FERTINET

OCI Administration Guide

FortiProxy 7.6

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

November 15, 2024
FortiProxy 7.6 OCI Administration Guide
45-760-1099602-20241115

TABLE OF CONTENTS

Change log

Date	Change description
2024-11-15	Initial document release.

Overview

Oracle Cloud Infrastructure Compute provides bare metal compute capacity that delivers performance, flexibility, and control without compromise. It is powered by Oracle’s next generation, internet-scale infrastructure designed to help you develop and run your most demanding applications and workloads in the cloud.

As of FortiProxy 7.6, FortiProxy-VM is supported in OCI Dedicated Region Cloud@Customer (DRCC). For more information, see Dedicated Region Cloud@Customer.

The following sections explain how to deploy the FortiProxy-VM on Oracle Cloud Infrastructure.

Instance type support

You can deploy FortiProxy-VM as bring your own license (BYOL) on OCI on all available instances that the FortiProxy-VM supports. Supported instances on OCI for new deployments may change without notice.

Models

FortiProxy-VM is available with different CPU sizes. You can deploy FortiProxy-VM on various private and public cloud platforms. The following table shows the models conventionally available to order, also known as bring your own license (BYOL) models. See Licensing on page 5.

Model name	vCPU	
	Minimum	Maximum
VM02	1	4
VM04	1	8
VM08	1	16
VM16	1	32
VMUL	1	Unlimited

For information about each model's order information, capacity limits, and adding VDOM, see the FortiProxy datasheet.

Licensing

You must have a license to deploy FortiProxy for OCI. On AWS, there is one order type for FortiProxy: bring-your-own-license (BYOL), which offers perpetual (normal series and v-series) and annual subscription (s-series) licensing. Subscription is month-based. BYOL licenses are available for purchase from resellers or your distributors, and the publicly available price list, which Fortinet updates quarterly, lists prices. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

For BYOL, cloud vendors charge separately for resource consumption on computing instances, storage, and so on, without use of software running on top of it (in this case the FortiProxy-VM). You typically order a combination of products and services including support entitlement.

To proceed with licensing a BYOL deployment and make use of Fortinet technical support, you must obtain a license, register it in FortiCloud, and activate the FortiProxy-VM:

1. Obtain licenses for the BYOL licensing model through any Fortinet partner. If you do not have a partner, contact jerrywang@fortinet.com for assistance in purchasing a license. You will receive a PDF with an activation code.
2. If you do not have a FortiCloud account, create one here by following the instructions in the FortiCloud documentation.
3. Register your license in your FortiCloud account by following the instructions in the FortiCloud documentation. Doing so allows our support team to identify your registration in the system.
4. Download the license (`.lic`) file to your computer as you will be prompted to upload this license to activate the FortiProxy-VM during the first login. Activation is required before you can configure the FortiProxy-VM.

It may take up to 30 minutes for Fortinet servers to fully recognize the new license. If you get an error that the license is invalid when uploading the license (`.lic`) file to activate the FortiProxy-VM, wait 30 minutes and try again.

Single FortiProxy-VM deployment

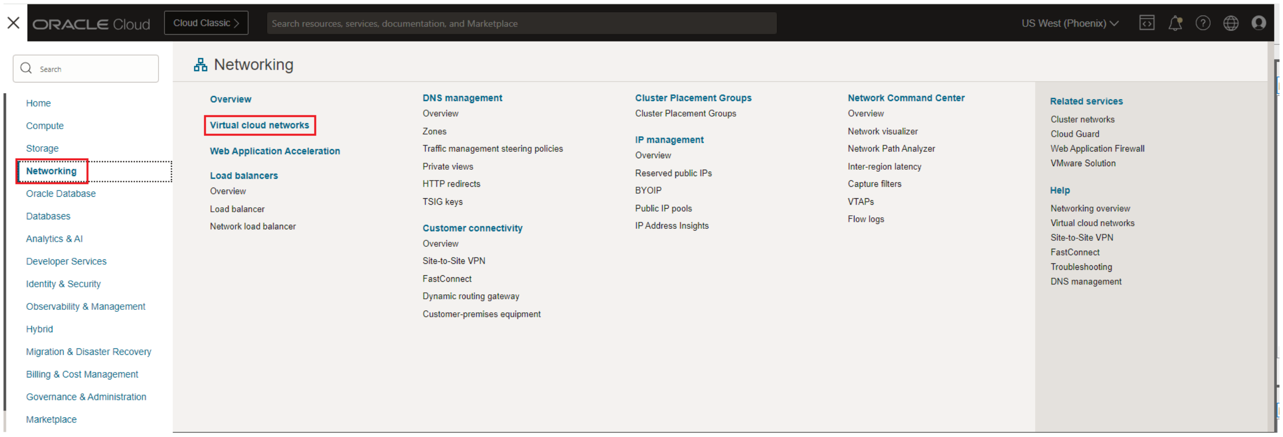
You can deploy a single FortiProxy-VM on OCI in in paravirtualized or emulated mode. The following sections describe the process:

1. Creating a virtual cloud network (VCN) with public-facing subnets on page 7
2. Creating a FortiProxy-VM instance on page 12
3. Accessing the FortiProxy-VM on page 24

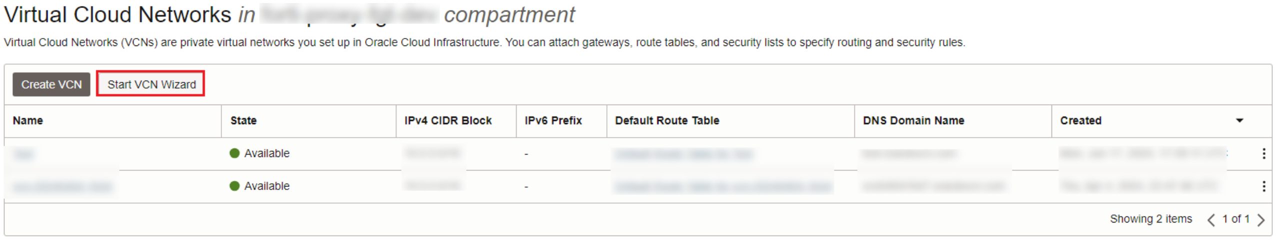
Creating a virtual cloud network (VCN) with public-facing subnets

To create a VCN with public-facing subnets:

1. In OCI, go to *Networking* > *Virtual cloud networks*.



2. Click *Start VCN Wizard* to create the Internet gateway, routing table, and subnet all together using Oracle default settings.
   You can also choose to create each resource separately by clicking *Create VCN*.

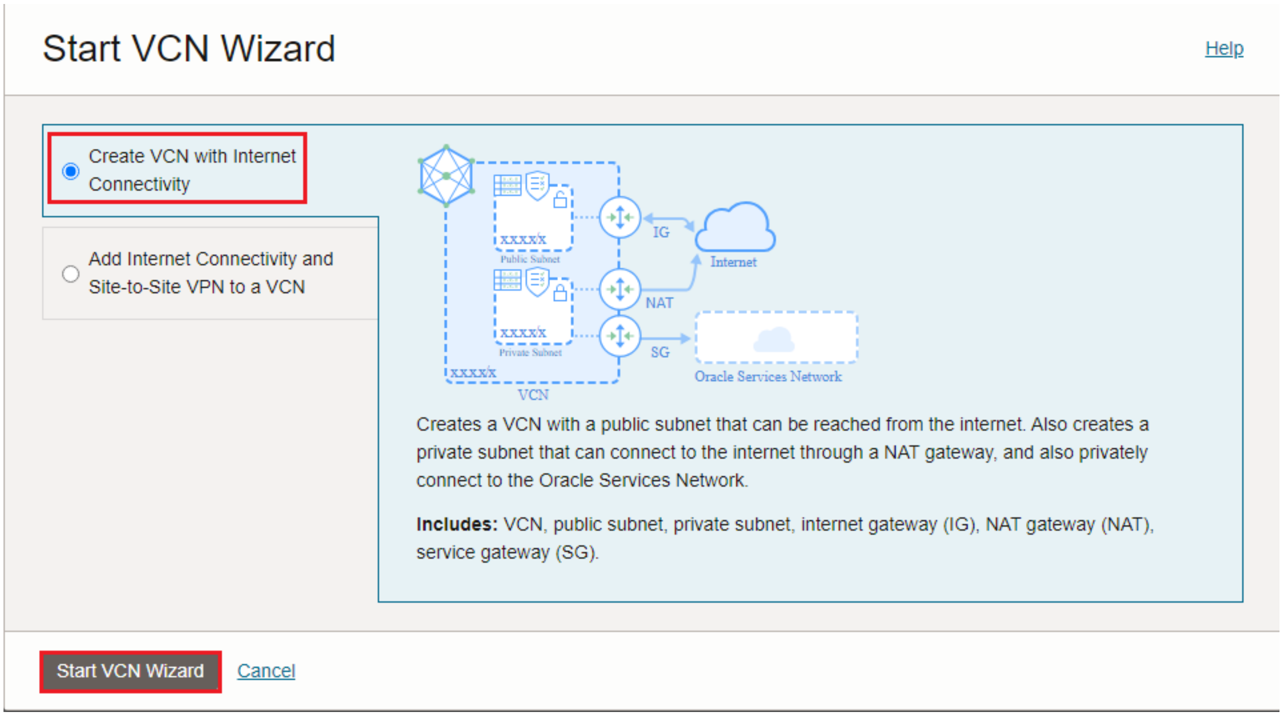

Virtual Cloud Networks *in* [redacted] *compartment*

Virtual Cloud Networks (VCNs) are private virtual networks you set up in Oracle Cloud Infrastructure. You can attach gateways, route tables, and security lists to specify routing and security rules.

Name	State	IPv4 CIDR Block	IPv6 Prefix	Default Route Table	DNS Domain Name	Created
[redacted]	● Available	[redacted]	-	[redacted]	[redacted]	[redacted]
[redacted]	● Available	[redacted]	-	[redacted]	[redacted]	[redacted]

Showing 2 items < 1 of 1 >

3. Select *Create VCN with Internet Connectivity* and click *Start VCN Wizard*.



Start VCN Wizard

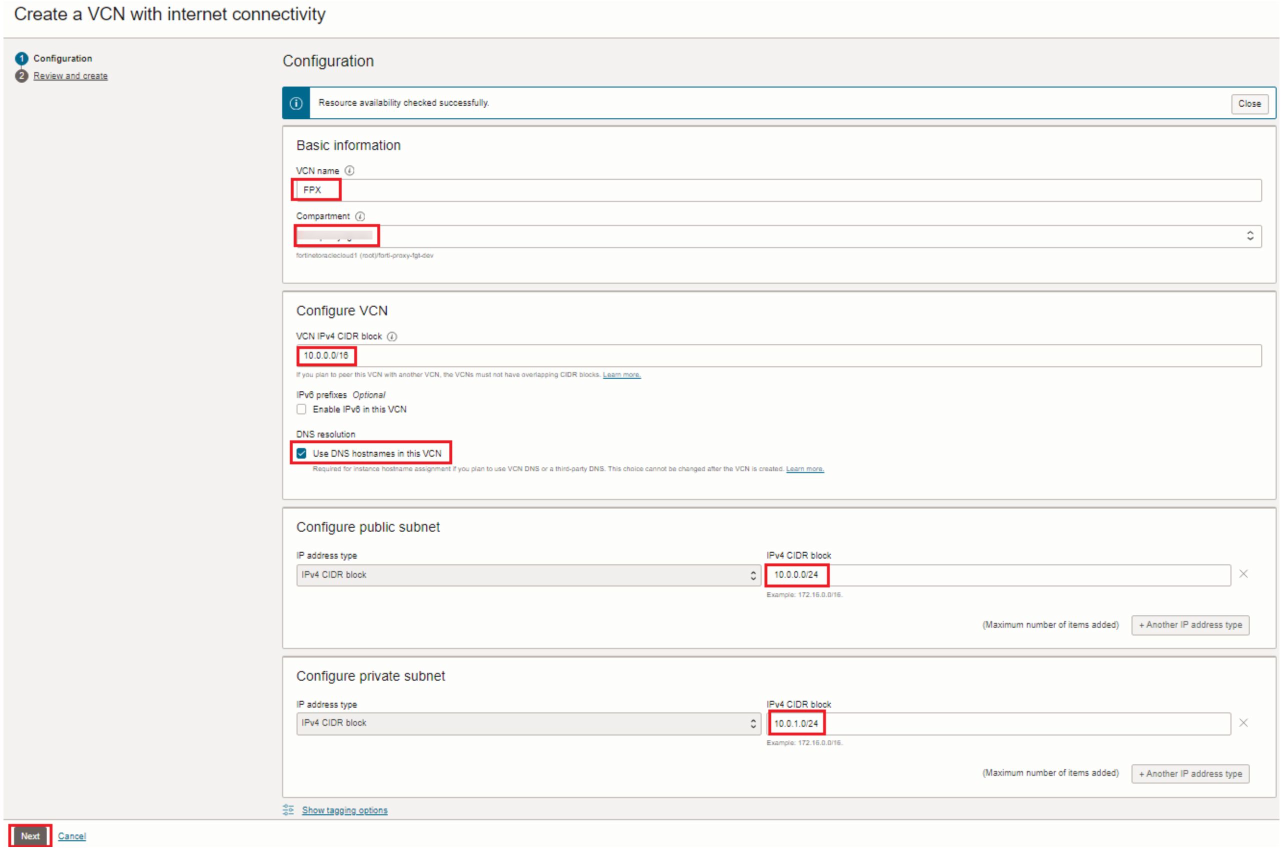
● Create VCN with Internet Connectivity

○ Add Internet Connectivity and Site-to-Site VPN to a VCN

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).

4. Configure the following options:



Create a VCN with internet connectivity

Configuration

Resource availability checked successfully.

Basic information

VCN name: FPX

Compartment: [redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Configure VCN

VCN IPv4 CIDR block: 10.0.0.0/16

If you plan to peer this VCN with another VCN, the VCNs must not have overlapping CIDR blocks. Learn more.

IPv6 prefixes *Optional*

□ Enable IPv6 in this VCN

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.

Configure public subnet

IP address type: IPv4 CIDR block

IPv4 CIDR block: 10.0.0.0/24

Example: 172.16.0.0/16.

(Maximum number of items added)

Configure private subnet

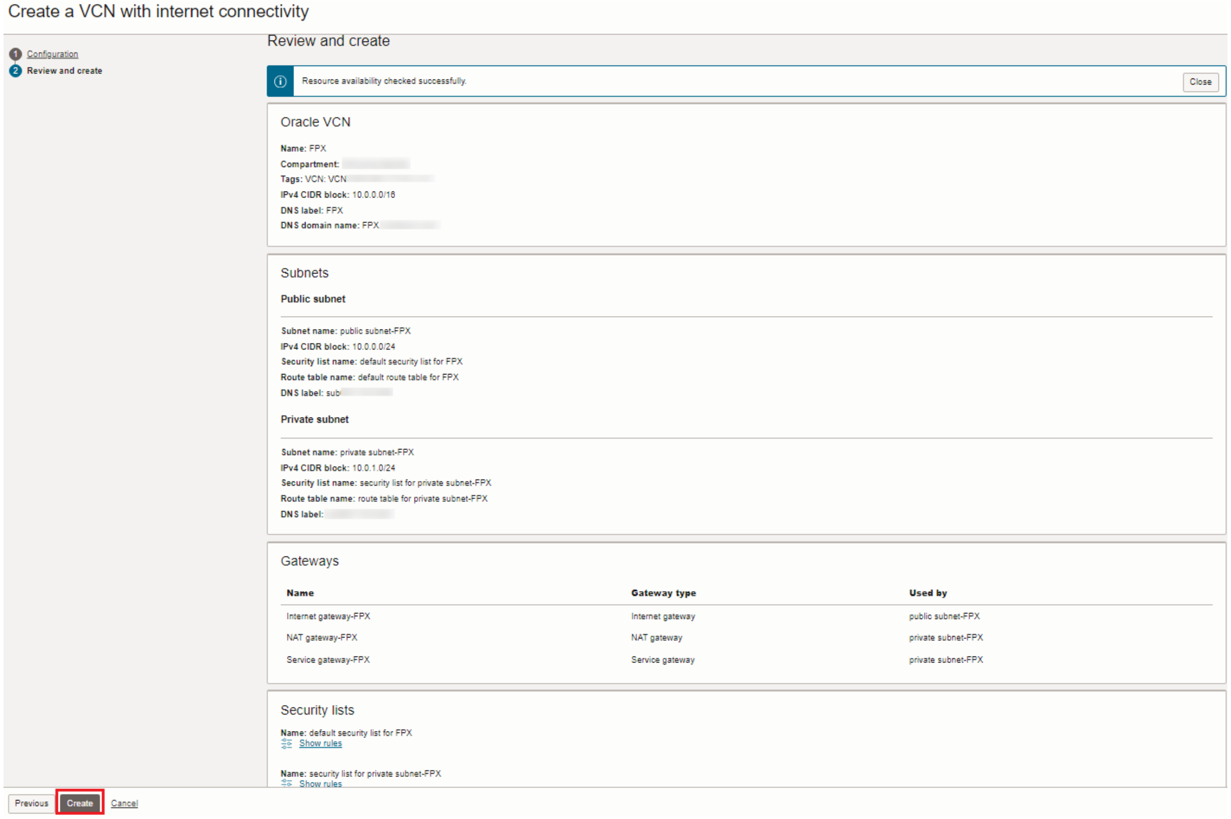
IP address type: IPv4 CIDR block

IPv4 CIDR block: 10.0.1.0/24

Example: 172.16.0.0/16.

(Maximum number of items added)

a. In the *VCN name* field, enter the VCN name.
b. In the *Compartment* field, select the compartment for the VCN.
c. In the *IPv4 CIDR block* field, specify the IPv4 CIDR block.
d. Select the *Use DNS hostnames in this VCN* option.
e. Configure subnets as needed.
f. Click *Next*.
g. Confirm the configuration details and click *Create* at the bottom of the screen.



Create a VCN with internet connectivity

1 Configuration
2 Review and create

Review and create

Resource availability checked successfully.

Oracle VCN

Name: FPX
Compartment: [redacted]
Tags: VCN: VCN[redacted]
IPv4 CIDR block: 10.0.0.0/16
DNS label: FPX
DNS domain name: FPX[redacted]

Subnets

Public subnet

Subnet name: public subnet-FPX
IPv4 CIDR block: 10.0.0.0/24
Security list name: default security list for FPX
Route table name: default route table for FPX
DNS label: sub[redacted]

Private subnet

Subnet name: private subnet-FPX
IPv4 CIDR block: 10.0.1.0/24
Security list name: security list for private subnet-FPX
Route table name: route table for private subnet-FPX
DNS label: [redacted]

Gateways

Name	Gateway type	Used by
Internet gateway-FPX	Internet gateway	public subnet-FPX
NAT gateway-FPX	NAT gateway	private subnet-FPX
Service gateway-FPX	Service gateway	private subnet-FPX

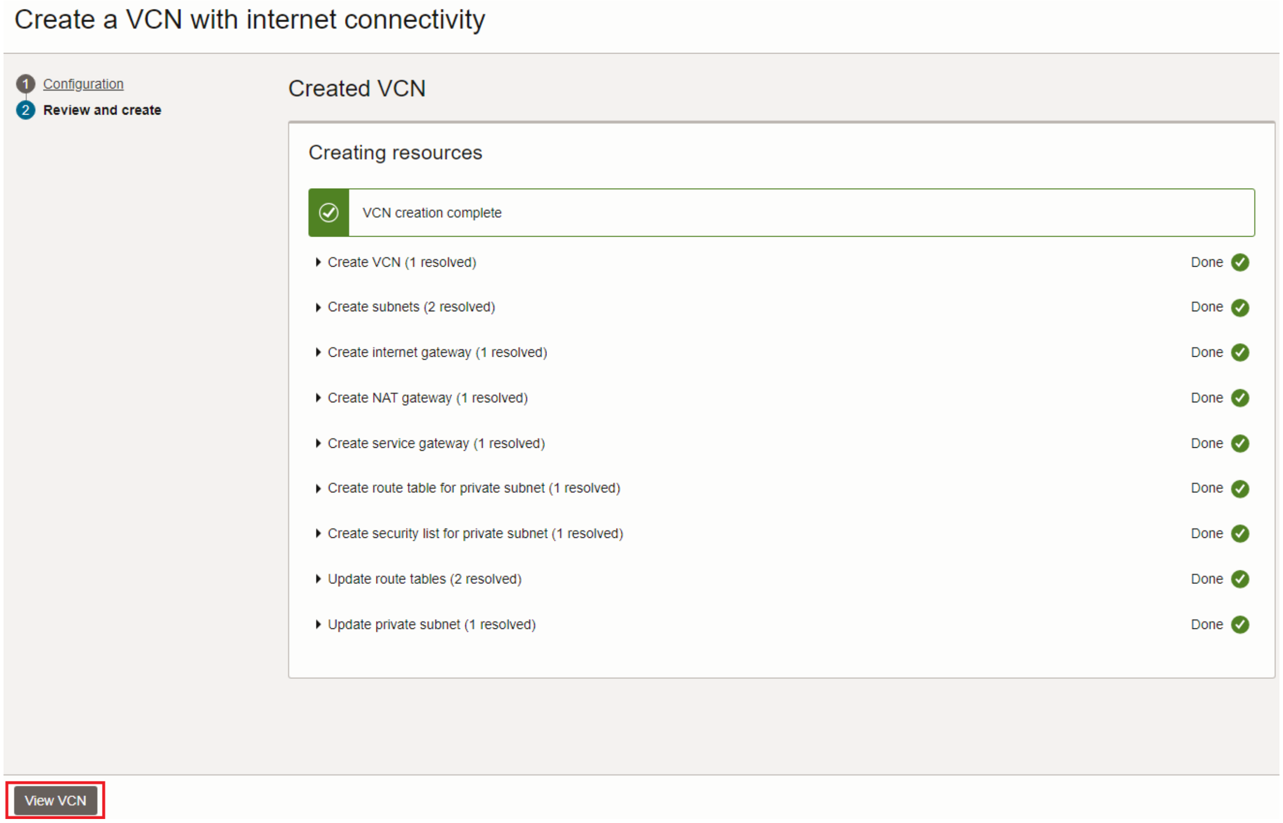
Security lists

Name: default security list for FPX
Show rules

Name: security list for private subnet-FPX
Show rules

This configures the related resources. There are two subnets, one for public access and the other for private access, each of which will belong to an AD. In this example, (1) is 10.0.x.x/24. You can access the FortiProxy over the Internet once it is deployed via HTTPS through the GUI management screen or via SSH.

5. Click *View VCN*.



Create a VCN with internet connectivity

Created VCN

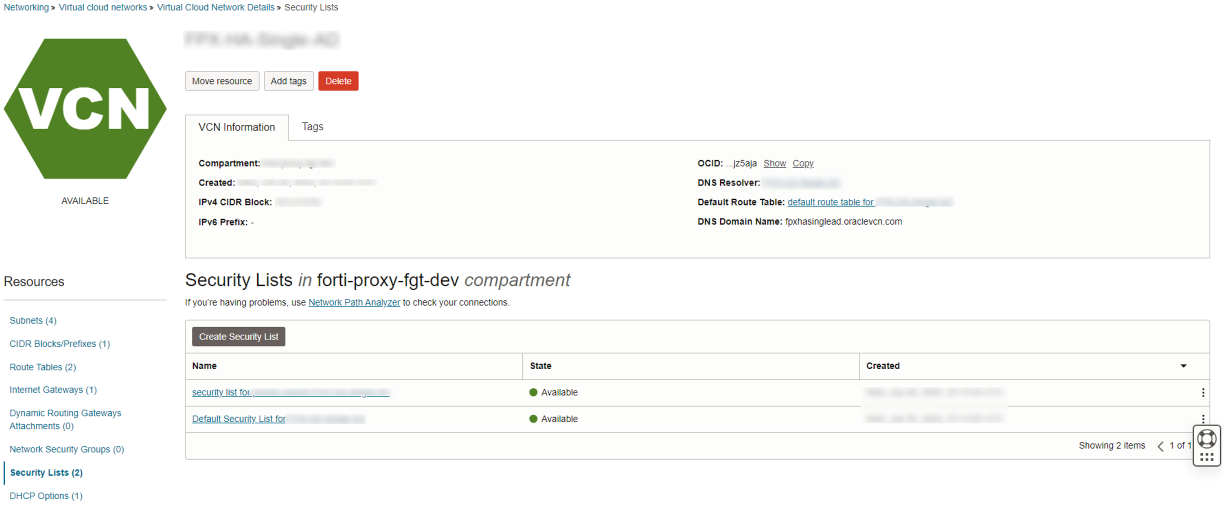
Creating resources

VCN creation complete

Create VCN (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 ✓

6. Update the default security list to allow access to the required ports as listed in FortiProxy ports:

   a. In the *Security Lists* tab of the VCN details page, click the link of the default security list. By default, port 22 is allowed.



[redacted]

Compartment: [redacted]
Created: [redacted]
IPv4 CIDR Block: [redacted]
IPv6 Prefix: -
OCID: ...jz5aja Show Copy
DNS Resolver: [redacted]
Default Route Table: default route table for [redacted]
DNS Domain Name: fpxhasinglead.oraclevcn.com

Security Lists *in* forti-proxy-fgt-dev *compartment*

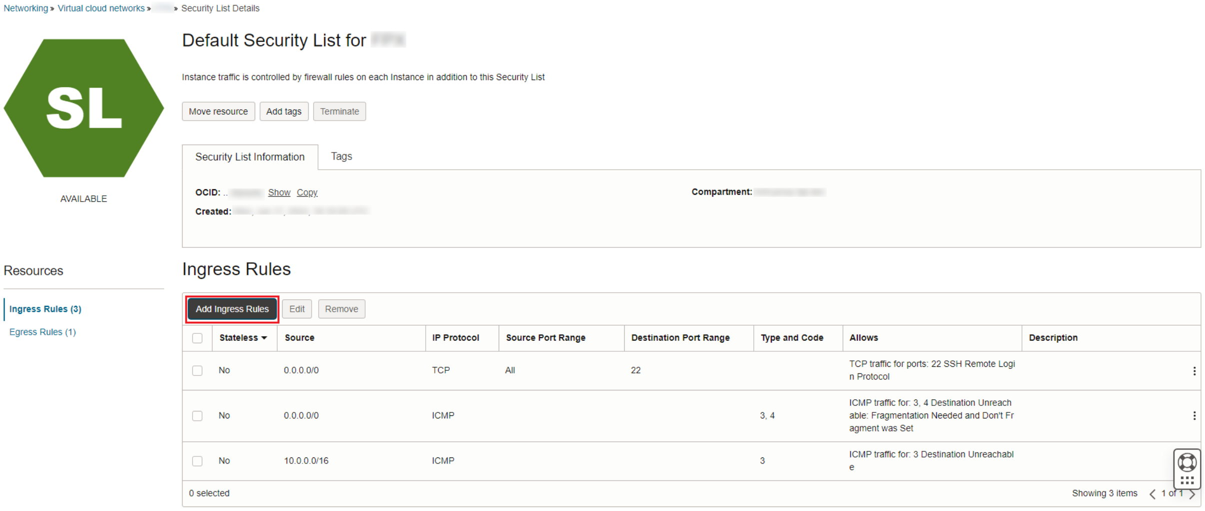
If you're having problems, use Network Path Analyzer to check your connections.

Create Security List

Name	State	Created
security list for [redacted]	● Available	[redacted]
Default Security List for [redacted]	● Available	[redacted]

Showing 2 items 1 of 1

b. Click *Add Ingress Rules*.



Networking » Virtual cloud networks » [redacted] » Security List Details

Default Security List for [redacted]

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

OCID: .. [redacted] Show Copy

Compartment: [redacted]

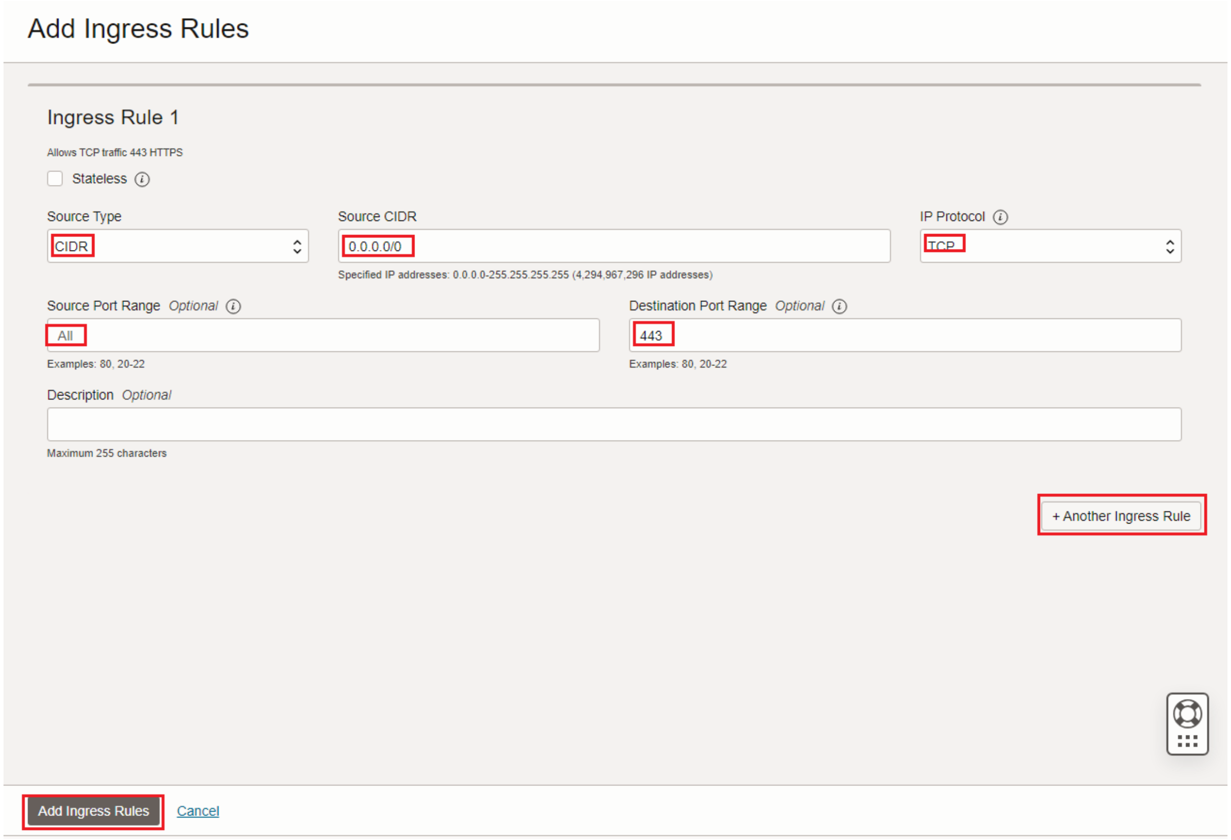
Created: [redacted]

Ingress Rules

□	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
□	No	0.0.0.0/0	TCP	All	22		TCP traffic for ports: 22 SSH Remote Logi n Protocol	
□	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreach able: Fragmentation Needed and Don't Fr agment was Set	
□	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachabl e	

0 selected Showing 3 items 1 of 1

c. Configure a rule to allow TCP port 443 and add any other rules for specific ports as needed.



Add Ingress Rules

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

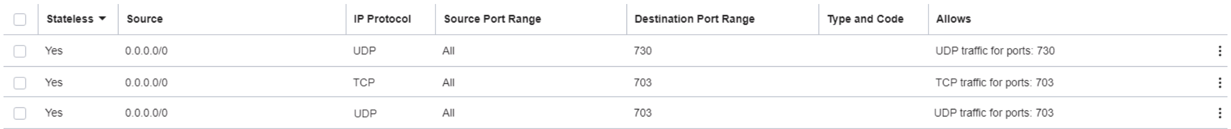
Destination Port Range *Optional*: 443

Examples: 80, 20-22

Description *Optional*

Maximum 255 characters

For example, for Heartbeat sync ports, you must have the following included in the security list:



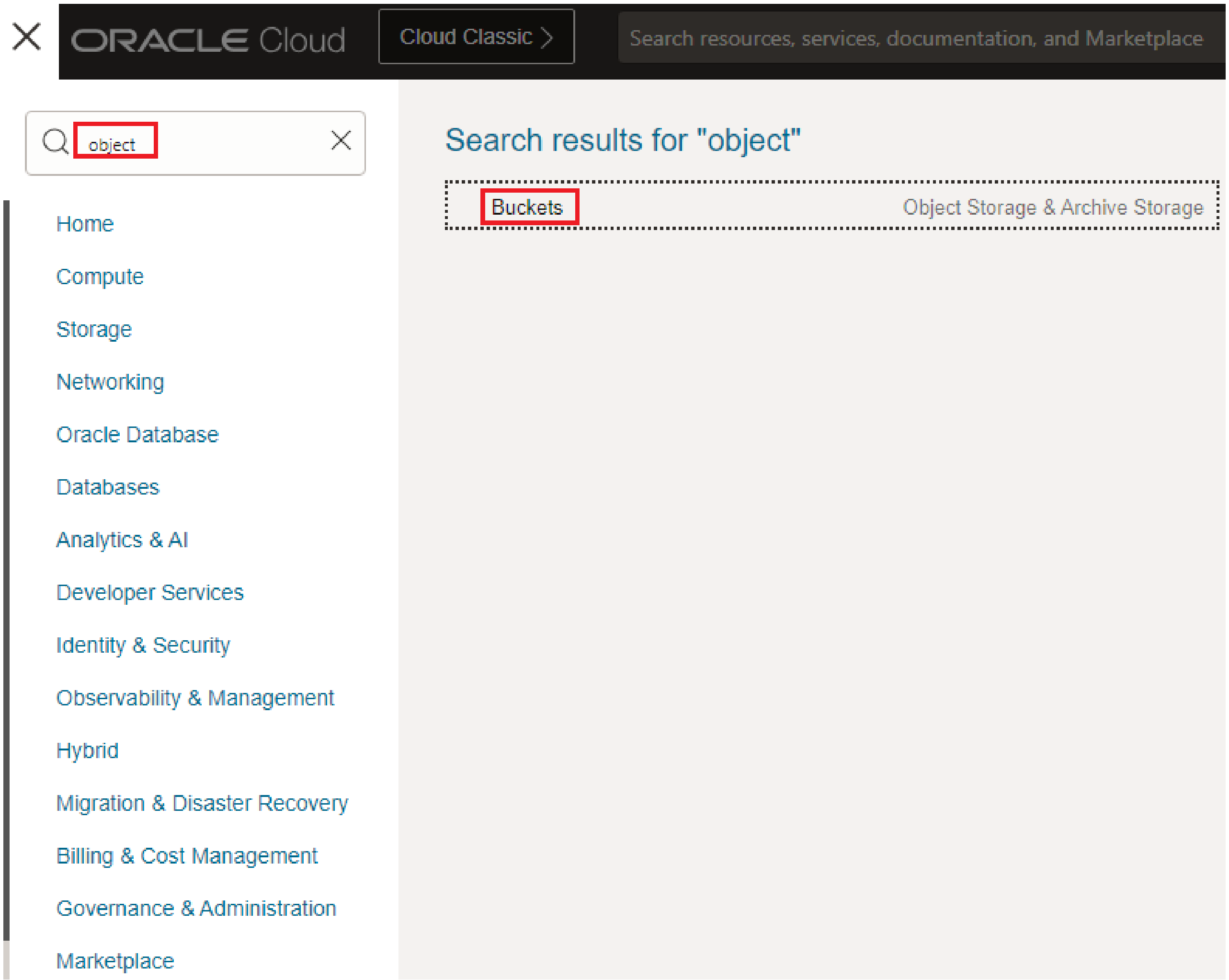
□	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows
□	Yes	0.0.0.0/0	UDP	All	730		UDP traffic for ports: 730
□	Yes	0.0.0.0/0	TCP	All	703		TCP traffic for ports: 703
□	Yes	0.0.0.0/0	UDP	All	703		UDP traffic for ports: 703

Creating a FortiProxy-VM instance

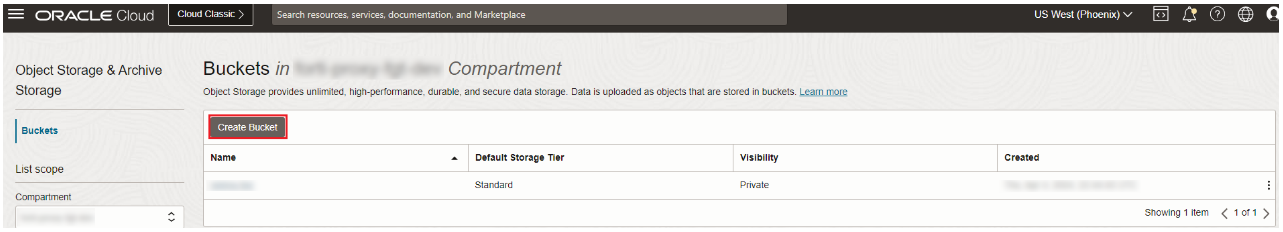
Create a FortiProxy-VM instance by obtaining the deployment image file and importing the file into the OCI portal.

To obtain the deployment image file and place it in your bucket:

1. Obtain the deployment image file:
   a. Go to Customer Service & Support.
   b. Click *Support* > *Downloads* > *Firmware Download* in the top menu.
   c. In the *Select Product* dropdown list, select *FortiProxy*.
   d. In the *Download* tab, navigate to the FortiProxy version folder.
   e. Obtain the *FPX_KVM_OPC-vX-buildXXXX-FORTINET.out.kvm.zip* file, where *XXXX* is the build number. Ensure that the file name includes *kvm*.
   f. After downloading, unzip the file. You will find the *fortiproxy.qcow2* file, which is needed to deploy the FortiProxy-VM on OCI.
2. In OCI, go to *Object Storage* > *Buckets*.


ORACLE Cloud
Cloud Classic >
Search resources, services, documentation, and Marketplace
object
Search results for "object"
Buckets
Object Storage & Archive Storage
Home
Compute
Storage
Networking
Oracle Database
Databases
Analytics & AI
Developer Services
Identity & Security
Observability & Management
Hybrid
Migration & Disaster Recovery
Billing & Cost Management
Governance & Administration
Marketplace

3. Click *Create Bucket* to create a standard storage bucket.



Object Storage & Archive Storage

Buckets

List scope

Compartment [redacted]

Buckets *in* [redacted] *Compartment*

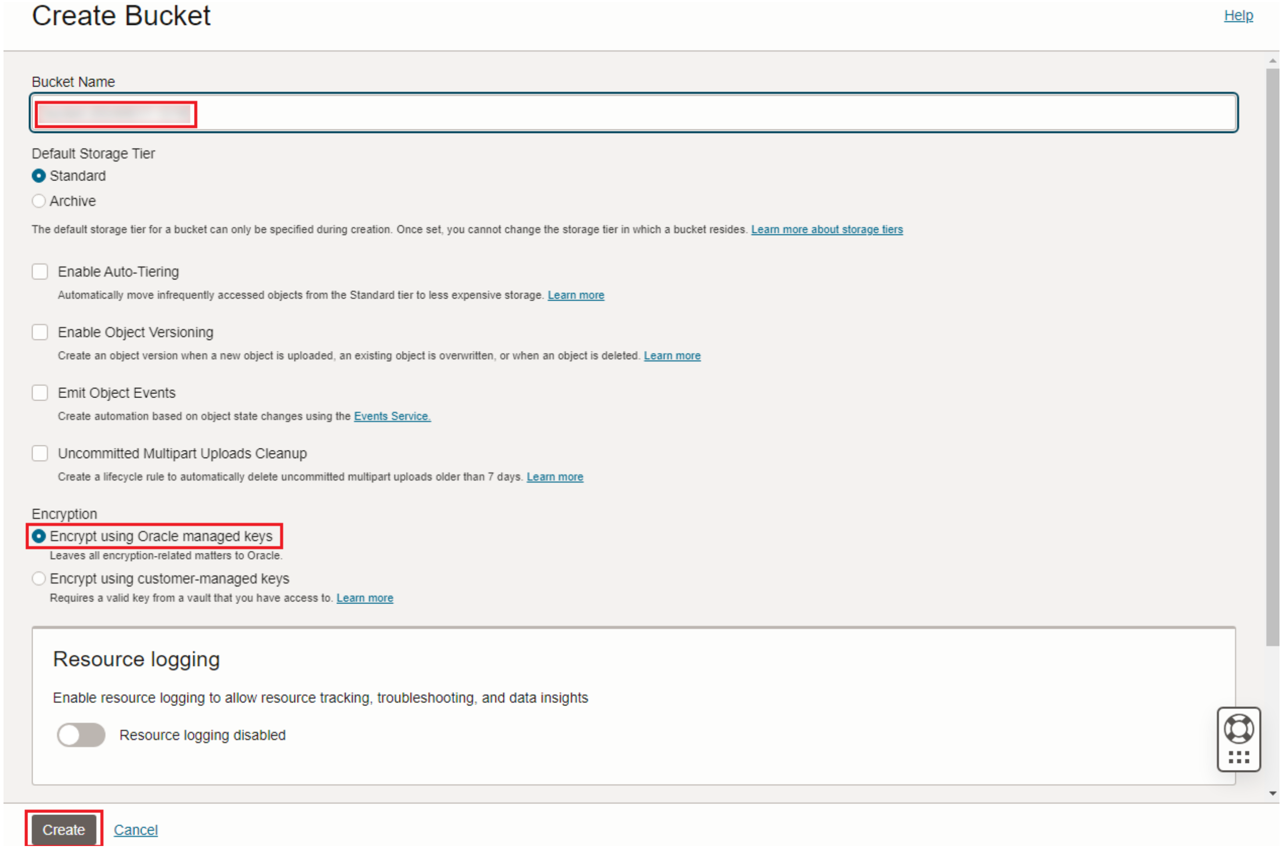
Object Storage provides unlimited, high-performance, durable, and secure data storage. Data is uploaded as objects that are stored in buckets. Learn more

Create Bucket

Name	Default Storage Tier	Visibility	Created
[redacted]	Standard	Private	[redacted]

Showing 1 item < 1 of 1 >

4. Configure the standard storage bucket as shown below and click *Create*:



Create Bucket

Help

Bucket Name

[redacted]

Default Storage Tier

● Standard

○ Archive

The default storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides. Learn more about storage tiers

□ Enable Auto-Tiering

Automatically move infrequently accessed objects from the Standard tier to less expensive storage. Learn more

□ Enable Object Versioning

Create an object version when a new object is uploaded, an existing object is overwritten, or when an object is deleted. Learn more

□ Emit Object Events

Create automation based on object state changes using the Events Service.

□ Uncommitted Multipart Uploads Cleanup

Create a lifecycle rule to automatically delete uncommitted multipart uploads older than 7 days. Learn more

Encryption

● Encrypt using Oracle managed keys

Leaves all encryption-related matters to Oracle.

