



OCI Deployment Guide

FortiMail 7.2.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

October 22, 2024

FortiMail 7.2.0 OCI Deployment Guide

06-720-000000-20241022

TABLE OF CONTENTS

Change Log	4
Introduction	5
Creating a Virtual Cloud Network and Public-facing Subnet	6
Creating a FortiMail-VM Instance	12
Attaching Storage to FortiMail	18
Accessing FortiMail	20

Change Log

Date	Change Description
2024-10-22	Initial release of FortiMail 7.2.0 OCI Deployment Guide

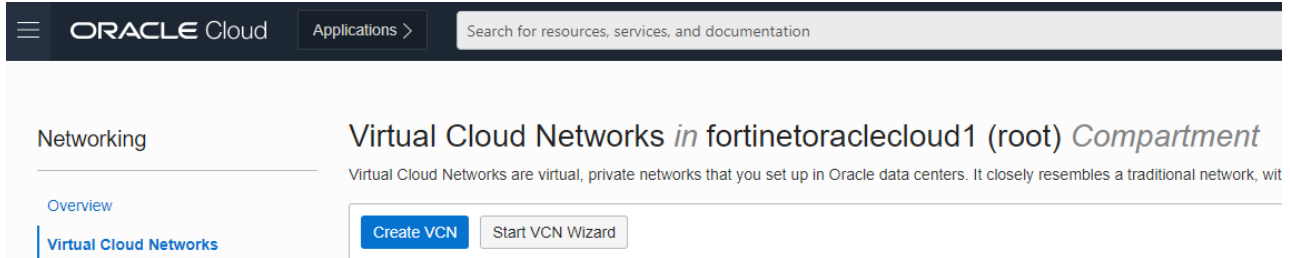
Introduction

This document describes how to deploy FortiMail VM on Oracle Cloud Infrastructure (OCI). Note that some company or product related information is hidden on purpose in the screen captures.

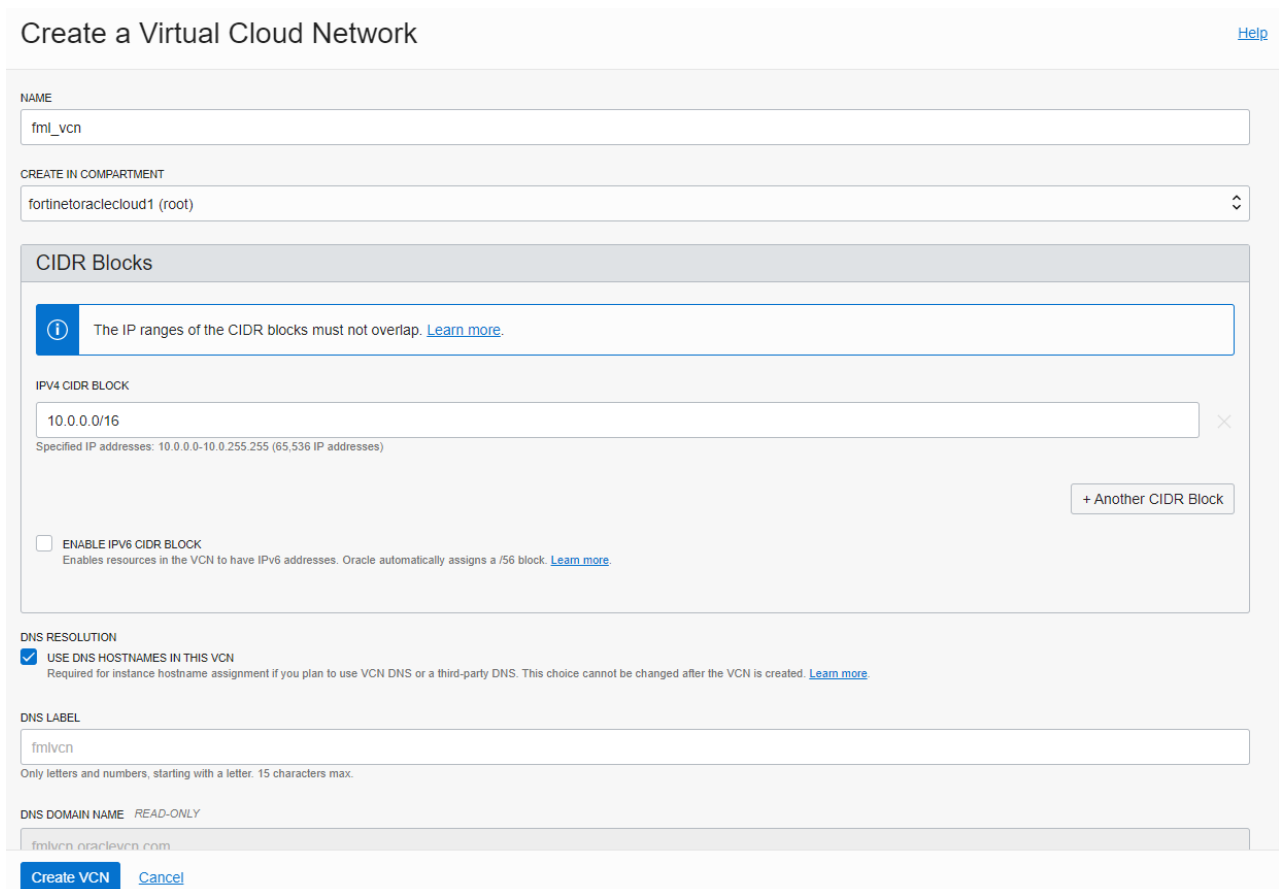
For details about how to use FortiMail, see the FortiMail Administration Guide on <https://docs.fortinet.com>.

