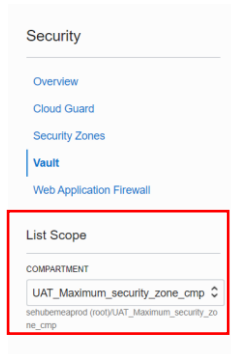
PASSWORD

[Sign In](#) [Forgot Password?](#)

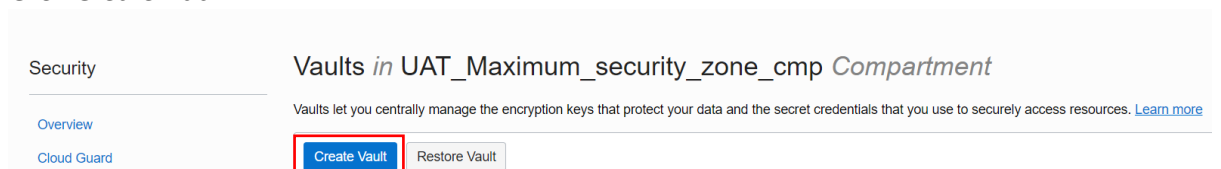
2. In the OCI Console, on the left side click Menu – Security – Vault:



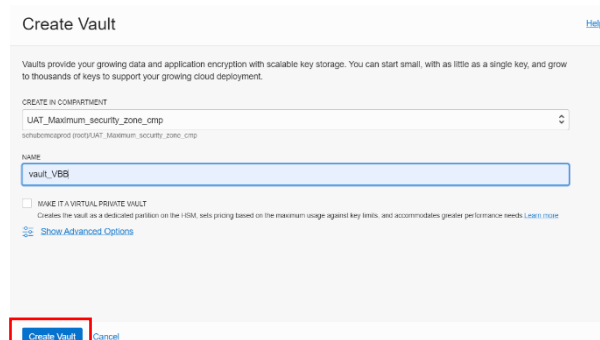
3. On the left choose the compartment UAT_Maximum_security_zone_cmp



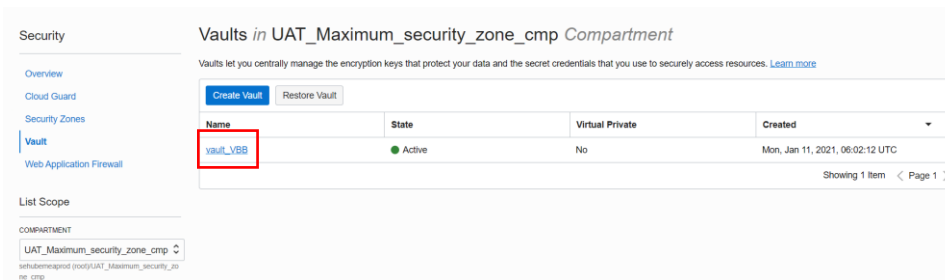
4. Click Create Vault



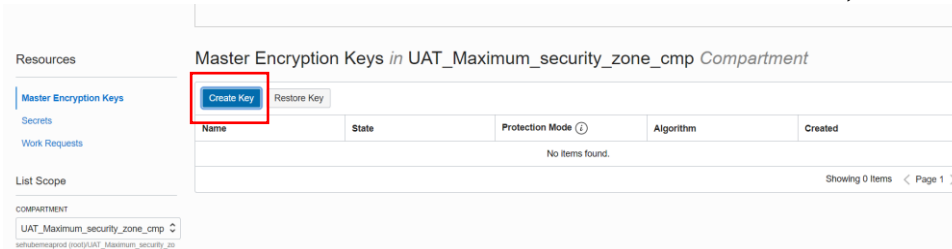
5. Fill in the below details
- Name: Select a name for your vault (eg: vault_VBB)
 - Click Create Vault



6. Click the Vault that we've just created: vault_VBB



7. You will be redirected to the Vault console, where you can see the Vault Information and at the bottom the resources associated to this Vault. Click Create key



8. Fill in the required fields:
- In Create Compartment choose: UAT_Maximum_security_zone_cmp
 - Protection mode: HSM
 - Enter a name to identify the key: VM2-Key
 - Leave the Key Shape Length to 128 bits
 - Click Create Key

Create Key [Help](#)

CREATE IN COMPARTMENT

UAT_Maximum_security_zone_cmp

sehubemeaprod (root)UAT_Maximum_security_zone_cmp

PROTECTION MODE ⓘ

HSM

NAME

VM2-KEY

KEY SHAPE: ALGORITHM

AES

KEY SHAPE: LENGTH

128 bits

☐ IMPORT EXTERNAL KEY

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

[Show Advanced Options](#)

[Create Key](#) [Cancel](#)

10.5 Summary

So far, we have created one compartment, three Policies for the existing NetworkAdmins, InstanceAdmins and SecurityAdmins groups, which was created in the earlier section, one policy for the root compartment, one Vault and key for the computes instance.