○ Encrypt using customer-managed keys

Requires a valid key from a vault that you have access to. Learn more

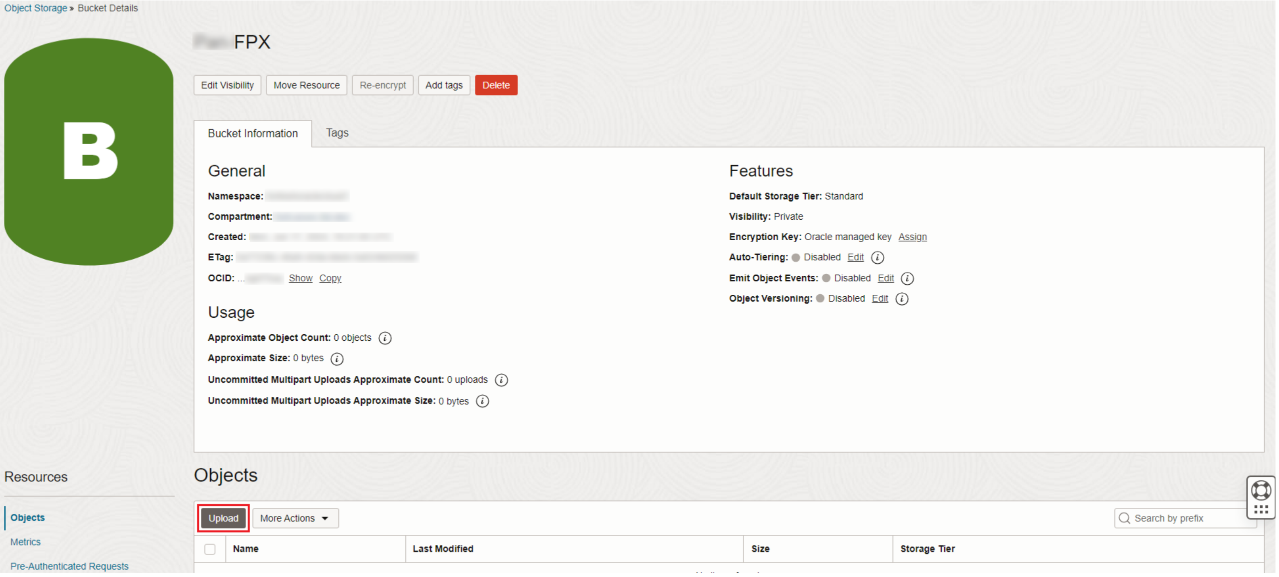
Resource logging

Enable resource logging to allow resource tracking, troubleshooting, and data insights

Resource logging disabled

Create Cancel

5. Select the bucket, then click *Upload*.



Object Storage » Bucket Details

[redacted] FPX

General

Namespace: [redacted]
Compartment: [redacted]
Created: [redacted]
ETag: [redacted]
OCID: ...[redacted] Show Copy

Usage

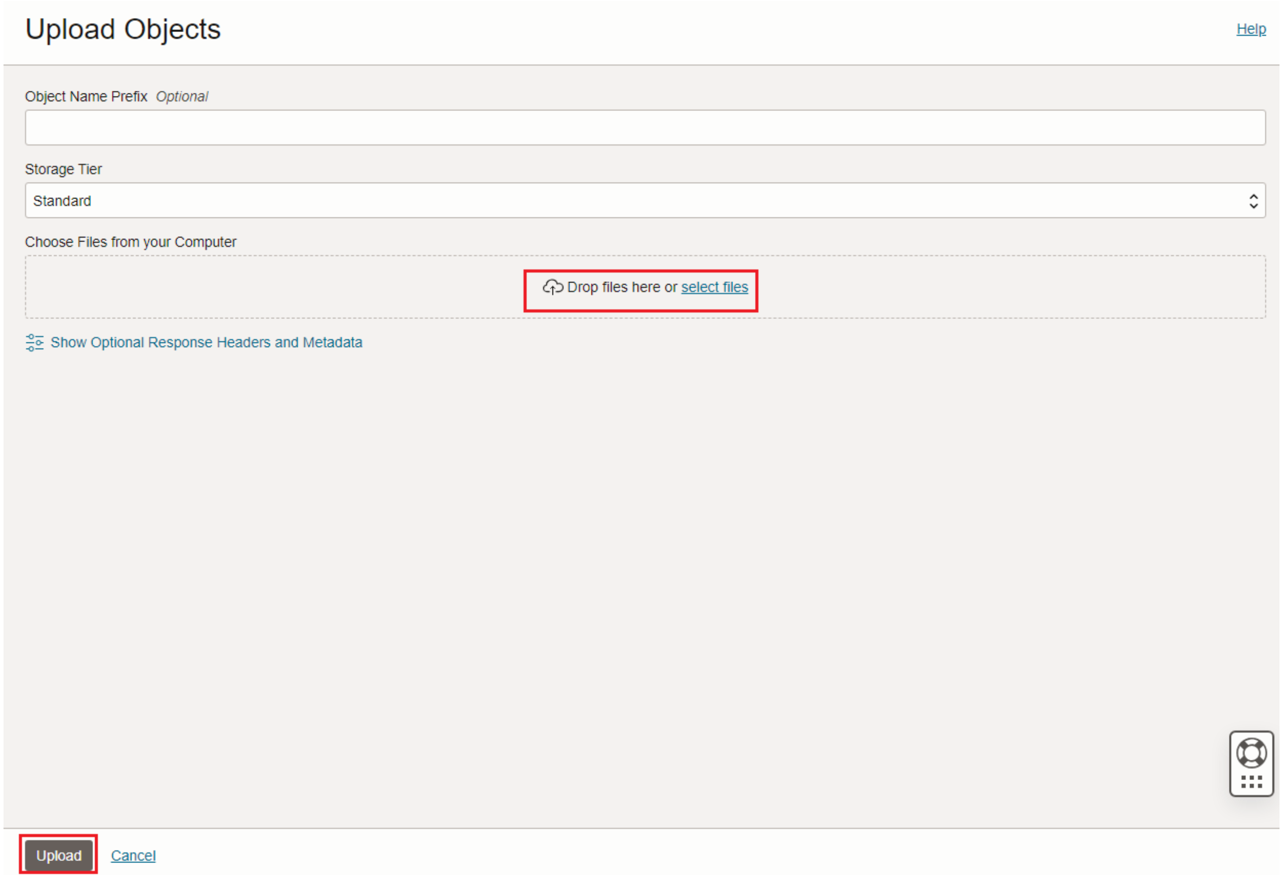
Approximate Object Count: 0 objects
Approximate Size: 0 bytes
Uncommitted Multipart Uploads Approximate Count: 0 uploads
Uncommitted Multipart Uploads Approximate Size: 0 bytes

Features

Default Storage Tier: Standard
Visibility: Private
Encryption Key: Oracle managed key Assign
Auto-Tiering: ● Disabled Edit
Emit Object Events: ● Disabled Edit
Object Versioning: ● Disabled Edit

□	Name	Last Modified	Size	Storage Tier

6. Drop or select the deployment image file *fortiproxy.qcow2* and click *Upload*.



Upload Objects

Object Name Prefix *Optional*

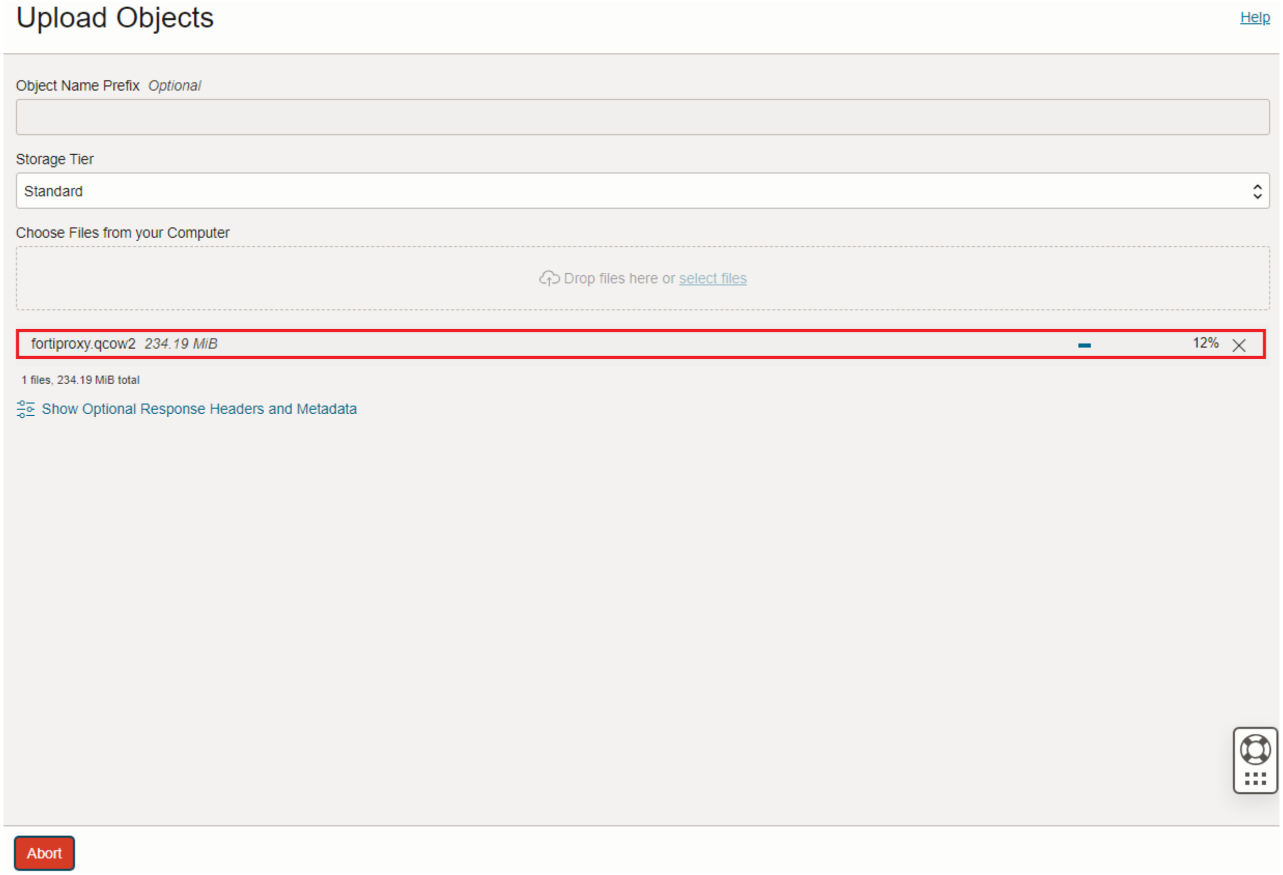
Storage Tier

Standard

Choose Files from your Computer

Drop files here or select files
Show Optional Response Headers and Metadata
Upload
Cancel

The dialog shows the upload progress.



Upload Objects

Object Name Prefix *Optional*

Storage Tier

Standard

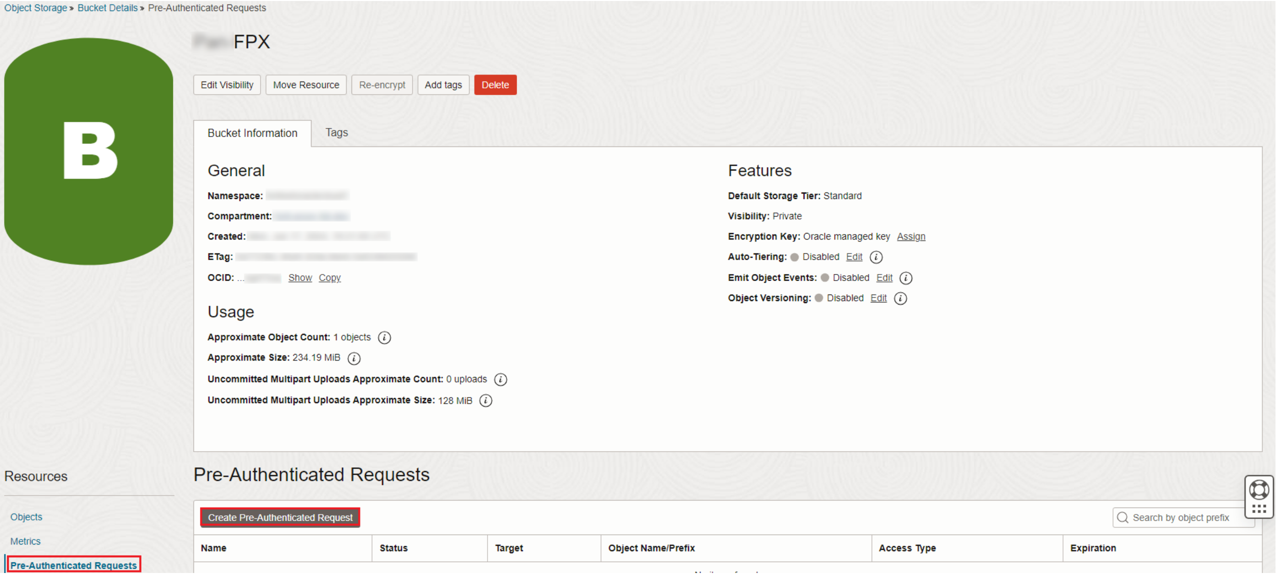
Choose Files from your Computer

Drop files here or select files

fortiproxy.qcow2 *234.19 MiB* 12%

1 files, 234.19 MiB total

7. After the upload is complete, click *Close*.
8. Click *Pre-Authenticated Requests* and then *Create Pre-Authenticated Requests*.



Object Storage » Bucket Details » Pre-Authenticated Requests

[redacted] FPX

General

Namespace: [redacted]

Compartment: [redacted]

Created: [redacted]

ETag: [redacted]

OCID: ...[redacted] Show Copy

Usage

Approximate Object Count: 1 objects

Approximate Size: 234.19 MiB

Uncommitted Multipart Uploads Approximate Count: 0 uploads

Uncommitted Multipart Uploads Approximate Size: 128 MiB

Features

Default Storage Tier: Standard

Visibility: Private

Encryption Key: Oracle managed key Assign

Auto-Tiering: ● Disabled Edit

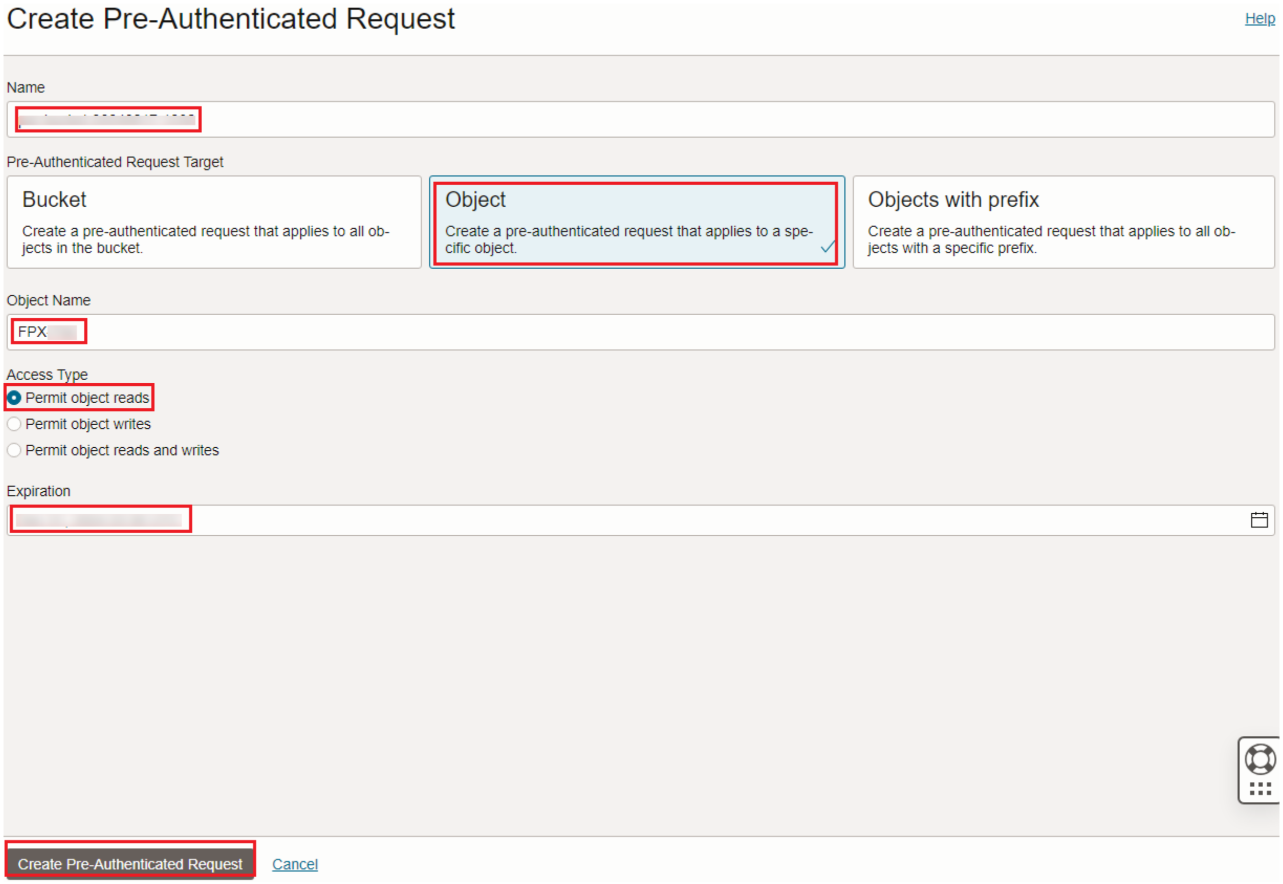
Emit Object Events: ● Disabled Edit

Object Versioning: ● Disabled Edit

Pre-Authenticated Requests

Name	Status	Target	Object Name/Prefix	Access Type	Expiration

9. Configure the following options and click *Create Pre-Authenticated Requests*:



Create Pre-Authenticated Request

Name

[redacted]

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

FPX[redacted]

Access Type

● Permit object reads

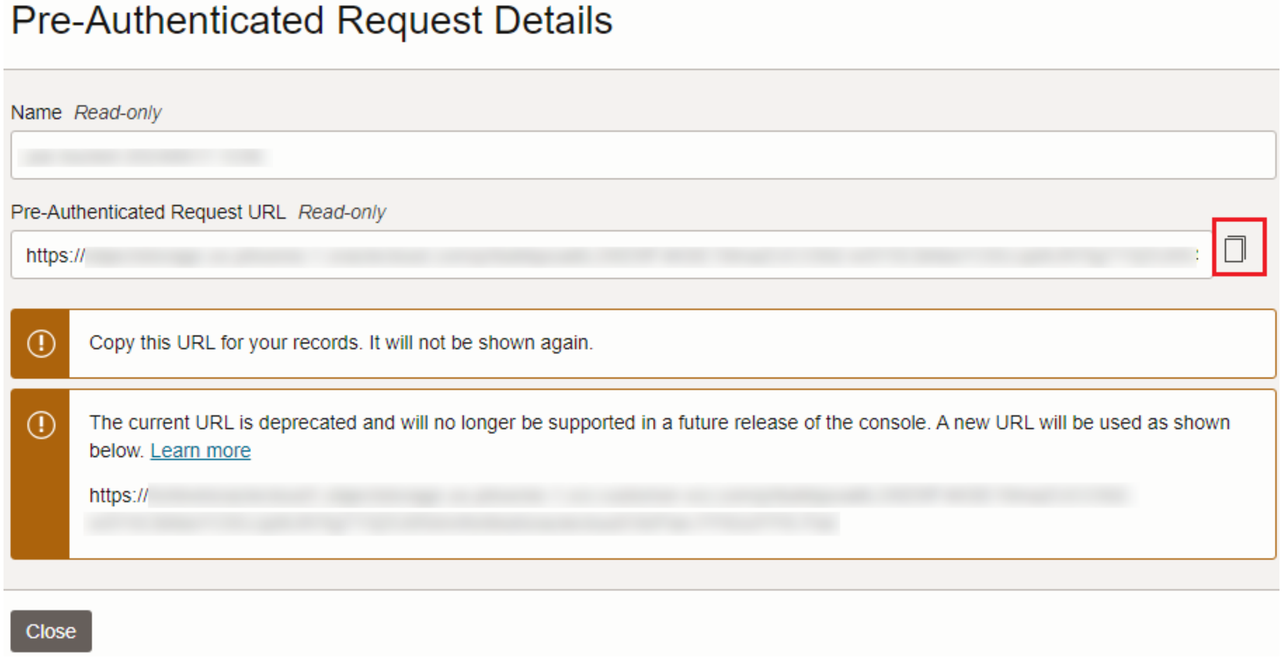
○ Permit object writes

○ Permit object reads and writes

Expiration

[redacted]

10. Copy this URL and save it somewhere for usage in later steps. Click *Close*.



Pre-Authenticated Request Details

Name *Read-only*

[redacted]

Pre-Authenticated Request URL *Read-only*

https://[redacted]

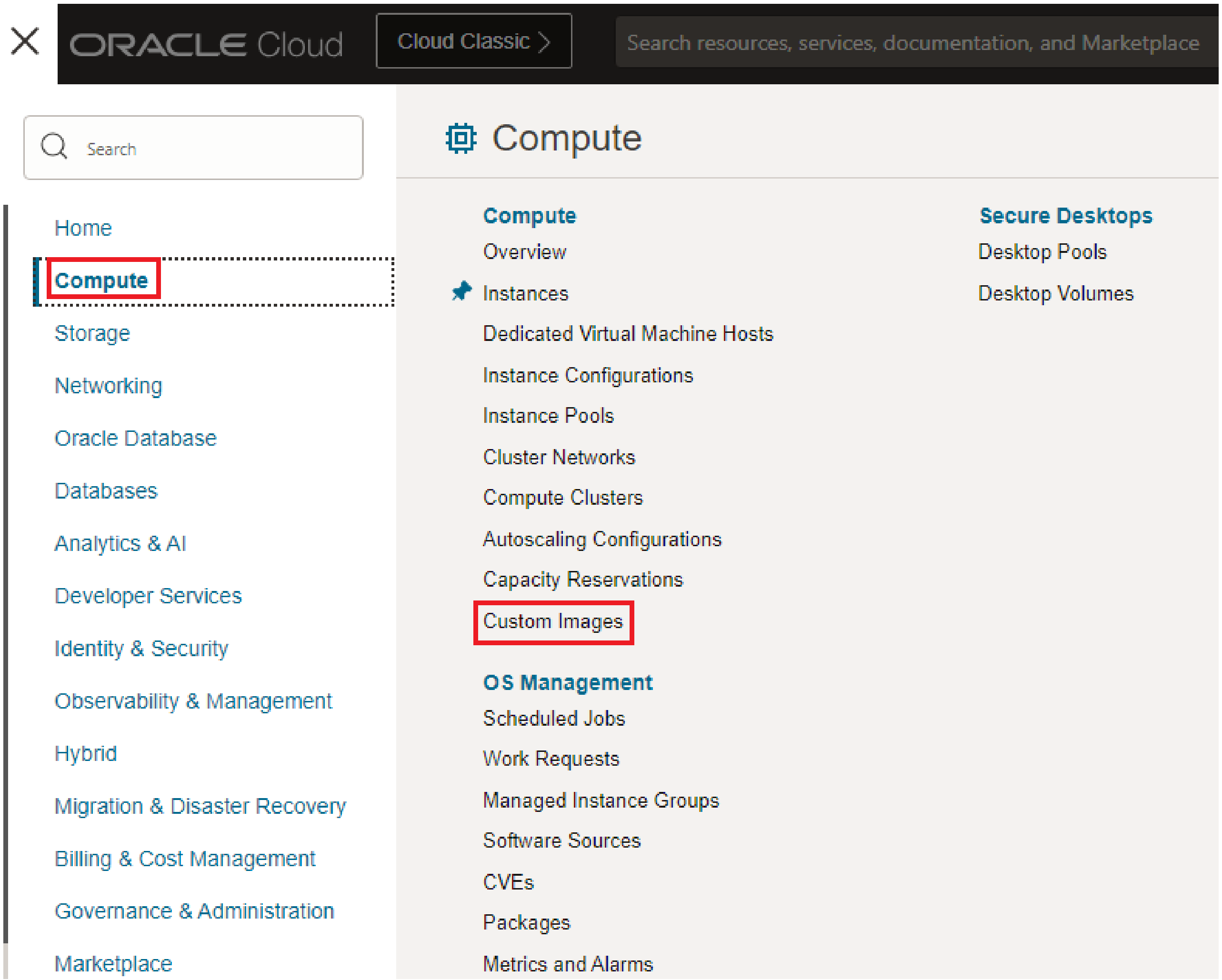
Copy this URL for your records. It will not be shown again.

The current URL is deprecated and will no longer be supported in a future release of the console. A new URL will be used as shown below. Learn more

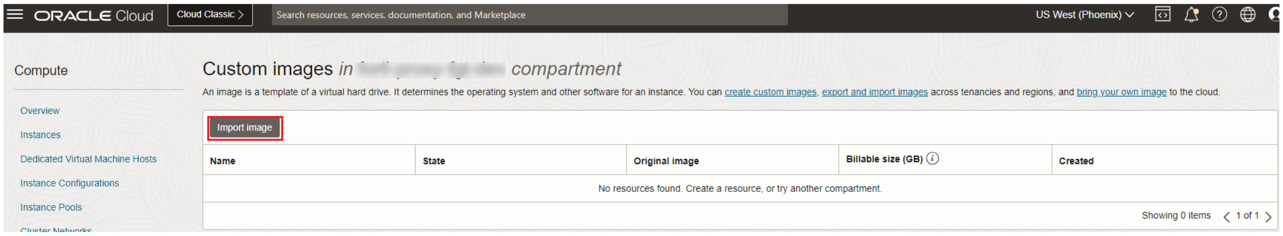
https://[redacted]

To import the image:

1. Go to *Compute* > *Custom Images*.



2. Click *Import Image*.



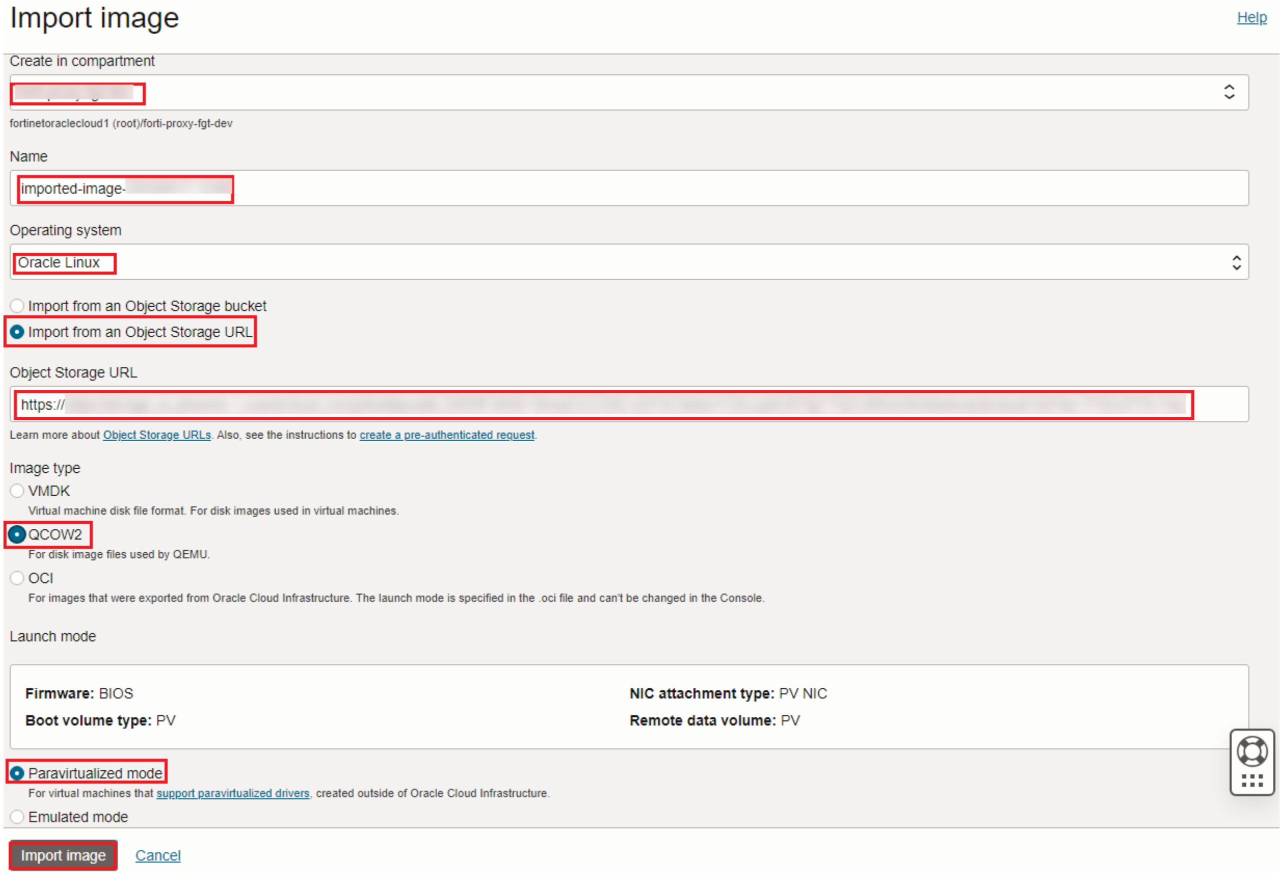
Custom images *in [redacted] compartment*

An image is a template of a virtual hard drive. It determines the operating system and other software for an instance. You can create custom images, export and import images across tenancies and regions, and bring your own image to the cloud.

Name	State	Original image	Billable size (GB)	Created
No resources found. Create a resource, or try another compartment.				

Showing 0 items 1 of 1

3. Configure the following options and click *Import image*. In the *Object Storage URL* field, enter the URL link obtained earlier and place it in your bucket.



Import image

Create in compartment

[redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Name

imported-image-[redacted]

Operating system

Oracle Linux

○ Import from an Object Storage bucket

● Import from an Object Storage URL

Object Storage URL

https://[redacted]

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

Boot volume type: PV

NIC attachment type: PV NIC

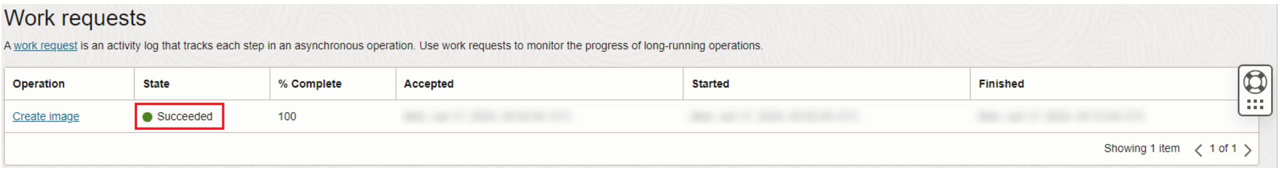
Remote data volume: PV

● Paravirtualized mode

For virtual machines that support paravirtualized drivers, created outside of Oracle Cloud Infrastructure.

○ Emulated mode

4. Wait until the state of the *Create image* operation changes to *Succeeded*.



Work requests

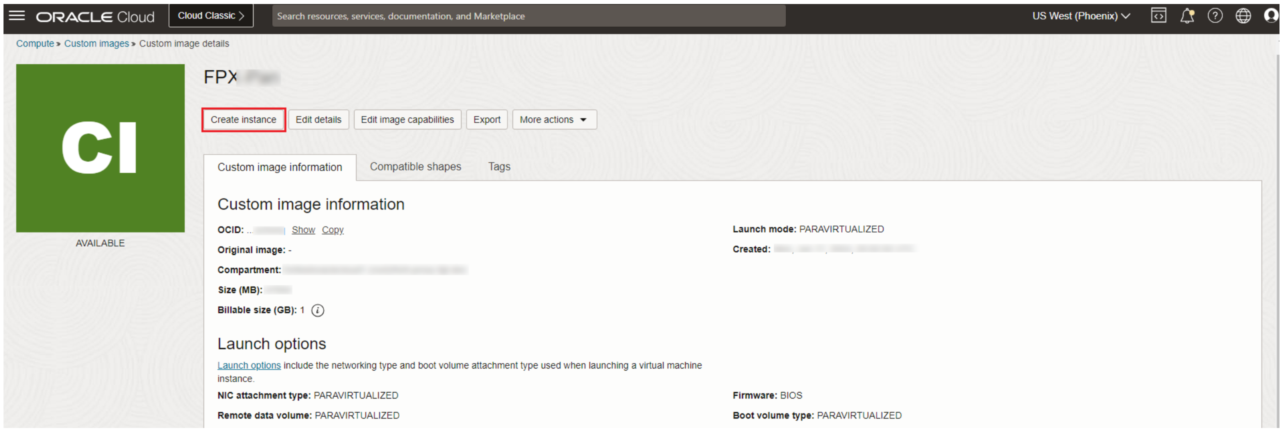
A work request is an activity log that tracks each step in an asynchronous operation. Use work requests to monitor the progress of long-running operations.

Operation	State	% Complete	Accepted	Started	Finished
Create image	● Succeeded	100	[redacted]	[redacted]	[redacted]

Showing 1 item ‹ 1 of 1 ›

To create the FortiProxy-VM instance:

1. From the newly imported image, click *Create Instance*.



Compute » Custom images » Custom image details

FPX [redacted]

AVAILABLE

Create instance | Edit details | Edit image capabilities | Export | More actions

Custom image information | Compatible shapes | Tags

Custom image information

OCID: ...[redacted] Show Copy

Original image: -

Compartment: [redacted]

Size (MB): [redacted]

Billable size (GB): 1

Launch mode: PARAVIRTUALIZED

Created: [redacted]

Launch options

Launch options include the networking type and boot volume attachment type used when launching a virtual machine instance.

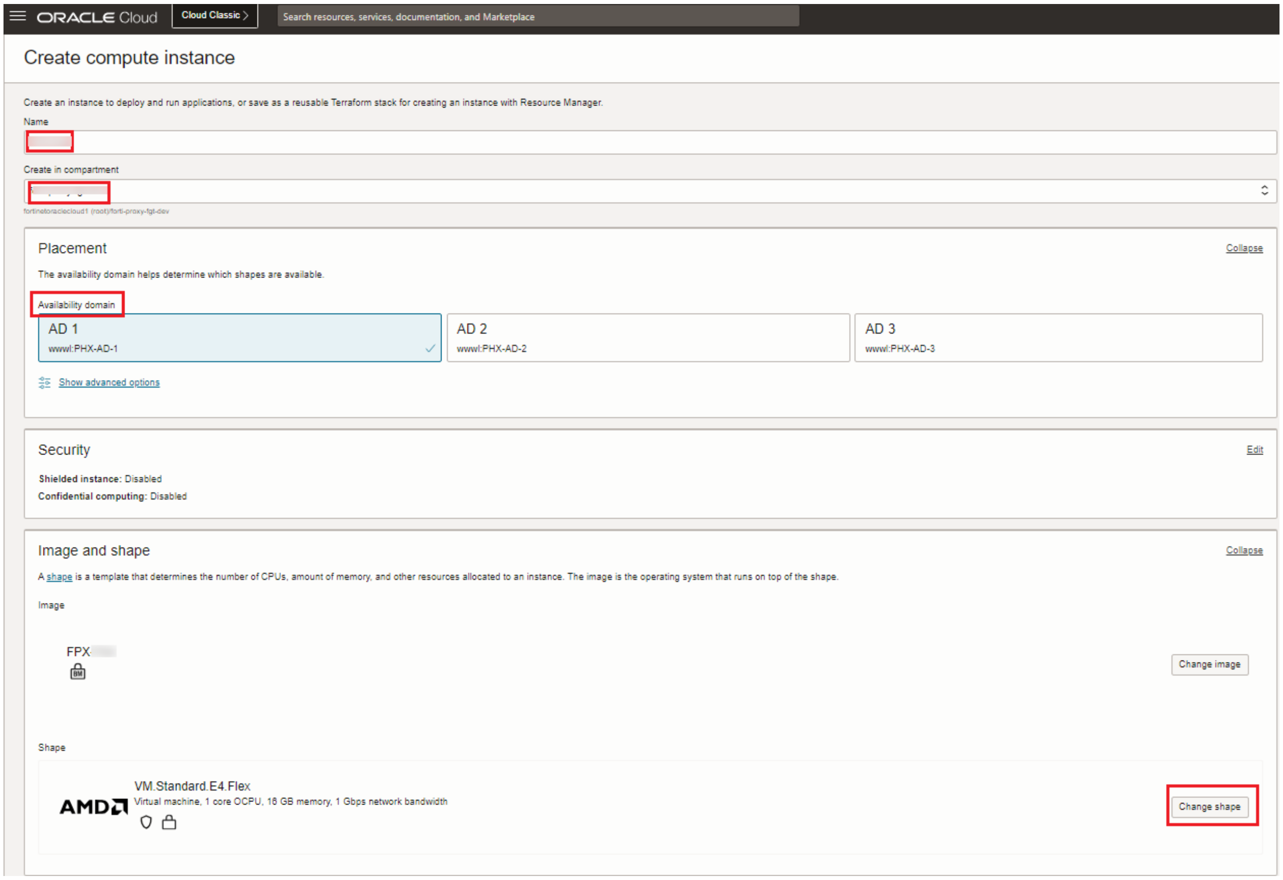
NIC attachment type: PARAVIRTUALIZED

Remote data volume: PARAVIRTUALIZED

Firmware: BIOS

Boot volume type: PARAVIRTUALIZED

2. Configure the parameters:



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

[redacted]

Create in compartment

[redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Placement

Collapse

The availability domain helps determine which shapes are available.

Availability domain

AD 1 wwwl:PHX-AD-1 ✓ | AD 2 wwwl:PHX-AD-2 | AD 3 wwwl:PHX-AD-3

Show advanced options

Security

Edit

Shielded instance: Disabled

Confidential computing: Disabled

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

FPX [redacted]

Change image

Shape

VM.Standard.E4.Flex

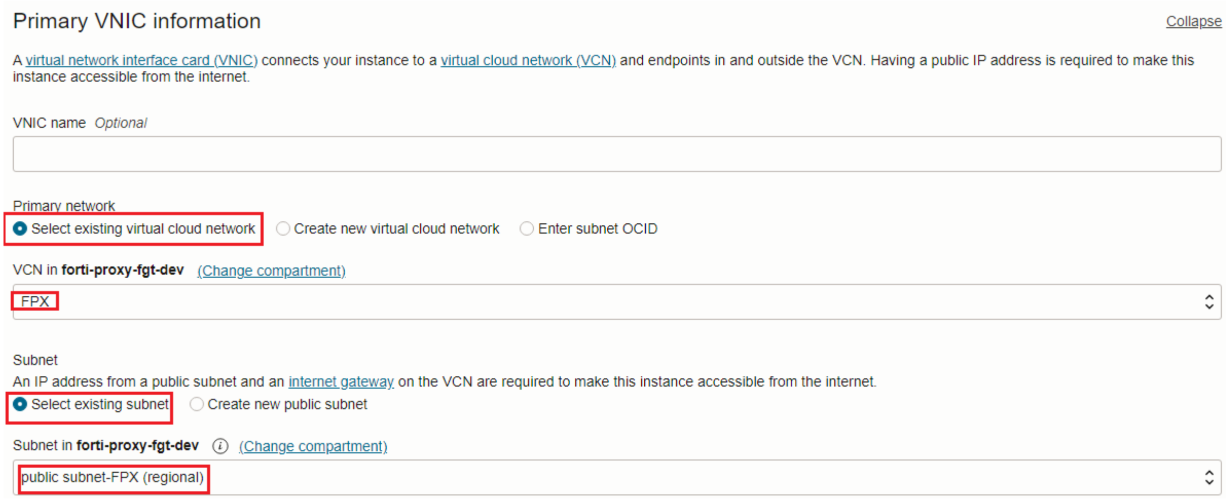
Virtual machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth

Change shape

a. In the *Name* field, enter the desired name to identify the instance.
b. Under *Create in compartment*, select the compartment for the instance.
c. Under *Availability domain*, select the desired domain.
d. Under *Image and shape*, click *Change shape*.
e. Under *Instance type*, select *Virtual Machine*.

f. Configure other shaping options as needed and click *Select shape*.

g. In the *Primary VNIC information* section, specify the VNIC name and select a network to launch the instance.



Primary VNIC information

A virtual network interface card (VNIC) connects your instance to a virtual cloud network (VCN) and endpoints in and outside the VCN. Having a public IP address is required to make this instance accessible from the internet.

VNIC name *Optional*

Primary network

● Select existing virtual cloud network ○ Create new virtual cloud network ○ Enter subnet OCID

VCN in **forti-proxy-fgt-dev** (Change compartment)

FPX

Subnet

An IP address from a public subnet and an internet gateway on the VCN are required to make this instance accessible from the internet.

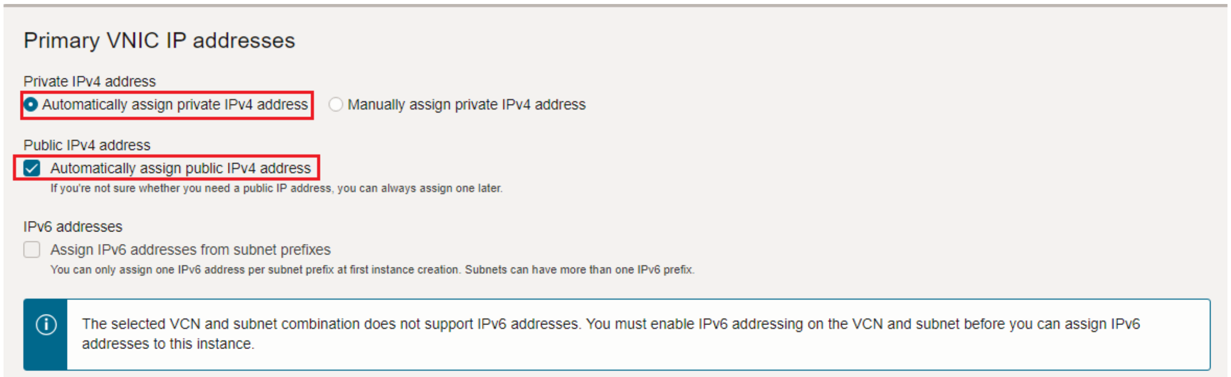
● Select existing subnet ○ Create new public subnet

Subnet in **forti-proxy-fgt-dev** (Change compartment)

public subnet-FPX (regional)

h. In the *Subnet* field, select a subnet on the Internet-facing side of the network.

i. In the *Primary VNIC IP addresses* section, configure the following.
Ensure *Automatically assign public IPv4 address* is selected so you can access the FortiProxy-VM over the Internet. You can disable this once you have configured everything as desired.