Creating a Virtual Cloud Network and Public-facing Subnet

1. In OCI, go to **Networking > Virtual Cloud Networks**, and click **Create Virtual Cloud Network**.




2. Enter the **NAME** and **IPV4 CIDR BLOCK**, then **Create VCN**.



3. In the **VCN details** page, create a public-facing subnet.

Creating a Virtual Cloud Network and Public-facing Subnet

Networking » Virtual Cloud Networks » Virtual Cloud Network Details



VCN

AVAILABLE

fml_vcn

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

VCN Information | Tags

Compartment: fortinetoraclecloud1 (root) **OCID:** ...5qr4sa [Show](#) [Copy](#)

Created: Wed, Apr 21, 2021, 06:11:07 UTC **DNS Resolver:** [fml_vcn](#)

IPv4 CIDR Block: 10.0.0.0/16 **Default Route Table:** [Default Route Table for fml_vcn](#)

IPv6 CIDR Block: No Value **DNS Domain Name:** fmlvcn.oraclevcn.com

Resources

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

Subnets *in fortinetoraclecloud1 (root) Compartment*

[Create Subnet](#)

Name	State	IPv4 CIDR Block	Subnet Access
No items found.			

4. When creating the subnet, choose **SUBNET TYPE** as **Regional** and **SUBNET ACCESS** as **Public Subnet**.

Create Subnet

NAME
fml_vcn_public_sub

CREATE IN COMPARTMENT
fortinetoraclecloud1 (root)

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 FORTINETORACLECLOUD1 (ROOT) [\(CHANGE COMPARTMENT\)](#)
Default Route Table for fml_vcn

SUBNET ACCESS

Private Subnet
Prohibit public IP addresses for Instances in this Subnet

Public Subnet
Allow public IP addresses for Instances in this Subnet ✓

Leave **ROUTE TABLE**, **DHCP OPTIONS**, and **SECURITY LIST** as default, and you will need to modify them later.

DNS LABEL

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

DNS DOMAIN NAME READ-ONLY

DHCP OPTIONS COMPARTMENT IN FORTINETORACLECLOUD1 (ROOT) [\(CHANGE COMPARTMENT\)](#)

Security Lists

You can associate up to 5 network security lists with the subnet.

SECURITY LIST COMPARTMENT IN FORTINETORACLECLOUD1 (ROOT) [\(CHANGE COMPARTMENT\)](#)

[+ Another Security List](#)

[Show Tagging Options](#)

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

5. To access FortiMail with HTTPS, add an **Ingress Rule in **Default Security List**.**

You will see that three rules are set up by default, including port 22 for SSH access. There would be more ports needed for later testing, such as port 25 for SMTP, and you can always add or modify these rules later.