We will use the same users mentioned in previous section userVM and userNetwork

Good job so far, and let's proceed now to the scenarios where maximum-security zone can helps us in preventing the cloud security misconfigurations.

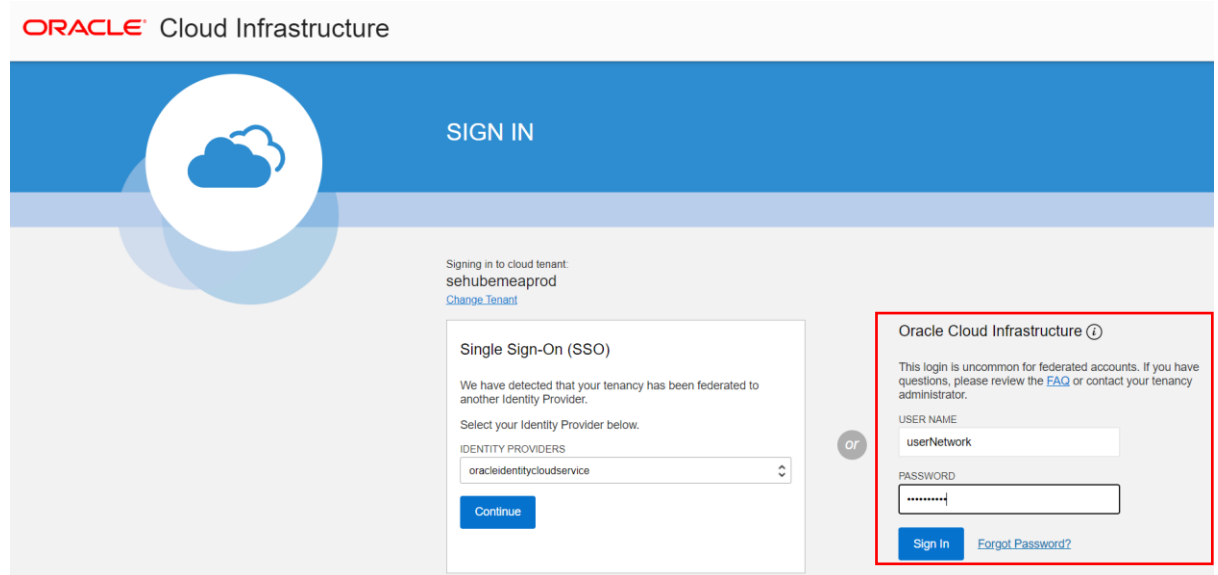
10.6 Use cases

10.6.1 Scenario 1: Create a subnet that allows public IPs in a compartment

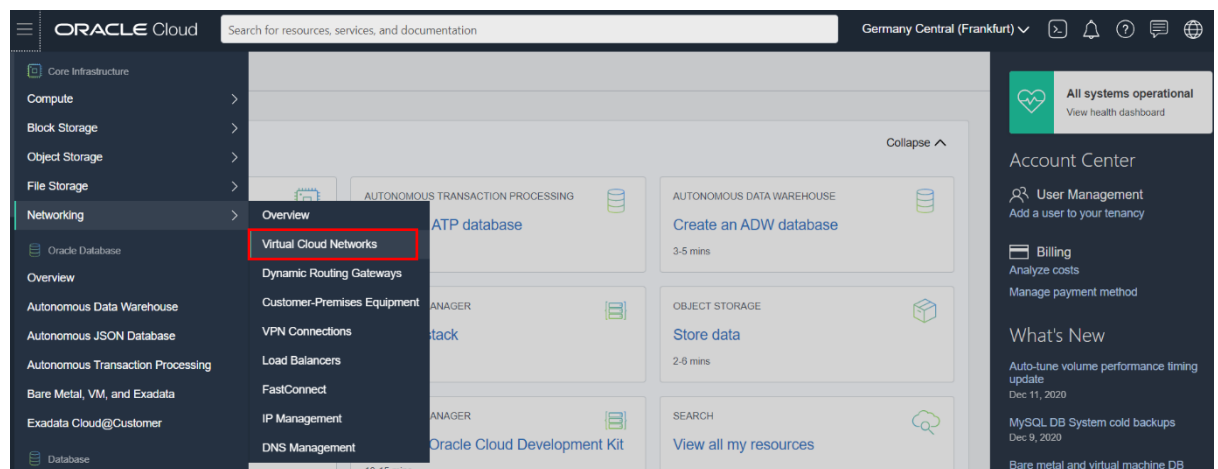
UAT_Maximum_security_zone_cmp (Which is in Maximum security Zone)

Access the OCI Console using the user – userNetworks.