Primary VNIC IP addresses

Private IPv4 address

● Automatically assign private IPv4 address ○ Manually assign private IPv4 address

Public IPv4 address

☑ Automatically assign public IPv4 address

If you're not sure whether you need a public IP address, you can always assign one later.

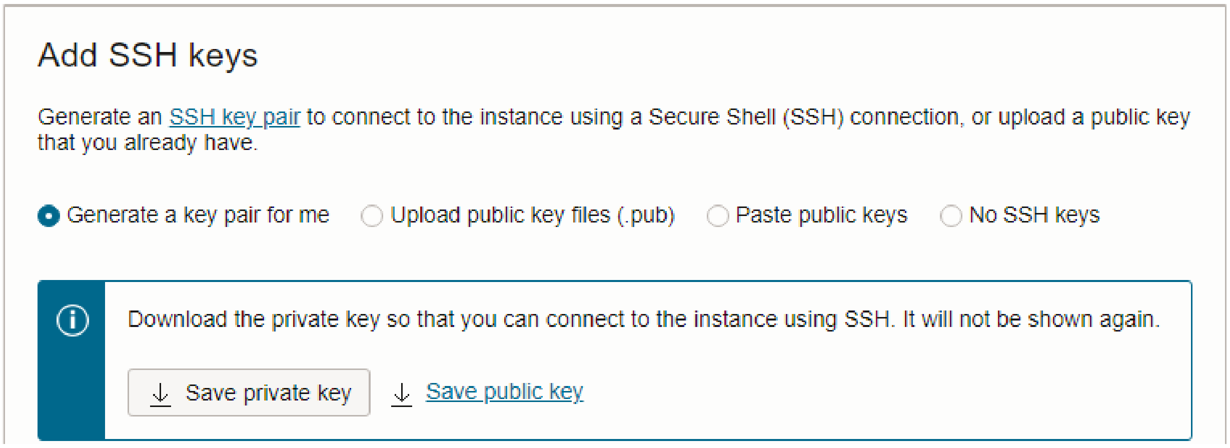
IPv6 addresses

□ Assign IPv6 addresses from subnet prefixes

You can only assign one IPv6 address per subnet prefix at first instance creation. Subnets can have more than one IPv6 prefix.

The selected VCN and subnet combination does not support IPv6 addresses. You must enable IPv6 addressing on the VCN and subnet before you can assign IPv6 addresses to this instance.

j. In the *Add SSH key* section, generate an SSH key pair or upload a public key that you already have to connect to the instance using a Secure Shell (SSH) connection.



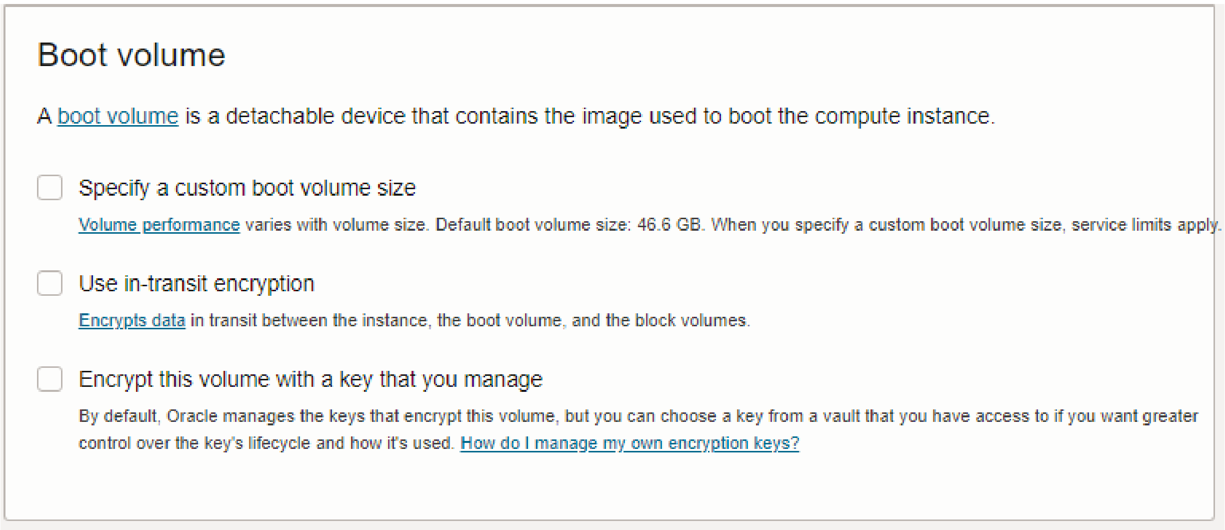
Add SSH keys

Generate an SSH key pair to connect to the instance using a Secure Shell (SSH) connection, or upload a public key that you already have.

● Generate a key pair for me ○ Upload public key files (.pub) ○ 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.

k. In the *Boot volume* section, select an option and configure as needed.



Boot volume

A boot volume is a detachable device that contains the image used to boot the compute instance.

□ Specify a custom boot volume size

Volume performance varies with volume size. Default boot volume size: 46.6 GB. When you specify a custom boot volume size, service limits apply.

□ Use in-transit encryption

Encrypts data in transit between the instance, the boot volume, and the block volumes.

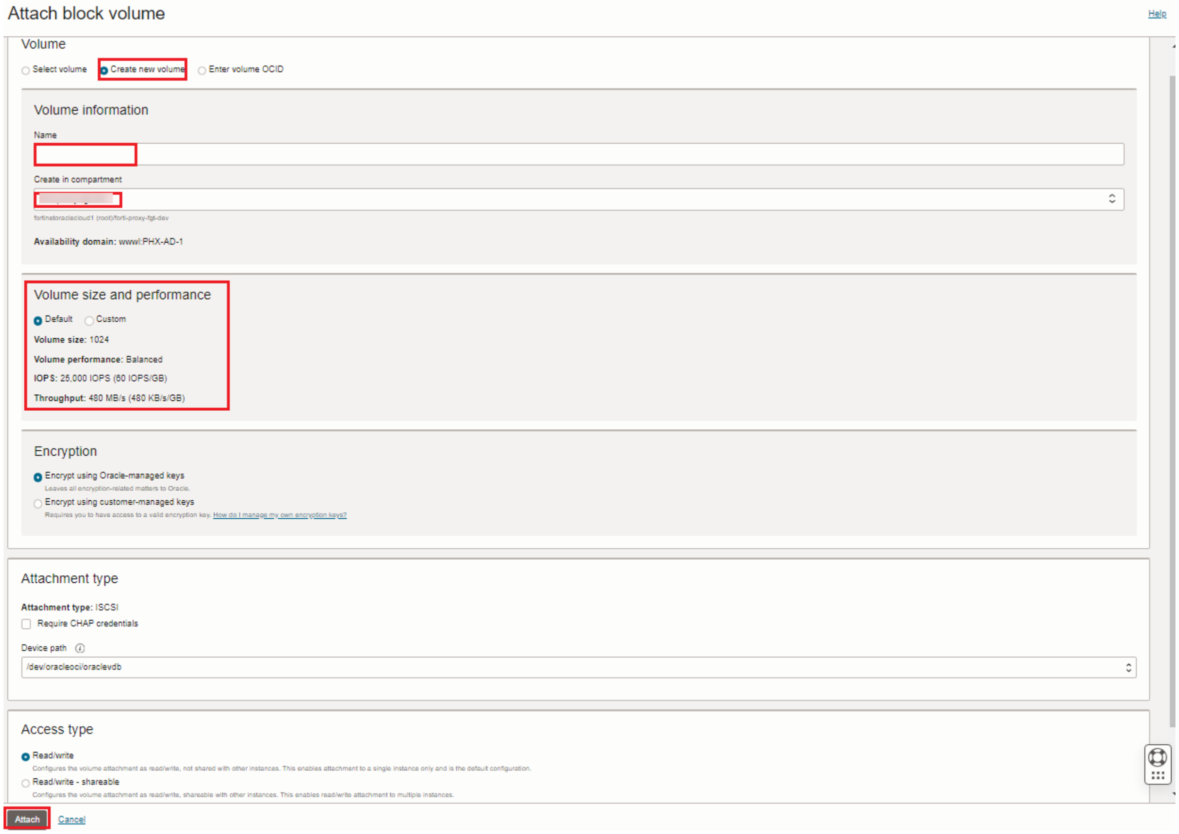
□ Encrypt this volume with a key that you manage

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. How do I manage my own encryption keys?

l. In the *Block volumes* section, add a volume for storing log and web cache data.

i. Click *Attach block volume*.

ii. Select an existing block volume or create a new one. The size should be around 50 GB.



Attach block volume

Volume

○ Select volume ● Create new volume ○ Enter volume OCID

Volume information

Name

Create in compartment

[redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Availability domain: wwwl:PHX-AD-1

Volume size and performance

● Default ○ Custom

Volume size: 1024

Volume performance: Balanced

IOPS: 25,000 IOPS (60 IOPS/GB)

Throughput: 480 MB/s (480 KB/s/GB)

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 encryption key. How do I manage my own encryption keys?

Attachment type

Attachment type: ISCSI

□ Require CHAP credentials

Device path

/dev/oracleoci/oraclevdb

Access type

● 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.

iii. Click *Attach*.

m. **(Optional)** Add bootstrapping of FortiProxy CLI commands and a BYOL license at the time of initial bootup as part of instance creation:

i. At the bottom of the page, click *Show Advanced Options*.

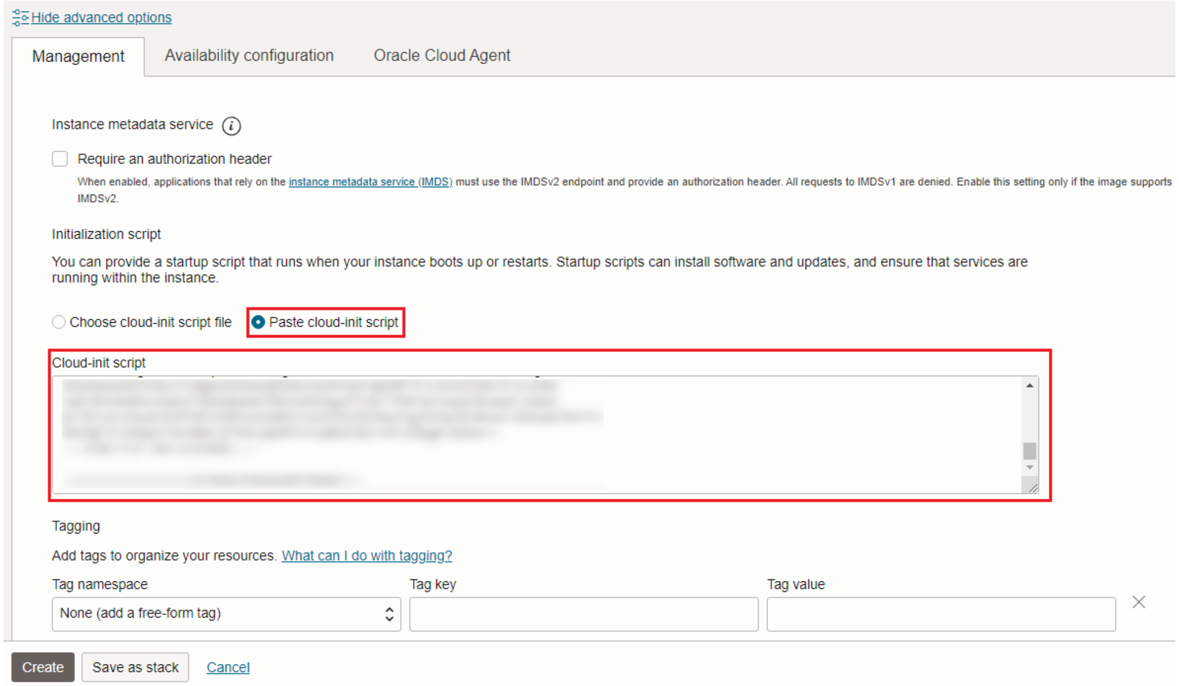
ii. On the *Management* tab, select *Paste cloud-ini script*.

iii. Customize the following sample code (in MIME format) according to your needs.

- Replace the `config system global` commands with your own set of CLI commands as needed. The timezone is set to GMT-9 Alaska in the sample code.
- Replace the license string with the license file content that you download from Customer Service & Support after registering your product code.

```
Content-Type: multipart/mixed; boundary="===============0740947994048919689=="
MIME-Version: 1.0

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"

config system global
 set timezone 03
end

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"

-----BEGIN FPX VM LICENSE-----
Replace with your own license file
-----END FPX VM LICENSE-----
```

iv. In the *Cloud-init script* field, enter your custom version of the sample code (including the CLI commands and your license) from the previous step.



Instance metadata service

□ Require an authorization header

When enabled, applications that rely on the instance metadata service (IMDS) must use the IMDSv2 endpoint and provide an authorization header. All requests to IMDSv1 are denied. Enable this setting only if the image supports IMDSv2.

Initialization script

You can provide a startup script that runs when your instance boots up or restarts. Startup scripts can install software and updates, and ensure that services are running within the instance.

○ Choose cloud-init script file ● Paste cloud-init script

Cloud-init script

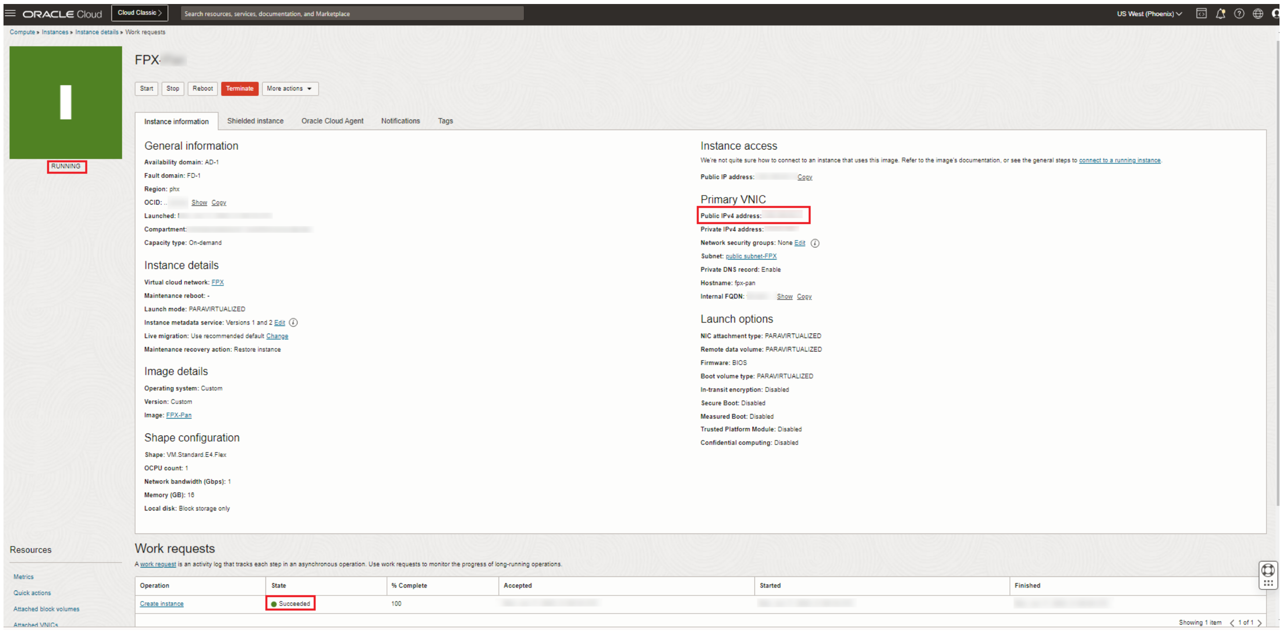
[redacted]

Tagging

Add tags to organize your resources. What can I do with tagging?

Tag namespace	Tag key	Tag value
None (add a free-form tag)		

3. Click *Create*. Wait until the *PROVISIONING…* status changes to *RUNNING* and verify that the *Create instance* operation status changes to *Succeeded*.
   You can also check the FortiProxy's public IP address in this screen once it becomes available.



General information

Availability domain: AD-1
Fault domain: FD-1
Region: phx
OCID: [redacted] Show Copy
Launched: [redacted]
Compartment: [redacted]
Capacity type: On-demand

Instance details

Virtual cloud network: FPX
Maintenance reboot: -
Launch mode: PARAVIRTUALIZED
Instance metadata service: Versions 1 and 2 Edit
Live migration: Use recommended default Change
Maintenance recovery action: Restore instance

Image details

Operating system: Custom
Version: Custom
Image: FPX-Pan

Shape configuration

Shape: VM.Standard.E4.Flex
OCPU count: 1
Network bandwidth (Gbps): 1
Memory (GB): 16
Local disk: Block storage only

Instance access

We're not quite sure how to connect to an instance that uses this image. Refer to the image's documentation, or see the general steps to connect to a running instance.

Public IP address: [redacted] Copy

Primary VNIC

Public IPv4 address: [redacted]
Private IPv4 address: [redacted]
Network security groups: None Edit
Subnet: public subnet-FPX
Private DNS record: Enable
Hostname: fpx-pan
Internal FQDN: [redacted] Show Copy

Launch options

NIC attachment type: PARAVIRTUALIZED
Remote data volume: PARAVIRTUALIZED
Firmware: BIOS
Boot volume type: PARAVIRTUALIZED
In-transit encryption: Disabled
Secure Boot: Disabled
Measured Boot: Disabled
Trusted Platform Module: Disabled
Confidential computing: Disabled

Work requests

A work request is an activity log that tracks each step in an asynchronous operation. Use work requests to monitor the progress of long-running operations.

Operation	State	% Complete	Accepted	Started	Finished
Create instance	● Succeeded	100	[redacted]	[redacted]	[redacted]

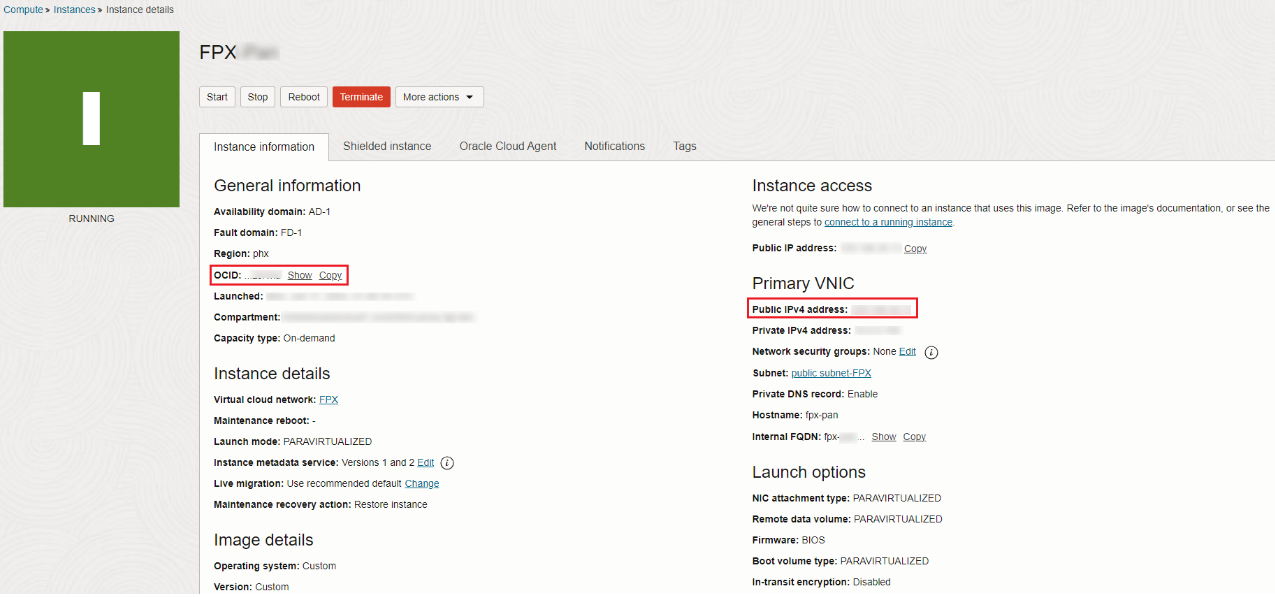
Showing 1 item 1 of 1

Once you have created a FortiProxy-VM, continue to Accessing the FortiProxy-VM on page 24.

Accessing the FortiProxy-VM

To access the FortiProxy-VM:

1. In the FortiProxy-VM instance, find the OCID and public IP address. Your IP address will differ from the example.



General information

Availability domain: AD-1

Fault domain: FD-1

Region: phx

OCID: [redacted] Show Copy

Launched: [redacted]

Compartment: [redacted]

Capacity type: On-demand

Instance details

Virtual cloud network: FPX

Maintenance reboot: -

Launch mode: PARAVIRTUALIZED

Instance metadata service: Versions 1 and 2 Edit

Live migration: Use recommended default Change

Maintenance recovery action: Restore instance

Image details

Operating system: Custom

Version: Custom

Instance access

We're not quite sure how to connect to an instance that uses this image. Refer to the image's documentation, or see the general steps to connect to a running instance.

Public IP address: [redacted] Copy

Primary VNIC

Public IPv4 address: [redacted]

Private IPv4 address: [redacted]

Network security groups: None Edit

Subnet: public subnet-FPX

Private DNS record: Enable

Hostname: fpx-pan

Internal FQDN: fpx-[redacted]... Show Copy

Launch options

NIC attachment type: PARAVIRTUALIZED

Remote data volume: PARAVIRTUALIZED

Firmware: BIOS

Boot volume type: PARAVIRTUALIZED

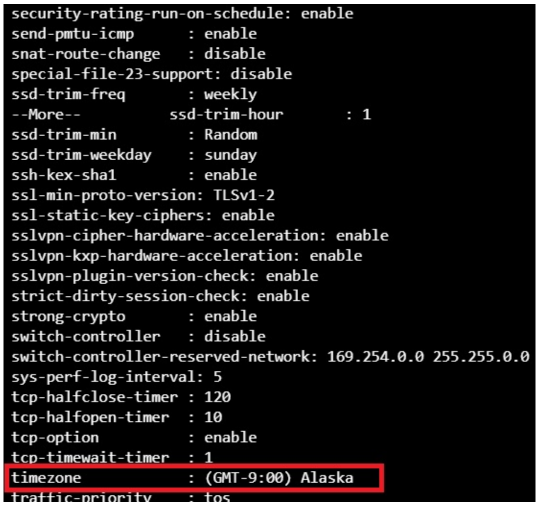
In-transit encryption: Disabled

2. In a browser, go to *https://<public_IP_address>*. The default username is “admin” for new installations. For upgrades, the existing opc user is kept. The default password is the OCID.
3. Upload the FortiProxy license file when prompted. See Licensing on page 5 for instructions about obtaining, registering, and downloading a license.

> It may take up to 30 minutes for Fortinet servers to fully recognize the new license. If you get an error that the license is invalid when uploading the license (`.lic`) file to activate the FortiProxy-VM, wait 30 minutes and try again.

4. If you added a license by following the instructions in step l in Creating a FortiProxy-VM instance on page 12, the system should display the dashboard instead of a license upload window, since the license is already activated. You can check if the command succeeded in the following way:
   a. In the CLI console, enter `diag debug cloudinit show`. If the cloud-init succeeded, the CLI shows `Finish running script` with no errors.

b. Check the timezone by running `config system global` and `get` commands.



```
security-rating-run-on-schedule: enable
send-pmtu-icmp      : enable
snat-route-change   : disable
special-file-23-support: disable
ssd-trim-freq       : weekly
--More--          ssd-trim-hour       : 1
ssd-trim-min        : Random
ssd-trim-weekday    : sunday
ssh-kex-sha1        : enable
ssl-min-proto-version: TLSv1-2
ssl-static-key-ciphers: enable
sslvpn-cipher-hardware-acceleration: enable
sslvpn-kxp-hardware-acceleration: enable
sslvpn-plugin-version-check: enable
strict-dirty-session-check: enable
strong-crypto       : enable
switch-controller   : disable
switch-controller-reserved-network: 169.254.0.0 255.255.0.0
sys-perf-log-interval: 5
tcp-halfclose-timer : 120
tcp-halfopen-timer  : 10
tcp-option          : enable
tcp-timewait-timer  : 1
timezone            : (GMT-9:00) Alaska
traffic-priority    : tos
```

If the timezone changed to Alaska as expected, it means the bootstrapping CLI command succeeded.

Deploying FortiProxy-VM active-passive HA on OCI within one AD

You can configure FortiProxy's native active-passive high availability (HA) feature (without using an OCI supplementary mechanism such as a load balancer) with two FortiProxy-VM instances: one acting as the primary node and the other as the secondary node, both located in the same availability domain (AD). This is called "unicast HA" and is specific to cloud environments, including OCI, to comply to their network restrictions in comparison to an equivalent feature that physical FortiProxies provided.

The FortiProxy-VMs run heartbeats between dedicated ports and synchronize operating system configurations. When the primary node fails, the secondary node takes over as the primary node so endpoints continue to communicate with external resources over the FortiProxy-VM. The FortiProxies also synchronize sessions at the time of failover.

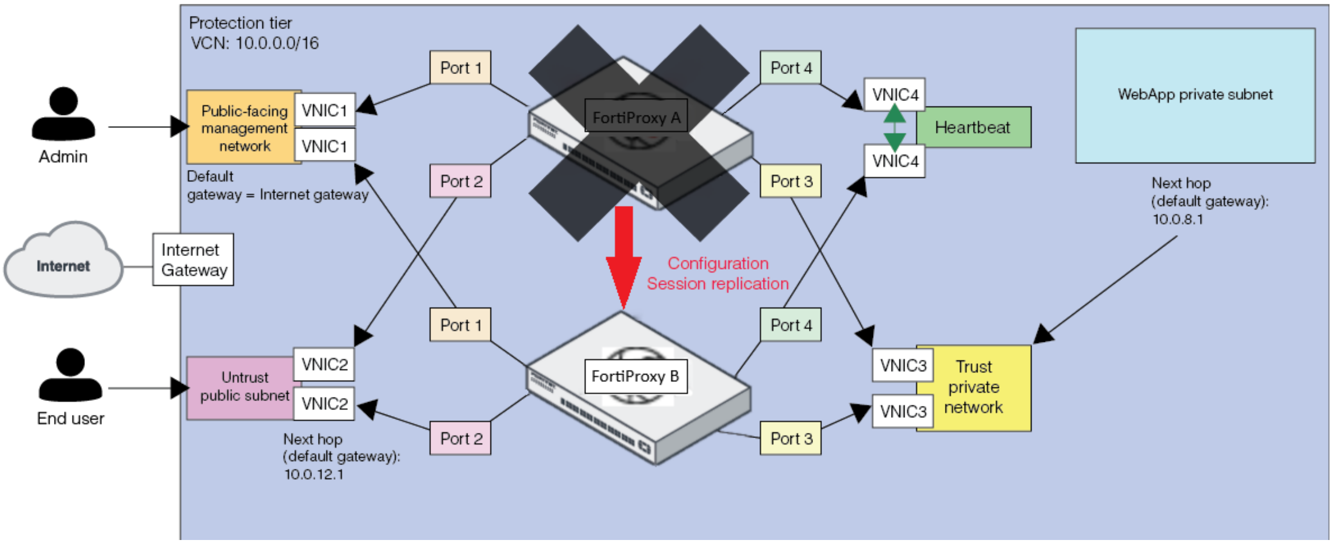
The following sections provides an example of deploying FortiProxy-VM active-passive HA on OCI within one AD:

1. Reviewing the network topology on page 26
2. Creating a VCN for single-AD HA topology on page 28
3. Creating two FortiProxy-VM instances on page 32
4. Configuring a route table for the private subnet on page 48
5. Configuring the OCI HA interfaces on page 48
6. Configuring active-passive HA on page 55
7. Configuring an OCI SND connector on page 52

Reviewing the network topology

For this example HA deployment, you will create a VCN and configure two FortiProxy-VM instances with four network interfaces attached to each instance .

Your deployment will have different IP addresses than in the diagram.



The following table describes the port definition used in this example deployment. Port1 and 2 are on public (or untrusted) subnets with public IP addresses allocated.

While port2, port 3, and port4 are interchangeable, port 1 must be defined as the dedicated management interface. Fortinet recommends defining each port in a different subnet.

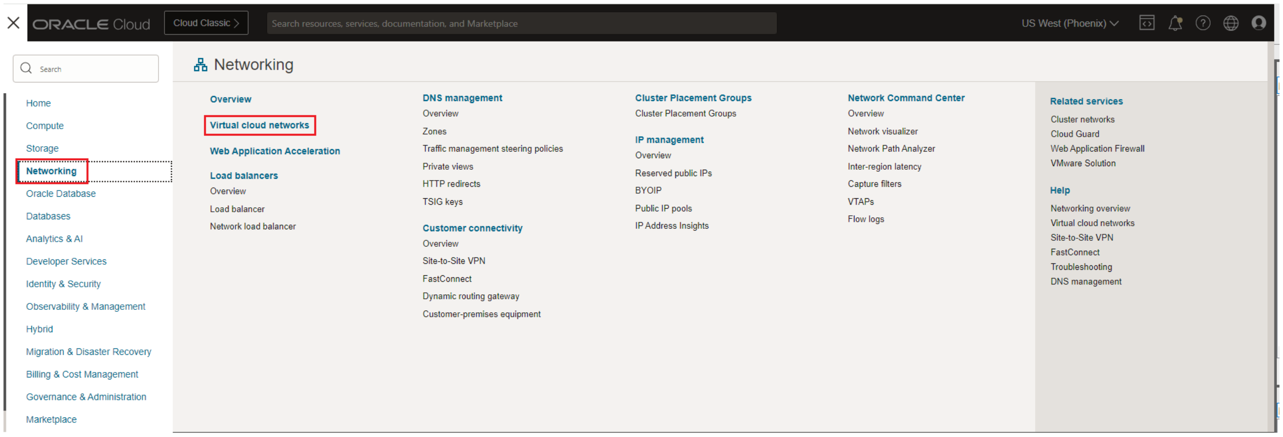
Port	Description
Port 1	Dedicated management interface. In case of heartbeat failure, the passive firewall needs a dedicated port through which to communicate with OCI to issue failover-related commands. This port is always available, regardless of node status (active/passive), except when a node is down. DNS must work with port 1 to resolve OCI's API endpoint URLs at the time of HA failover.
Port 2	External data interface on the public network-facing side. A public IP address for the protected server is associated with the active node's private IP address. FortiProxy performs NAT for inbound traffic and outbound traffic.
Port 3	Internal data traffic interface on the protected/trusted network-facing side.
Port 4	Heartbeat between two FortiProxy nodes. This is unicast communication. This heartbeat interface has its dedicated "hbdev" VDOM and cannot be used for any other purpose.

You must configure primary private IP addresses, even where not mentioned in the diagram. Although not required for HA purposes, you must be do this to comply with general networking requirements.

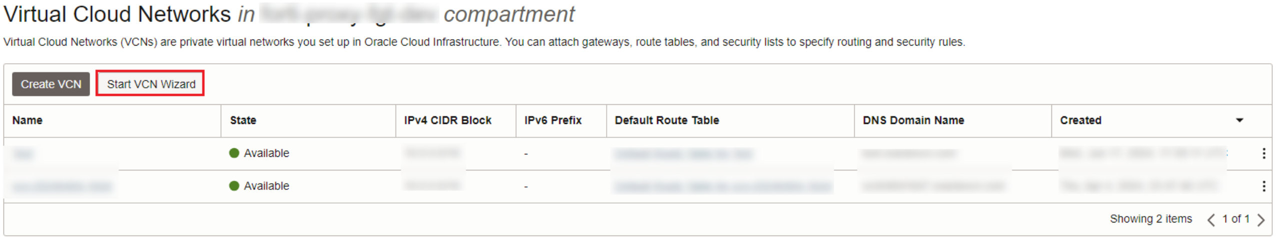
Creating a VCN for single-AD HA topology

To create a VCN with four subnets:

1. In OCI, go to *Networking* > *Virtual cloud networks*.



2. Click *Start VCN Wizard* to create the Internet gateway, routing table, and subnet all together using Oracle default settings.
   You can also choose to create each resource separately by clicking *Create VCN*.



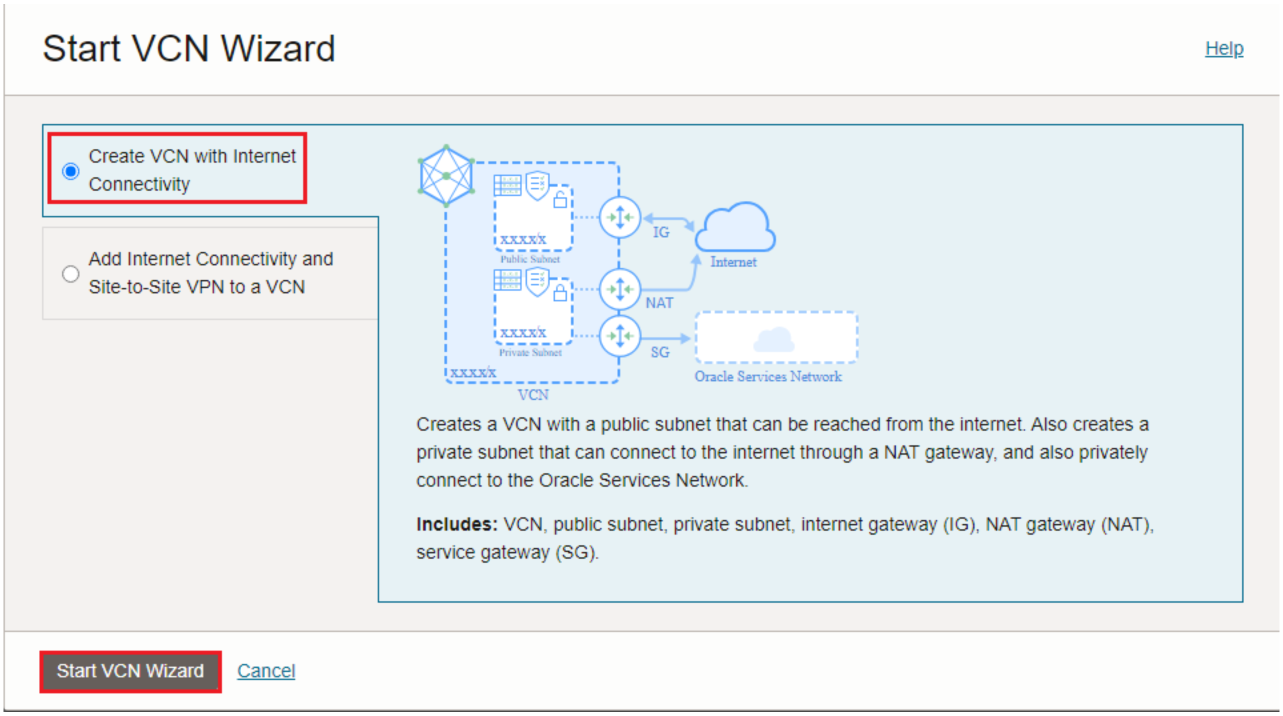
Virtual Cloud Networks *in [redacted] compartment*

Virtual Cloud Networks (VCNs) are private virtual networks you set up in Oracle Cloud Infrastructure. You can attach gateways, route tables, and security lists to specify routing and security rules.

Name	State	IPv4 CIDR Block	IPv6 Prefix	Default Route Table	DNS Domain Name	Created
[redacted]	● Available	[redacted]	-	[redacted]	[redacted]	[redacted]
[redacted]	● Available	[redacted]	-	[redacted]	[redacted]	[redacted]

Showing 2 items 1 of 1

3. Select *Create VCN with Internet Connectivity* and click *Start VCN Wizard*.



Start VCN Wizard

Help

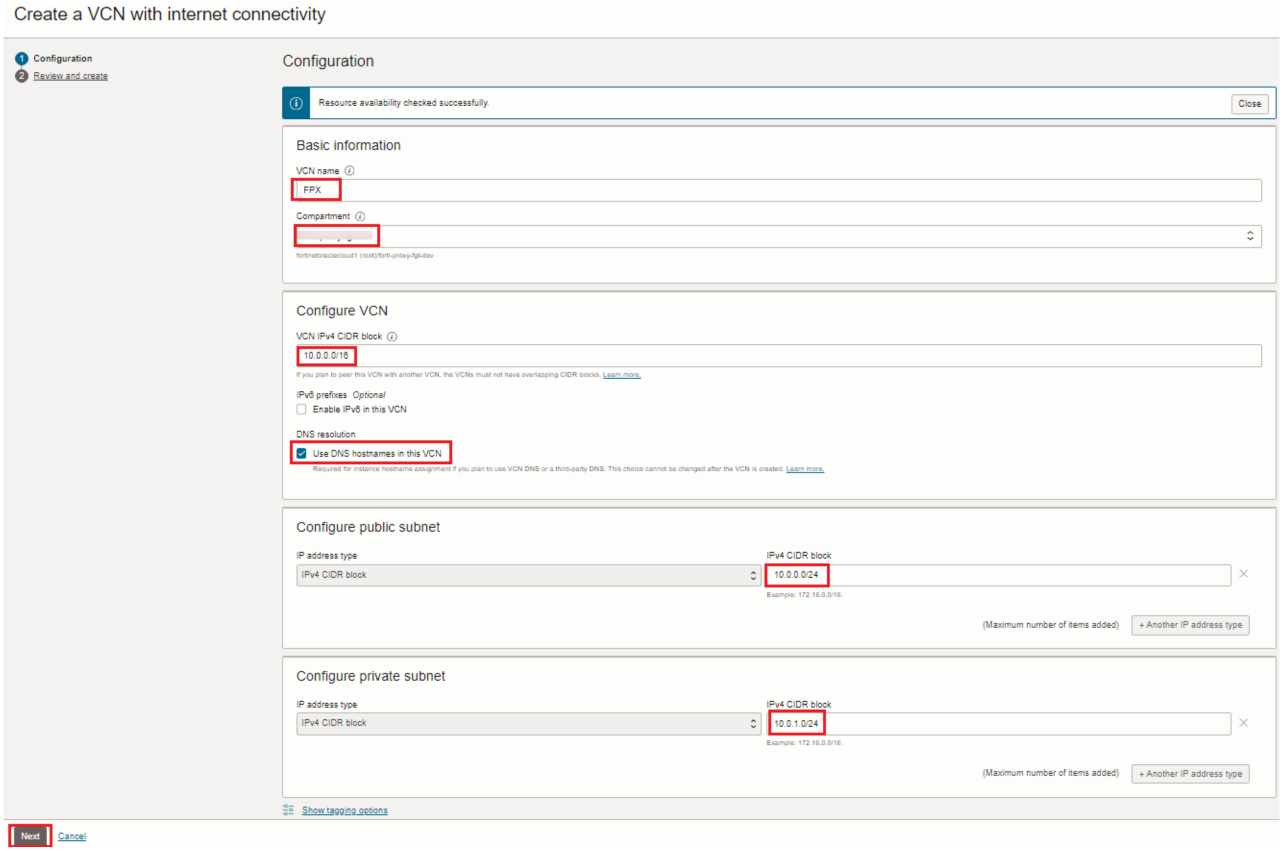
● Create VCN with Internet Connectivity

○ Add Internet Connectivity and Site-to-Site VPN to a VCN

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).

4. Configure the following options:



Create a VCN with internet connectivity

Configuration

Resource availability checked successfully.

Basic information

VCN name: FPX

Compartment: [redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Configure VCN

VCN IPv4 CIDR block: 10.0.0.0/16

If you plan to peer this VCN with another VCN, the VCNs must not have overlapping CIDR blocks. Learn more.

IPv6 prefixes *Optional*

□ Enable IPv6 in this VCN

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.

Configure public subnet

IP address type	IPv4 CIDR block
IPv4 CIDR block	10.0.0.0/24

Example: 172.16.0.0/16.

(Maximum number of items added)

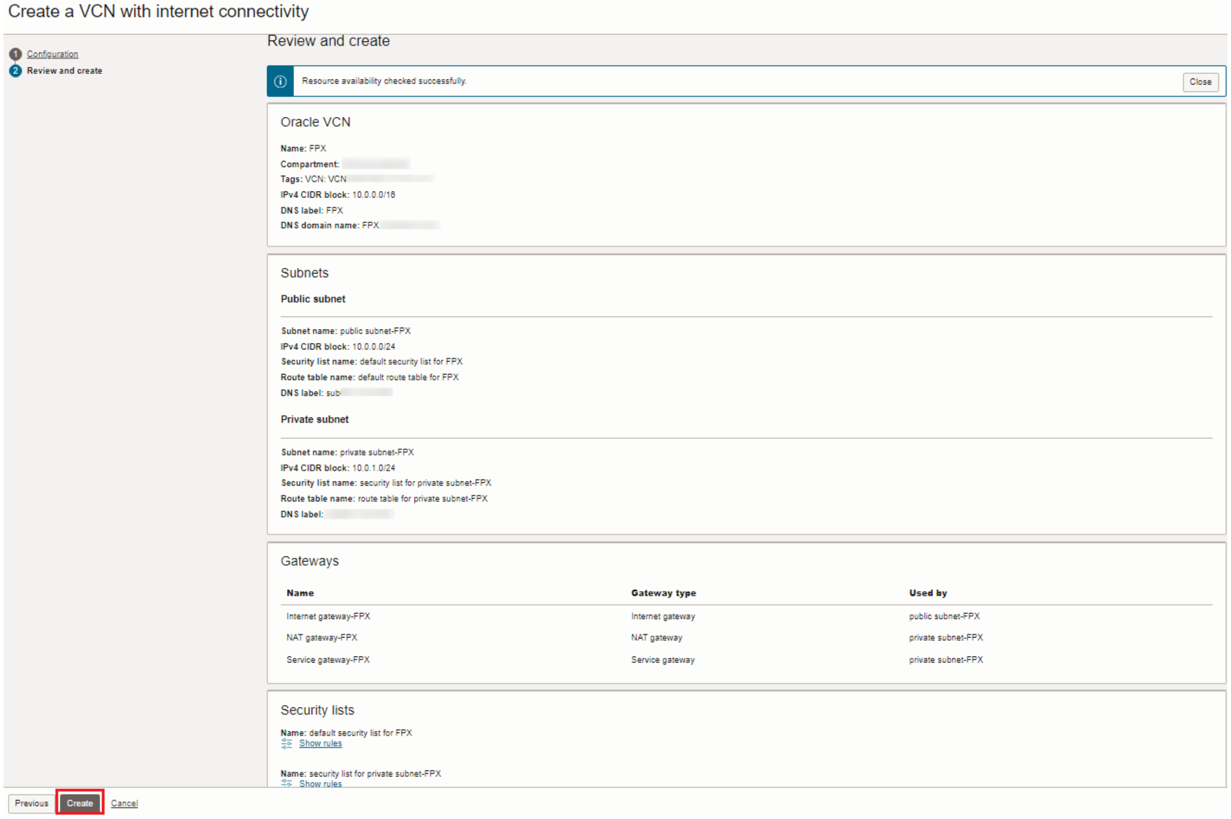
Configure private subnet

IP address type	IPv4 CIDR block
IPv4 CIDR block	10.0.1.0/24

Example: 172.16.0.0/16.