Networking > Virtual Cloud Networks > fml_vcn > Security List Details Subnet provisioning successfully initiated.

Default Security List for fml_vcn

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: ...3xwjpq [Show](#) [Copy](#) Compartment: fortinetoraclecloud1 (root)

Created: Wed, Apr 21, 2021, 06:11:07 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	0.0.0.0/0	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

Add an **Ingress Rule** as below, and set **IP PROTOCOL** as **TCP** and **DESTINATION PORT** as **443**.

Ingress Rule 1

Allows TCP traffic 443 HTTPS

STATELESS ⓘ

SOURCE TYPE: CIDR

SOURCE CIDR: 0.0.0.0/0
Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

IP PROTOCOL ⓘ: TCP

SOURCE PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22

DESTINATION PORT RANGE OPTIONAL ⓘ: 443
Examples: 80, 20-22

DESCRIPTION OPTIONAL

Maximum 255 characters

The Egress Rules are set for ALL TRAFFIC FOR ALL PORTS, and there is no need to modify it.

Resources

Egress Rules


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

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

0 Selected Showing 1 item < 1 of 1 >

6. Create an Internet Gateway for your VCN.

Networking > Virtual Cloud Networks > Virtual Cloud Network Details > Internet Gateways



fml_vcn

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

VCN Information | [Tags](#)

Compartment: fortinetoraclecloud1 (root)
Created: Wed, Apr 21, 2021, 06:11:07 UTC
IPv4 CIDR Block: 10.0.0.0/16
IPv6 CIDR Block: No Value

OCID: ...5qr4sa [Show](#) [Copy](#)
DNS Resolver: [fml_vcn](#)
Default Route Table: [Default Route Table for fml_vcn](#)
DNS Domain Name: fmlvcn.oraclevcn.com

Resources

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

Internet Gateways in fortinetoraclecloud1 (root) Compartment

[Create Internet Gateway](#)

Name	State	Created
No items found.		

Create Internet Gateway [Help](#) [Cancel](#)

NAME

fml_vcn-gateway

CREATE IN COMPARTMENT

fortinetoraclecloud1 (root)

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) ×

[+ Additional Tag](#)

[Create Internet Gateway](#) [Cancel](#)

7. Add a **Route Rule** for the **Default Route Table**.

[Networking](#) » [Virtual Cloud Networks](#) » [fml_vcn](#) » Route Table Details



AVAILABLE

Default Route Table for fml_vcn

Move Resource
Add Tags
Terminate

Route Table Information
Tags

OCID: ...s7666q [Show](#) [Copy](#)

Created: Wed, Apr 21, 2021, 06:11:07 UTC

Resources

Route Rules (0)

Route Rules

Add Route Rules
Edit
Remove

	Destination	Target Type
<input type="checkbox"/>		

0 Selected

8. Choose **TARGET TYPE** as **Internet Gateway**, and choose the gateway you just created, and you can set **DESTINATION CIDR BLOCK** as **0.0.0.0/0** for all.

Add Route Rules

[Help](#)

Important:
For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

Route Rule

TARGET TYPE
Internet Gateway

DESTINATION CIDR BLOCK
0.0.0.0/0
Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