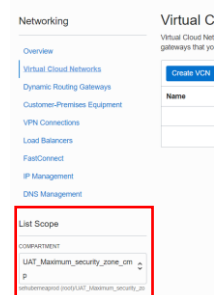
1. Sign out with your current user (default administrator user) and log in with userNetworks



2. In the OCI Console on the left side of the menu Networking – Virtual cloud networks



3. In List Scope select UAT_Maximum_security_zone_cmp Compartment, if not already selected



4. Click Create VCN and fill in the below details
 - o Name: Maximum_security_zone_VCN
 - o CIDR Blocks: 10.0.0.0/16
 - o Click create VCN

Create a Virtual Cloud Network [Help](#)

NAME
Maximum_security_zone_VCN

CREATE IN COMPARTMENT
UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

CIDR Blocks

i The IP ranges of the CIDR blocks must not overlap. [Learn more.](#)

CIDR BLOCK
10.0.0.0/16
Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

[+ Another CIDR Block](#)

DNS RESOLUTION

[Create VCN](#) [Cancel](#)

5. VCN is created, now click on Create subnet

Networking » Virtual Cloud Networks » Virtual Cloud Network Details

Maximum_security_zone_VCN

[Move Resource](#) [Add Tags](#) [Terminate](#)

VCN
AVAILABLE

VCN Information **Tags**

Compartment: UAT_Maximum_security_zone_cmp
Created: Sun, Jan 10, 2021, 19:54:25 UTC
CIDR Block: 10.0.0.0/16

OCID: ...dx796q [Show](#) [Copy](#)
DNS Resolver: ...w7ptsa [Show](#) [Copy](#)
Default Route Table: [Default Route Table for Maximum_security_zone_VCN](#)
DNS Domain Name: maximumsecurity.oraclevcn.com

Resources

- Subnets (0)**
- CIDR Blocks (1)
- Route Tables (1)
- Internet Gateways (0)

Subnets in UAT_Maximum_security_zone_cmp Compartment

[Create Subnet](#)

Name	State	CIDR Block	Subnet Access	Created
No items found.				

6. Fill in the below details in subnet creation page
 - o Name: Public subnet
 - o Create in compartment: UAT_Maximum_security_zone_cmp
 - o Subnet Type: Regional
 - o CIDR Block: 10.0.0.0/24
 - o Subnet Access: Public Subnet
 - o Leave everything else default and Click create subnet

Create Subnet

NAME
Public_subnet

CREATE IN COMPARTMENT
UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

SUBNET TYPE

Regional (Recommended)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability. ✓

Availability Domain-specific
Instances in the subnet can only be created in one availability domain in the region.

CIDR Block

CIDR BLOCK
10.0.0.0/24
Specified IP addresses: 10.0.0.0-10.0.0.255 (256 IP addresses)

ROUTE TABLE COMPARTMENT IN UAT_MAXIMUM_SECURITY_ZONE_CMP [\(CHANGE COMPARTMENT\)](#)

Create Subnet Cancel

7. The Create action should be denied with the message: **Security Zone Violation: Subnets cannot be public. All subnets in a security zone must be private.**

Create Subnet

NAME
Public_subnet

CREATE IN COMPARTMENT
UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

SUBNET TYPE

Regional (Recommended)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability. ✓

Availability Domain-specific
Instances in the subnet can only be created in one availability domain in the region.

CIDR Block

CIDR BLOCK
10.0.0.0/24
Specified IP addresses: 10.0.0.0-10.0.0.255 (256 IP addresses)

Security Zone Violation: Subnets cannot be public. All subnets in a security zone must be private.

Create Subnet Cancel

The prevention of creating a public subnet in a Security Zone, is the expected behaviour of Security zone and a Scenario PASS.

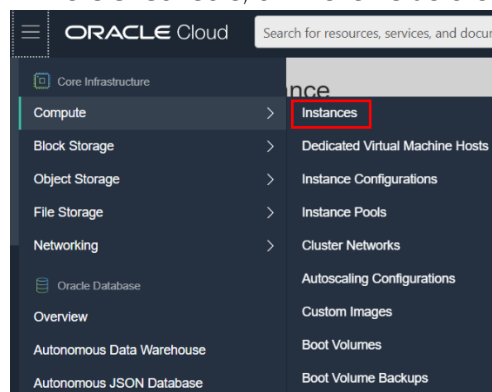
10.6.2 Scenario 2: Create an instance in a security zone compartment (UAT_Maximum_security_zone_cmp) with an associated subnet not in a security zone (Production)

Access the OCI Console using the user – userVM.