(Maximum number of items added)

   a. In the *VCN name* field, enter the VCN name.
   b. In the *Compartment* field, select the compartment for the VCN.
   c. In the *IPv4 CIDR block* field, specify the IPv4 CIDR block.
   d. Select the *Use DNS hostnames in this VCN* option.
   e. Configure subnets as needed.
   f. Click *Next*.
   g. Confirm the configuration details and click *Create* at the bottom of the screen.



Create a VCN with internet connectivity

Review and create

Resource availability checked successfully.

Oracle VCN

Name: FPX
Compartment: [redacted]
Tags: VCN: VCN[redacted]
IPv4 CIDR block: 10.0.0.0/16
DNS label: FPX
DNS domain name: FPX[redacted]

Subnets

Public subnet

Subnet name: public subnet-FPX
IPv4 CIDR block: 10.0.0.0/24
Security list name: default security list for FPX
Route table name: default route table for FPX
DNS label: sub[redacted]

Private subnet

Subnet name: private subnet-FPX
IPv4 CIDR block: 10.0.1.0/24
Security list name: security list for private subnet-FPX
Route table name: route table for private subnet-FPX
DNS label: [redacted]

Gateways

Name	Gateway type	Used by
Internet gateway-FPX	Internet gateway	public subnet-FPX
NAT gateway-FPX	NAT gateway	private subnet-FPX
Service gateway-FPX	Service gateway	private subnet-FPX

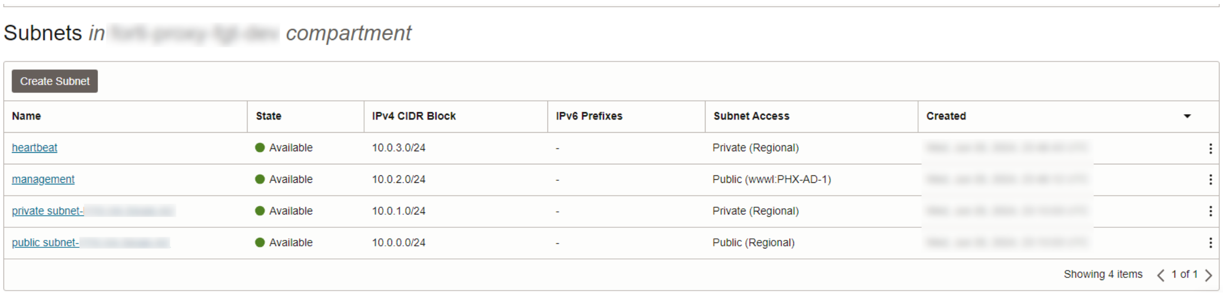
Security lists

Name: default security list for FPX
Show rules

Name: security list for private subnet-FPX
Show rules

This configures the related resources, including two subnets: one for public access and the other for private access, each of which will belong to an AD. In this example, (1) is 10.0.x.x/24. You can access the FortiProxy over the Internet once it is deployed via HTTPS through the GUI management screen or via SSH.

5. Click *View VCN*.
6. Create two more subnets: one for management and the other for heartbeat:
   a. Click *Create Subnet*.
   b. Specify a name to identify the subnet, such as management or heartbeat.
   c. For *Subnet Type*, select *Availability Domain-specific* for management and *Regional* for heartbeat.
   d. **(management only)** Select the availability domain.
   e. Specify the value for *IPv4 CIDR Block*. This example uses 10.0.2.0/24 for management and 10.0.3.0/24 for heartbeat.
   f. For *Security Lists*, select the default security list for the VCN.
   g. For *Subnet Access*, select *Public Subnet* for management and *Private* for heartbeat.
   h. Click *Create Subnet*.
   i. Repeat the steps above to create a subnets for heartbeat.
      The following shows the final result of four subnets:



Subnets *in* [redacted] *compartment*

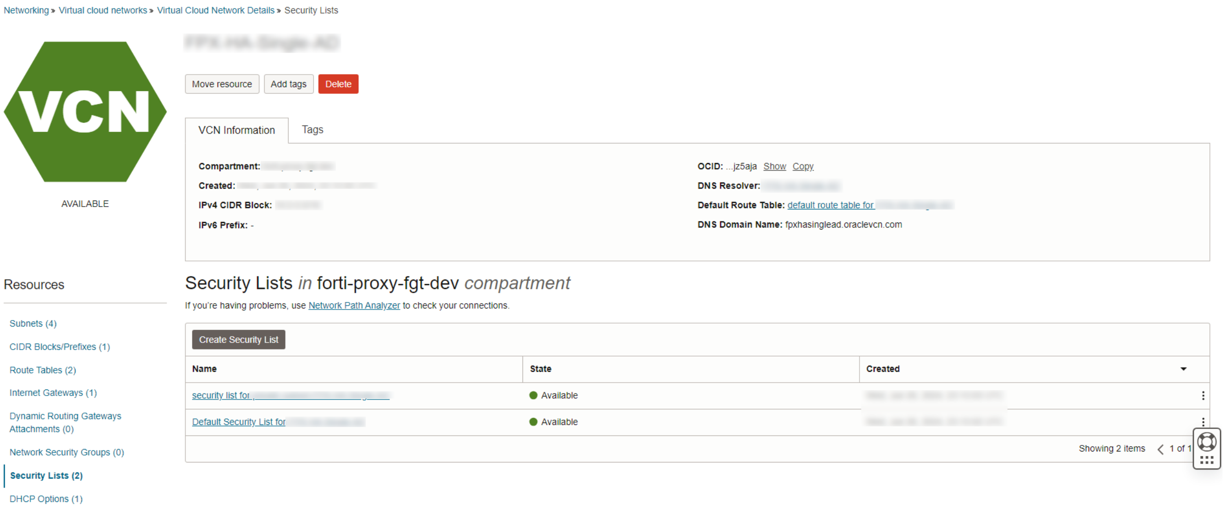
Create Subnet

Name	State	IPv4 CIDR Block	IPv6 Prefixes	Subnet Access	Created
heartbeat	● Available	10.0.3.0/24	-	Private (Regional)	[redacted]
management	● Available	10.0.2.0/24	-	Public (wwwl:PHX-AD-1)	[redacted]
private subnet-[redacted]	● Available	10.0.1.0/24	-	Private (Regional)	[redacted]
public subnet-[redacted]	● Available	10.0.0.0/24	-	Public (Regional)	[redacted]

Showing 4 items 1 of 1

7. Update the default security list to allow access to the required ports as listed in FortiProxy ports:

   a. In the *Security Lists* tab of the VCN details page, click the link of the default security list. By default, port 22 is allowed.



Networking » Virtual cloud networks » Virtual Cloud Network Details » Security Lists

[redacted]

Move resource | Add tags | Delete

VCN Information | Tags

Compartment: [redacted]
Created: [redacted]
IPv4 CIDR Block: [redacted]
IPv6 Prefix: -
OCID: ...jz5aja Show Copy
DNS Resolver: [redacted]
Default Route Table: default route table for [redacted]
DNS Domain Name: fpxhasinglead.oraclevcn.com

AVAILABLE

Resources

- Subnets (4)
- CIDR Blocks/Prefixes (1)
- Route Tables (2)
- Internet Gateways (1)
- Dynamic Routing Gateways Attachments (0)
- Network Security Groups (0)
- Security Lists (2)
- DHCP Options (1)

Security Lists *in* forti-proxy-fgt-dev *compartment*

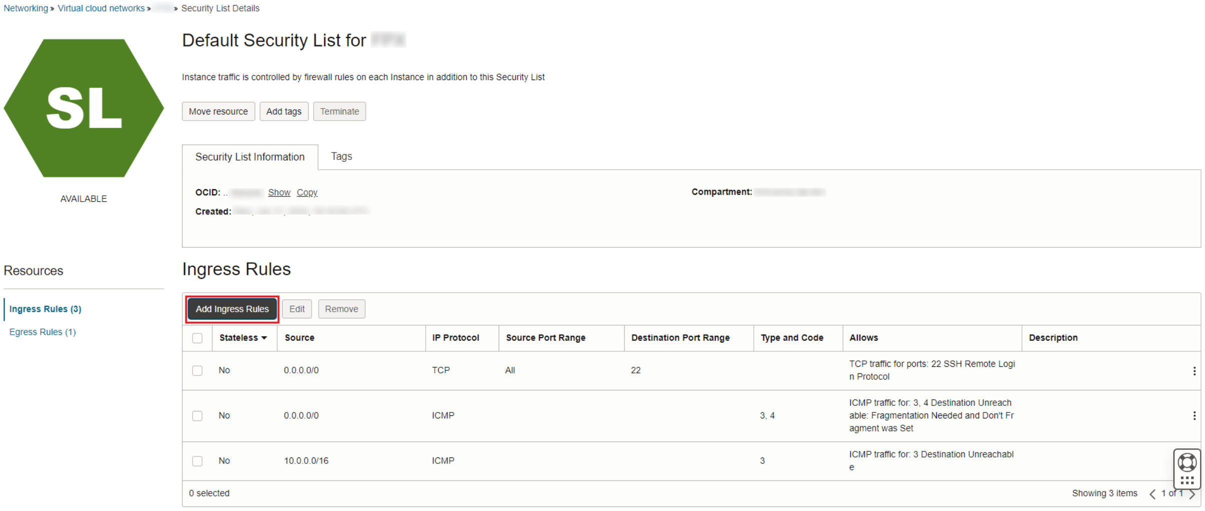
If you're having problems, use Network Path Analyzer to check your connections.

Create Security List

Name	State	Created
security list for [redacted]	● Available	[redacted]
Default Security List for [redacted]	● Available	[redacted]

Showing 2 items 1 of 1

   b. Click *Add Ingress Rules*.



Networking » Virtual cloud networks » [redacted] » Security List Details

Default Security List for [redacted]

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: ...[redacted] Show Copy
Created: [redacted]
Compartment: [redacted]

AVAILABLE

Resources

- Ingress Rules (3)
- Egress Rules (1)

Ingress Rules

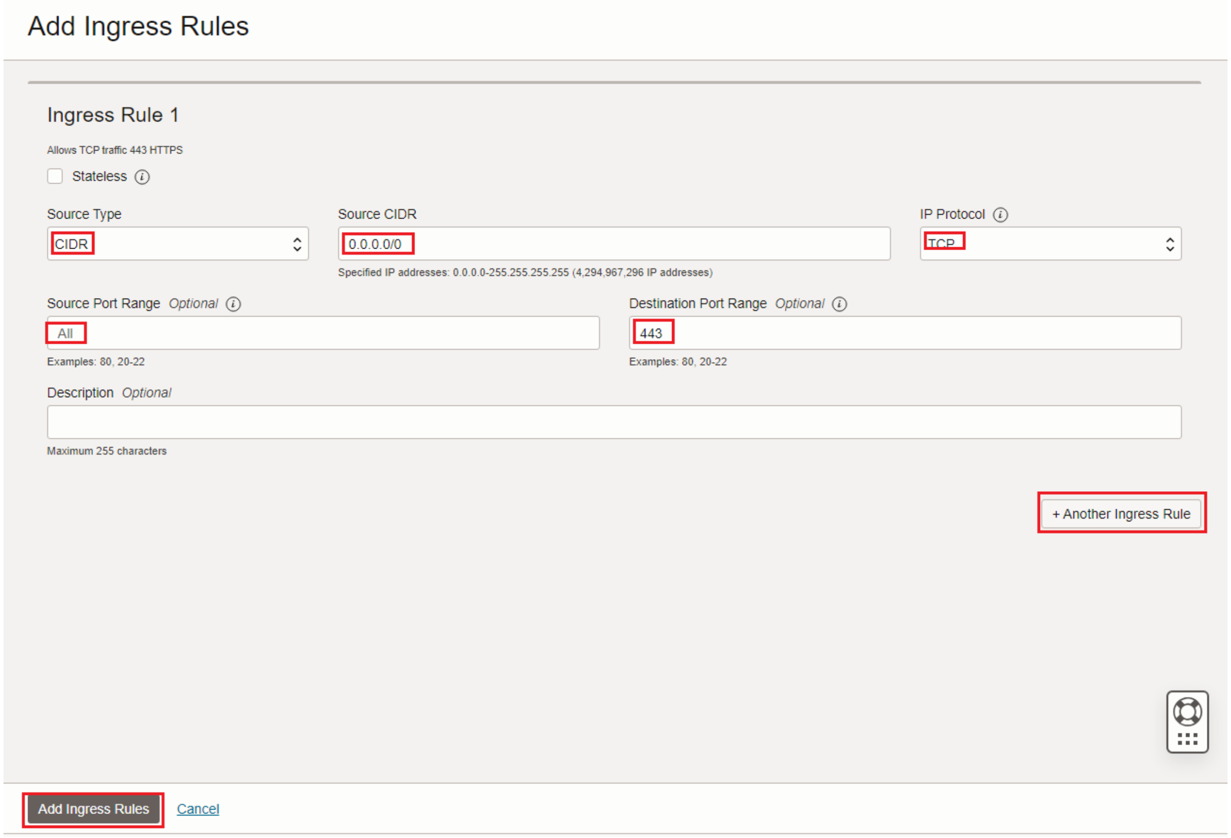
Add Ingress Rules | Edit | Remove

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

0 selected

Showing 3 items 1 of 1

c. Configure a rule to allow TCP port 443 and add any other rules for specific ports as needed.



Add Ingress Rules

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

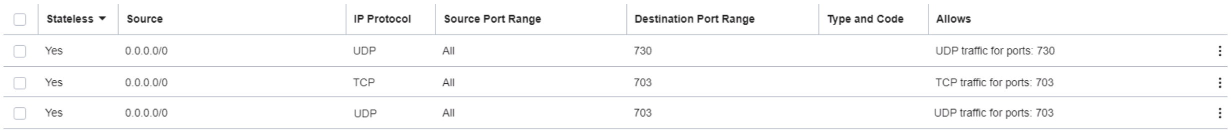
Destination Port Range *Optional*: 443

Examples: 80, 20-22

Description *Optional*

Maximum 255 characters

For example, for Heartbeat sync ports, you must have the following included in the security list:



☐	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows
☐	Yes	0.0.0.0/0	UDP	All	730		UDP traffic for ports: 730
☐	Yes	0.0.0.0/0	TCP	All	703		TCP traffic for ports: 703
☐	Yes	0.0.0.0/0	UDP	All	703		UDP traffic for ports: 703

d. Click *Add Ingress Rules*.

Creating two FortiProxy-VM instances

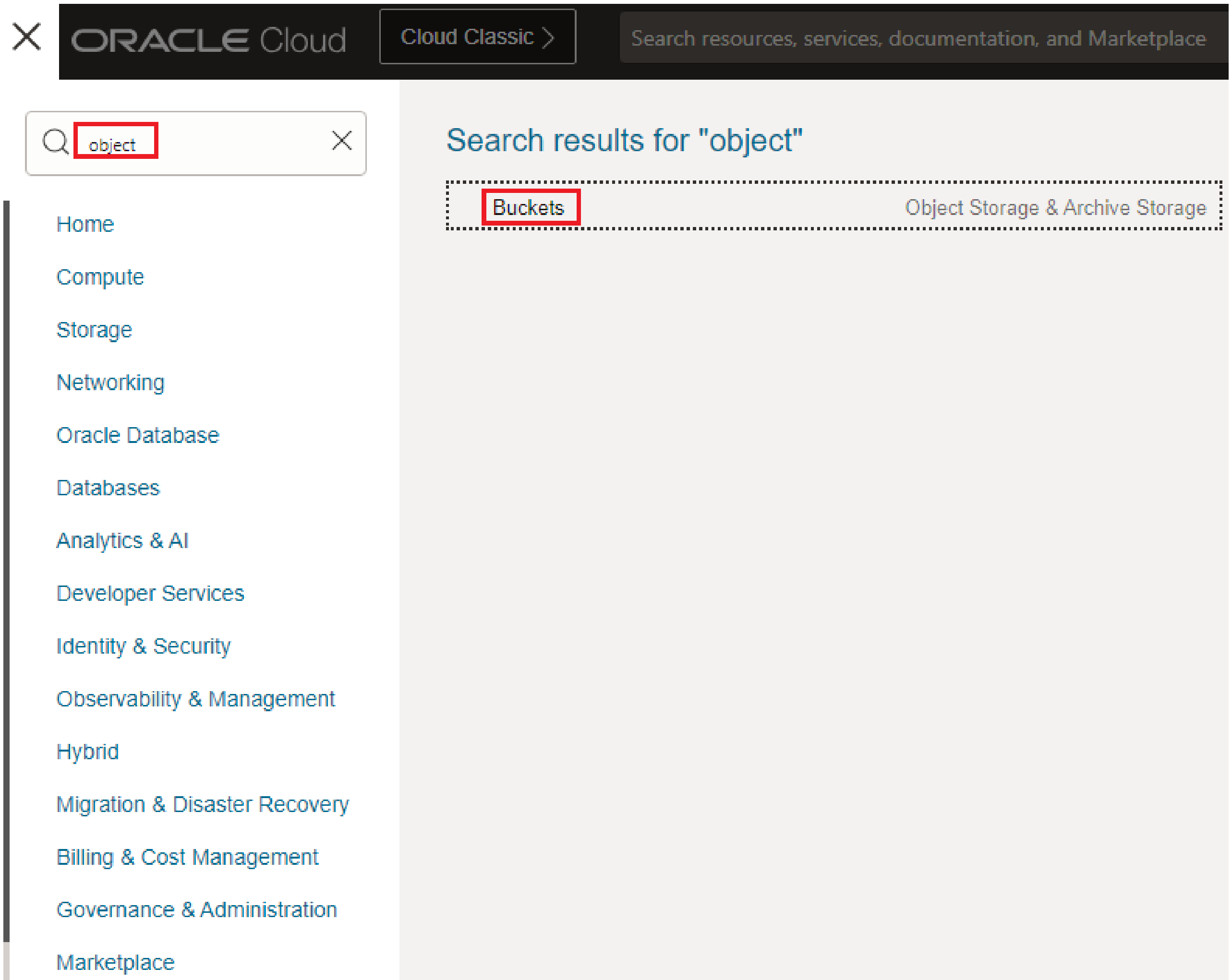
You must create two FortiProxy-VM instances for HA deployment, one for primary and one for secondary. To do so, you must first obtain the deployment image file and importing the file into the OCI bucket.

To obtain the deployment image file and place it in your bucket:

1. Obtain the deployment image file:
   a. Go to Customer Service & Support.
   b. Click *Support* > *Downloads* > *Firmware Download* in the top menu.
   c. In the *Select Product* dropdown list, select *FortiProxy*.
   d. In the *Download* tab, navigate to the FortiProxy version folder.
   e. Obtain the *FPX_KVM_OPC-vX-buildXXXX-FORTINET.out.kvm.zip* file, where *XXXX* is the build number. Ensure that the file name includes *kvm*.

f. After downloading, unzip the file. You will find the *fortiproxy.qcow2* file, which is needed to deploy the FortiProxy-VM on OCI.

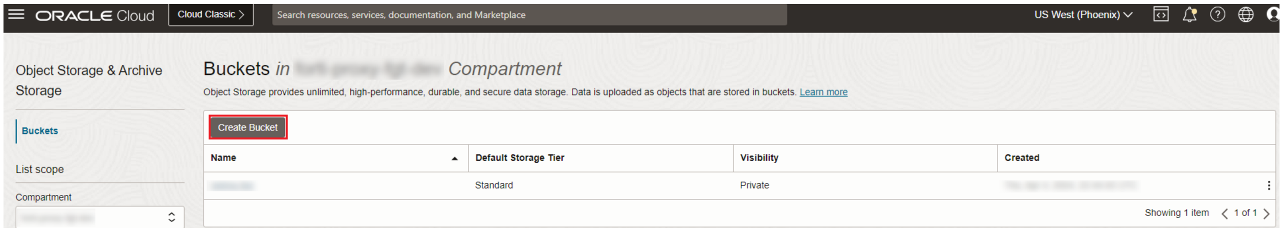
2. In OCI, go to *Object Storage* > *Buckets*.


ORACLE Cloud
Cloud Classic >
Search resources, services, documentation, and Marketplace
object
Home
Compute
Storage
Networking
Oracle Database
Databases
Analytics & AI
Developer Services
Identity & Security
Observability & Management
Hybrid
Migration & Disaster Recovery
Billing & Cost Management
Governance & Administration
Marketplace

Search results for "object"

Buckets	Object Storage & Archive Storage

3. Click *Create Bucket* to create a standard storage bucket.


ORACLE Cloud
Cloud Classic >
Search resources, services, documentation, and Marketplace
US West (Phoenix)
Object Storage & Archive Storage
Buckets
List scope
Compartment
Create Bucket

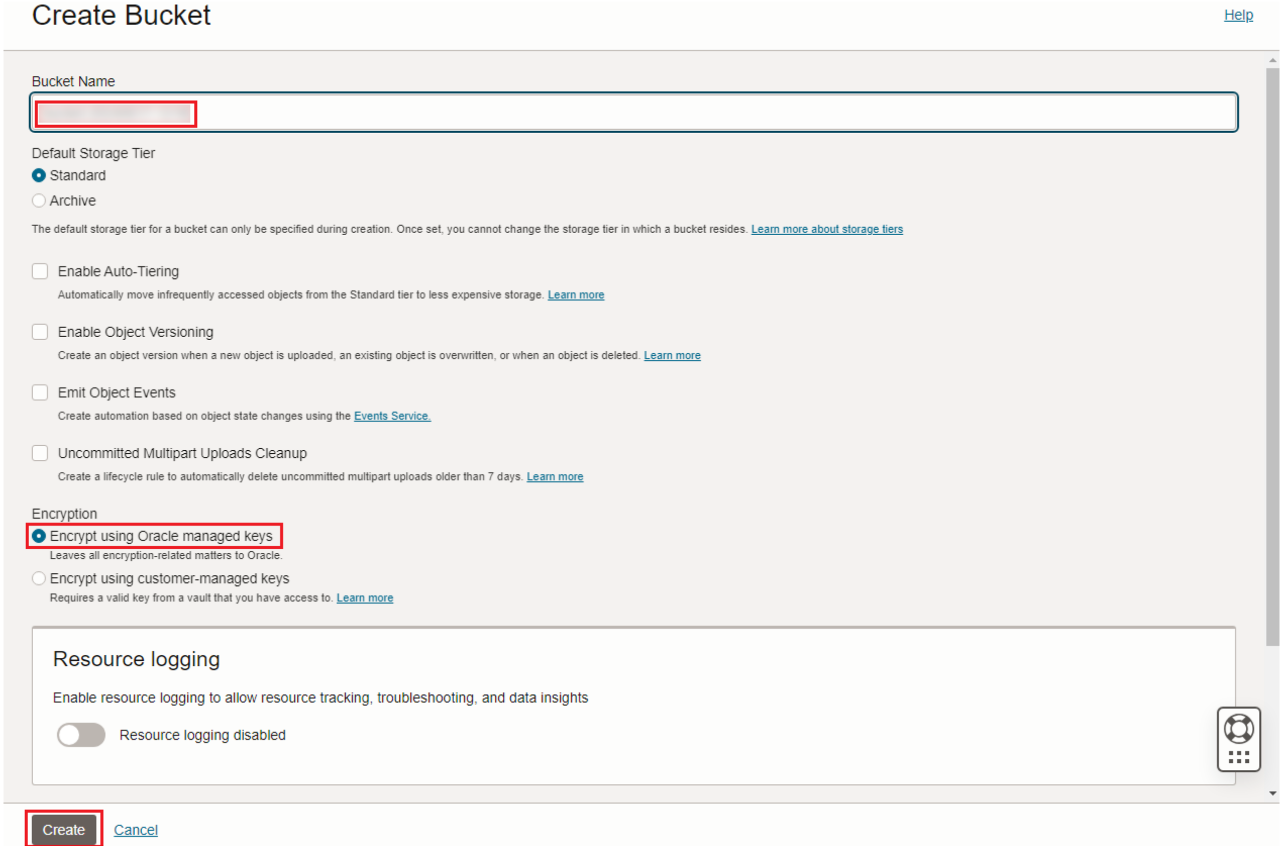
Buckets *in* [redacted] *Compartment*

Object Storage provides unlimited, high-performance, durable, and secure data storage. Data is uploaded as objects that are stored in buckets. Learn more

Name	Default Storage Tier	Visibility	Created
[redacted]	Standard	Private	[redacted]

Showing 1 item 1 of 1

4. Configure the standard storage bucket as shown below and click *Create*:



Create Bucket

Bucket Name

[redacted]

Default Storage Tier

● Standard

○ Archive

The default storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides. Learn more about storage tiers

□ Enable Auto-Tiering

Automatically move infrequently accessed objects from the Standard tier to less expensive storage. Learn more

□ Enable Object Versioning

Create an object version when a new object is uploaded, an existing object is overwritten, or when an object is deleted. Learn more

□ Emit Object Events

Create automation based on object state changes using the Events Service.

□ Uncommitted Multipart Uploads Cleanup

Create a lifecycle rule to automatically delete uncommitted multipart uploads older than 7 days. Learn more

Encryption

● Encrypt using Oracle managed keys

Leaves all encryption-related matters to Oracle.

○ Encrypt using customer-managed keys

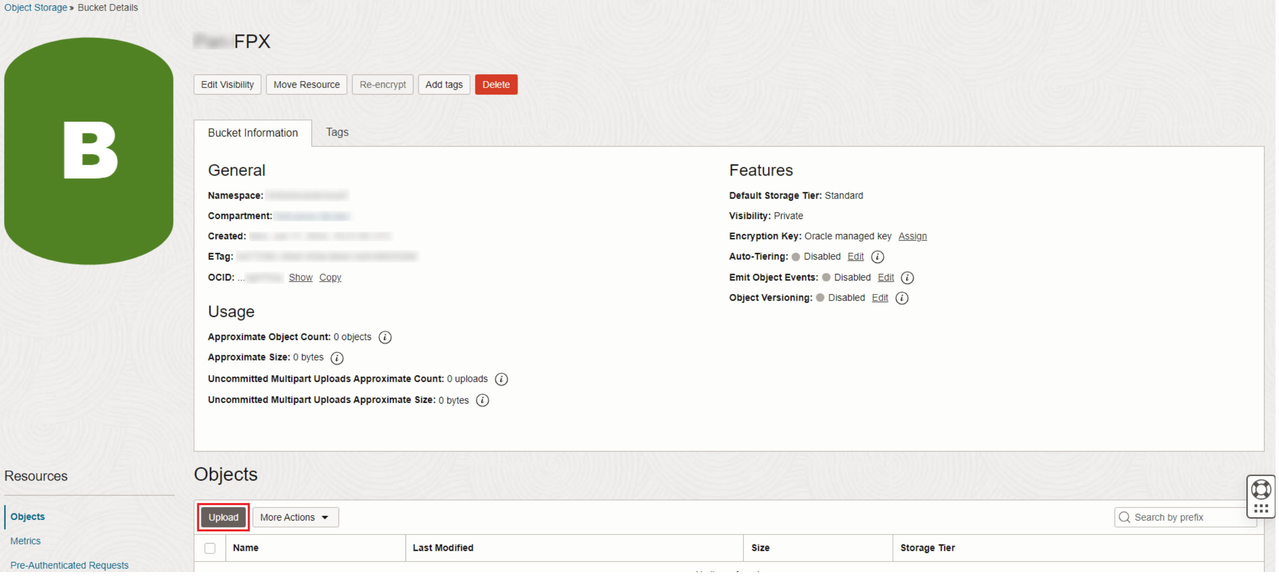
Requires a valid key from a vault that you have access to. Learn more

Resource logging

Enable resource logging to allow resource tracking, troubleshooting, and data insights

Resource logging disabled

5. Select the bucket, then click *Upload*.



[redacted] FPX

General

Namespace: [redacted]

Compartment: [redacted]

Created: [redacted]

ETag: [redacted]

OCID: ...[redacted] Show Copy

Usage

Approximate Object Count: 0 objects

Approximate Size: 0 bytes

Uncommitted Multipart Uploads Approximate Count: 0 uploads

Uncommitted Multipart Uploads Approximate Size: 0 bytes

Features

Default Storage Tier: Standard

Visibility: Private

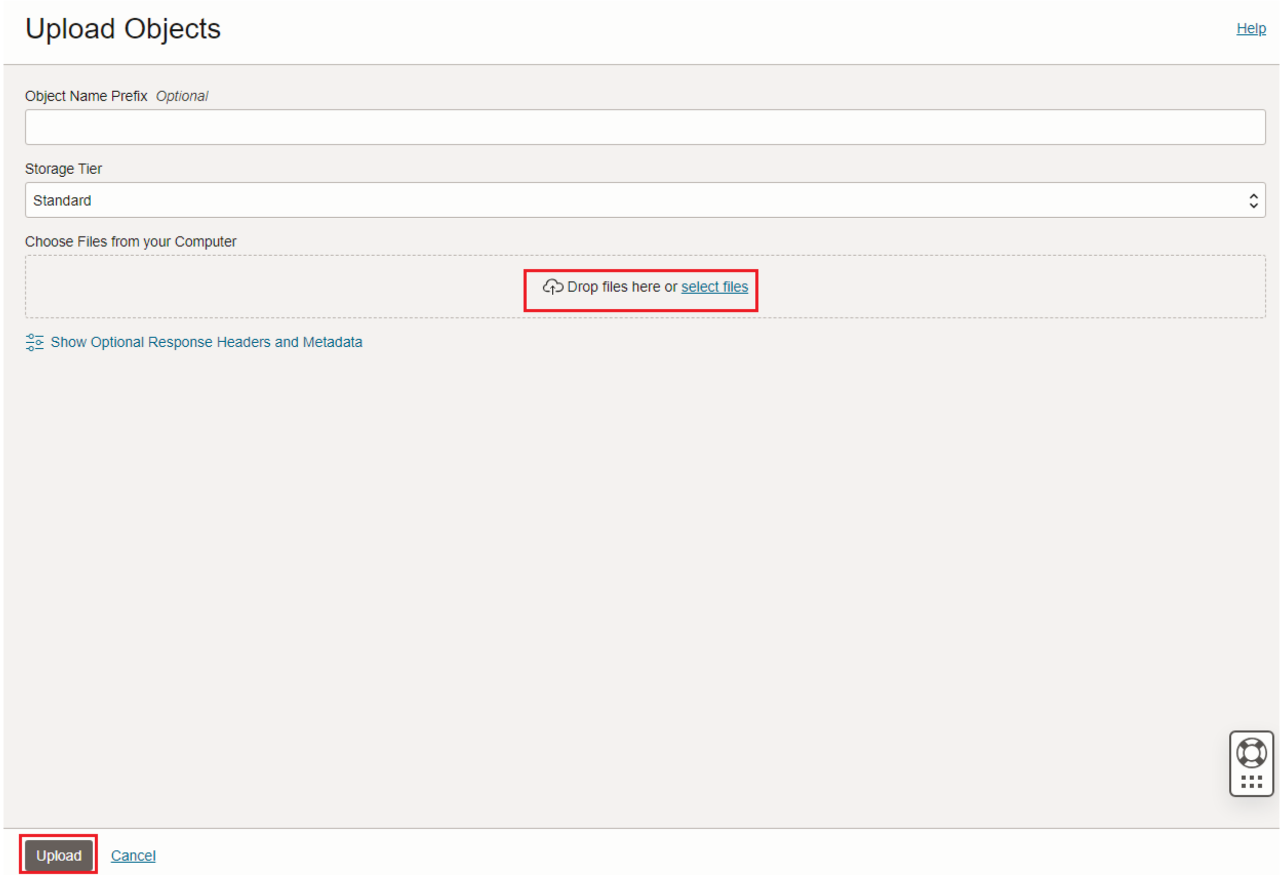
Encryption Key: Oracle managed key Assign

Auto-Tiering: Disabled Edit

Emit Object Events: Disabled Edit

Object Versioning: Disabled Edit

6. Drop or select the deployment image file *fortiproxy.qcow2* and click *Upload*.



Upload Objects

Object Name Prefix *Optional*

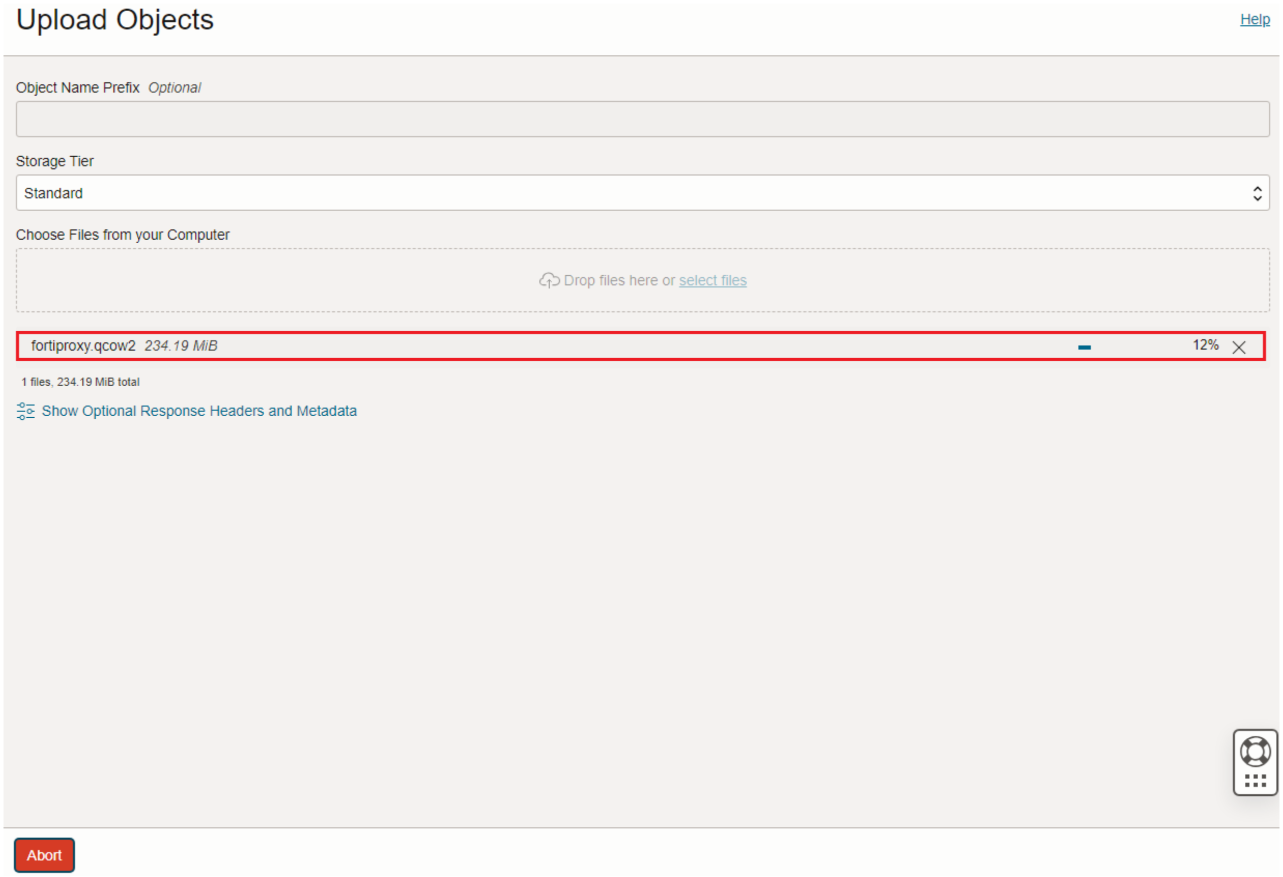
Storage Tier

Standard

Choose Files from your Computer

Drop files here or select files

The dialog shows the upload progress.



Upload Objects

Object Name Prefix *Optional*

Storage Tier: Standard

Choose Files from your Computer

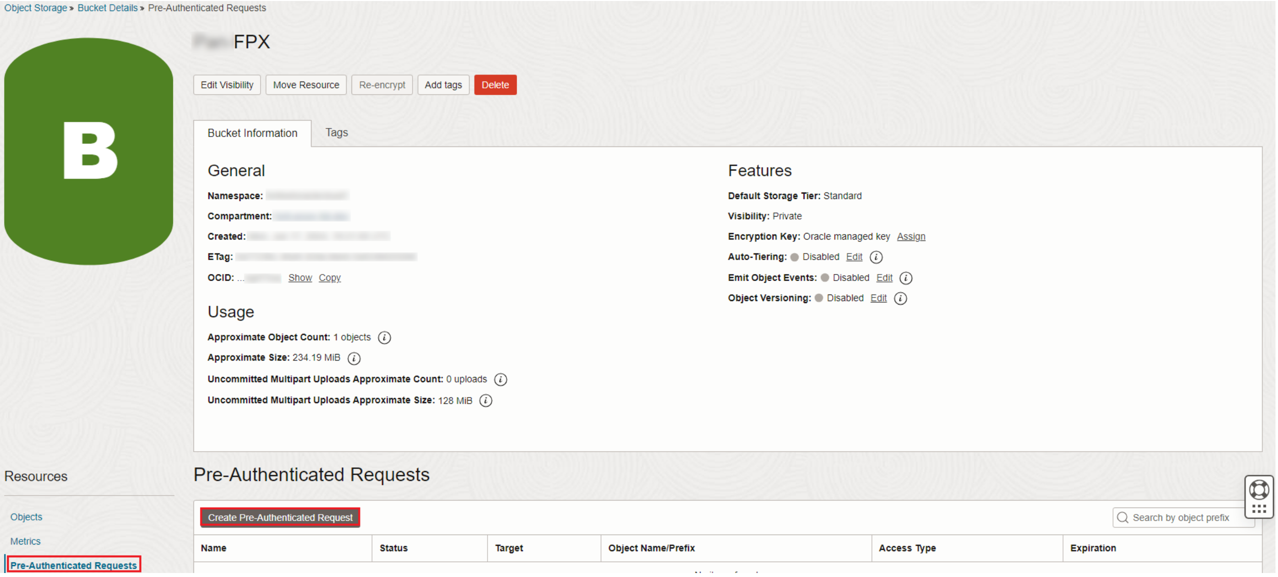
Drop files here or select files

fortiproxy.qcow2 *234.19 MiB* 12%

1 files, 234.19 MiB total

Show Optional Response Headers and Metadata

7. After the upload is complete, click *Close*.
8. Click *Pre-Authenticated Requests* and then *Create Pre-Authenticated Requests*.