TARGET INTERNET GATEWAY IN FORTINETORACLECLOUD1 (ROOT) [\(CHANGE COMPARTMENT\)](#)
fml_vcn-gateway

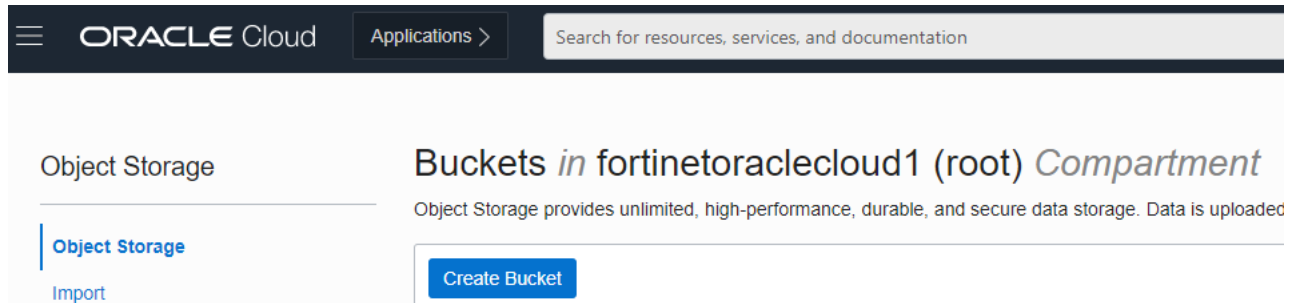
DESCRIPTION OPTIONAL

Maximum 255 characters

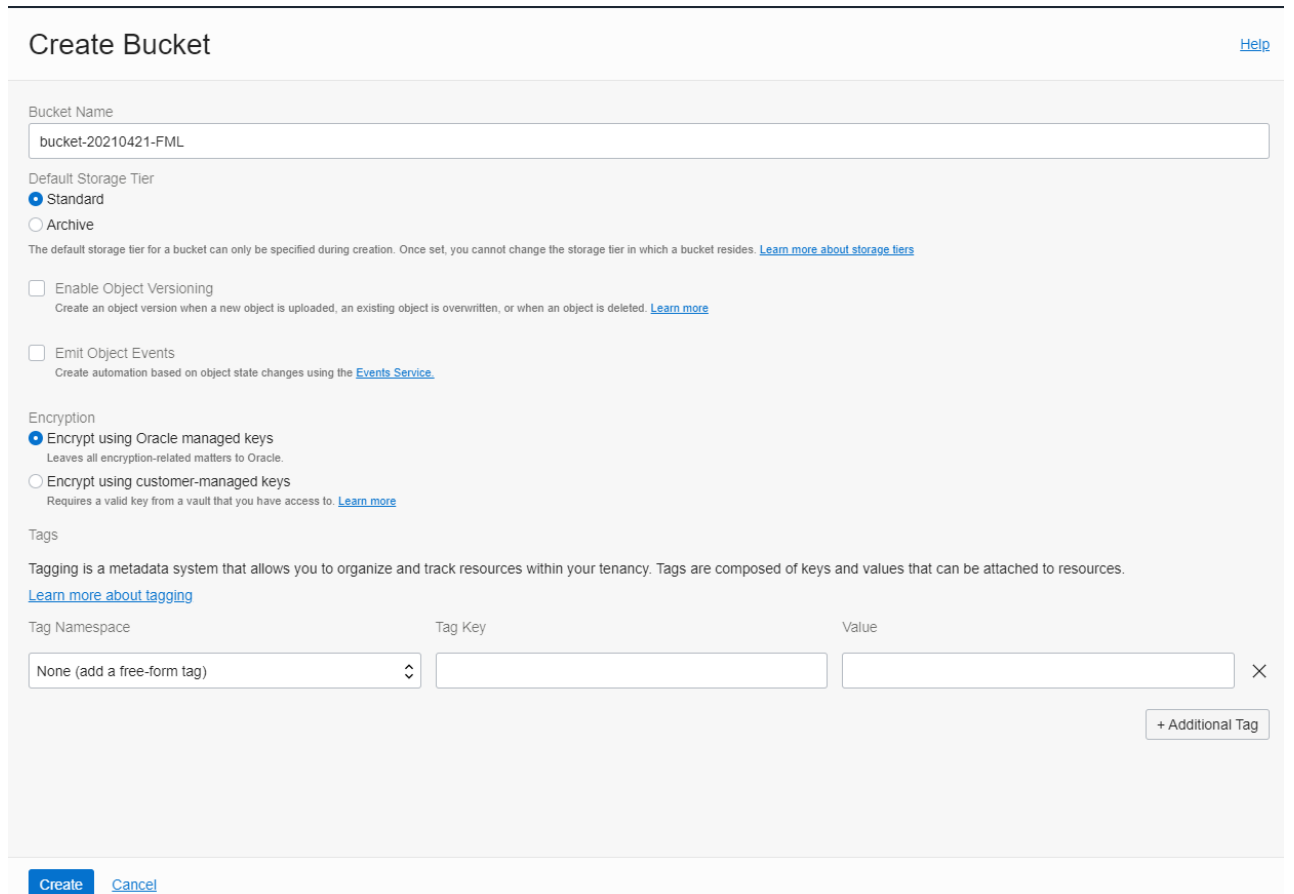
[+ Another Route Rule](#)

Creating a FortiMail-VM Instance

1. Go to <https://support.fortinet.com> and download the FortiMail VM image FML_VMOC-64-vxx-build0xxx-FORTINET.out.openxen.zip file. Unzip it to get the 'fortimail-opc.qcow2' file, which is needed to deploy FortiMail on OCI.
2. On OCI, go to **Object Storage**, then click **Create Bucket** to create a standard storage bucket.