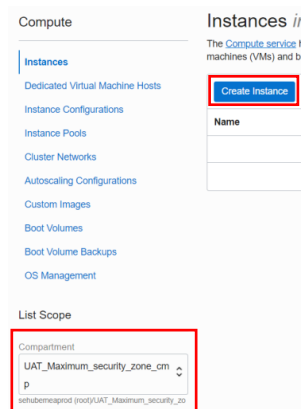
1. Sign out with your current user (userNetworks) and log in with userVM

ORACLE Cloud Infrastructure

2. In the OCI Console, on the left side click Menu – Compute – Instances.



3. On the left choose the compartment UAT_Maximum_security_zone_cmp, and click Create Instance:



4. Fill in the required details:
 - o Enter the name of the Instance: ComputeVM
 - o Select any of the Availability domain: eg AD1

Create Compute Instance

Name
ComputeVM

Create in compartment
UAT_Maximum_security_zone_cmp
setubemeresprod (pool)UAT_Maximum_security_zone_cmp

Configure placement and hardware Collapse

The [availability domain](#) helps determine which shapes are available. A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Availability domain

AD 1 ILR:EU-FRANKFURT-1-AD-1 ✓	AD 2 ILR:EU-FRANKFURT-1-AD-2	AD 3 ILR:EU-FRANKFURT-1-AD-3
-----------------------------------	---------------------------------	---------------------------------

☐ Choose a fault domain for this instance
If you don't select a fault domain, Oracle will choose the best placement for you. [Learn more](#)

- o Leave the OS image to Oracle Linux 7.9
- o Leave the default shape AMD VM. Standard.E3. Flex

Image

ORACLE Linux
Oracle Linux 7.9
Image build: 2020.11.10-1 Change Image

Shape

AMD VM.Standard.E3.Flex
Virtual Machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth Change Shape

- o Under the Network click Change Compartment and change it to Production and VCN-VBA Virtual cloud network which we created in previous section.
- o Under the Subnet click Change compartment and change it to Production and select the existing Public subnet/private subnet available, which we created in previous section.

Configure networking Collapse

[Networking](#) is how your instance connects to the Internet and other resources in the Console. To make sure you can [connect to your instance](#), assign a public IP address to the instance.

Network

☒ Select existing virtual cloud network ☐ Create new virtual cloud network ☐ Enter subnet OCID

Virtual cloud network in **Production** [\(Change Compartment\)](#)

VCN-VBA

Subnet

☒ Select existing subnet ☐ Create new public subnet

Subnet in **Production** [\(Change Compartment\)](#)

Public Subnet-VCN-VBA (Regional)

☐ Use network security groups to control traffic [?](#)

- o Leave the section Add SSH keys as it is

Add SSH keys

Linux-based instances use an [SSH key pair](#) instead of a password to authenticate remote users. Generate a key pair or upload your own public key now. When you [connect to the instance](#), you will provide the associated private key.

☒ Generate SSH key pair ☐ Choose public key files ☐ Paste public keys ☐ No SSH keys

i Download the private key so that you can connect to the instance using SSH. It will not be shown again.

[Save Private Key](#) [Save Public Key](#)

- Under the configure Boot volume
 - Select the Use in-transit encryption check box: Enable encryption between the VM and the boot volume.
 - Select Encrypt This Volume with A Key That You Manage: Boot volumes are encrypted by default, but you can optionally use your own Vault service encryption key to encrypt the data in this volume. If you enable this option, this key is used for both data at rest encryption and in-transit encryption
- Vault Compartment: UAT_Maximum_security_zone_cmp
- Vault: Choose the Vault created in Section 10.4 (vault_VBB)
- Master Encryption Key Compartment: UAT_Maximum_security_zone_cmp
- Master Encryption Key: Select the Key created in Section 10.4 (VM2-KEY)
- Click Create

Configure boot volume

Your **boot volume** is a detachable device that contains the image used to boot your compute instance.

☐ Specify a custom boot volume size
[Volume performance](#) varies with volume size. Default boot volume size: 46.6 GB

☒ Use in-transit encryption
[Encrypts data](#) in transit between the instance, the boot volume, and the block volumes.

☒ Encrypt this volume with a key that you manage
 By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. [Learn more about managing your own encryption keys](#)

Vault compartment: UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Vault: vault_VBB

Master encryption key compartment: UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Master encryption key: VM2-KEY

[Show Advanced Options](#)

Create Create as Stack Cancel

- New dialogue box appears since we have not given any SSH keys, click yes, Create Instance Anyway

Create Compute Instance

Name: ComputeVM

Create in compartment: UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Configure placement and hardware

No SSH Access [Help](#)

You will not be able to connect to this instance using SSH because you have not saved the private SSH key. Are you sure you want to create the instance without SSH access?

Yes, Create Instance Anyway Cancel

The [availability domain](#) helps determine which shapes are available. A [shape](#) is a template that determines the number of CPUs, amount of memory,

- The Create action should be denied with the message: Security Zone Violation: The compute instance is in a security zone, but a subnet used by the compute instance is not in a security zone.