Object Storage » Bucket Details » Pre-Authenticated Requests

[redacted] FPX

General

Namespace: [redacted]

Compartment: [redacted]

Created: [redacted]

ETag: [redacted]

OCID: ...[redacted] Show Copy

Usage

Approximate Object Count: 1 objects

Approximate Size: 234.19 MiB

Uncommitted Multipart Uploads Approximate Count: 0 uploads

Uncommitted Multipart Uploads Approximate Size: 128 MiB

Features

Default Storage Tier: Standard

Visibility: Private

Encryption Key: Oracle managed key Assign

Auto-Tiering: Disabled Edit

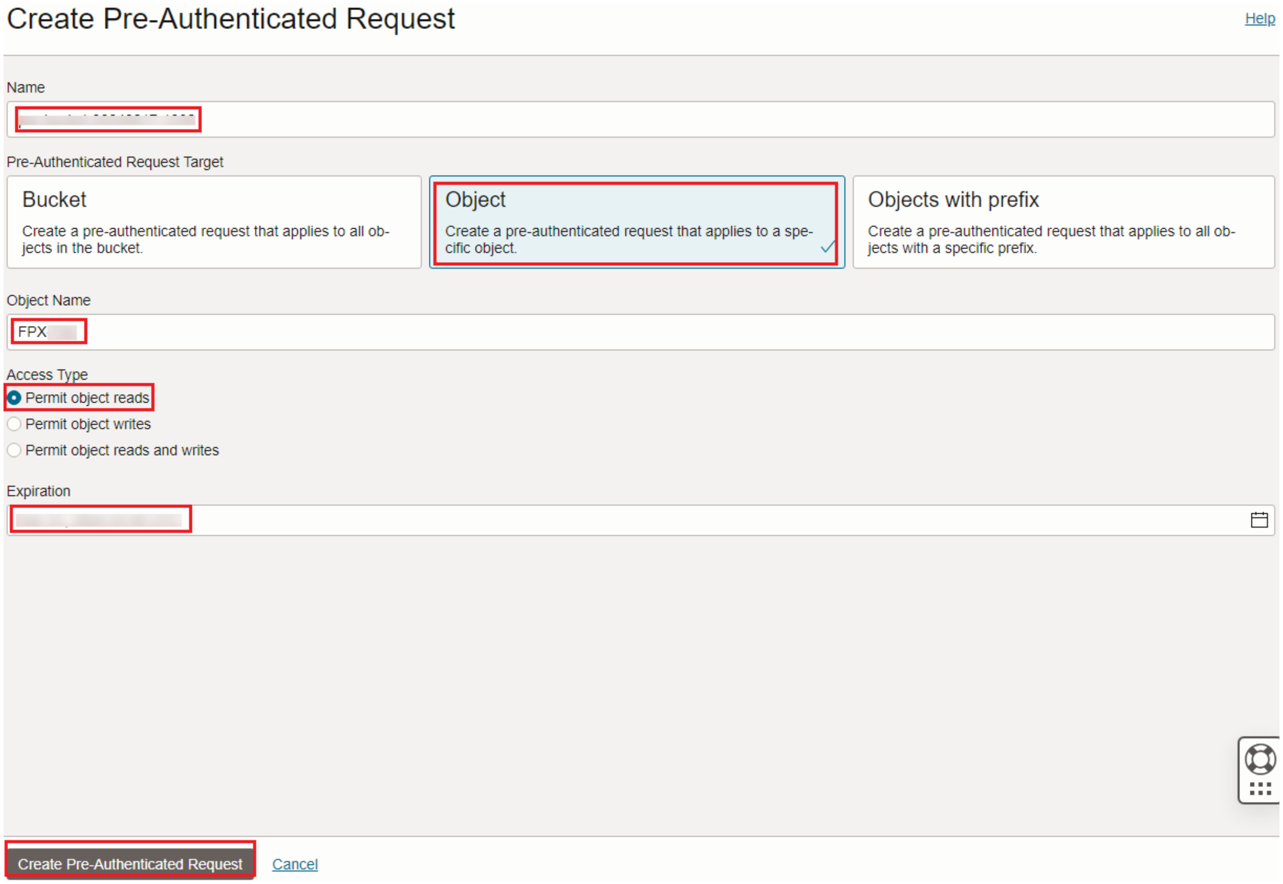
Emit Object Events: Disabled Edit

Object Versioning: Disabled Edit

Pre-Authenticated Requests

Name	Status	Target	Object Name/Prefix	Access Type	Expiration

9. Configure the following options and click *Create Pre-Authenticated Requests*:



Create Pre-Authenticated Request

Name

[redacted]

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

FPX[redacted]

Access Type

● Permit object reads

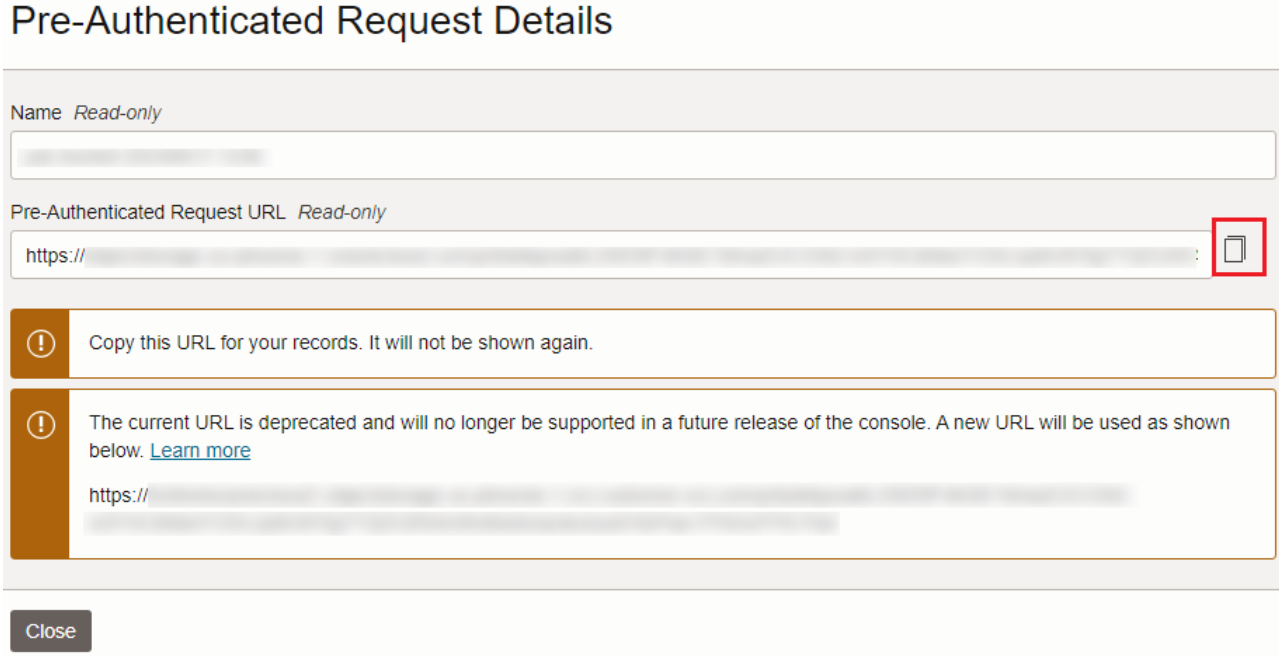
○ Permit object writes

○ Permit object reads and writes

Expiration

[redacted]

10. Copy this URL and save it somewhere for usage in later steps. Click *Close*.



Pre-Authenticated Request Details

Name *Read-only*

[redacted]

Pre-Authenticated Request URL *Read-only*

https://[redacted]

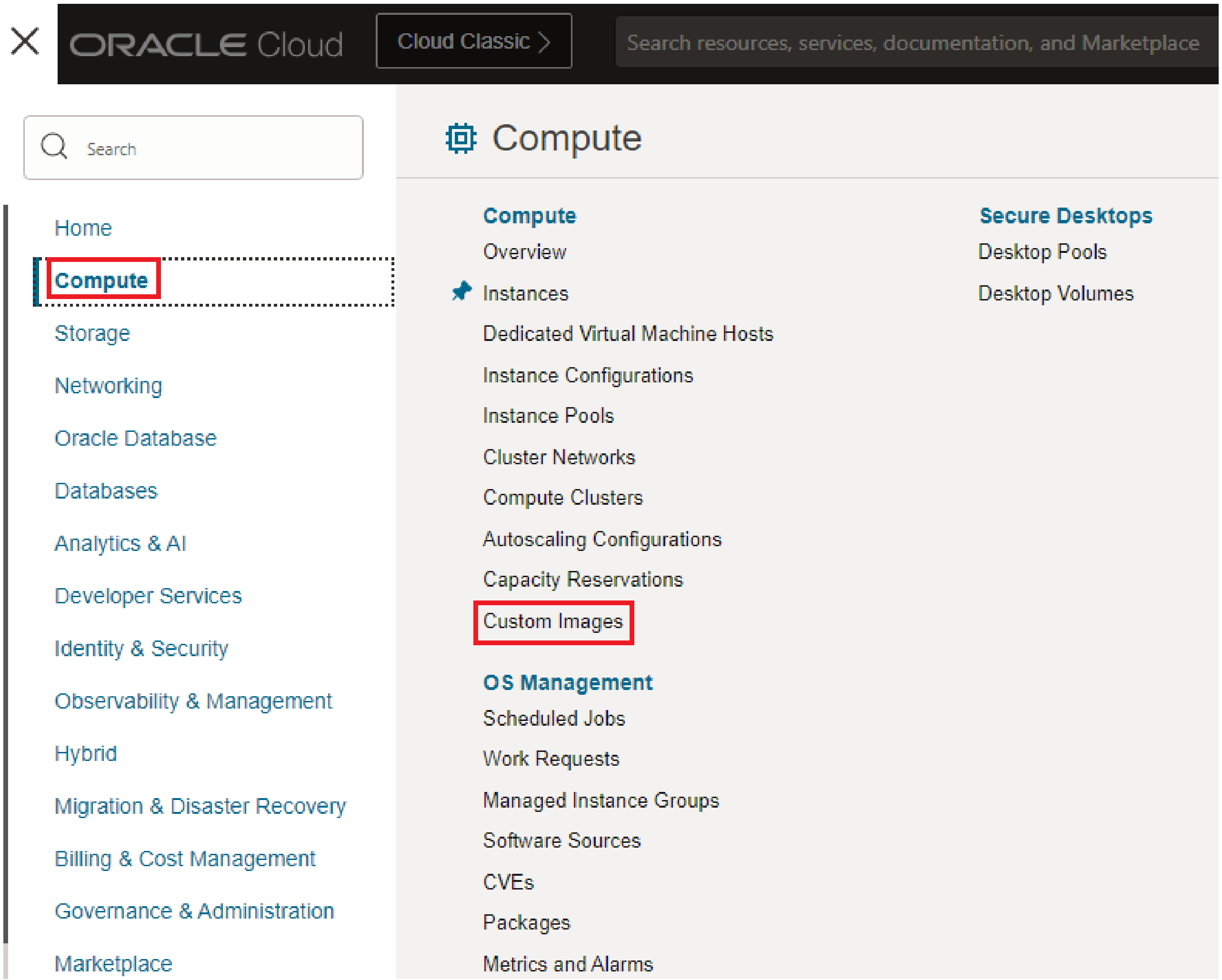
Copy this URL for your records. It will not be shown again.

The current URL is deprecated and will no longer be supported in a future release of the console. A new URL will be used as shown below. Learn more

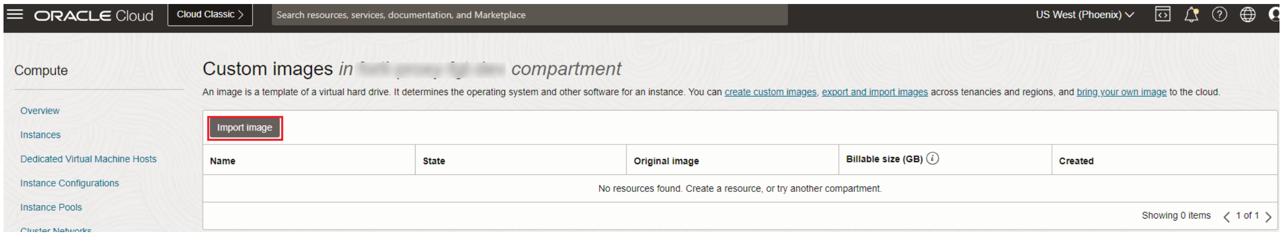
https://[redacted]

To import the image:

1. Go to *Compute* > *Custom Images*.



2. Click *Import Image*.



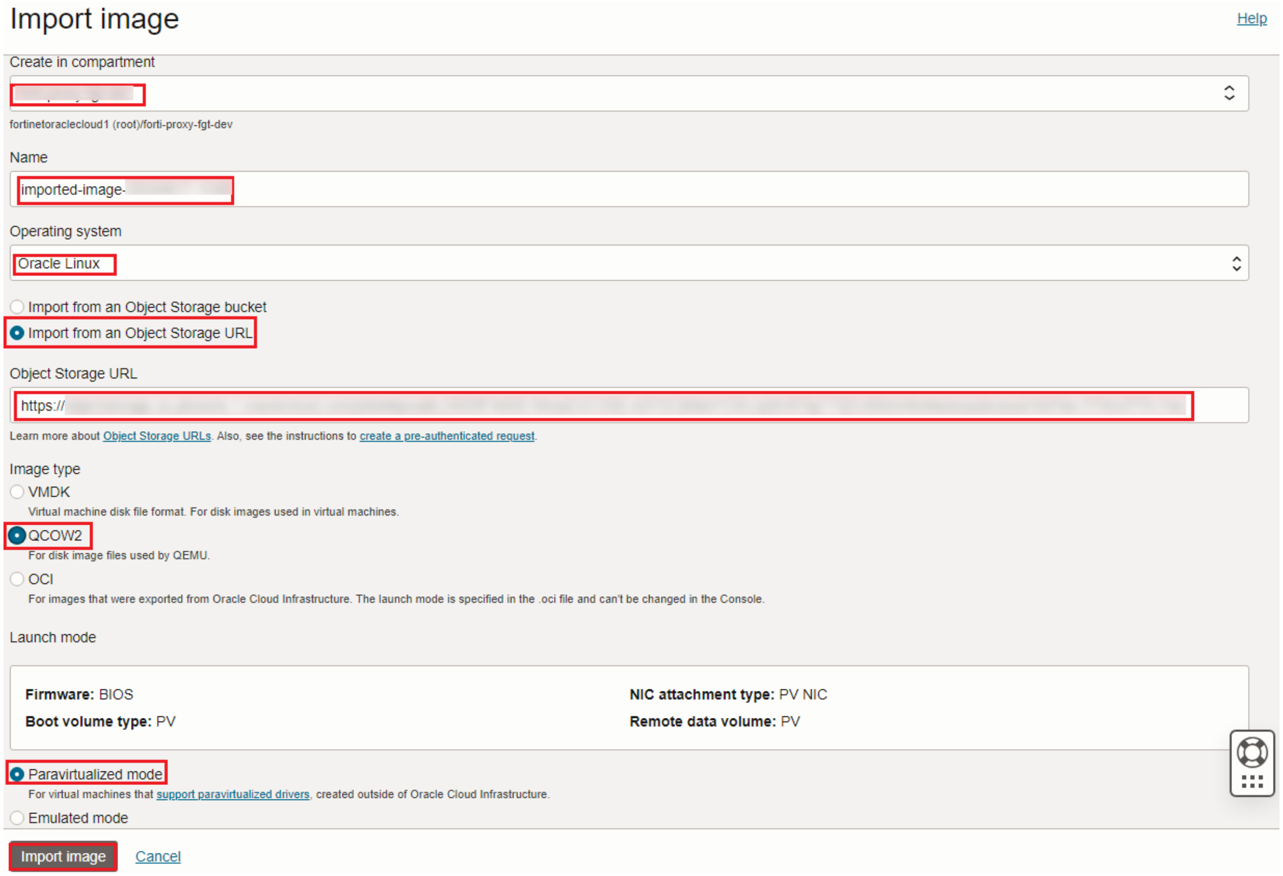
Custom images *in* [redacted] *compartment*

An image is a template of a virtual hard drive. It determines the operating system and other software for an instance. You can create custom images, export and import images across tenancies and regions, and bring your own image to the cloud.

Name	State	Original image	Billable size (GB)	Created
No resources found. Create a resource, or try another compartment.				

Showing 0 items < 1 of 1 >

3. Configure the following options and click *Import image*. In the *Object Storage URL* field, enter the URL link obtained earlier and place it in your bucket.



Import image

Help

Create in compartment

[redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Name

imported-image-[redacted]

Operating system

Oracle Linux

○ Import from an Object Storage bucket

● Import from an Object Storage URL

Object Storage URL

https://[redacted]

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

Boot volume type: PV

NIC attachment type: PV NIC

Remote data volume: PV

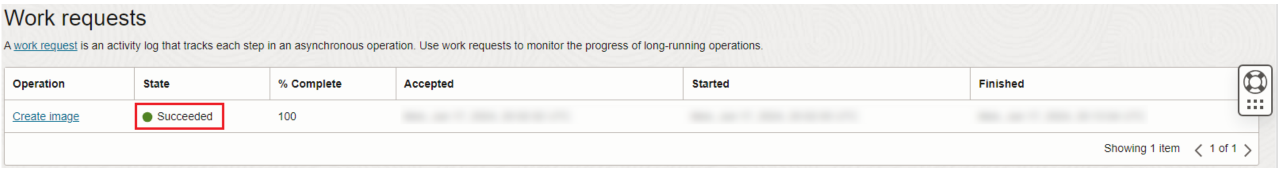
● Paravirtualized mode

For virtual machines that support paravirtualized drivers, created outside of Oracle Cloud Infrastructure.

○ Emulated mode

Import image Cancel

4. Wait until the state of the *Create image* operation changes to *Succeeded*.



Work requests

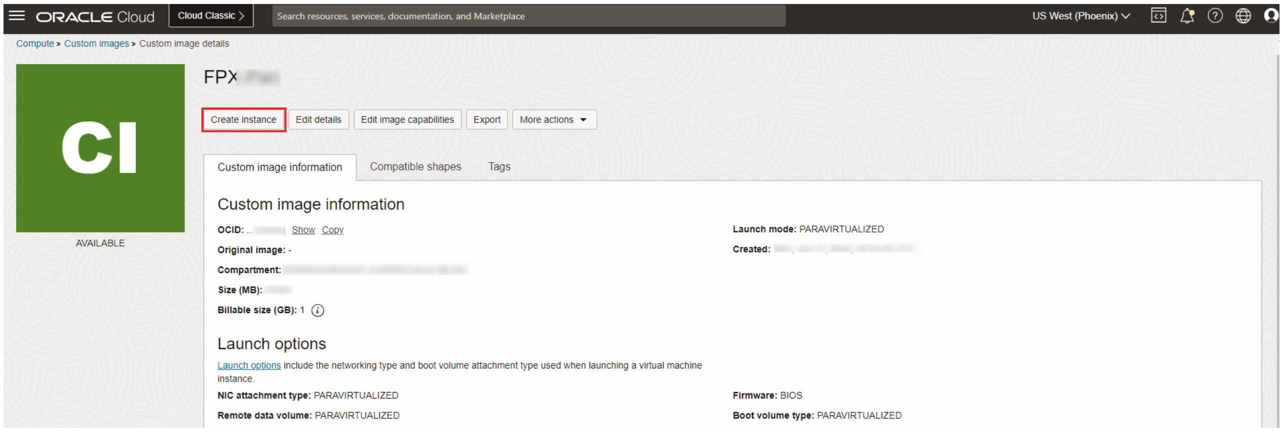
A work request is an activity log that tracks each step in an asynchronous operation. Use work requests to monitor the progress of long-running operations.

Operation	State	% Complete	Accepted	Started	Finished
Create image	● Succeeded	100	[redacted]	[redacted]	[redacted]

Showing 1 item ‹ 1 of 1 ›

To create the two FortiProxy-VM instances:

1. From the newly imported image, click *Create Instance*.



Compute » Custom images » Custom image details

FPX[redacted]

Create instance | Edit details | Edit image capabilities | Export | More actions

Custom image information | Compatible shapes | Tags

Custom image information

OCID: ...[redacted] Show Copy

Original image: -

Compartment: [redacted]

Size (MB): [redacted]

Billable size (GB): 1

Launch mode: PARAVIRTUALIZED

Created: [redacted]

Launch options

Launch options include the networking type and boot volume attachment type used when launching a virtual machine instance.

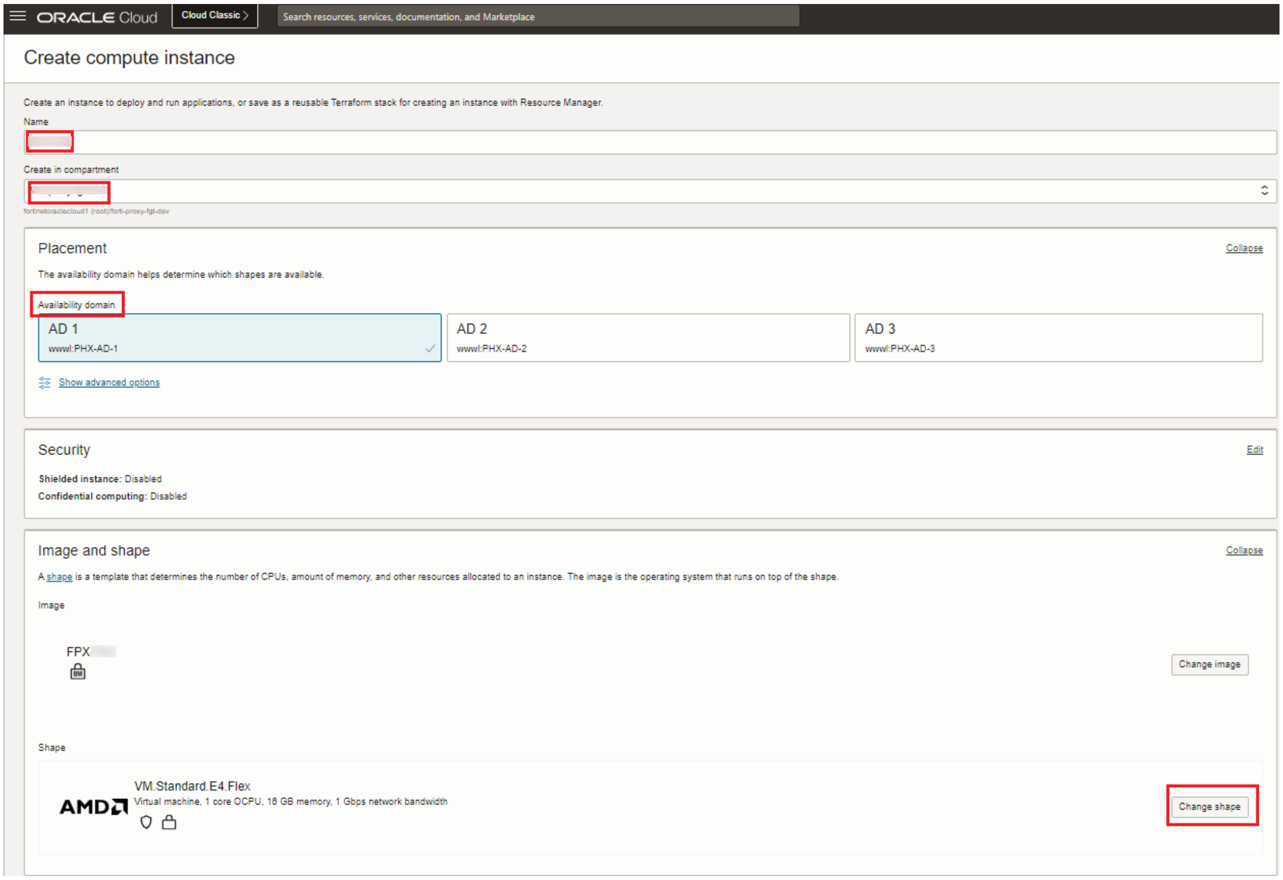
NIC attachment type: PARAVIRTUALIZED

Remote data volume: PARAVIRTUALIZED

Firmware: BIOS

Boot volume type: PARAVIRTUALIZED

2. Configure the parameters for the FortiProxy-VM instance:



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

Create in compartment

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Placement

The availability domain helps determine which shapes are available.

Availability domain

AD 1 wwwl:PHX-AD-1 ✓ | AD 2 wwwl:PHX-AD-2 | AD 3 wwwl:PHX-AD-3

Security

Shielded instance: Disabled
Confidential computing: Disabled

Image and shape

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

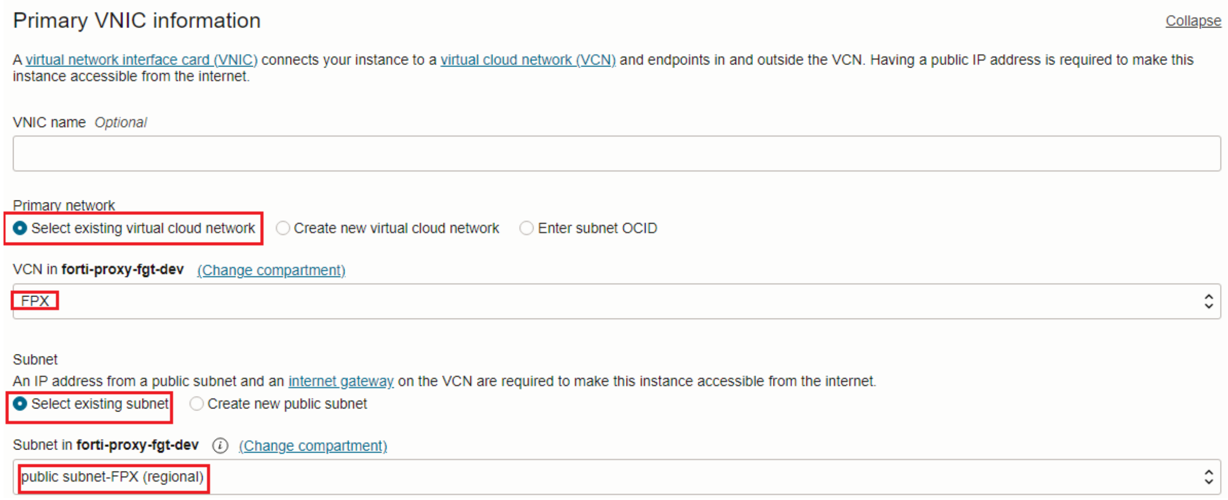
FPX

Shape

VM.Standard.E4.Flex
Virtual machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth

a. In the *Name* field, enter the desired name to identify the instance. For example, FortiProxy A.
b. Under *Create in compartment*, select the compartment for the instance.
c. Under *Availability domain*, select the desired domain.
d. Under *Image and shape*, click *Change shape*.
e. Under *Instance type*, select *Virtual Machine*.
f. Select a shape that can accommodate four network interfaces.
g. Configure other shaping options as needed and click *Select shape*.

h. In the *Primary VNIC information* section, specify the VNIC name and select a network to launch the instance.



Primary VNIC information

A virtual network interface card (VNIC) connects your instance to a virtual cloud network (VCN) and endpoints in and outside the VCN. Having a public IP address is required to make this instance accessible from the internet.

VNIC name *Optional*

Primary network

● Select existing virtual cloud network ○ Create new virtual cloud network ○ Enter subnet OCID

VCN in **forti-proxy-fgt-dev** (Change compartment)

FPX

Subnet

An IP address from a public subnet and an internet gateway on the VCN are required to make this instance accessible from the internet.

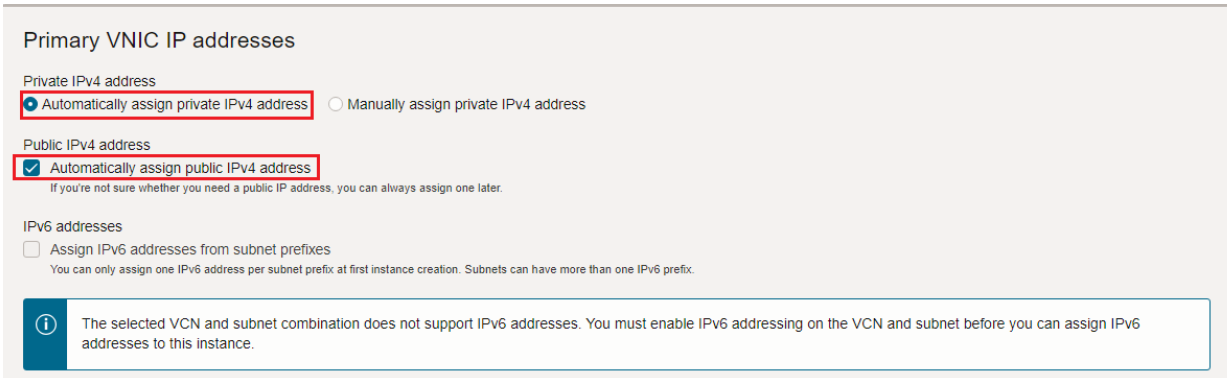
● Select existing subnet ○ Create new public subnet

Subnet in **forti-proxy-fgt-dev** (Change compartment)

public subnet-FPX (regional)

i. In the *Subnet* field, select a subnet on the Internet-facing side of the network.

j. In the *Primary VNIC IP addresses* section, configure the following.
Ensure *Automatically assign public IPv4 address* is selected so you can access the FortiProxy-VM over the Internet. You can disable this once you have configured everything as desired.



Primary VNIC IP addresses

Private IPv4 address

● Automatically assign private IPv4 address ○ Manually assign private IPv4 address

Public IPv4 address

☑ Automatically assign public IPv4 address

If you're not sure whether you need a public IP address, you can always assign one later.

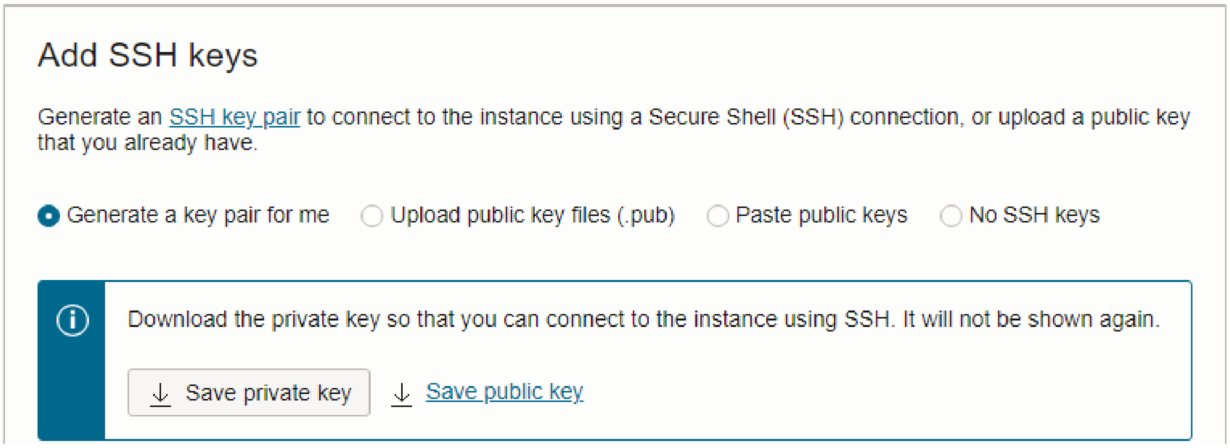
IPv6 addresses

□ Assign IPv6 addresses from subnet prefixes

You can only assign one IPv6 address per subnet prefix at first instance creation. Subnets can have more than one IPv6 prefix.

The selected VCN and subnet combination does not support IPv6 addresses. You must enable IPv6 addressing on the VCN and subnet before you can assign IPv6 addresses to this instance.

k. In the *Add SSH key* section, generate an SSH key pair or upload a public key that you already have to connect to the instance using a Secure Shell (SSH) connection.



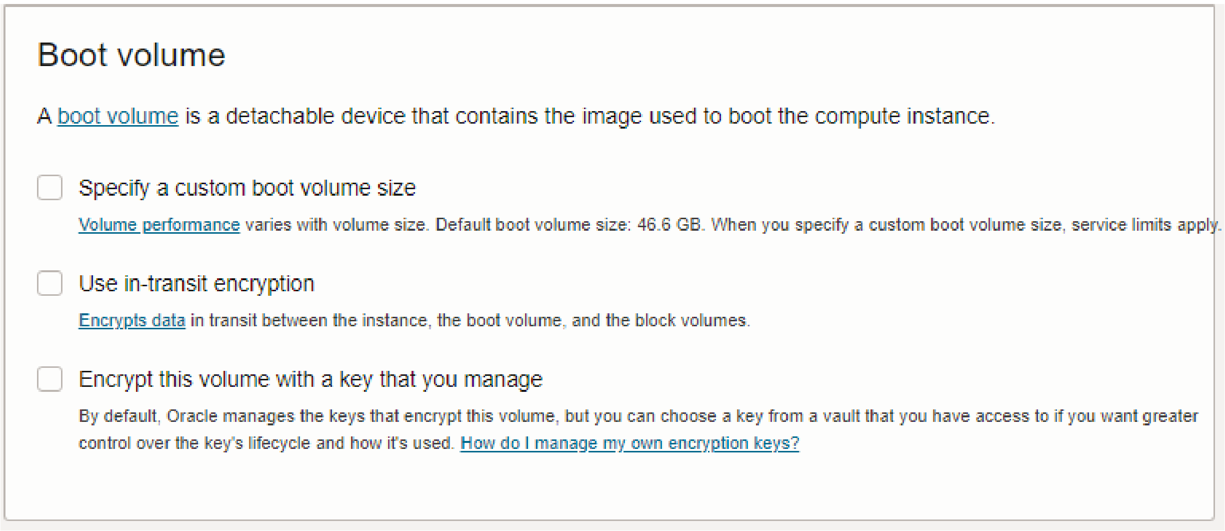
Add SSH keys

Generate an SSH key pair to connect to the instance using a Secure Shell (SSH) connection, or upload a public key that you already have.

● Generate a key pair for me ○ Upload public key files (.pub) ○ 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.

l. In the *Boot volume* section, select an option and configure as needed.



Boot volume

A boot volume is a detachable device that contains the image used to boot the compute instance.

☐ Specify a custom boot volume size

Volume performance varies with volume size. Default boot volume size: 46.6 GB. When you specify a custom boot volume size, service limits apply.

☐ Use in-transit encryption

Encrypts data in transit between the instance, the boot volume, and the block volumes.

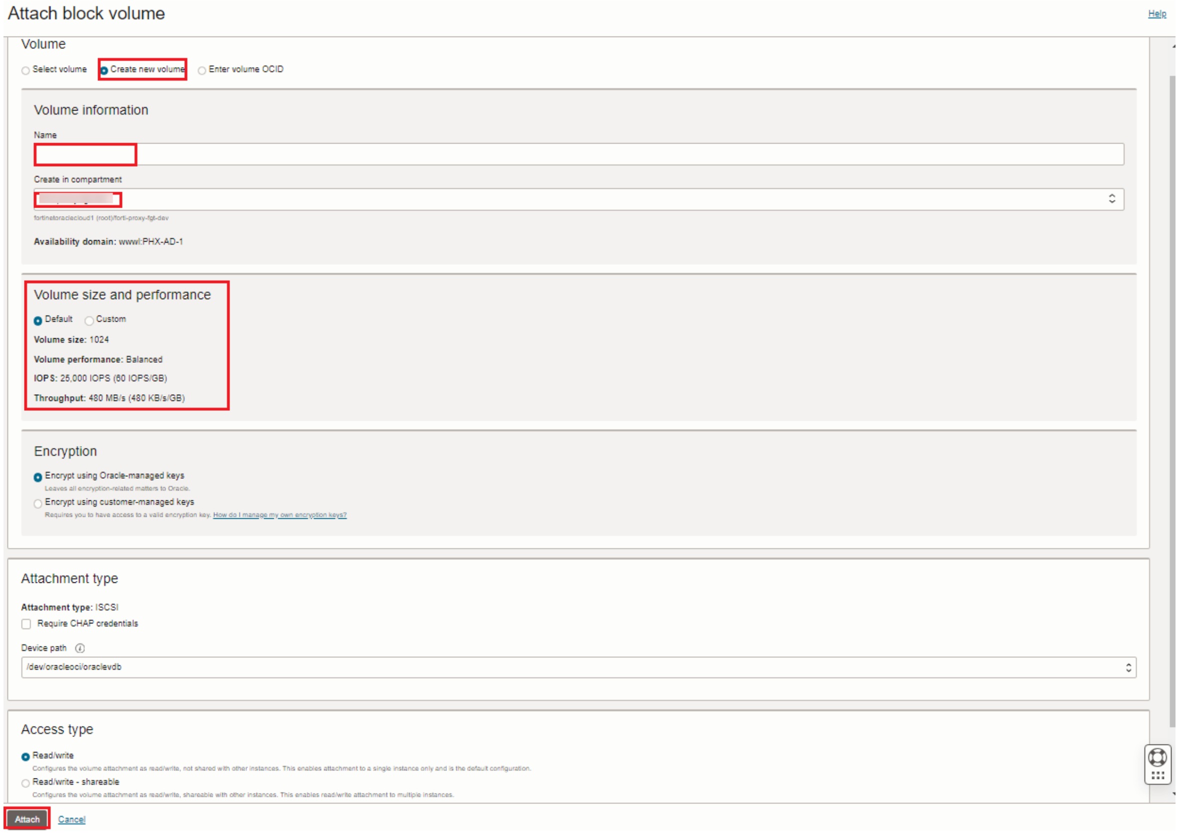
☐ Encrypt this volume with a key that you manage

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. How do I manage my own encryption keys?

m. In the *Block volumes* section, add a volume for storing log and web cache data.

i. Click *Attach block volume*.

ii. Select an existing block volume or create a new one. The size should be around 50 GB.



Attach block volume

Volume

○ Select volume ● Create new volume ○ Enter volume OCID

Volume information

Name

Create in compartment

[redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Availability domain: wwwl:PHX-AD-1

Volume size and performance

● Default ○ Custom

Volume size: 1024

Volume performance: Balanced

IOPS: 25,000 IOPS (60 IOPS/GB)

Throughput: 480 MB/s (480 KB/s/GB)

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 encryption key. How do I manage my own encryption keys?

Attachment type

Attachment type: ISCSI

☐ Require CHAP credentials

Device path

/dev/oracleoci/oraclevdb

Access type

● 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.

iii. Click *Attach*.

n. **(Optional)** Add bootstrapping of FortiProxy CLI commands and a BYOL license at the time of initial bootup as part of instance creation:

i. At the bottom of the page, click *Show Advanced Options*.

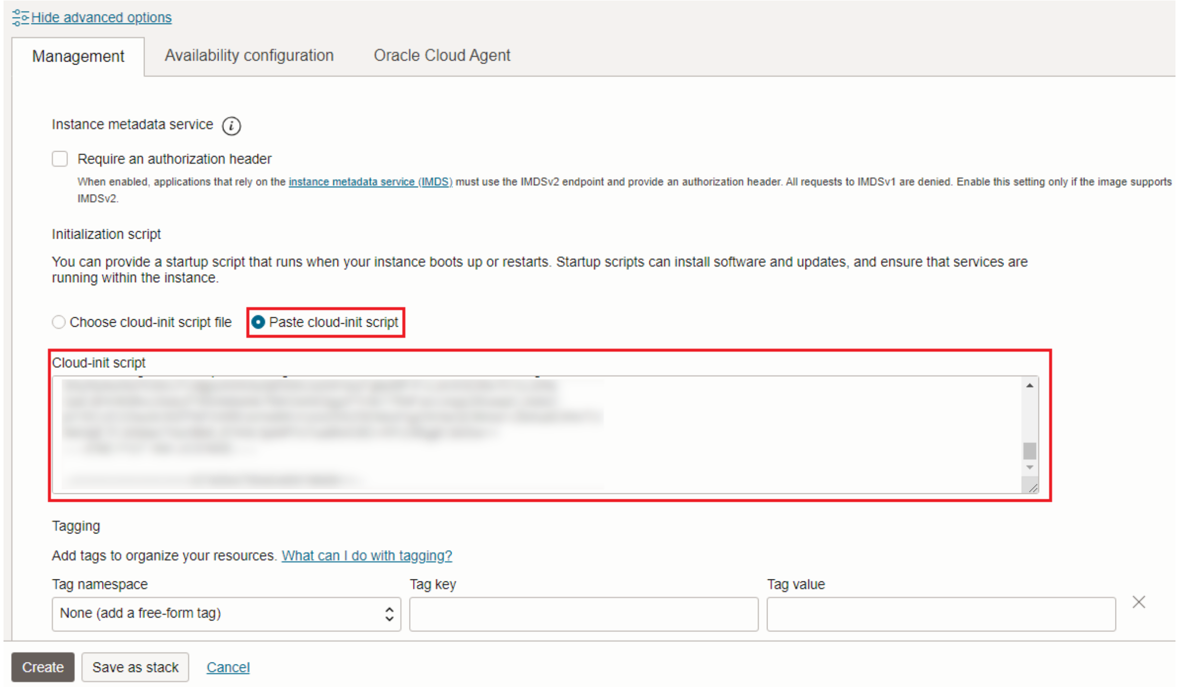
ii. On the *Management* tab, select *Paste cloud-ini script*.

iii. Customize the following sample code (in MIME format) according to your needs.

- Replace the `config system global` commands with your own set of CLI commands as needed. The timezone is set to GMT-9 Alaska in the sample code.
- Replace the license string with the license file content that you download from Customer Service & Support after registering your product code.

```
Content-Type: multipart/mixed; boundary="===============0740947994048919689=="
MIME-Version: 1.0

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"

config system global
 set timezone 03
end

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"

-----BEGIN FPX VM LICENSE-----
Replace with your own license file
-----END FPX VM LICENSE-----
```

iv. In the *Cloud-init script* field, enter your custom version of the sample code (including the CLI commands and your license) from the previous step.



Hide advanced options

Management | Availability configuration | Oracle Cloud Agent

Instance metadata service

□ Require an authorization header

When enabled, applications that rely on the instance metadata service (IMDS) must use the IMDSv2 endpoint and provide an authorization header. All requests to IMDSv1 are denied. Enable this setting only if the image supports IMDSv2.

Initialization script

You can provide a startup script that runs when your instance boots up or restarts. Startup scripts can install software and updates, and ensure that services are running within the instance.

○ Choose cloud-init script file ● Paste cloud-init script

Cloud-init script

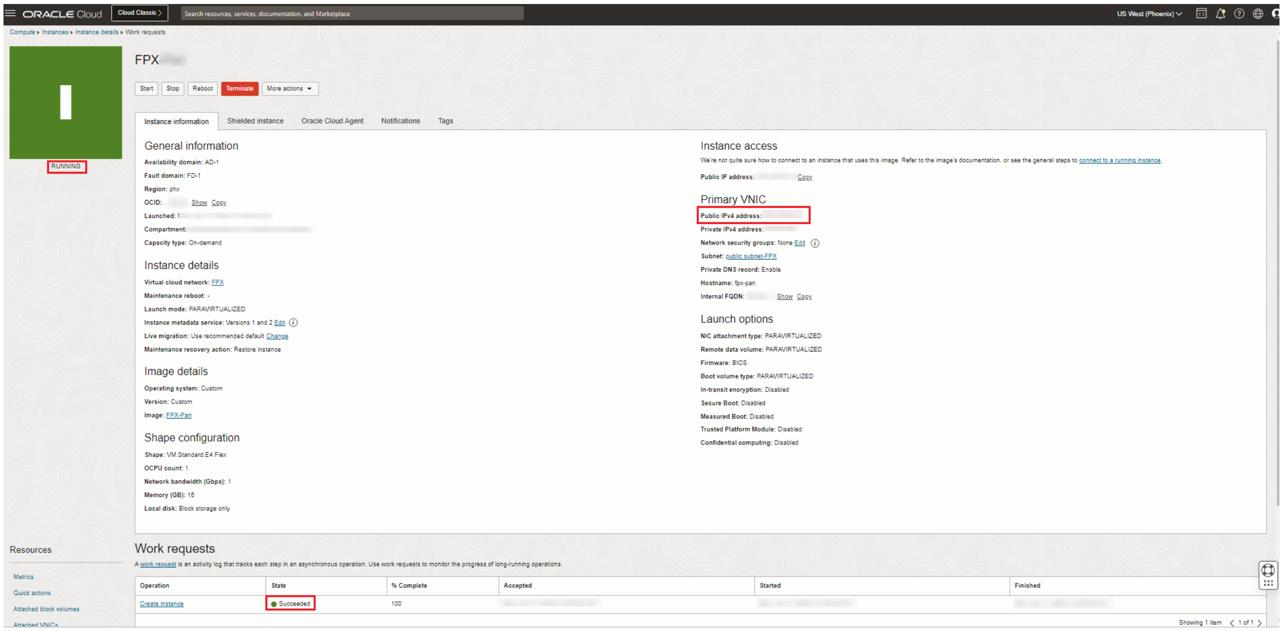
[redacted]

Tagging

Add tags to organize your resources. What can I do with tagging?

Tag namespace	Tag key	Tag value
None (add a free-form tag)		

3. Click *Create*. Wait until the *PROVISIONING…* status changes to *RUNNING* and verify that the *Create instance* operation status changes to *Succeeded*.
   You can also check the FortiProxy's public IP address in this screen once it becomes available.



FPX[redacted]

RUNNING

General information

Availability domain: AD-1
Fault domain: FD-1
Region: phx
OCID: ...[redacted] Show Copy
Launched: [redacted]
Compartment: [redacted]
Capacity type: On-demand

Instance details

Virtual cloud network: FPX
Maintenance reboot: -
Launch mode: PARAVIRTUALIZED
Instance metadata service: Versions 1 and 2 Edit
Live migration: Use recommended default Change
Maintenance recovery action: Restore instance

Image details

Operating system: Custom
Version: Custom
Image: FPX-Pan

Shape configuration

Shape: VM.Standard.E4.Flex
OCPU count: 1
Network bandwidth (Gbps): 1
Memory (GB): 16
Local disk: Block storage only

Instance access

We're not quite sure how to connect to an instance that uses this image. Refer to the image's documentation, or see the general steps to connect to a running instance.