You can create the bucket with default settings.



3. Click into the bucket you just created and upload the *.qcow2 file to **Objects**.

[Object Storage](#) » Bucket Details



bucket-20210421-FML

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

Bucket Information [Tags](#)

Visibility: Private
Namespace: fortinetoraclecloud1
Default Storage Tier: Standard
Approximate Count: 0 objects ⓘ
ETag: b5e06036-c049-450a-a6d0-52c6780a4e8e
OCID: ...i2i6hooa [Show](#) [Copy](#)

Resources

[Objects](#)

[Metrics](#)

[Pre-Authenticated Requests](#)

Objects

[Upload](#) [More Actions](#) ▼

<input type="checkbox"/>	Name	Last Modified
--------------------------	------	---------------

Upload Objects

Object Name Prefix *Optional*

FML_v70116_image

Storage Tier

Standard

Choose Files from your Computer

Drop files here or [select files](#)

fortimail-opc.qcow2 108.38 MiB

1 files, 108.38 MiB total

[Show Optional Response Headers and Metadata](#)

4. After the image file is uploaded, create a **Pre-Authenticated Request**.

Resources

- Objects
- Metrics
- Pre-Authenticated Requests
- Work Requests

Pre-Authenticated Requests

Create Pre-Authenticated Request

Name	Status	Target

Create Pre-Authenticated Request

Help

Name

Pre-Authenticated Request Target

Bucket

Create a pre-authenticated request that applies to all objects in the bucket.

Object

Create a pre-authenticated request that applies to a specific object. ✓

Objects with prefix

Create a pre-authenticated request that applies to all objects with a specific prefix.

Object Name

Access Type

Permit object reads

Permit object writes

Permit object reads and writes

Expiration

5. After the request is created, you will see the details window. Copy and save this URL, which will be used in later steps.

Pre-Authenticated Request Details

Name *Read-Only*

Pre-Authenticated Request URL *Read-Only*

!

Copy this URL for your records. It will not be shown again.

Close

6. Go to **Compute > Custom Images**. Click **Import Image**. Choose **Import from an Object Storage URL** and paste the previous URL. Under **IMAGE TYPE**, select **QCOW2**. Under **LAUNCH MODE**, select **PARAVIRTUALIZED MODE** or **EMULATED MODE**. Native mode is not supported.

Import Image [Help](#)

Create in compartment

fortinetoraclecloud1 (root)

Name

fml-v70116

Operating system

Linux

Import from an Object Storage bucket
 Import from an Object Storage URL

Object Storage URL

https://objectstorage.us-phoenix-1.oraclecloud.com/p/N7_av1CUKWuXlGTv8yG6-COAmw8eQEmIPBxDNMjHeAxzR9MDHareGtw3-uQw2Yv1n/fortinetoraclecloud1/b/bucket-20210421-FML

Learn more about [Object Storage URLs](#). Also, see the instructions to [create a pre-authenticated request](#).

Image type

VMDK
 Virtual machine disk file format. For disk images used in virtual machines.

QCOW2
 For disk image files used by QEMU.

OCI
 For images that were exported from Oracle Cloud Infrastructure. The launch mode is specified in the .oci file and can't be changed in the Console.

Launch mode

Firmware: BIOS **NIC attachment type:** PV NIC

Boot volume type: PV **Remote data volume:** PV

Paravirtualized Mode
 For virtual machines that [support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure.

Emulated Mode
 For virtual machines that [don't support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure from older on-premises physical or virtual machines.

Native Mode
 For images that were exported from Oracle Cloud Infrastructure.

Import Image [Cancel](#)

7. From the newly imported image, click **Create Instance**. Take note of the **Compatible Shapes**, and make sure to choose a shape from this list in later steps.