Configure placement and hardware [Collapse](#)

The [availability domain](#) helps determine which shapes are available. A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Availability domain

AD 1 ILRI:EU-FRANKFURT-1-AD-1 ✓	AD 2 ILRI:EU-FRANKFURT-1-AD-2	AD 3 ILRI:EU-FRANKFURT-1-AD-3
---	---	---

☐ Choose a fault domain for this instance
If you don't select a fault domain, Oracle will choose the best placement for you. [Learn more](#)

Security Zone Violation: The compute instance is in a security zone, but a subnet used by the compute instance is not in a security zone.

[Create](#) [Create as Stack](#) [Cancel](#)

[Terms of Use and Privacy](#) [Cookie Preferences](#)

- The prevention of creating an Instance with a subnet that is not in a Security Zone, is the expected behaviour of SZ and a Scenario PASS.

10.6.3 Scenario 3: Create an instance in a security zone without sanctioned image (which is not an Oracle image)

- Sign out with your current user (userVM) and log in with userNetworks

ORACLE Cloud Infrastructure

SIGN IN

Signing in to cloud tenant: **sehubemeaprod**
[Change Tenant](#)

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

IDENTITY PROVIDERS
oracleidentitycloudservice

[Continue](#)

Oracle Cloud Infrastructure

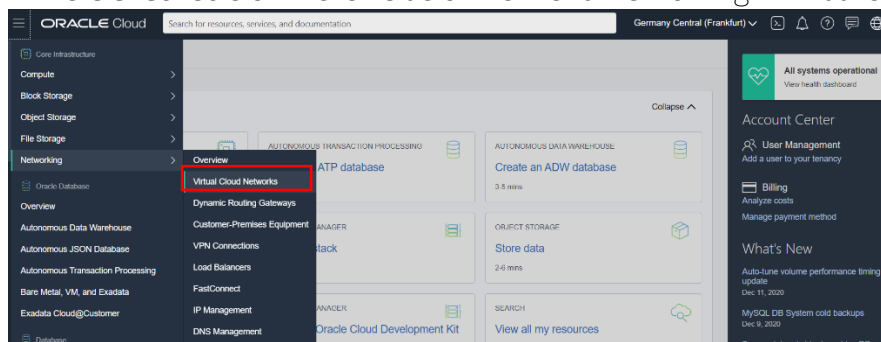
This login is uncommon for federated accounts. If you have questions, please review the [FAQ](#) or contact your tenancy administrator.

USER NAME
userNetwork

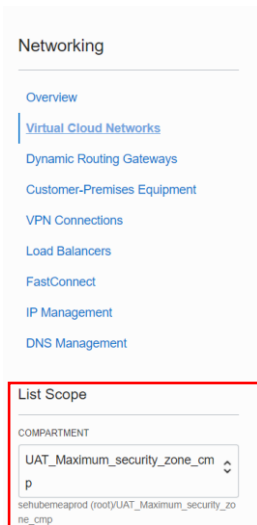
PASSWORD

[Sign In](#) [Forgot Password?](#)

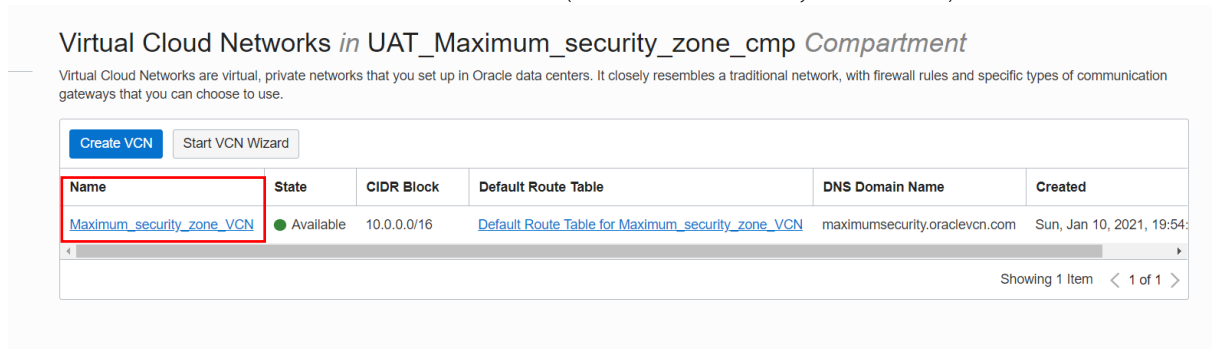
- In the OCI Console on the left side of the menu Networking – Virtual cloud networks