Public IP address: [redacted] Copy

Primary VNIC

Public IPv4 address: [redacted]
Private IPv4 address: [redacted]
Network security groups: None Edit
Subnet: public subnet-FPX
Private DNS record: Enable
Hostname: fpx-pan
Internal FQDN: [redacted] Show Copy

Launch options

NIC attachment type: PARAVIRTUALIZED
Remote data volume: PARAVIRTUALIZED
Firmware: BIOS
Boot volume type: PARAVIRTUALIZED
In-transit encryption: Disabled
Secure Boot: Disabled
Measured Boot: Disabled
Trusted Platform Module: Disabled
Confidential computing: Disabled

Work requests

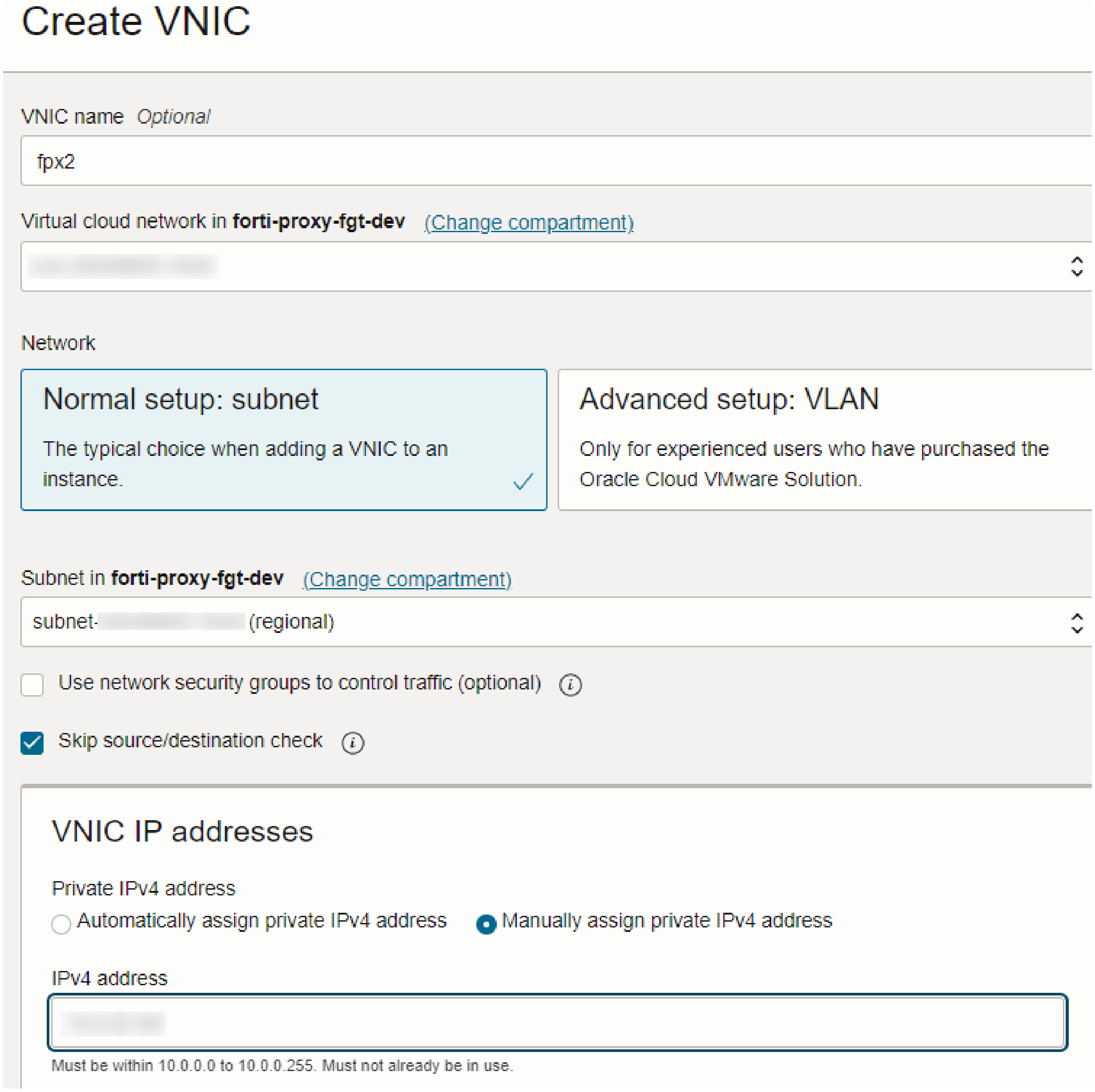
A work request is an activity log that tracks each step in an asynchronous operation. Use work requests to monitor the progress of long-running operations.

Operation	State	% Complete	Accepted	Started	Finished
Create instance	● Succeeded	100	[redacted]	[redacted]	[redacted]

Showing 1 item 1 of 1

Refer to Accessing the FortiProxy-VM on page 24 for details about how to access the FortiProxy-VM instance.

4. Configure three extra VNICs for the FortiProxy-VM instance by repeating the following steps for each VNIC:
   a. In the FortiProxy-VM instance details page, click *Attached VNICs > Create VNIC*.
   b. Create the virtual network interface by specifying the name, VNC, and the subnet created earlier.



Create VNIC

VNIC name *Optional*

fpx2

Virtual cloud network in **forti-proxy-fgt-dev** (Change compartment)

[redacted]

Network

Normal setup: subnet

The typical choice when adding a VNIC to an instance. ✓

Advanced setup: VLAN

Only for experienced users who have purchased the Oracle Cloud VMware Solution.

Subnet in **forti-proxy-fgt-dev** (Change compartment)

subnet-[redacted] (regional)

□ Use network security groups to control traffic (optional)

☑ Skip source/destination check

VNIC IP addresses

Private IPv4 address

○ Automatically assign private IPv4 address ● Manually assign private IPv4 address

IPv4 address

[redacted]

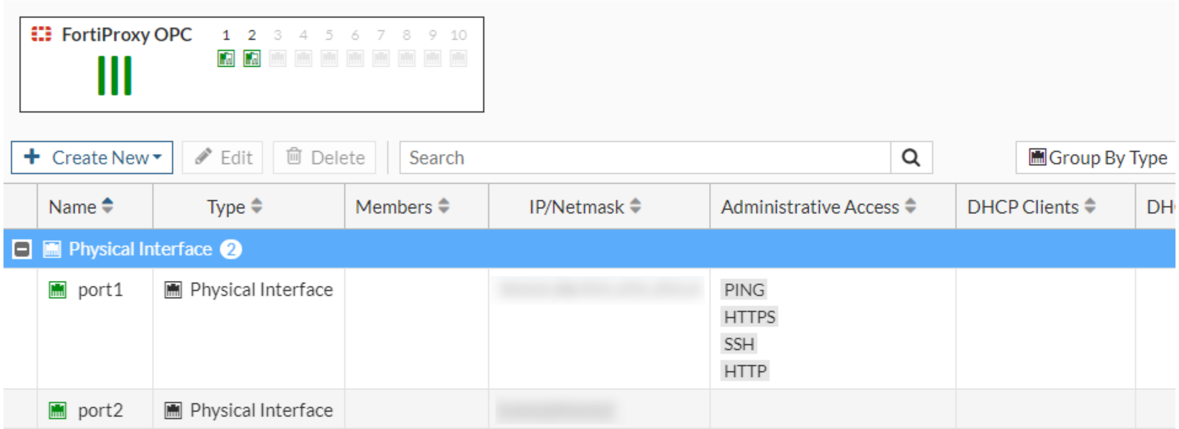
Must be within 10.0.0.0 to 10.0.0.255. Must not already be in use.

c. Select *Skip Source/Destination Check*. Enter an IP address, and click *Save changes*.
The network interface is attached to the FortiProxy-VM.

d. Configure the VNIC in FortiProxy:

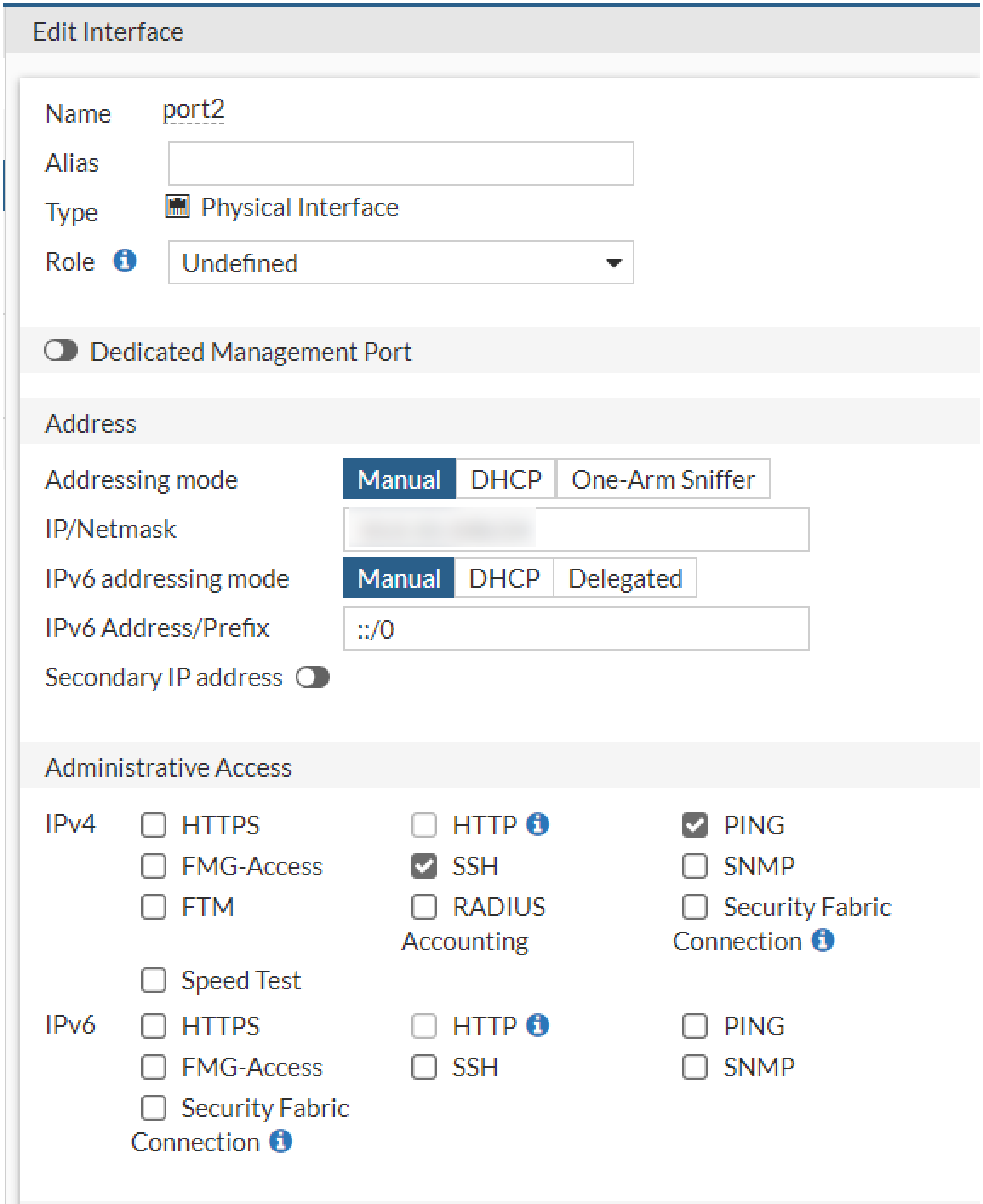
i. Reboot the FortiProxy-VM instance and then log into the GUI console.

ii. In *Network* > *Interfaces*, select the corresponding port (such as port2) and then click *Edit*.



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DH
Physical Interface 2						
port1	Physical Interface		[redacted]	PING HTTPS SSH HTTP		
port2	Physical Interface		[redacted]			

iii. Specify the IP address and netmask as defined in OCIfor the port. Allow administrative access to PING, SSH, and so on as desired. Click *OK*.



Edit Interface

Name port2

Alias

Type Physical Interface

Role Undefined

○ Dedicated Management Port

Address

Addressing mode [✓ Manual] DHCP One-Arm Sniffer

IP/Netmask [redacted]

IPv6 addressing mode [✓ Manual] DHCP Delegated

IPv6 Address/Prefix ::/0

Secondary IP address ○

Administrative Access

IPv4 □ HTTPS □ HTTP ☑ PING □ FMG-Access ☑ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection □ Speed Test

IPv6 □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ Security Fabric Connection

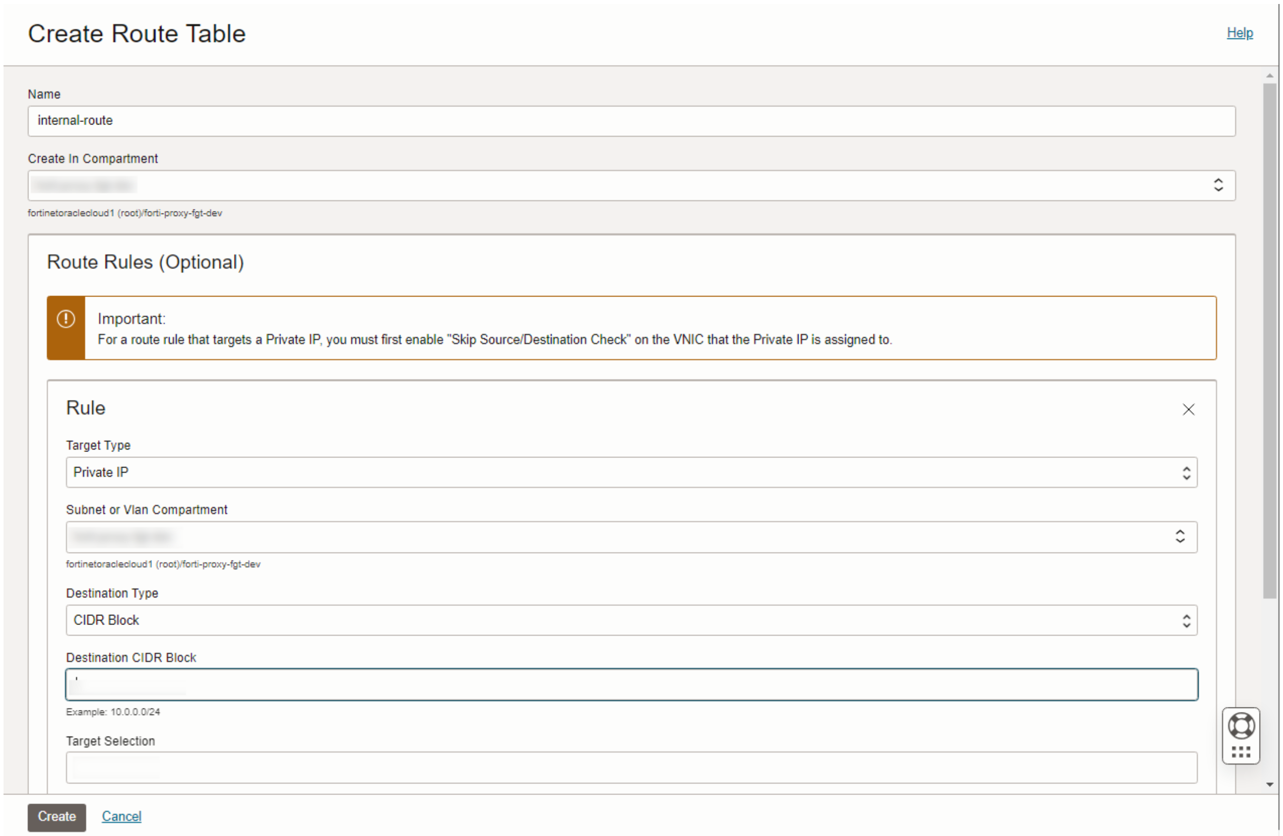
e. Repeat the steps above to create the remaining two interfaces for the FortiProxy-VM instance.

5. Repeat the previous steps to create another FortiProxy-VM instance with four VNICs.

Configuring a route table for the private subnet

Fortinet recommends that you create a separate route table for the private subnet to point to the private IP address on the active FortiProxy.

1. Go to *Networking* > *Virtual Cloud Networks* and open the VCN you created earlier for this deployment.
2. In the *Route Tables* tab, click *Create Route Table*.
3. Specify the route table to point to the private IP address on the active FortiProxy:



Create Route Table

Name: internal-route

Create In Compartment: [redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Route Rules (Optional)

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.

Rule

Target Type: Private IP

Subnet or Vlan Compartment: [redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Destination Type: CIDR Block

Destination CIDR Block: [redacted]

Example: 10.0.0.0/24

Target Selection: [redacted]

4. In the *Subnets* tab, click the private subnet and click *Edit*.
5. Under *Route Table*, select the route table you just created.

Configuring the OCI HA interfaces

OCI recommends leaving VM NIC interfaces set to DHCP to avoid potential misaligned configurations. However, when configuring an NVA, you need to ignore this recommendation and ensure that the IP addresses correspond with those intended so that the configurations match as required.

In the case of HA, OCI API calls enable the failover through the OCI Fabric connector only for IP addresses configured as secondary in the OCI VNIC. You must configure the FortiProxy-VMs with the correct static IP addresses for proper failover between the two instances. Moreover, API calls initiated from within a VCN must be made by a primary interface with a public address with DNS properly configured.

Fortinet recommends that you perform interface IP address and route configuration via the console as you may lose connection to the instance during the process.

Primary FortiProxy

port1

The primary VNIC associated with the FortiProxy NVA must have a primary IP address with a corresponding public IP address, and so needs to be configured in a public subnet. This is used as a management interface and also the interface from which API calls are made. You assign this in the HA configuration. Make sure the FortiProxy-VM port 1 configuration matches the interface's OCI configuration.

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.0.2.1 255.255.255.0
      set allowaccess ping https ssh http fgfm
      set description "management"
      set mtu-override enable
      set mtu 9000
   next
end
```

port2

This example uses port2 as the public/WAN-facing interface. You must use the non-primary private IP address instead of the primary IP address for its interface IP address because the primary IP address is not relocatable to the secondary FortiProxy in the event of HA failover. In this example, the FortiProxy uses a single secondary IP address with an associated public IP address. In the case of a failover, the secondary IP address and associated public IP address are migrated from the active to the passive FortiProxy. Therefore, if the setup uses any extra non-primary private IP addresses in the setup, you must explicitly reference these IP addresses in the interface configuration by enabling secondary IP addresses.

```
config system interface
   edit "port2"
   set vdom "root"
      set ip 10.0.0.3 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "untrust"
      set secondary-IP enable
      set mtu-override enable
      set mtu 9000
      config secondaryip
         edit 1
            set ip 10.0.12.5 255.255.255.0
            set allowaccess ping https ssh fgfm
         next
      end
   next
end
```

port3

This example configures port3 as the private port, which the configuration uses to connect to internal resources on local subnets, peered VCNs, and so on. However, as aforementioned, FortiProxy does not use the primary IP address. You must still attach the VNIC to the instance with the primary IP address. However, the configuration is synced from the primary FortiProxy.

```
config system interface
   edit "port3"
      set vdom "root"
      set ip 10.0.1.3 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "trusted"
      set mtu-override enable
      set mtu 9000
   next
end
```

Enabling *Skip Source/Destination Check* for the VNIC is recommended.

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.

```
config system interface
   edit "port4"
      set vdom "root"
      set ip 10.0.3.3 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "heartbeat"
      set mtu-override enable
      set mtu 9000
   next
end
```

Additional configuration

For any unconnected subnets or networks, the FortiProxy needs a route assigned to know how to get to them. Typically, you connect these via the private designated interface. In this case, this is port3. Therefore, a route with a next hop or gateway of the first IP address of the subnet to which port3 belongs is necessary. This can be a specific host route or summary route of some sort.

See the following, where a summary route is configured for 10.0.0.0/16. If this route is not added, the FortiProxy communicates with any unconnected routes through the default (0.0.0.0/0) route, which typically should be out the WAN interface (port2 in this example). Since all interfaces are being configured statically and you are not configuring a default route through DHCP, you must also add this default route. If you do not set a destination, FortiProxy assumes the default route of 0.0.0.0/0. Therefore, the 2 configuration is the default route.

```
config router static
   edit 2
      set gateway 10.0.12.1
      set device "port2"
   next
   edit 3
```

```
        set dst 10.0.0.0 255.0.0.0
        set gateway 10.0.8.1
        set device "port3"
    next
end
```

Secondary FortiProxy

For the secondary FortiProxy, you do not need to configure port2 or port3 as these configurations should sync from the primary FortiProxy.

port1

The primary VNIC associated with the FortiProxy NVA must have a primary IP address with a corresponding public IP address, and so must be configured in a public subnet. This is used as a management interface and also the interface from which API calls are made. You assign this in the HA configuration. Make sure the FortiProxy-VM port 1 configuration matches the interface's OCI configuration.

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.0.2.4 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set description "management"
        set mtu-override enable
        set mtu 9000
    next
end
```

port2

You must attach the VNIC to the instance with the primary IP address. However, the FortiProxy syncs the configuration from the primary unit.

port3

You must attach the VNIC to the instance with the primary IP address. However, the FortiProxy syncs the configuration from the primary unit.

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.

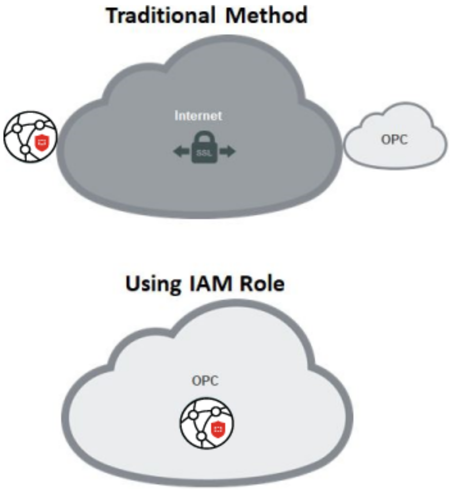
```
config system interface
    edit "port4"
        set vdom "root"
        set ip 10.0.3.4 255.255.255.0
        set allowaccess ping https ssh fgfm
        set description "heartbeat"
    next
end
```

Configuring an OCI SND connector

To allow calling APIs to OCI during HA failover, you must configure an OCI SDN connector with HA enabled. The OCI SDN connector can be certificate-based or IAM role-based based on the authentication type:

- A certificate-based OCI SDN connector uses traditional certificate authentication from the FortiProxy-VM to OCI over TCP/IP.
- An IAM-role based OCI SDN connector uses IAM roles to control the permissions to grant to the FortiProxy instance so that the instance can implicitly access metadata information and communicate to the SDN connector on its own private internal network without further authentication.

The following topology compares the two authentication types of the OCI SDN connector:



Creating an OCI SDN connector using certificates

Use the `config system sdn-connector` command to configure a certificate-based OCI SDN connector in FortiProxy. Make sure HA is enabled.

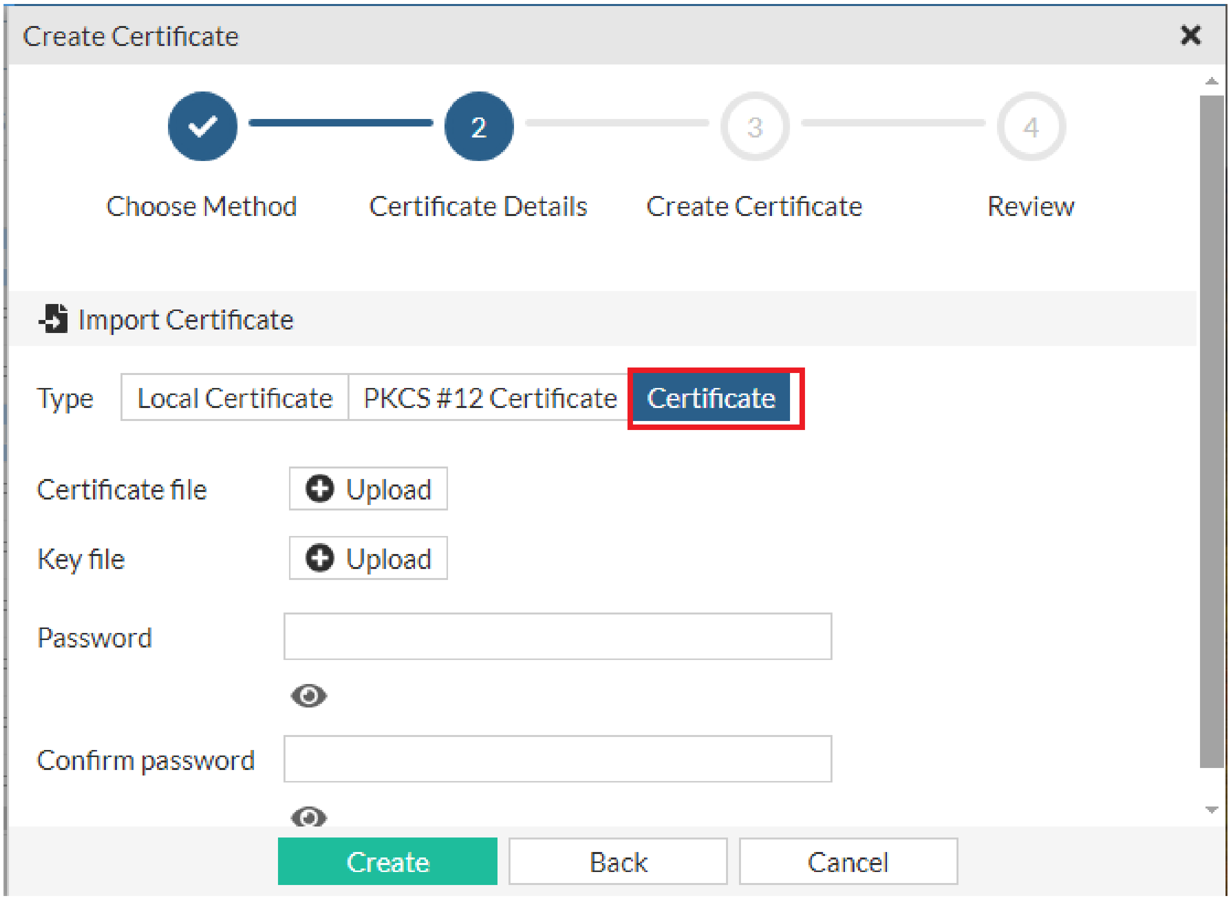
- For `user-id`, specify the OCID of an OCI user that belongs to the administrator group with the following minimum privileges:
    - Allow dynamic-group <group_name> to read compartments in tenancy
    - Allow dynamic-group <group_name> to read instances in tenancy
    - Allow dynamic-group <group_name> to read vnic-attachments in tenancy
    - Allow dynamic-group <group_name> to read private-ips in tenancy
    - Allow dynamic-group <group_name> to read public-ips in tenancy
    - Allow group <group_name> to manage private-ips in tenancy
    - Allow group <group_name> to manage public-ips in tenancy
    - Allow group <group_name> to manage vnics in tenancy

- For `oci-cert`, you can specify the built-in FortiProxy certificate called "Fortinet_Factory" or a custom certificate. To use a custom certificate, you need a certificate file and key file for use on the FortiProxy and a PEM file for use on OCI. The signing algorithm must be RSA SHA-256. For details about the certificates that OCI requires, see Request Signatures.

You may want to switch from the default certificate to a custom one after some time, or if you have multiple sets of A-P HA clusters, you may want to use a different certificate for each cluster initially.

To configure the OCI SND connector to use a custom certificate:

a. Import the certificate to the primary FortiProxy (see Import a local certificate and image below). The secondary FortiProxy will then synchronize the configuration and use the same certificate.



b. Add an API key for the OCI user using the custom certificate's PEM. See the OCI documentation for detailed instructions.

c. Reference the custom certificate in the `oci-cert` option when configuring the OCI SDN connector.

Creating an OCI SDN connector using IAM roles

To configure an OCI SDN connector using IAM roles, complete the following steps:

1. Configure an IAM role on OCI:
   1. In OCI, go to *Compute* > *Instances*, and select the desired FortiProxy-VM instance.
   2. On the *Instance Details* page, note the instance's OCID.
   3. Open the OPC menu and go to *Identity* > *Dynamic Groups*. Create a dynamic group with rules that allow instances that match the FortiProxy-VM's instance ID. Use the syntax "ALL {instance.id ='instanceID'}" when creating the rule. To include multiple instances in the dynamic group, create multiple rules.
   4. Go to *Identity* > *Policies*. Create a policy that allows the dynamic group to manage the environment. This allows the instance referenced in the dynamic group to query metadata and move resources around if the SDN connector is used for HA. In the *STATEMENT* field, use the syntax "Allow dynamic-group <group-name> to manage all-resources in TENANCY".
2. Configure an IAM role-based OCI SDN connector using the `config system sdn-connector` command in FortiProxy. Make sure HA is enabled.

   For `user-id`, specify the OCID of an OCI user that belongs to the administrator group with the following minimum privileges:

   - Allow dynamic-group <group_name> to read compartments in tenancy
   - Allow dynamic-group <group_name> to read instances in tenancy
   - Allow dynamic-group <group_name> to read vnic-attachments in tenancy
   - Allow dynamic-group <group_name> to read private-ips in tenancy
   - Allow dynamic-group <group_name> to read public-ips in tenancy
   - Allow group <group_name> to manage private-ips in tenancy
   - Allow group <group_name> to manage public-ips in tenancy
   - Allow group <group_name> to manage vnics in tenancy

   Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

   You can also use resource tags to further control the API calls, as follows:

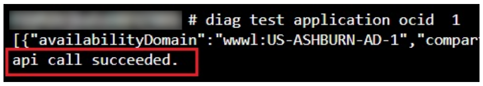
   - Allow dynamic-group <group_name> to manage private-ips in tenancy
   - Allow dynamic-group <group_name> to manage public-ips in tenancy where any { target.resource.tag.<namespace>.<tag key>= 'value'}
   - Allow dynamic-group <group_name> to manage vnics in tenancy where any { target.resource.tag.<namespace>.<tag key>= 'value'}

   - If you have security concerns about the policy allowing the dynamic group access to the entire environment, follow the concept of least privileges detailed in the OPC documentation. For example, if you are not using the SDN connector for failover and instead are using it for querying, you can assign the dynamic group read-only permissions.
   - Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

Troubleshooting SDN connector configuration issues

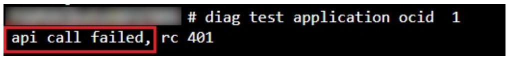
In case of issues with connector configuration, try the following methods to troubleshoot:

- Ensure the SDN connector is connected to OCIby running the `diagnose sys sdn status` command. The output should display that the SDN connector has a connected status.
- Ensure you can successfully call APIs to OCI by running `diagnose test application ocid 1`. The following shows an example of a successful configuration:



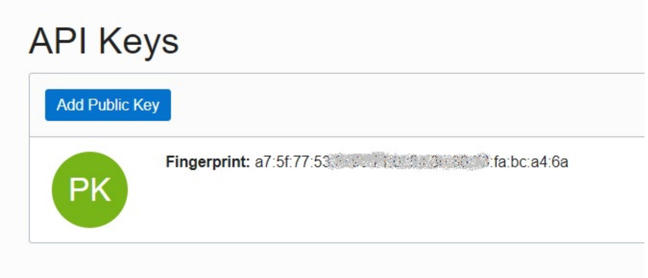
```
[redacted] # diag test application ocid  1
[{"availabilityDomain":"wwwl:US-ASHBURN-AD-1","compar
api call succeeded.
```

The following shows an example of a failed configuration:



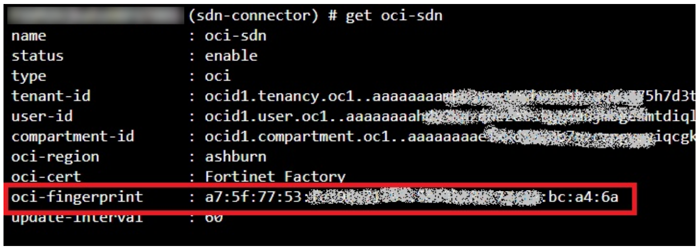
```
[redacted] # diag test application ocid  1
api call failed, rc 401
```

- Check the following to see if you made other unexpected changes:
  - Tenant ID
  - User ID
  - Compartment ID
  - Does the specified OCI user belong to the Administrator group on the OCI portal?
  - Does the fingerprint on the OCI portal match the one that the specified user has on the FortiProxy-VM? If you change the certificate, its corresponding fingerprint must be updated or added to the OCI user on the OCI portal. In the earlier example, the fingerprint on the OCI portal and the SDN connector settings match.



API Keys

Fingerprint: a7:5f:77:53[redacted]:fa:bc:a4:6a



```
[redacted] (sdn-connector) # get oci-sdn
name                : oci-sdn
status              : enable
type                : oci
tenant-id           : ocid1.tenancy.oc1..aaaaaaaa[redacted]5h7d3t
user-id             : ocid1.user.oc1..aaaaaaaah[redacted]mtdiql
compartment-id      : ocid1.compartment.oc1..aaaaaaaae[redacted]iqcgk
oci-region          : ashburn
oci-cert            : Fortinet Factory
oci-fingerprint     : a7:5f:77:53[redacted]:bc:a4:6a
update-interval     : 60
```

  - Does the OCI security list on the Internet-facing subnet allow proper outgoing access from the FortiProxy?

Configuring active-passive HA

This step shows you how to configure A-P HA settings by using CLI commands on the GUI or via SSH.

In the commands, note the following:

- Port4 is the hbdev port used for heartbeat connection.
- For the management interface, you must use port1, as OCI allows only port 1 for metadata access.
- When setting priority on FortiProxy B, set the priority to 100 (lower than FortiProxy A's priority level). The node with the lower priority level is determined as the secondary node.

- When setting the unicast heartbeat peer IP address (the last command), this is the IP address on the peer, which in the example is FortiProxy B, which has port4 IP address 10.0.3.4 in the example. When setting FortiProxy B's configuration, specify FortiProxy A's port4 IP address, which is 10.0.3.3.

The following is the primary FortiProxy configuration:

```
config system ha
   set group-id 30
   set group-name "ha-cluster"
   set mode a-p
   set hbdev "port4" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port1"
         set gateway 10.0.0.1
      next
   end
   set override disable
   set priority 200
   set unicast-hb enable
   set unicast-hb-peerip 10.0.3.4
end
```

Once configuration is complete, exit the CLI or SSH session.

The following is the secondary FortiProxy configuration:

```
config system ha
   set group-id 30
   set group-name "ha-cluster"
   set mode a-p
   set hbdev "port4" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port1"
         set gateway 10.0.0.1
      next
   end
   set override disable
   set priority 100
   set unicast-hb enable
   set unicast-hb-peerip 10.0.3.3
end
```

Deploying FortiProxy-VM active-passive HA on OCI between multiple ADs

When deploying FortiGate-VM active-passive HA on OCI between multiple ADs, the following differs from when deploying within one AD:

- You do not need to allocate a secondary private IP address for the OCI NIC because a private IP address cannot be moved across ADs.
- During failover, the public IP address detaches from the old primary FortiProxy NIC and attaches to the new primary FortiProxy NIC.
- Route next hop updates to point to the new primary FortiProxy NIC's primary private IP address.
- System interfaces, static route configurations, and sessions do not sync between FortiProxie when deployed between multiple ADs. They do sync when deploying within one AD.

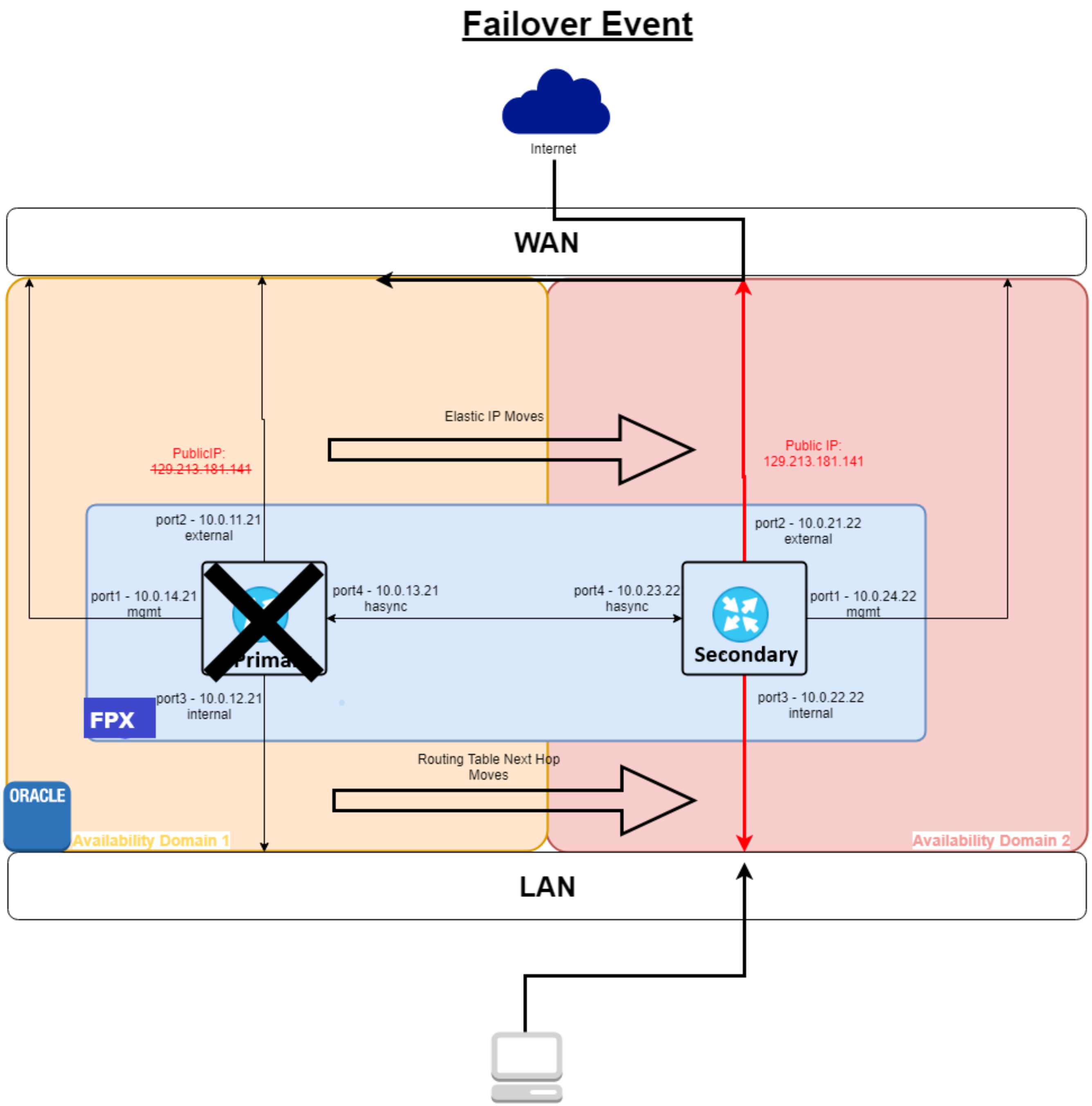
This guide refers to the primary FortiProxy in AD 1 as "FPX-A-AD1" and the secondary FortiProxy, located in AD2, as "FPX-B-AD2".

IPsec VPN phase 1 configuration does not synchronize between primary and secondary FortiProxies across ADs. Phase 2 configuration does synchronize.

The following sections provides an example of deploying FortiProxy-VM active-passive HA on OCI between multiple ADs:

1. Reviewing the network topology on page 58
2. Creating a VCN for multi-AD HA topology on page 59
3. Creating two FortiProxy-VM instances on page 63
4. Configuring the OCI HA interfaces on page 79
5. Configuring an OCI SND connector on page 81
6. Configuring active-passive HA on page 85
7. Checking the HA status and function on page 86

Reviewing the network topology



The following table describes the IP address assignments for FPX-A-AD1:

Port	OCI primary IP address	Subnet
Port 1	10.0.14.21	10.0.14.0/24 EIP1

Port	OCI primary IP address	Subnet
Port 2	10.0.11.21	10.0.11.0/24 EIP3
Port 3	10.0.12.21	10.0.12.0/24
Port 4	10.0.13.21	10.0.13.0/24

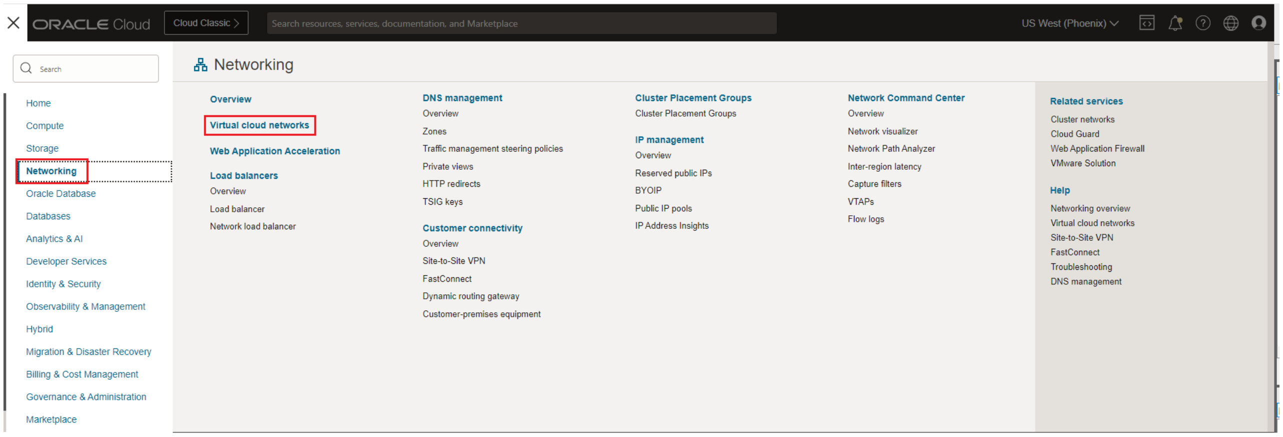
The following table describes the IP address assignments for FPX-B-AD2:

Port	OCI primary IP address	Subnet
Port 1	10.0.24.22	10.0.24.0/24 EIP1
Port 2	10.0.21.22	10.0.21.0/24 EIP3
Port 3	10.0.22.22	10.0.22.0/24
Port 4	10.0.23.22	10.0.23.0/24

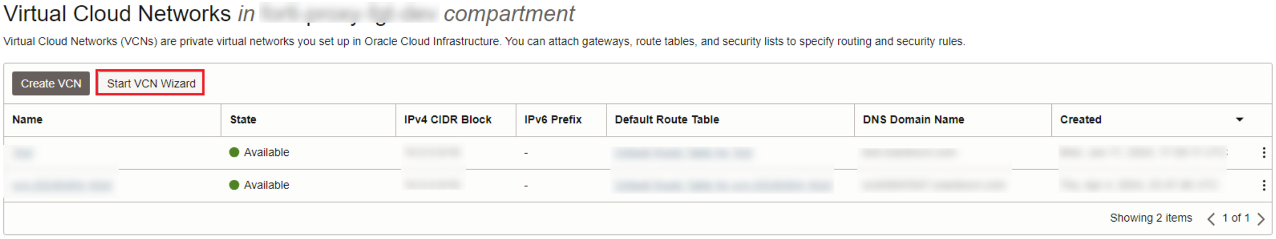
Creating a VCN for multi-AD HA topology

To create a VCN with eight subnets:

1. In OCI, go to *Networking* > *Virtual cloud networks*.



2. Click *Start VCN Wizard* to create the Internet gateway, routing table, and subnet all together using Oracle default settings.
   You can also choose to create each resource separately by clicking *Create VCN*.