Compute > Custom Images > Custom Image Details

CI

fml-v70116-20210421

Create Instance
Edit Details
Edit Image Capabilities
Export
More Actions

Custom Image Information

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

Original Image: -

Compartment: fortinetoraclecloud1 (root)

Launch Mode: PARAVIRTUALIZED

Created: Wed, Apr 21, 2021, 07:14:15 UTC

Compatible Shapes: VM.Standard.E3.Flex, VM.Standard2.1, VM.Standard2.2, VM.Standard2.4, VM.Standard2.8, VM.Standard2.16, VM.Standard2.24, VM.Standard1.1, VM.Standard1.2, VM.Standard1.4, VM.Standard1.8, VM.Standard1.16

Flex Shape Requirements: 1 OCPU minimum, 64 OCPU maximum

Launch Options

Launch options include the networking type and boot volume attachment type used when launching a virtual machine instance. [Learn more](#)

NIC Attachment Type: PARAVIRTUALIZED

Remote Data Volume: PARAVIRTUALIZED

Firmware: BIOS

Boot Volume Type: PARAVIRTUALIZED

8. You can choose either **Availability domain** and keep the advanced options as default.

Create Compute Instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name
fml-20210421-v70116

Create in compartment
fortinetoraclecloud1 (root)

Placement Collapse

The [availability domain](#) helps determine which shapes are available.

Availability domain

AD 1 www1:PHX-AD-1 ✓	AD 2 www1:PHX-AD-2	AD 3 www1:PHX-AD-3
--------------------------------	------------------------------	------------------------------

[Hide advanced options](#)

Capacity type

- On-demand capacity
Place the instance on a shared host using on-demand capacity.
- Preemptible capacity
Place the instance on a shared host using [preemptible capacity](#). This instance can be reclaimed at any time.
- Capacity reservation
Place the instance on a shared host, and have it count against a [capacity reservation](#).
- Dedicated host
Place the instance on a [dedicated virtual machine host](#).

Fault Domain
Let Oracle choose the best fault domain

[When should I specify a fault domain?](#)

Image and shape are chosen automatically. You can modify the shape as desired.

Image and shape Collapse

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.

Image

fml-v70116-20210421 Change Image

Shape

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

9. Choose your VCN and its public subnet. For public access to FortiMail, you must assign a public IPV4 address.

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 **fortinetoracled1 (root)** ([Change Compartment](#))

fml_vcn

Subnet
 Select existing subnet Create new public subnet

Subnet in **fortinetoracled1 (root)** ([Change Compartment](#))

fml_vcn_public_sub (Regional)

Public IP Address
 Assign a public IPv4 address Do not assign a public IPv4 address

! Assigning a public IP address makes this instance accessible from the internet. If you're not sure whether you need a public IP address, you can always assign one later.

[Show advanced options](#)

10. Click **Generate SSH key pair** and **Save Private Key**. The private key will be used for SSH accessing. You can also paste your own SSH public key or skip this step for now. Specify the customer boot volume size as minimum 50 GB.

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 Upload public key files (.pub) 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](#)

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

Boot volume size (GB)

50

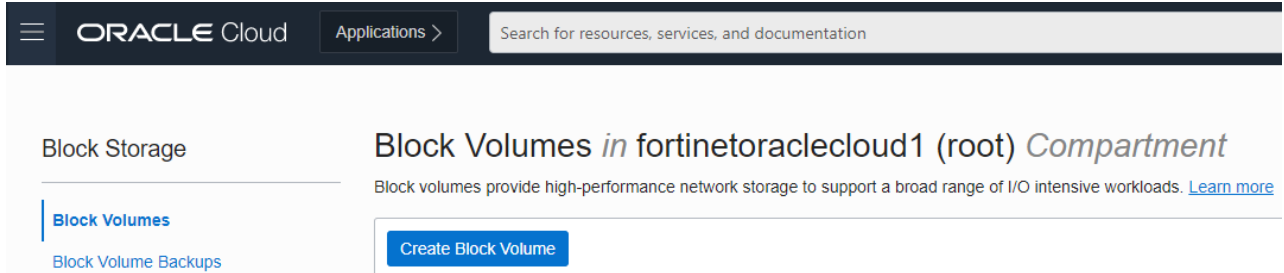
Integer between 50 GB and 32,768 GB (32 TB). Must be larger than the default boot volume size for the selected image.