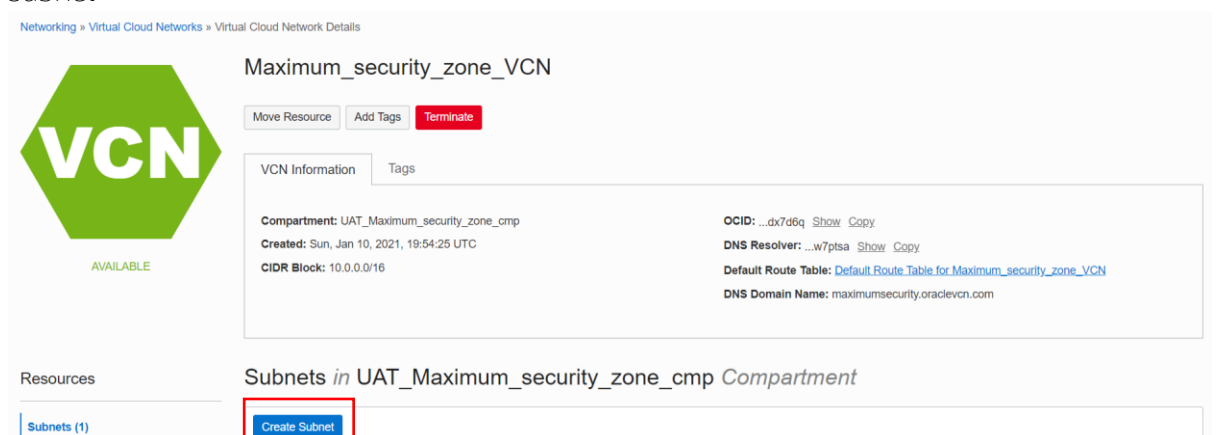
3. In List Scope select UAT_Maximum_security_zone_cmp Compartment, if not already selected



4. Click the VCN which we create in use-case 1 (Maximum_security_zone_vcn)



5. It will redirect to VCN console scroll down you can see the resources click on create subnet



6. Fill in the below details:
 - o Name: enter the any name for subnet (eg: Private_subnet)
 - o Compartment: Choose the maximum-security zone compartment (UAT_Maximum_security_zone_cmp)
 - o Subnet Type: Regional
 - o CIDR Block: 10.0.0.0/24

- o Subnet Access: Private Subnet
- o Leave the remaining options as it is and click Create Subnet.

Create Subnet

NAME
Private_subnet

CREATE IN COMPARTMENT
UAT_Maximum_security_zone_cmp
sehubemeaprod (root)UAT_Maximum_security_zone_cmp

SUBNET TYPE

Regional (Recommended)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability. ✓

Availability Domain-specific
Instances in the subnet can only be created in one availability domain in the region.

CIDR Block

CIDR BLOCK
10.0.0.0/24
Specified IP addresses: 10.0.0.0-10.0.0.255 (256 IP addresses)

Create Subnet

ROUTE TABLE COMPARTMENT IN UAT_MAXIMUM_SECURITY_ZONE_CMP [\(CHANGE COMPARTMENT\)](#)

Select a route table

SUBNET ACCESS

Private Subnet
Prohibit public IP addresses for Instances in this Subnet ✓

Public Subnet
Allow public IP addresses for Instances in this Subnet


DNS RESOLUTION
☒ USE DNS HOSTNAMES IN THIS SUBNET ⓘ
Allows assignment of DNS hostname when launching an Instance

DNS LABEL
Privatesubnet
Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME READ-ONLY
<dns-label>.maximumsecurity.oraclevcn.com

Create Subnet [Cancel](#)

7. Sign out with your current user (userNetworks) and log in with userVM
ORACLE Cloud Infrastructure



SIGN IN

Signing in to cloud tenant:
sehubemeaprod
[Change Tenant](#)

Single Sign-On (SSO)

We have detected that your tenancy has been federated to another Identity Provider.

Select your Identity Provider below.

IDENTITY PROVIDERS
oracleidentitycloudservice

Continue

Oracle Cloud Infrastructure ⓘ

This login is uncommon for federated accounts. If you have questions, please review the [FAQ](#) or contact your tenancy administrator.

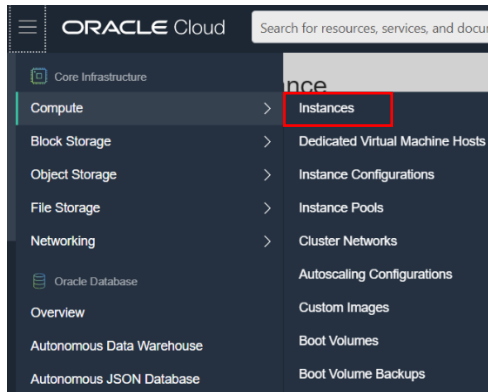
or

USER NAME
userVM

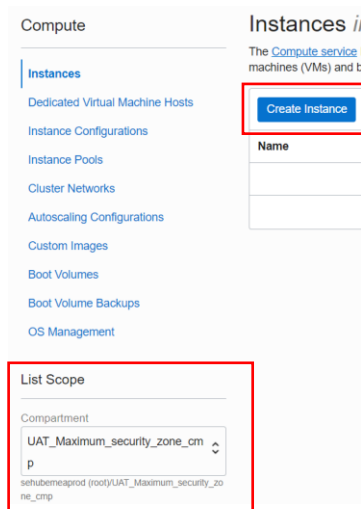
PASSWORD

Sign In [Forgot Password?](#)