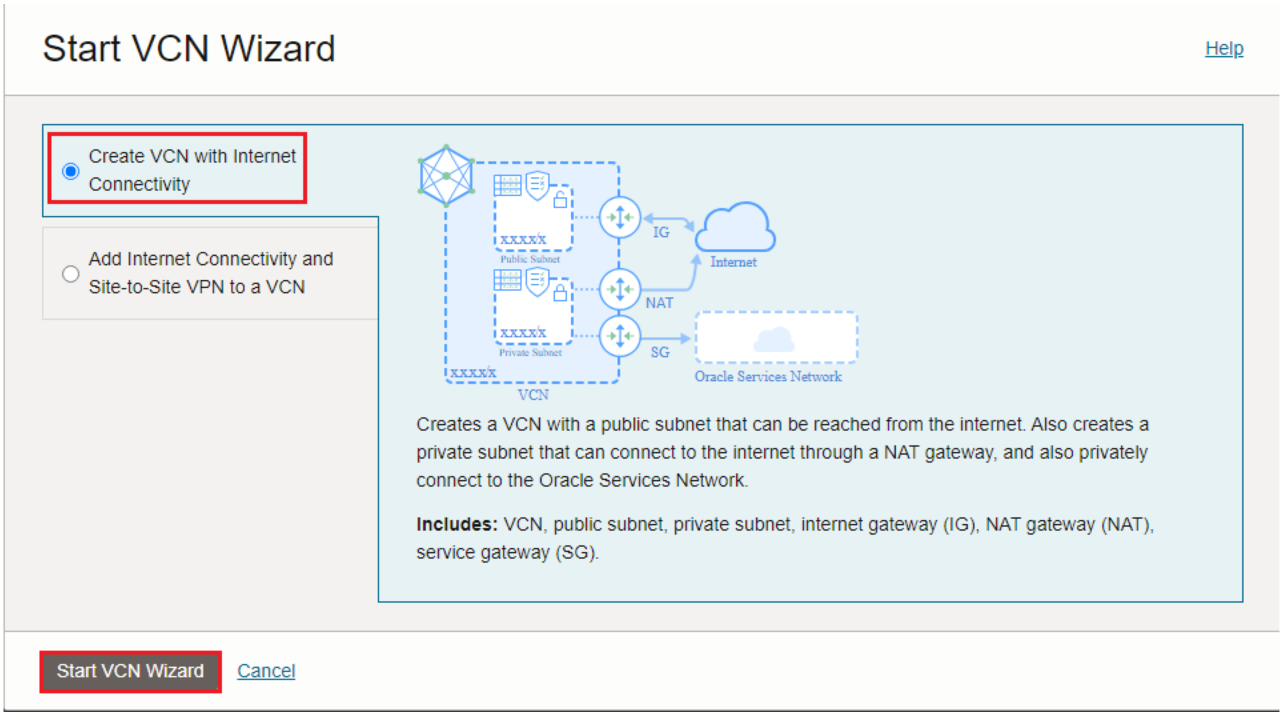
Virtual Cloud Networks *in* [redacted] *compartment*

Virtual Cloud Networks (VCNs) are private virtual networks you set up in Oracle Cloud Infrastructure. You can attach gateways, route tables, and security lists to specify routing and security rules.

Name	State	IPv4 CIDR Block	IPv6 Prefix	Default Route Table	DNS Domain Name	Created
[redacted]	● Available	[redacted]	-	[redacted]	[redacted]	[redacted]
[redacted]	● Available	[redacted]	-	[redacted]	[redacted]	[redacted]

Showing 2 items < 1 of 1 >

3. Select *Create VCN with Internet Connectivity* and click *Start VCN Wizard*.



Start VCN Wizard

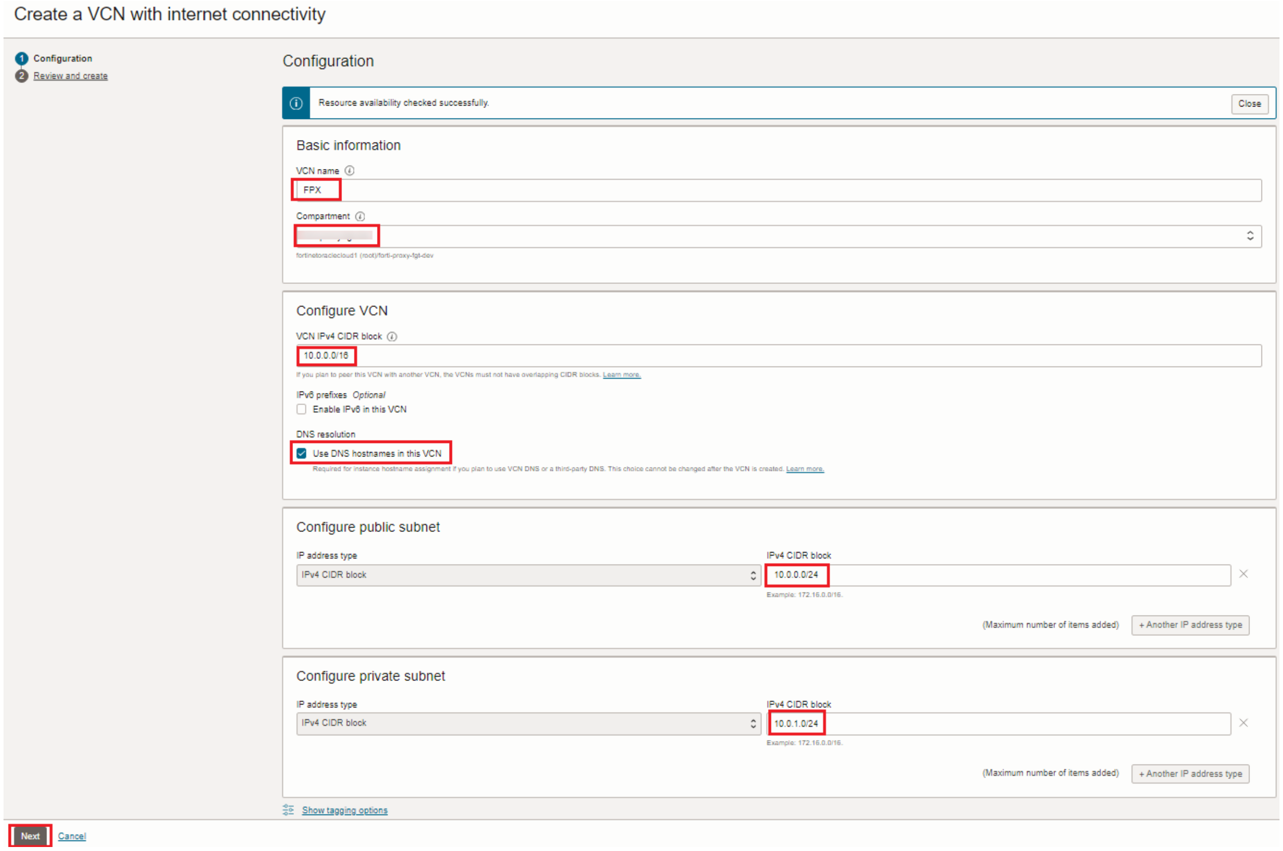
● Create VCN with Internet Connectivity

○ Add Internet Connectivity and Site-to-Site VPN to a VCN

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).

4. Configure the following options:



Create a VCN with internet connectivity

Configuration

Resource availability checked successfully.

Basic information

VCN name: FPX

Compartment: [redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Configure VCN

VCN IPv4 CIDR block: 10.0.0.0/16

If you plan to peer this VCN with another VCN, the VCNs must not have overlapping CIDR blocks. Learn more.

IPv6 prefixes *Optional*

☐ Enable IPv6 in this VCN

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.

Configure public subnet

IP address type: IPv4 CIDR block

IPv4 CIDR block: 10.0.0.0/24

Example: 172.16.0.0/16.

(Maximum number of items added)

Configure private subnet

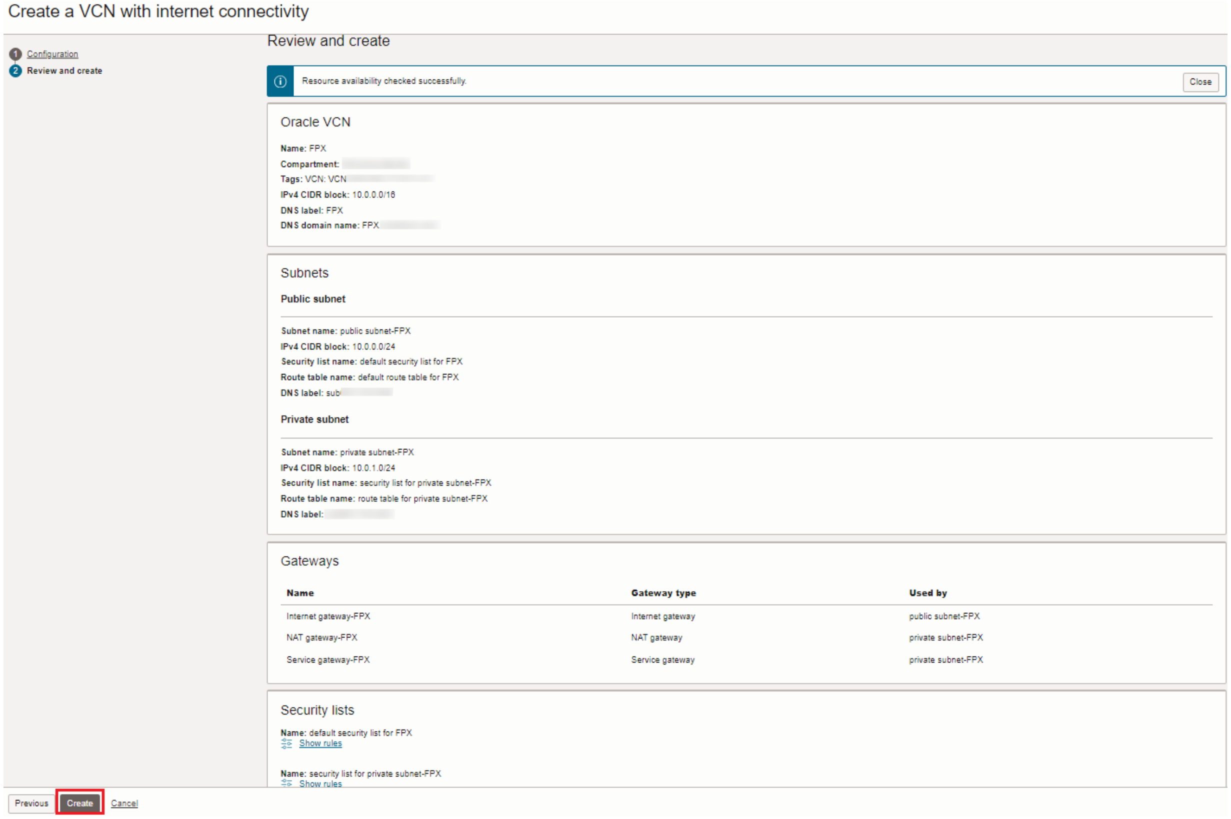
IP address type: IPv4 CIDR block

IPv4 CIDR block: 10.0.1.0/24

Example: 172.16.0.0/16.

(Maximum number of items added)

a. In the *VCN name* field, enter the VCN name.
b. In the *Compartment* field, select the compartment for the VCN.
c. In the *IPv4 CIDR block* field, specify the IPv4 CIDR block.
d. Select the *Use DNS hostnames in this VCN* option.
e. Configure subnets as needed.
f. Click *Next*.
g. Confirm the configuration details and click *Create* at the bottom of the screen.



Create a VCN with internet connectivity

Review and create

Resource availability checked successfully.

Oracle VCN

Name: FPX
Compartment: [redacted]
Tags: VCN: VCN[redacted]
IPv4 CIDR block: 10.0.0.0/16
DNS label: FPX
DNS domain name: FPX[redacted]

Subnets

Public subnet

Subnet name: public subnet-FPX
IPv4 CIDR block: 10.0.0.0/24
Security list name: default security list for FPX
Route table name: default route table for FPX
DNS label: sub[redacted]

Private subnet

Subnet name: private subnet-FPX
IPv4 CIDR block: 10.0.1.0/24
Security list name: security list for private subnet-FPX
Route table name: route table for private subnet-FPX
DNS label: [redacted]

Gateways

Name	Gateway type	Used by
Internet gateway-FPX	Internet gateway	public subnet-FPX
NAT gateway-FPX	NAT gateway	private subnet-FPX
Service gateway-FPX	Service gateway	private subnet-FPX

Security lists

Name: default security list for FPX

Name: security list for private subnet-FPX

This configures the related resources, including two subnets: one for public access and the other for private access, each of which will belong to the first AD. You can access the FortiProxy over the Internet once it is deployed via HTTPS through the GUI management screen or via SSH.

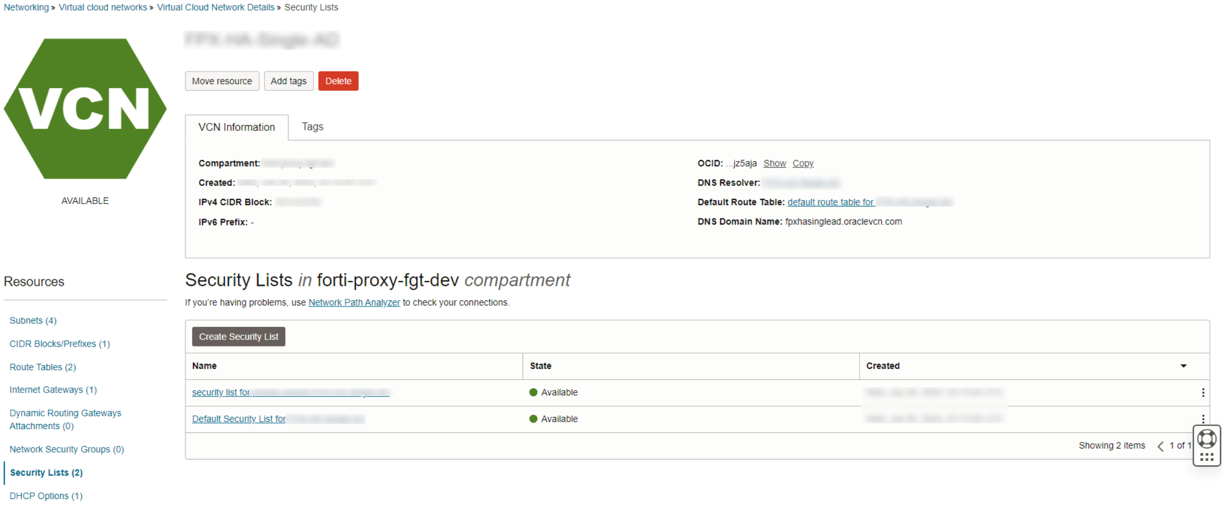
5. Click *View VCN*.
6. Create six more subnets: two will be the management and heartbeat for the first AD; four will be for the second AD. To do so, repeat the following steps for each subnet:
   a. Click *Create Subnet*.
   b. Specify a name to identify the subnet, such as management or heartbeat.
   c. For *Subnet Type*, select *Availability Domain-specific* for management and *Regional* for others.
   d. **(management only)** Select the availability domain.
   e. Specify the value for *IPv4 CIDR Block*.
   f. For *Security Lists*, select the default security list for the VCN.
   g. For *Subnet Access*, select *Public Subnet* for management and *Private* for heartbeat.
   h. Click *Create Subnet*.

   After creating all the subnets, ensure that the VCN contains the following eight subnets (four in AD1 and four in AD2):

AD1 subnet	AD2 subnet	Purpose
net11-external	net21-external	External data traffic on the public network-facing side.
net12-internal	net22-internal	Internal data traffic on the protected/trusted network-facing side.
net13-heartbeat	net23-heartbeat	Heartbeat between two FortiGate nodes. This is unicast communication.
net14-mgmt	net24-mgmt	Dedicated management interface use.

7. Update the default security list to allow access to the required ports as listed in FortiProxy ports:

   a. In the *Security Lists* tab of the VCN details page, click the link of the default security list. By default, port 22 is allowed.



Networking » Virtual cloud networks » Virtual Cloud Network Details » Security Lists

[redacted]

Compartment: [redacted]
Created: [redacted]
IPv4 CIDR Block: [redacted]
IPv6 Prefix: -
OCID: ...jz5aja Show Copy
DNS Resolver: [redacted]
Default Route Table: default route table for [redacted]
DNS Domain Name: fpxhasinglead.oraclevcn.com

Resources

- Subnets (4)
- CIDR Blocks/Prefixes (1)
- Route Tables (2)
- Internet Gateways (1)
- Dynamic Routing Gateways Attachments (0)
- Network Security Groups (0)
- **Security Lists (2)**
- DHCP Options (1)

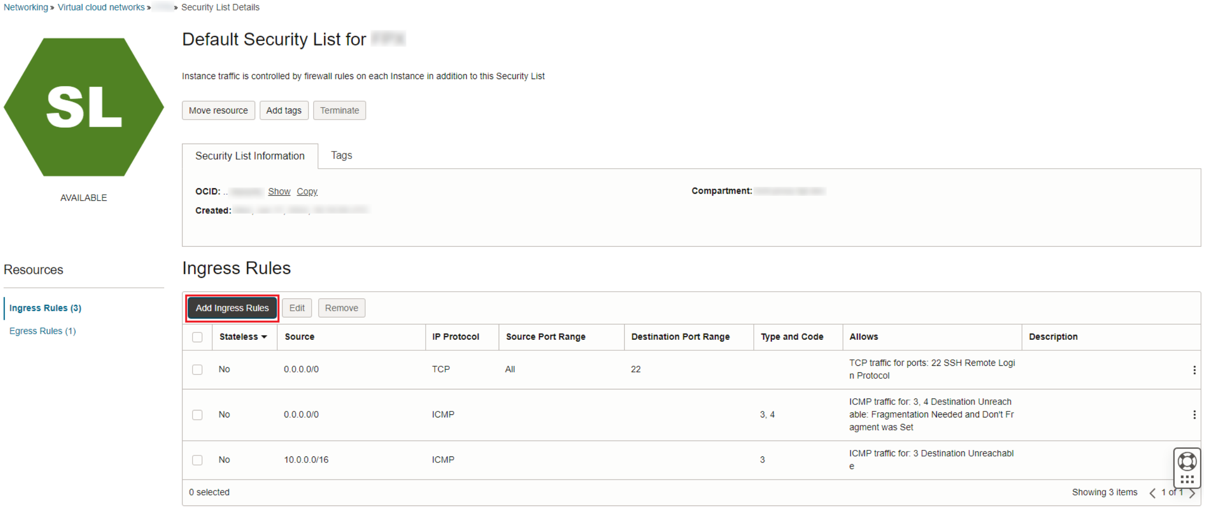
Security Lists *in* forti-proxy-fgt-dev *compartment*

If you're having problems, use Network Path Analyzer to check your connections.

Name	State	Created
security list for [redacted]	● Available	[redacted]
Default Security List for [redacted]	● Available	[redacted]

Showing 2 items < 1 of 1

   b. Click *Add Ingress Rules*.



Networking » Virtual cloud networks » [redacted] » Security List Details

Default Security List for [redacted]

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

OCID: .. [redacted] Show Copy
Created: [redacted]
Compartment: [redacted]

Resources

- **Ingress Rules (3)**
- Egress Rules (1)

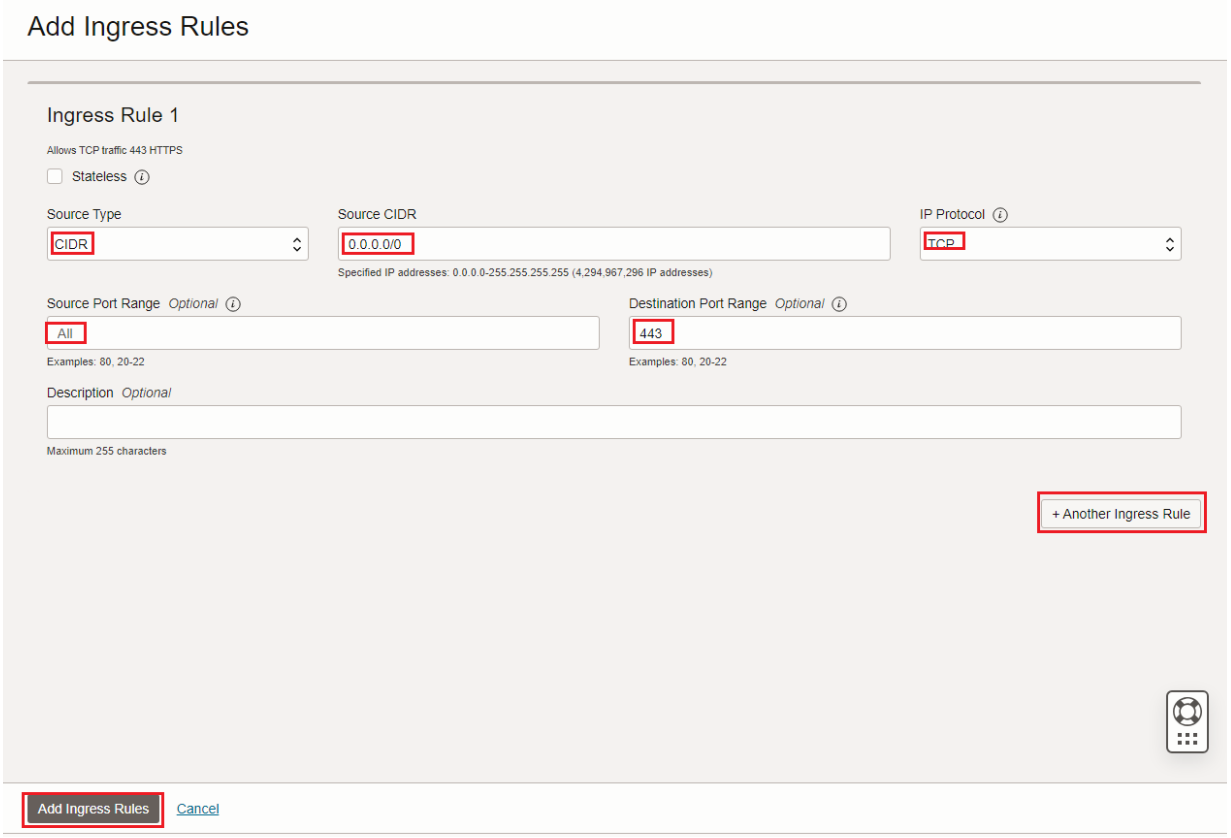
Ingress Rules

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

0 selected

Showing 3 items < 1 of 1 >

c. Configure a rule to allow TCP port 443 and add any other rules for specific ports as needed.



Add Ingress Rules

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

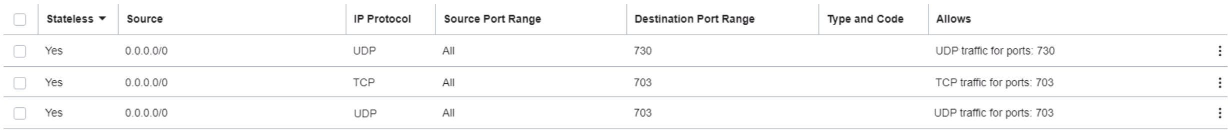
Destination Port Range *Optional* ⓘ: 443

Examples: 80, 20-22

Description *Optional*

Maximum 255 characters

For example, for Heartbeat sync ports, you must have the following included in the security list:



□	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	
□	Yes	0.0.0.0/0	UDP	All	730		UDP traffic for ports: 730	⋮
□	Yes	0.0.0.0/0	TCP	All	703		TCP traffic for ports: 703	⋮
□	Yes	0.0.0.0/0	UDP	All	703		UDP traffic for ports: 703	⋮

d. Click *Add Ingress Rules*.

Creating two FortiProxy-VM instances

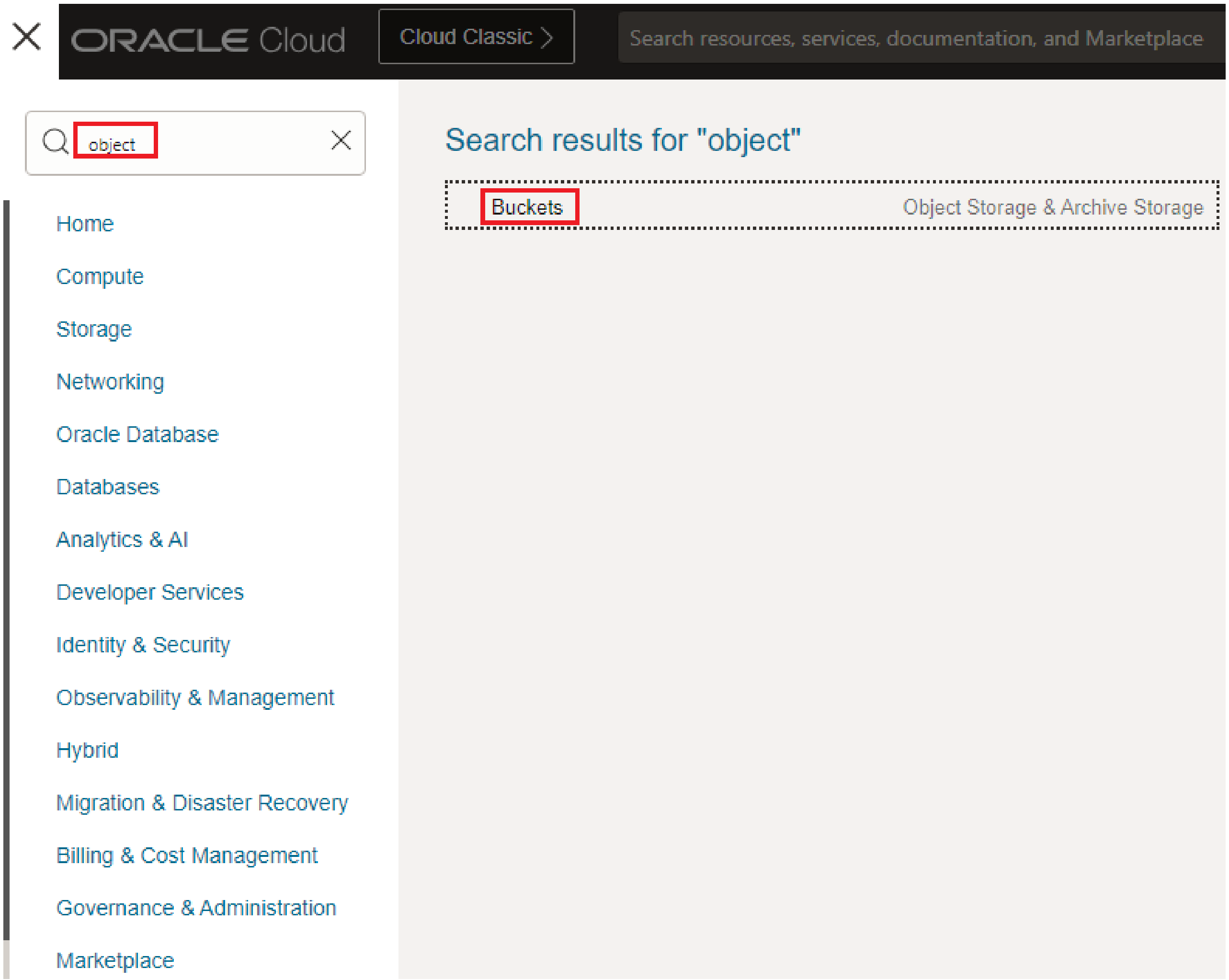
You must create two FortiProxy-VM instances for HA deployment, one for primary and one for secondary. To do so, you must first obtain the deployment image file and importing the file into the OCI bucket.

To obtain the deployment image file and place it in your bucket:

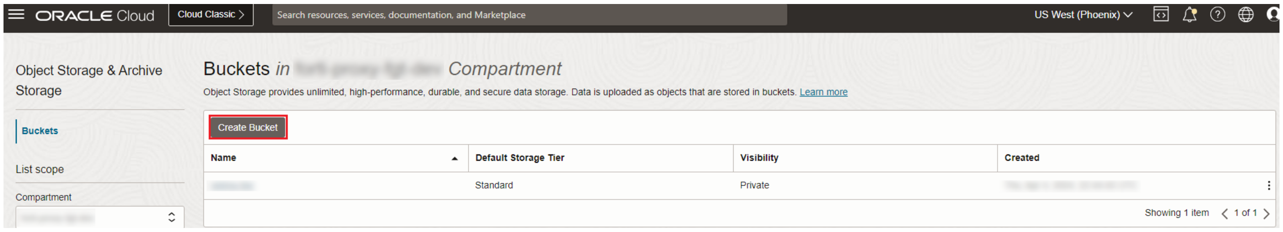
1. Obtain the deployment image file:
   a. Go to Customer Service & Support.
   b. Click *Support* > *Downloads* > *Firmware Download* in the top menu.
   c. In the *Select Product* dropdown list, select *FortiProxy*.
   d. In the *Download* tab, navigate to the FortiProxy version folder.
   e. Obtain the *FPX_KVM_OPC-vX-buildXXXX-FORTINET.out.kvm.zip* file, where *XXXX* is the build number. Ensure that the file name includes *kvm*.

f. After downloading, unzip the file. You will find the *fortiproxy.qcow2* file, which is needed to deploy the FortiProxy-VM on OCI.

2. In OCI, go to *Object Storage* > *Buckets*.


ORACLE Cloud
Cloud Classic >
Search resources, services, documentation, and Marketplace
object
Search results for "object"
Buckets
Object Storage & Archive Storage
Home
Compute
Storage
Networking
Oracle Database
Databases
Analytics & AI
Developer Services
Identity & Security
Observability & Management
Hybrid
Migration & Disaster Recovery
Billing & Cost Management
Governance & Administration
Marketplace

3. Click *Create Bucket* to create a standard storage bucket.

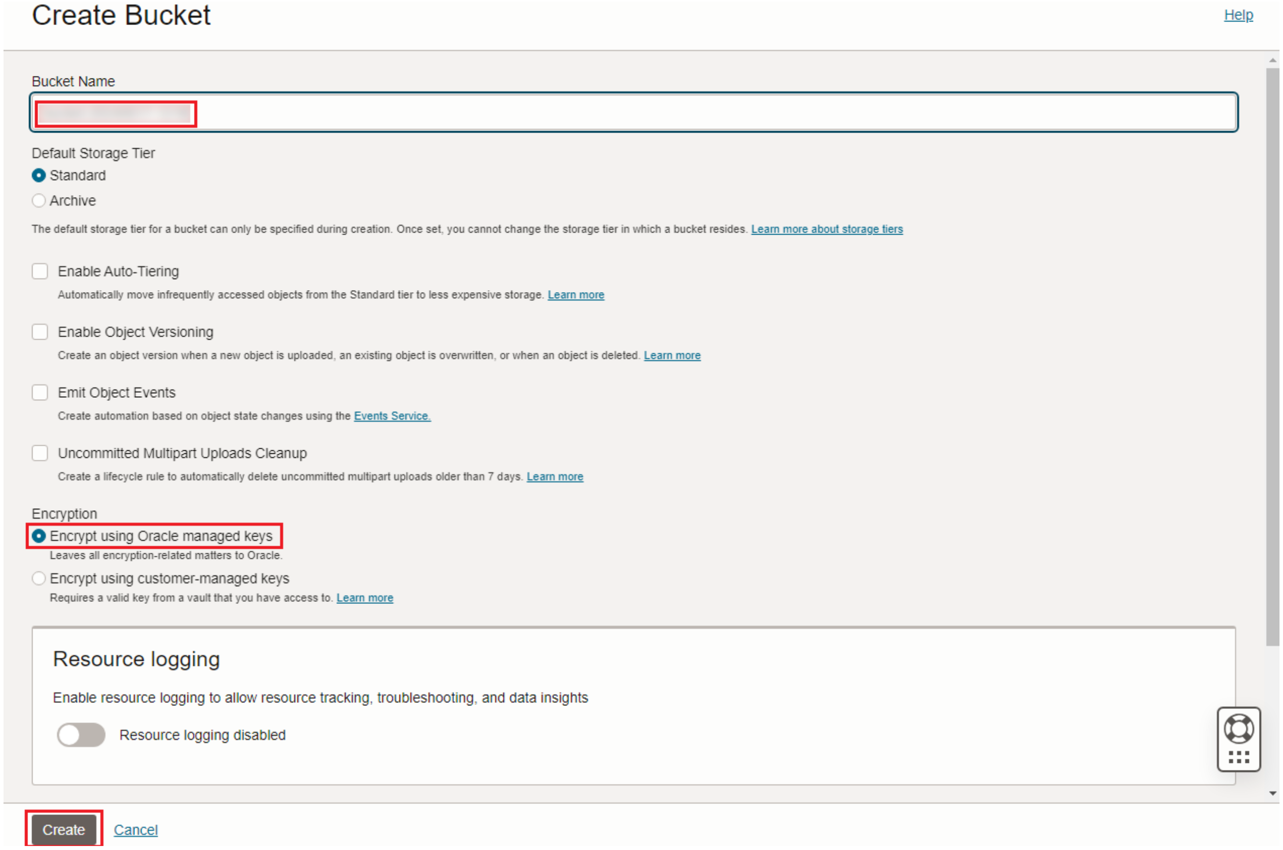


Buckets *in* [redacted] *Compartment*

Object Storage provides unlimited, high-performance, durable, and secure data storage. Data is uploaded as objects that are stored in buckets. Learn more

Name	Default Storage Tier	Visibility	Created
[redacted]	Standard	Private	[redacted]

4. Configure the standard storage bucket as shown below and click *Create*:



Create Bucket

Help

Bucket Name

[redacted]

Default Storage Tier

● Standard

○ Archive

The default storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides. Learn more about storage tiers

□ Enable Auto-Tiering

Automatically move infrequently accessed objects from the Standard tier to less expensive storage. Learn more

□ Enable Object Versioning

Create an object version when a new object is uploaded, an existing object is overwritten, or when an object is deleted. Learn more

□ Emit Object Events

Create automation based on object state changes using the Events Service.

□ Uncommitted Multipart Uploads Cleanup

Create a lifecycle rule to automatically delete uncommitted multipart uploads older than 7 days. Learn more

Encryption

● Encrypt using Oracle managed keys

Leaves all encryption-related matters to Oracle.

○ Encrypt using customer-managed keys

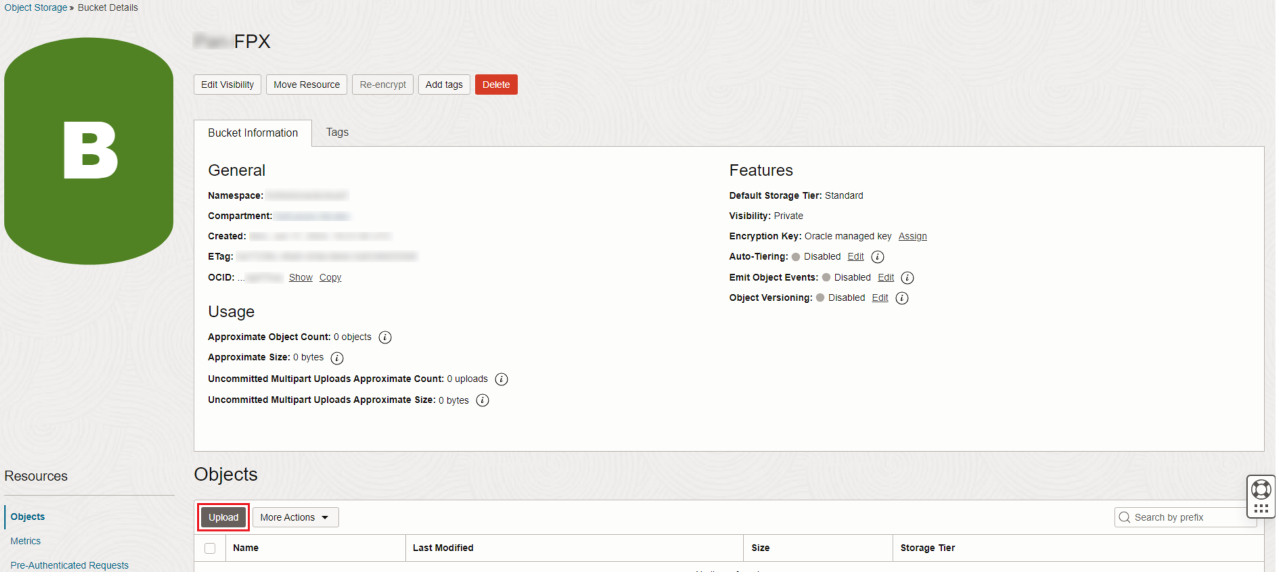
Requires a valid key from a vault that you have access to. Learn more

Resource logging

Enable resource logging to allow resource tracking, troubleshooting, and data insights

Resource logging disabled

5. Select the bucket, then click *Upload*.



[redacted] FPX

General

Namespace: [redacted]

Compartment: [redacted]

Created: [redacted]

ETag: [redacted]

OCID: ...[redacted] Show Copy

Usage

Approximate Object Count: 0 objects

Approximate Size: 0 bytes

Uncommitted Multipart Uploads Approximate Count: 0 uploads

Uncommitted Multipart Uploads Approximate Size: 0 bytes

Features

Default Storage Tier: Standard

Visibility: Private

Encryption Key: Oracle managed key Assign

Auto-Tiering: ● Disabled Edit

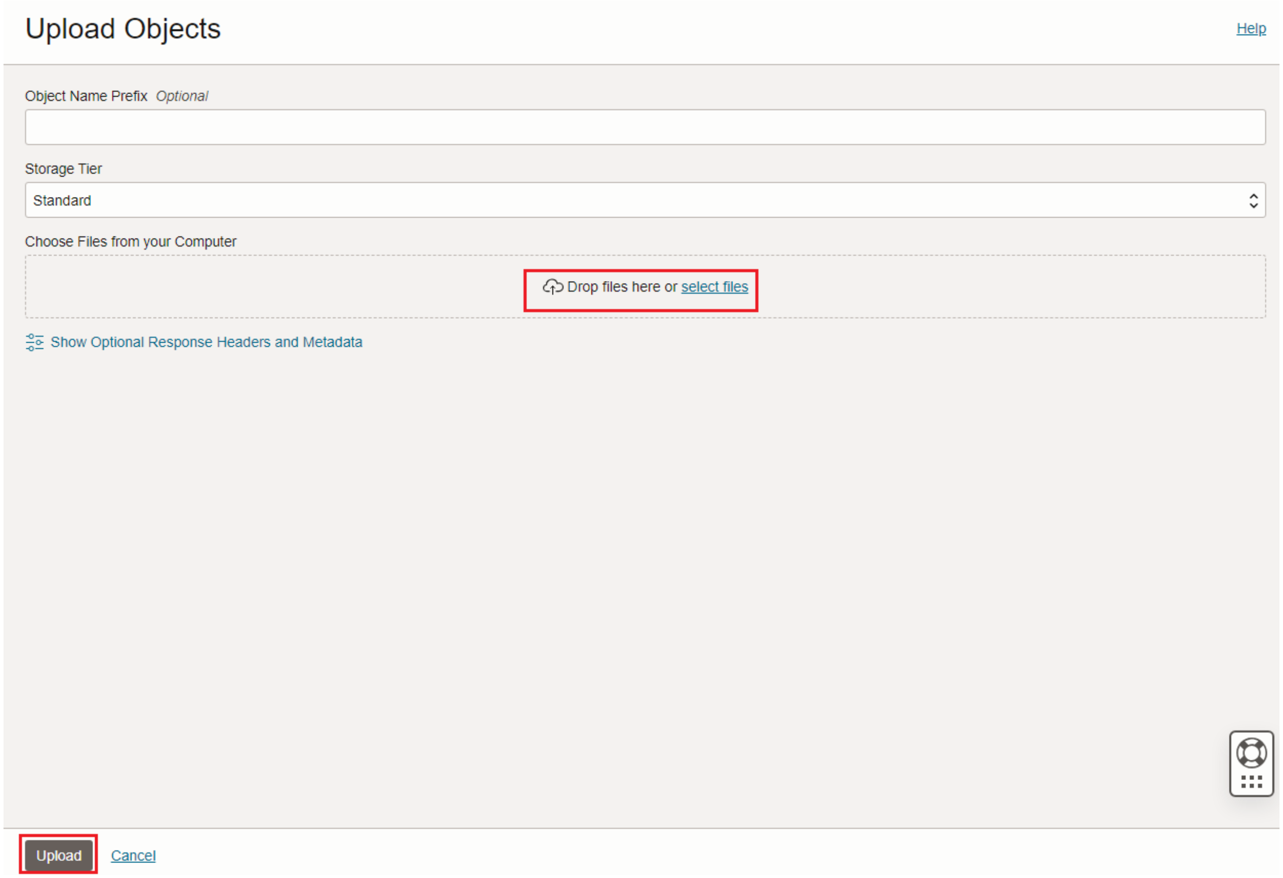
Emit Object Events: ● Disabled Edit

Object Versioning: ● Disabled Edit

Objects

□	Name	Last Modified	Size	Storage Tier

6. Drop or select the deployment image file *fortiproxy.qcow2* and click *Upload*.



Upload Objects

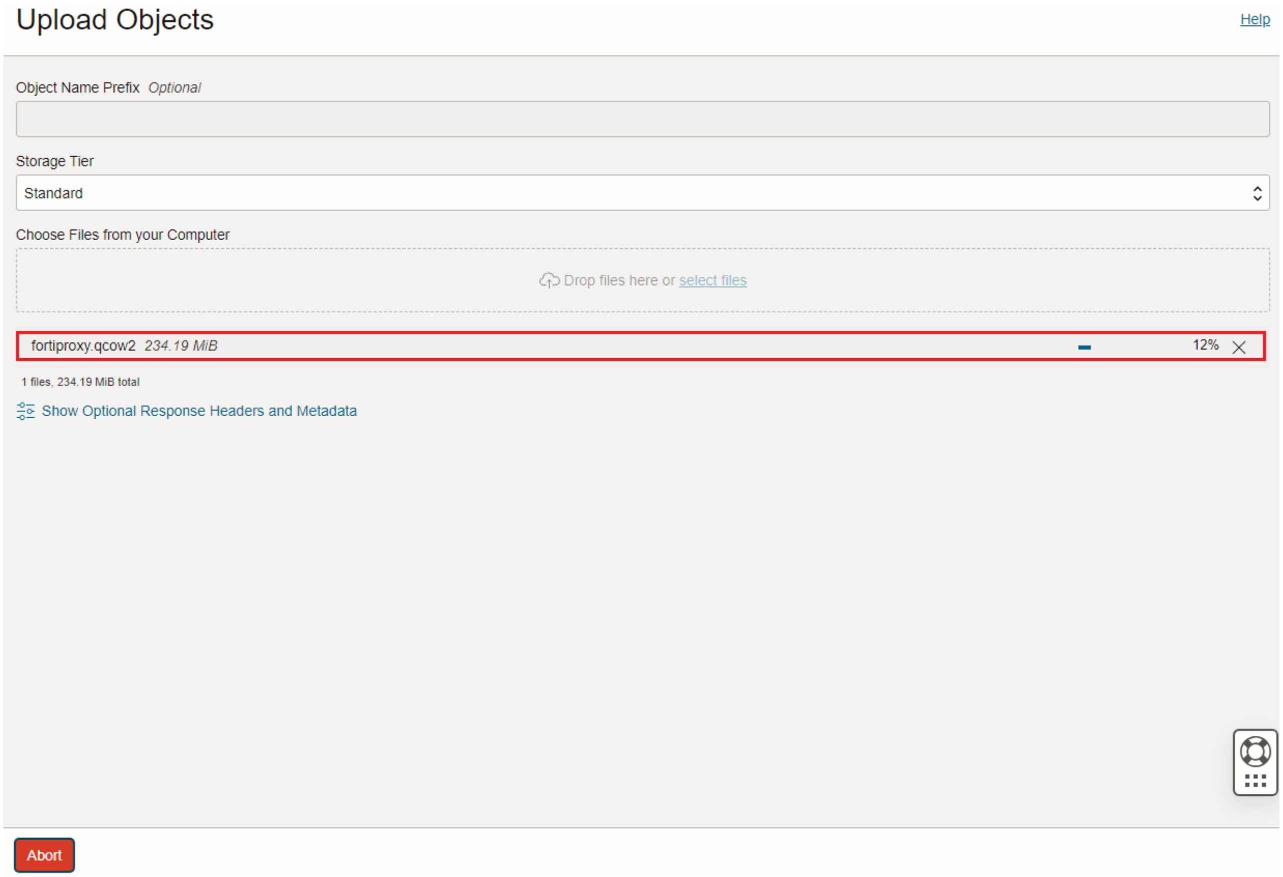
Object Name Prefix *Optional*

Storage Tier: Standard

Choose Files from your Computer

Help
Drop files here or select files
Show Optional Response Headers and Metadata
Upload
Cancel

The dialog shows the upload progress.