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](#)

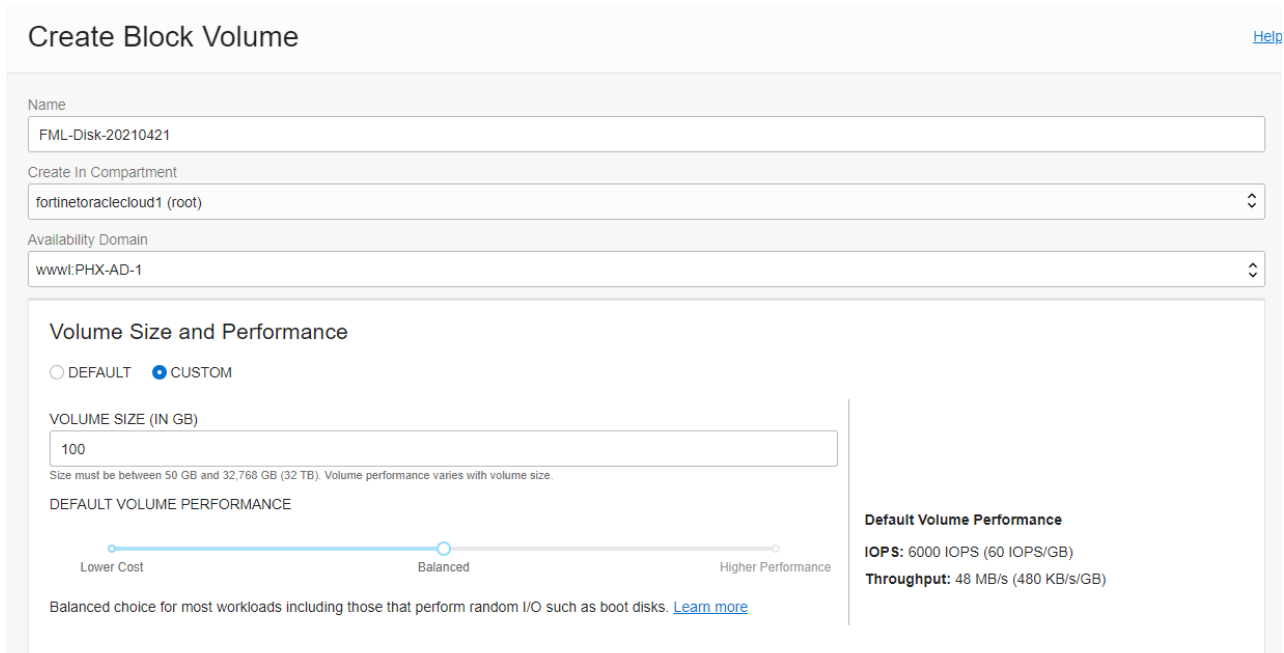
At this stage, the deployment is not complete yet. You also need to add a storage volume as a system log disk and attach it to the FortiMail instance. If you want FortiMail to run inline across two or multiple subnets, you will also need to add one or more virtual network interfaces and attach them to the FortiMail instance.

Attaching Storage to FortiMail

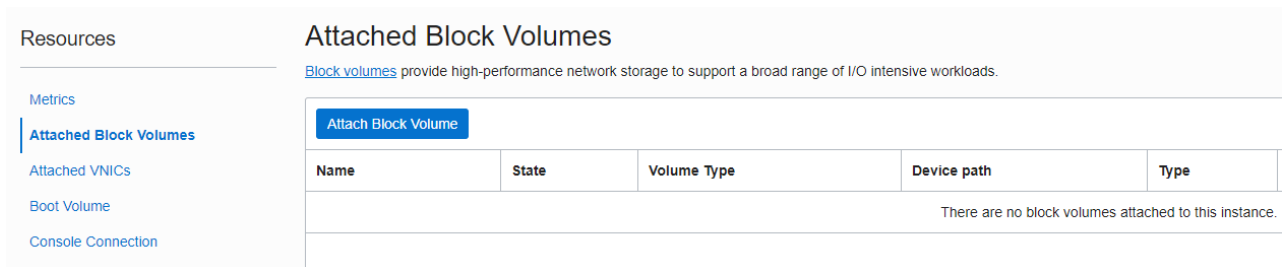
1. On OCI, go to **Storage > Block Volumes > Create Block Volume**.