8. In the OCI Console, on the left side click Menu – Compute – Instances.



9. On the left choose the compartment UAT_Maximum_security_zone_cmp, and click Create Instance:



10. Fill in the required details:
 - o Enter the name of the Instance: Partner_Image
 - o Select any of the Availability domain: eg AD1

Create Compute Instance

Name

Partner_Image

Create in compartment

UAT_Maximum_security_zone_cmp

sehubemeprod (root)UAT_Maximum_security_zone_cmp

Configure placement and hardware

The [availability domain](#) helps determine which shapes are available. A [shape](#) is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Availability domain

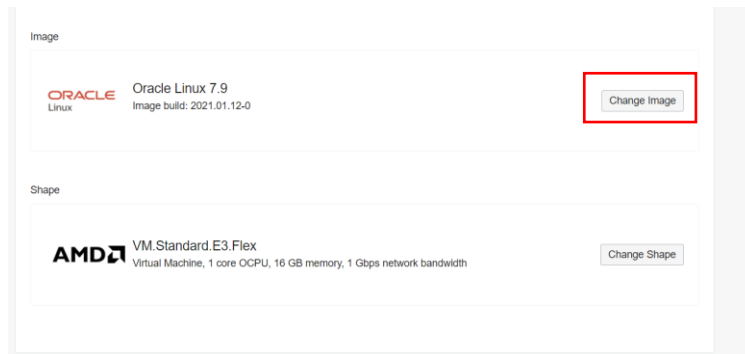
AD 1
ILRI:EU-FRANKFURT-1-AD-1 ✓

AD 2
ILRI:EU-FRANKFURT-1-AD-2

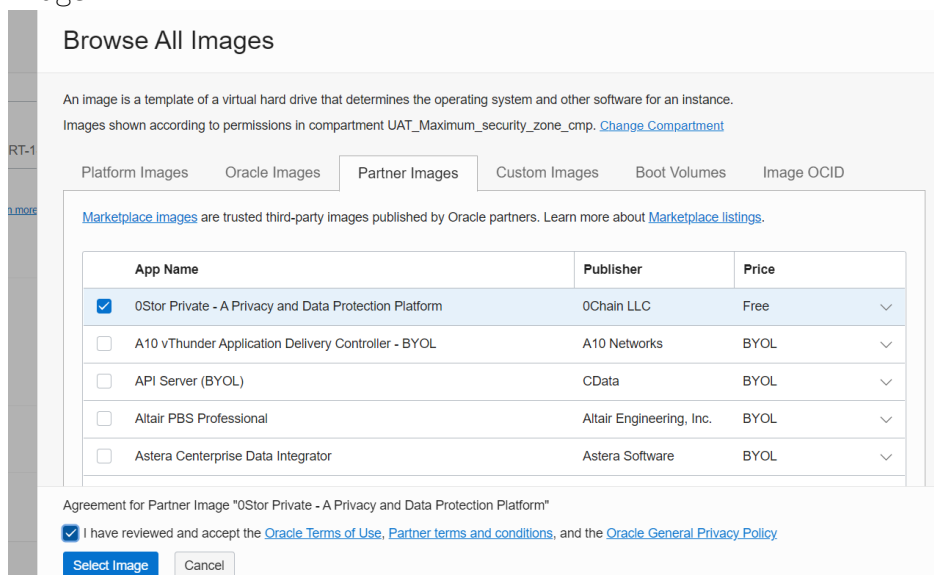
AD 3
ILRI:EU-FRANKFURT-1-AD-3

☐ Choose a fault domain for this instance
If you don't select a fault domain, Oracle will choose the best placement for you. [Learn more](#)

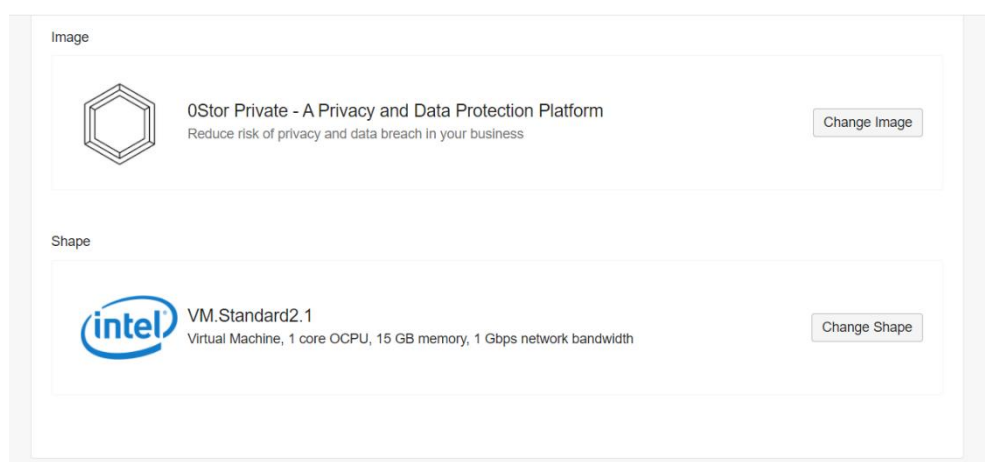
- o Click Change Image



- Click on Partner images tab
- Select any of the image and accept the terms and conditions and click select image



- Here I have selected Ostor Private image
- Leave the default image shape.