Make sure the **Availability Domain** is the same as your instance, and customize a smaller volume size, for example, 100 GB. Keep other settings as default.



2. Once provisioned, return to the FortiMail instance. Click **Attach Block Volume**.



3. Select the block volume that you created earlier and ensure the attachment type is **Paravirtualized**.

Attach Block Volume [Help](#)

Volume attachment type

Let Oracle Cloud Infrastructure choose the best attachment type

iSCSI

Paravirtualized

Use in-transit encryption

Volume

Select volume Enter volume OCID

Volume in **fortinetoraclecloud1 (root)** [Change Compartment](#)

FML-Disk-20210421

Access

Read/Write
Configures the volume attachment as read/write, not shared with other instances. This enables attachment to a single instance only and is the default configuration.

Read/Write - Shareable
Configures the volume attachment as read/write, shareable with other instances. This enables read/write attachment to multiple instances.

Read Only - Shareable
Configures the volume attachment as read-only, enabling attachment to multiple instances.



After attaching the block volume, make sure to reboot the FortiMail instance.

- The last step is to upload a valid FML VM license, and then you should be able to see the FortiMail Admin GUI.

The screenshot displays the FortiMail Admin GUI for a device named 'FortiMail VM02'. The interface is divided into several sections:

- System Information:** Shows details such as Serial number (FEVM0200000), Up time (0 day(s) 0 hour(s) 26 minute(s) 24 second(s)), System time (Wed, Apr 21, 2021 11:00:46 PDT), Reboot time (Wed, Apr 21, 2021 10:34:22 PDT), Firmware version (v7.0.0, build116, 2021.04.16), System configuration (Backup/Restore), Operation mode (Gateway), Current administrator (admin), HA mode (Configured Off), Log disk (Capacity 19 GB, Used 32 MB), Mailbox disk (Capacity 78 GB, Used 276 MB), and Email throughput (0 messages per minute).
- License Information:** Lists licenses for AntiVirus (No license), AV definition (Version 1.00000), AV engine (Version 6.00258), Virus outbreak (Licensed), AntiSpam (Licensed), AS definition (Version 1.00001), VM (Registered), FortiSandbox (Disabled), and FortiCloud (Not Activated).
- System Resource:** Displays usage metrics: CPU usage (0%), Memory usage (6%), System load (1%), and Log disk usage (0%).
- Statistics History (Count, 30 Days):** Shows 'No data!'.
- Statistics Summary (Today):** Shows 'No data!'.
- Statistics Summary:** A table showing message classification statistics:

Messages	Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	Subtotal	0	0	0	0	0	0
Spam Classified By	Subtotal	0	0	0	0	0	0
Virus Classified By	Subtotal	0	0	0	0	0	0
Total		0	0	0	0	0	0
- Throughput History (Scan Speed, 30 Days):** A line graph showing throughput over time, with a y-axis ranging from 2 KB/s to 10 KB/s.

- For further testing on this FortiMail instance, you may need to add more rules in **Security List**. For example, a rule to open port 25 is necessary for SMTP testing.

The screenshot shows the 'Add Ingress Rules' configuration page. The title is 'Ingress Rule 1'. The rule is configured to allow TCP traffic on port 25 (SMTP). The configuration includes:

- STATELESS:** (with an information icon).
- SOURCE TYPE:** CIDR (dropdown menu).
- SOURCE CIDR:** 0.0.0.0/0 (text input field).
- IP PROTOCOL:** TCP (dropdown menu).
- Specified IP addresses:** 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses).
- SOURCE PORT RANGE:** All (text input field).
- DESTINATION PORT RANGE:** 25 (text input field).
- Examples:** 80, 20-22 (for both source and destination port ranges).
- DESCRIPTION:** (Empty text input field, with a note 'Maximum 255 characters').
- + Another Ingress Rule:** Button at the bottom right.