- Select the VCN and private subnet present in UAT_Maximum_security_zone_cmp compartment

Configure networking [Collapse](#)

[Networking](#) is how your instance connects to the internet and other resources in the Console. To make sure you can [connect to your instance](#), assign a public IP address to the instance.

Network
☒ Select existing virtual cloud network ☐ Create new virtual cloud network ☐ Enter subnet OCID

Virtual cloud network in **UAT_Maximum_security_zone_cmp** [\(Change Compartment\)](#)
 Maximum_security_zone_VCN

Subnet
☒ Select existing subnet ☐ Create new public subnet

Subnet in **UAT_Maximum_security_zone_cmp** [\(Change Compartment\)](#)
 Private_subnet (Regional)

☐ Use network security groups to control traffic [?](#)

- o Leave Add SHS Keys as it is

Public IP Address
☐ Assign a public IPv4 address ☒ Do not assign a public IPv4 address
Requires a public subnet

Add SSH keys

Linux-based instances use an [SSH key pair](#) instead of a password to authenticate remote users. Generate a key pair or upload your own public key now. When you [connect to the instance](#), you will provide the associated private key.

☒ Generate SSH key pair ☐ Choose public key files ☐ Paste public keys ☐ No SSH keys

[?](#) Download the private key so that you can connect to the instance using SSH. It will not be shown again.

- o Under the configure Boot volume
 - Select the Use in-transit encryption check box: Enable encryption between the VM and the boot volume.
 - Select Encrypt This Volume with A Key That You Manage: Boot volumes are encrypted by default, but you can optionally use your own Vault service encryption key to encrypt the data in this volume. If you enable this option, this key is used for both data at rest encryption and in-transit encryption
- o Vault Compartment: UAT_Maximum_security_zone_cmp
- o Vault: Choose the Vault created in Section 10.4 (vault_VBB)
- o Master Encryption Key Compartment: UAT_Maximum_security_zone_cmp
- o Master Encryption Key: Select the Key created in Section 10.4 (VM2-KEY)
- o Click Create

Configure boot volume

Your [boot volume](#) is a detachable device that contains the image used to boot your compute instance.

☐ Specify a custom boot volume size
[Volume performance](#) varies with volume size. Default boot volume size: 46.6 GB

☒ Use in-transit encryption
[Encrypts data](#) in transit between the instance, the boot volume, and the block volumes.

☒ Encrypt this volume with a key that you manage
By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. [Learn more about managing your own encryption keys](#)

Vault compartment: UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Vault: vault_VBB

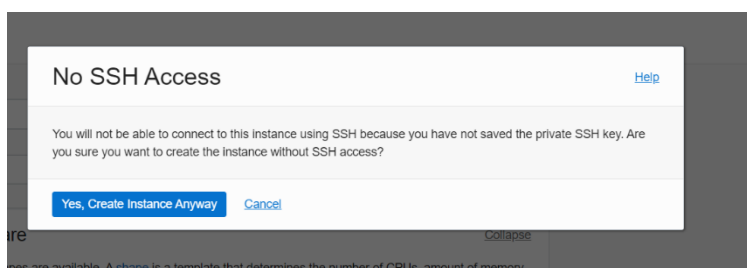
Master encryption key compartment: UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Master encryption key: VM2-KEY

[Show Advanced Options](#)

Create Create as Stack Cancel

- o New dialogue box appears since we have not given any SSH keys, click yes, Create Instance Anyway



- The Create action should be denied with the message: **Security Zone Violation: The compute instance uses a custom image. All instances in a security zone must use an Oracle-provided platform image.**

Vault compartment: UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Vault: vault_VBB

Master encryption key compartment: UAT_Maximum_security_zone_cmp
sehubemeaprod (root)/UAT_Maximum_security_zone_cmp

Master encryption key: VM2-KEY

[Show Advanced Options](#)

Security Zone Violation: The compute instance uses a custom image. All instances in a security zone must use an Oracle-provided platform image.

Create Create as Stack Cancel

- The prevention of creating an Instance with an Image that is not an Oracle-provided platform image in a Security Zone, is the expected behaviour of SZ and a Scenario PASS.

11 Conclusions

In this lab we have tested several OCI services and observed how for each of them we can apply flexible security measures.

Security is Oracle's main concern and the simplicity to implement them.

Congratulations for the completion of this lab and good luck!