Upload Objects
Help
Drop files here or select files
Show Optional Response Headers and Metadata
Abort

Object Name Prefix *Optional*

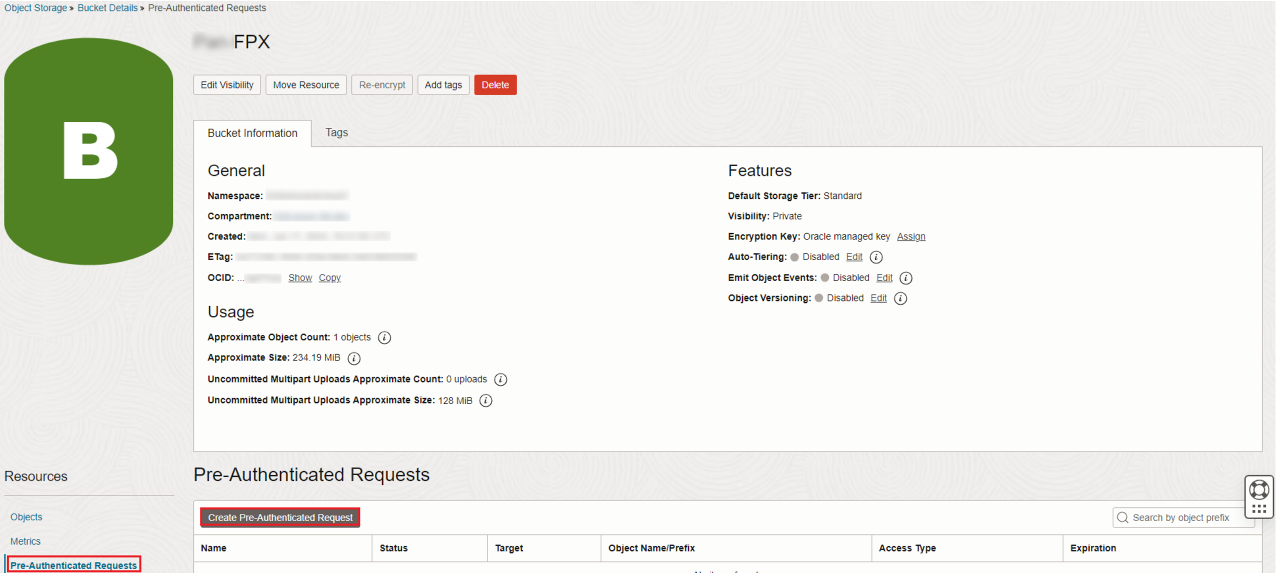
Storage Tier: Standard

Choose Files from your Computer

fortiproxy.qcow2 *234.19 MiB* 12%

1 files, 234.19 MiB total

7. After the upload is complete, click *Close*.
8. Click *Pre-Authenticated Requests* and then *Create Pre-Authenticated Requests*.



[redacted] FPX

General

Namespace: [redacted]
Compartment: [redacted]
Created: [redacted]
ETag: [redacted]
OCID: ...[redacted] Show Copy

Features

Default Storage Tier: Standard
Visibility: Private
Encryption Key: Oracle managed key Assign
Auto-Tiering: Disabled Edit
Emit Object Events: Disabled Edit
Object Versioning: Disabled Edit

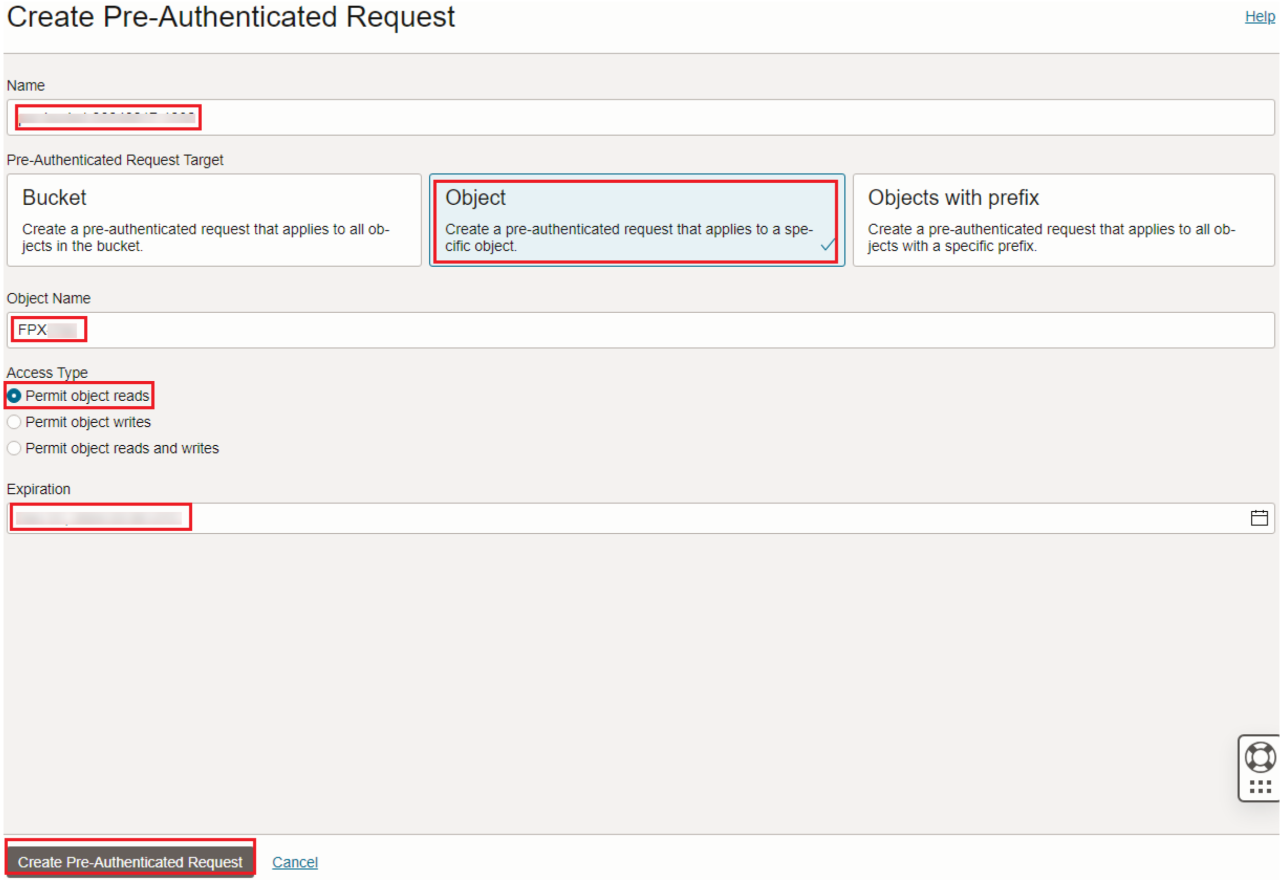
Usage

Approximate Object Count: 1 objects
Approximate Size: 234.19 MiB
Uncommitted Multipart Uploads Approximate Count: 0 uploads
Uncommitted Multipart Uploads Approximate Size: 128 MiB

Pre-Authenticated Requests

Name	Status	Target	Object Name/Prefix	Access Type	Expiration

9. Configure the following options and click *Create Pre-Authenticated Requests*:



Create Pre-Authenticated Request

Name

[redacted]

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

FPX[redacted]

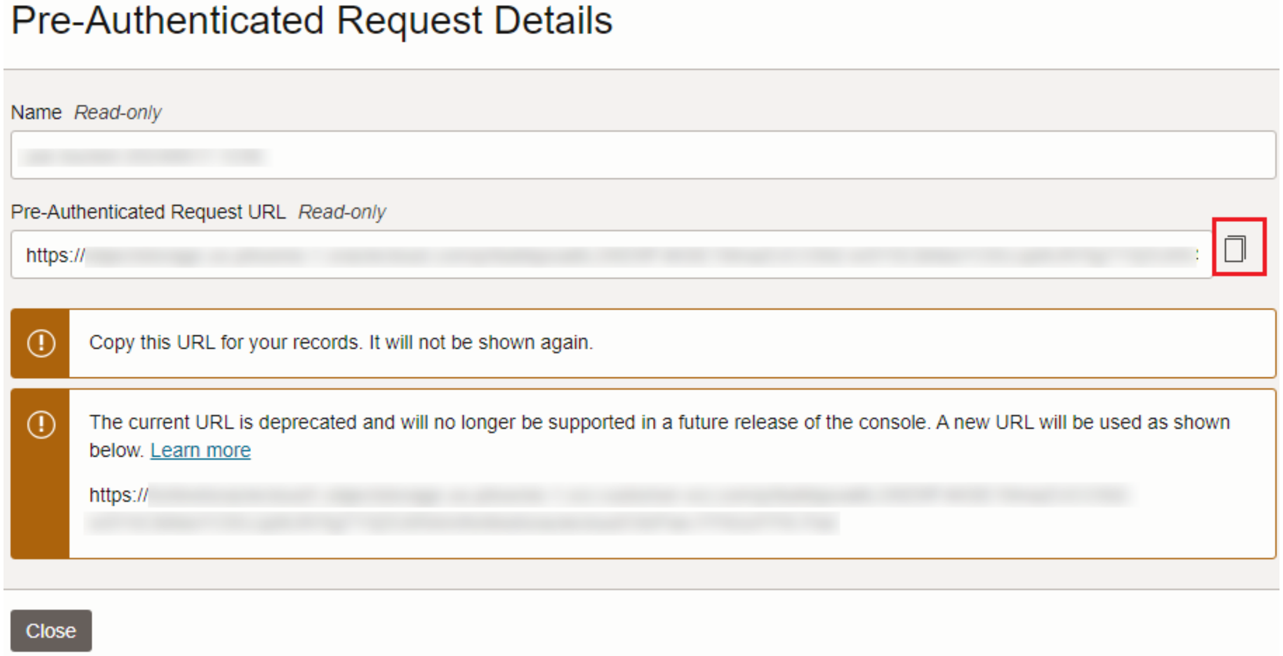
Access Type

● Permit object reads
○ Permit object writes
○ Permit object reads and writes

Expiration

[redacted]

10. Copy this URL and save it somewhere for usage in later steps. Click *Close*.



Pre-Authenticated Request Details

Name *Read-only*

[redacted]

Pre-Authenticated Request URL *Read-only*

https://[redacted]

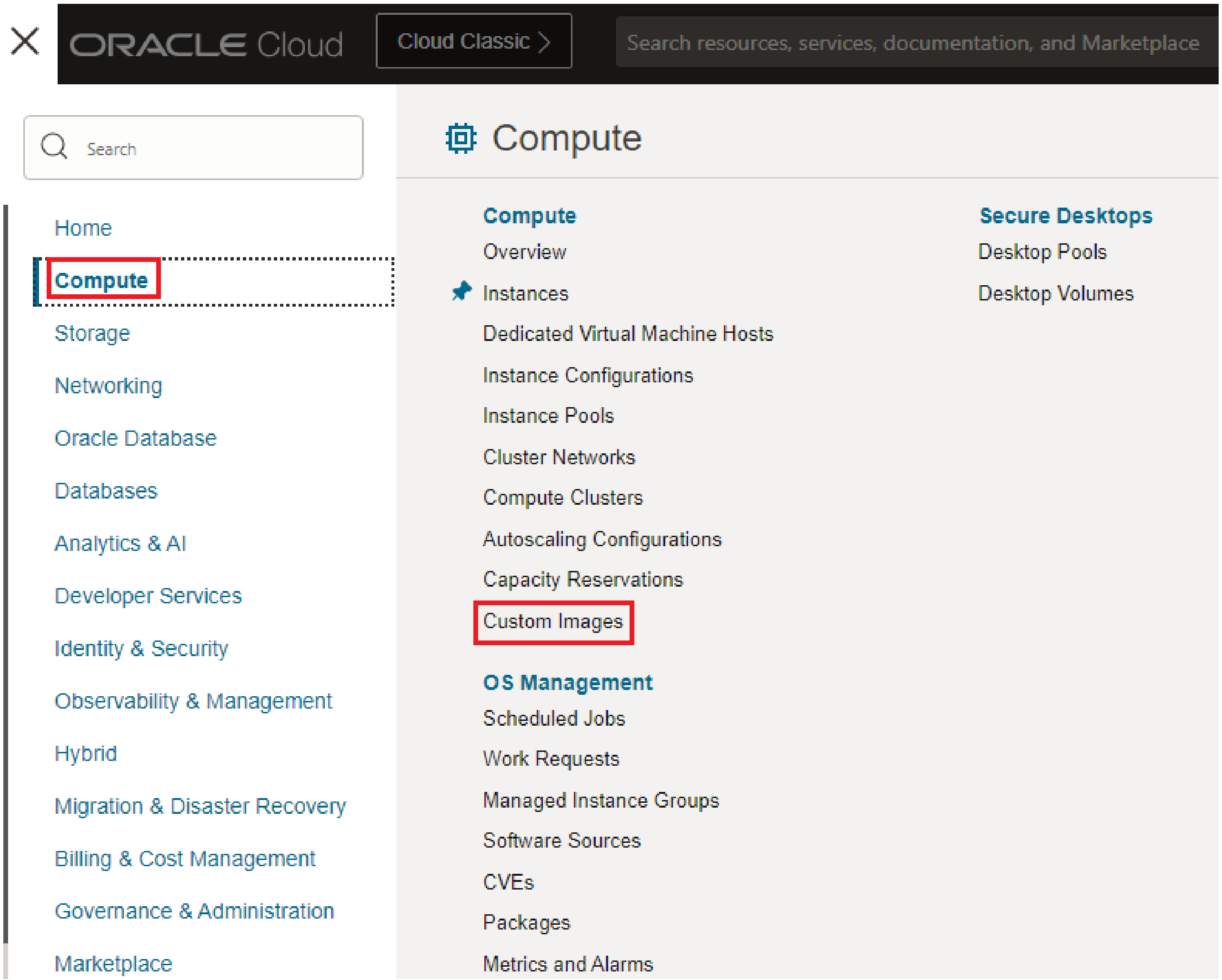
Copy this URL for your records. It will not be shown again.

The current URL is deprecated and will no longer be supported in a future release of the console. A new URL will be used as shown below. Learn more

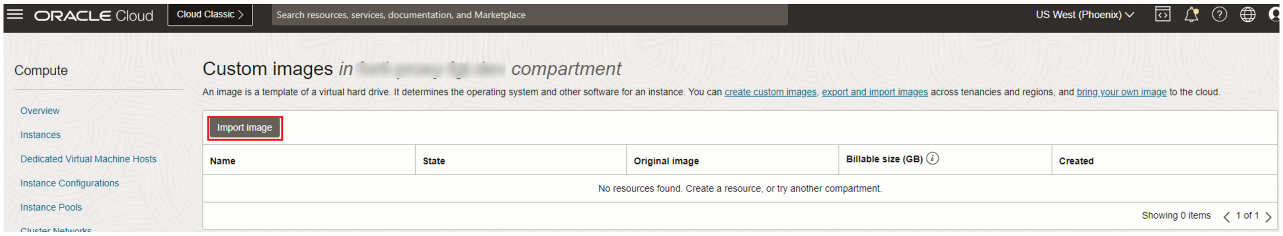
https://[redacted]

To import the image:

1. Go to *Compute* > *Custom Images*.



2. Click *Import Image*.



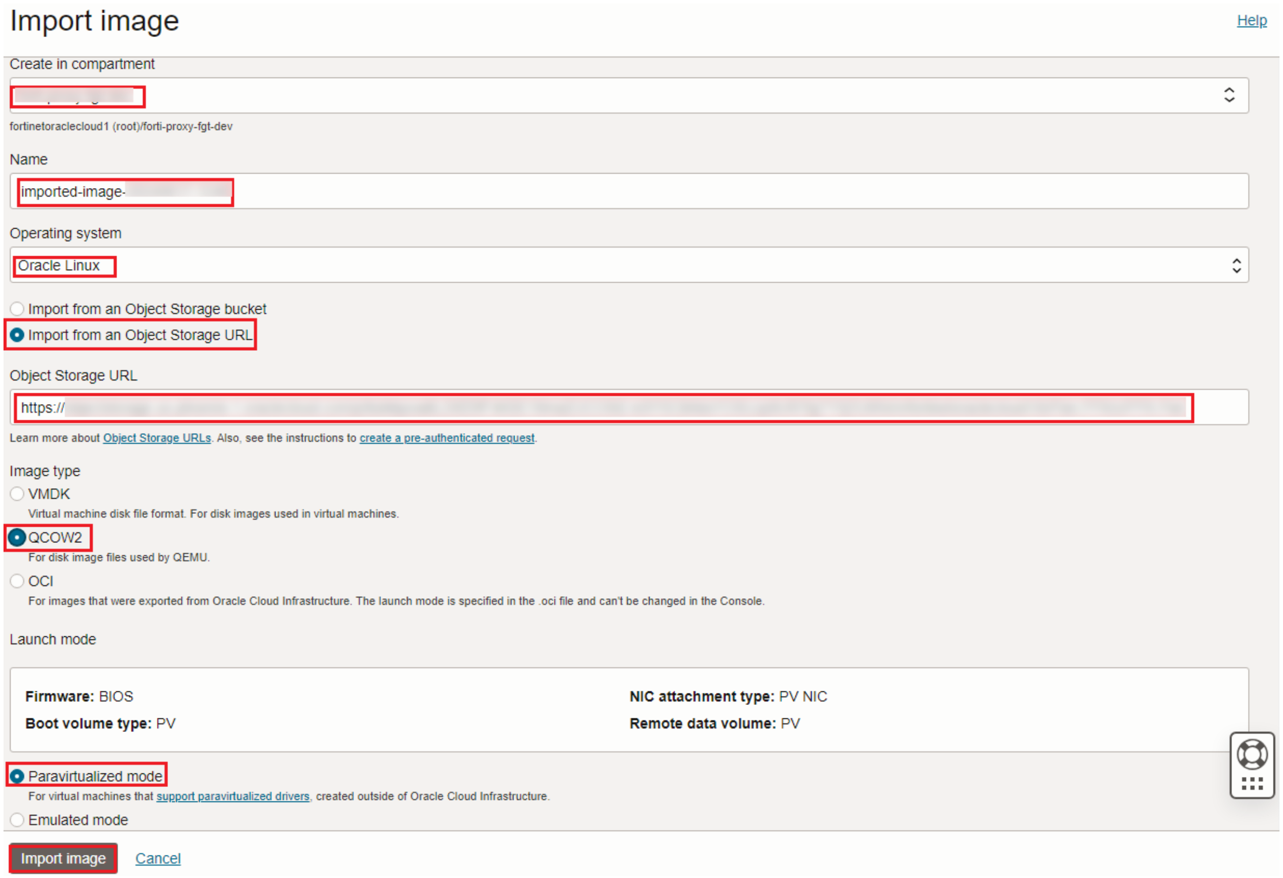
Custom images *in* [redacted] *compartment*

An image is a template of a virtual hard drive. It determines the operating system and other software for an instance. You can create custom images, export and import images across tenancies and regions, and bring your own image to the cloud.

Name	State	Original image	Billable size (GB) ⓘ	Created
No resources found. Create a resource, or try another compartment.				

Showing 0 items < 1 of 1 >

3. Configure the following options and click *Import image*. In the *Object Storage URL* field, enter the URL link obtained earlier and place it in your bucket.



Import image

Create in compartment

[redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Name

imported-image-[redacted]

Operating system

Oracle Linux

○ Import from an Object Storage bucket

● Import from an Object Storage URL

Object Storage URL

https://[redacted]

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

Boot volume type: PV

NIC attachment type: PV NIC

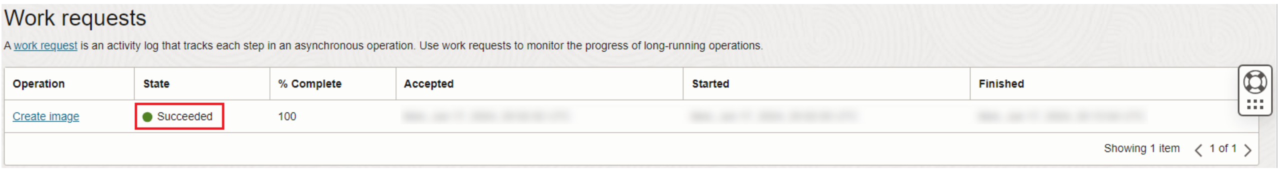
Remote data volume: PV

● Paravirtualized mode

For virtual machines that support paravirtualized drivers, created outside of Oracle Cloud Infrastructure.

○ Emulated mode

4. Wait until the state of the *Create image* operation changes to *Succeeded*.



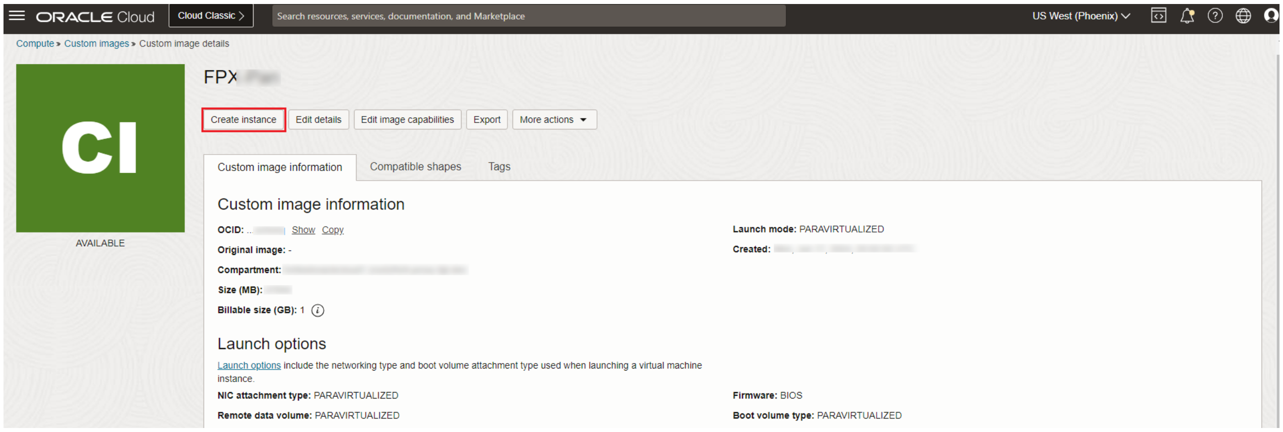
Work requests

A work request is an activity log that tracks each step in an asynchronous operation. Use work requests to monitor the progress of long-running operations.

Operation	State	% Complete	Accepted	Started	Finished
Create image	● Succeeded	100	[redacted]	[redacted]	[redacted]

To create the two FortiProxy-VM instances:

1. From the newly imported image, click *Create Instance*.



ORACLE Cloud
Cloud Classic
Search resources, services, documentation, and Marketplace
US West (Phoenix)
Compute » Custom images » Custom image details
CI
AVAILABLE

FPX[redacted]

Custom image information

OCID: ...[redacted] Show Copy

Original image: -

Compartment: [redacted]

Size (MB): [redacted]

Billable size (GB): 1

Launch mode: PARAVIRTUALIZED

Created: [redacted]

Launch options

Launch options include the networking type and boot volume attachment type used when launching a virtual machine instance.

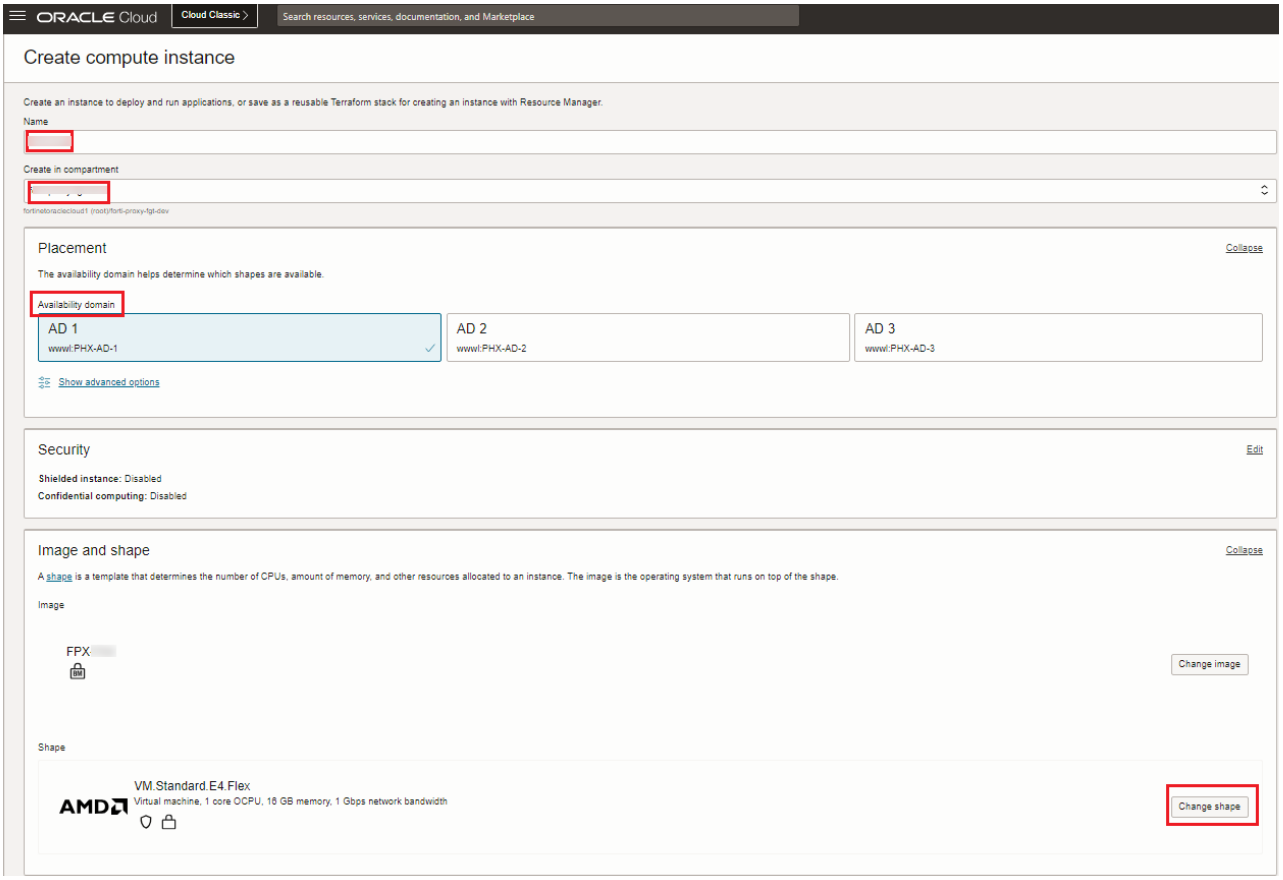
NIC attachment type: PARAVIRTUALIZED

Remote data volume: PARAVIRTUALIZED

Firmware: BIOS

Boot volume type: PARAVIRTUALIZED

2. Configure the parameters for the FortiProxy-VM instance:



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: [redacted]

Create in compartment: [redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Placement

The availability domain helps determine which shapes are available.

Availability domain

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

Security

Shielded instance: Disabled
Confidential computing: Disabled

Image and shape

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

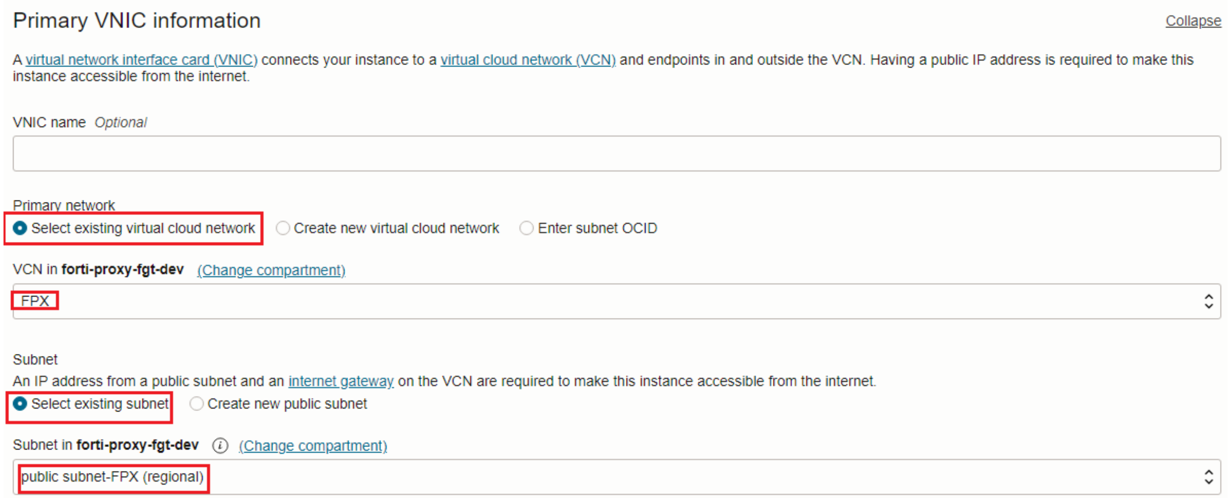
FPX[redacted]

Shape

VM.Standard.E4.Flex
Virtual machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth

a. In the *Name* field, enter the desired name to identify the instance. For example, FortiProxy A.
b. Under *Create in compartment*, select the compartment for the instance.
c. Under *Availability domain*, select the desired domain.
d. Under *Image and shape*, click *Change shape*.
e. Under *Instance type*, select *Virtual Machine*.
f. Select a shape that can accommodate four network interfaces.
g. Configure other shaping options as needed and click *Select shape*.

h. In the *Primary VNIC information* section, specify the VNIC name and select a network to launch the instance.



Primary VNIC information

A virtual network interface card (VNIC) connects your instance to a virtual cloud network (VCN) and endpoints in and outside the VCN. Having a public IP address is required to make this instance accessible from the internet.

VNIC name *Optional*

Primary network

● Select existing virtual cloud network ○ Create new virtual cloud network ○ Enter subnet OCID

VCN in **forti-proxy-fgt-dev** (Change compartment)

FPX

Subnet

An IP address from a public subnet and an internet gateway on the VCN are required to make this instance accessible from the internet.

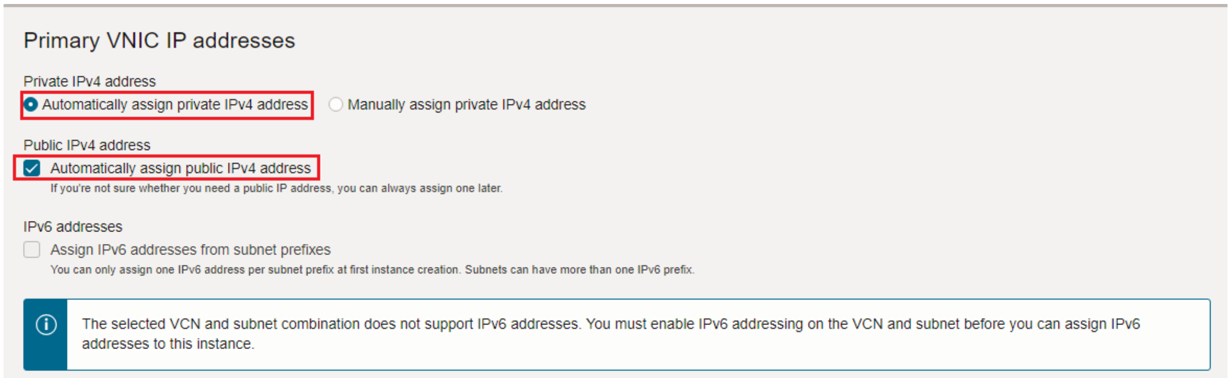
● Select existing subnet ○ Create new public subnet

Subnet in **forti-proxy-fgt-dev** (Change compartment)

public subnet-FPX (regional)

i. In the *Subnet* field, select a subnet on the Internet-facing side of the network.

j. In the *Primary VNIC IP addresses* section, configure the following.
Ensure *Automatically assign public IPv4 address* is selected so you can access the FortiProxy-VM over the Internet. You can disable this once you have configured everything as desired.



Primary VNIC IP addresses

Private IPv4 address

● Automatically assign private IPv4 address ○ Manually assign private IPv4 address

Public IPv4 address

☑ Automatically assign public IPv4 address

If you're not sure whether you need a public IP address, you can always assign one later.

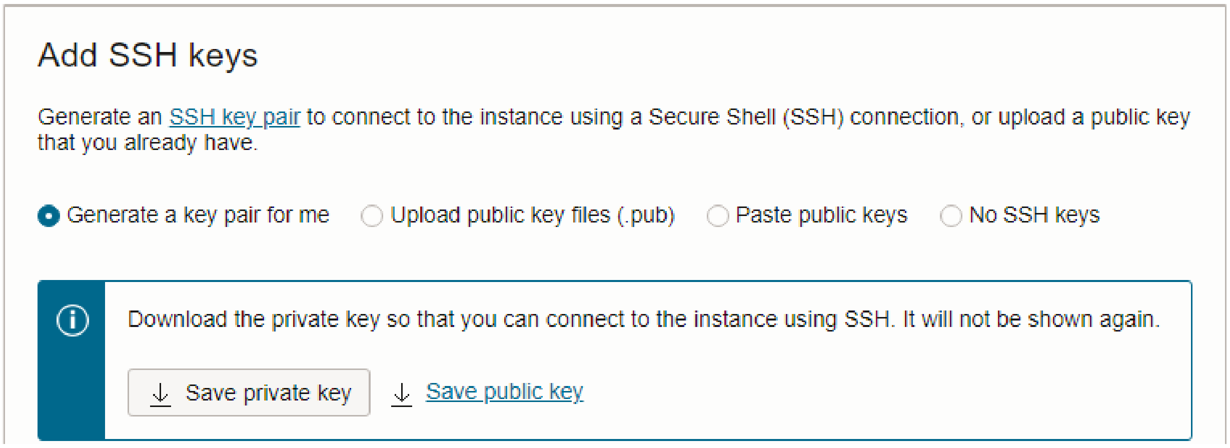
IPv6 addresses

□ Assign IPv6 addresses from subnet prefixes

You can only assign one IPv6 address per subnet prefix at first instance creation. Subnets can have more than one IPv6 prefix.

The selected VCN and subnet combination does not support IPv6 addresses. You must enable IPv6 addressing on the VCN and subnet before you can assign IPv6 addresses to this instance.

k. In the *Add SSH key* section, generate an SSH key pair or upload a public key that you already have to connect to the instance using a Secure Shell (SSH) connection.



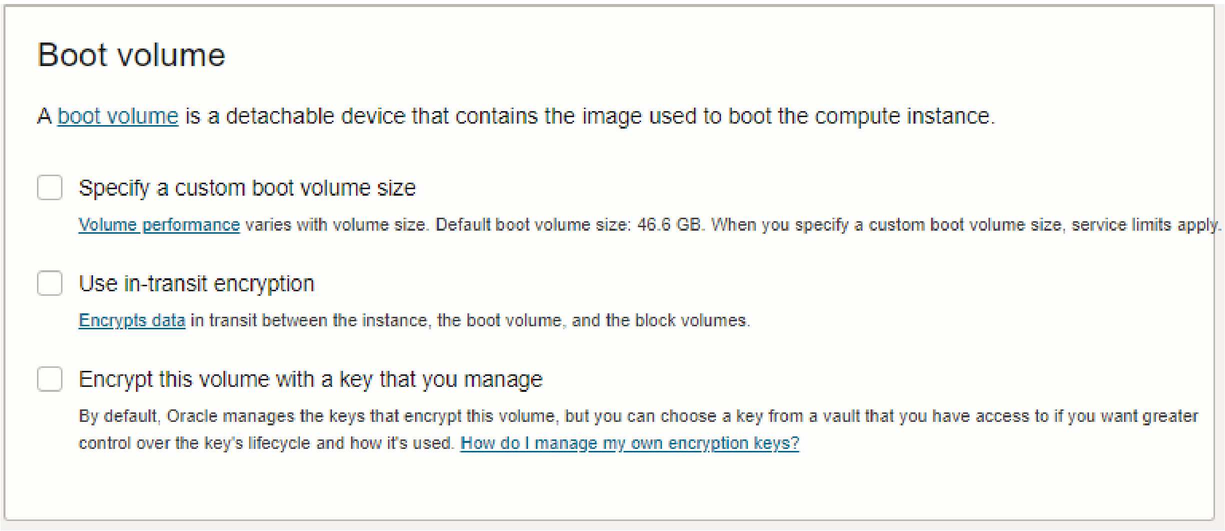
Add SSH keys

Generate an SSH key pair to connect to the instance using a Secure Shell (SSH) connection, or upload a public key that you already have.

● Generate a key pair for me ○ Upload public key files (.pub) ○ 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.

l. In the *Boot volume* section, select an option and configure as needed.



Boot volume

A boot volume is a detachable device that contains the image used to boot the compute instance.

□ Specify a custom boot volume size

Volume performance varies with volume size. Default boot volume size: 46.6 GB. When you specify a custom boot volume size, service limits apply.

□ Use in-transit encryption

Encrypts data in transit between the instance, the boot volume, and the block volumes.

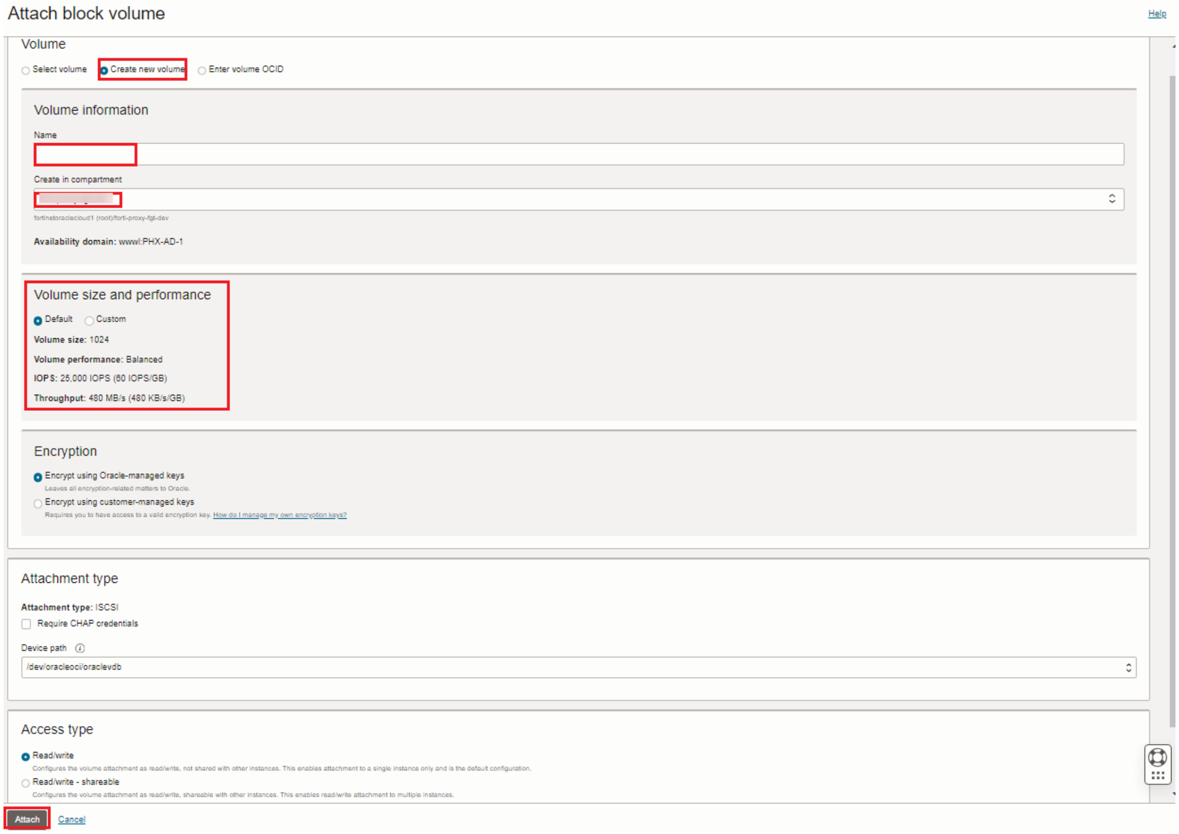
□ Encrypt this volume with a key that you manage

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. How do I manage my own encryption keys?

m. In the *Block volumes* section, add a volume for storing log and web cache data.

  i. Click *Attach block volume*.

  ii. Select an existing block volume or create a new one. The size should be around 50 GB.



Attach block volume

Help

Volume

○ Select volume ● Create new volume ○ Enter volume OCID

Volume information

Name

Create in compartment

[redacted]

fortinetoraclecloud1 (root)/forti-proxy-fgt-dev

Availability domain: wwwl:PHX-AD-1

Volume size and performance

● Default ○ Custom

Volume size: 1024

Volume performance: Balanced

IOPS: 25,000 IOPS (60 IOPS/GB)

Throughput: 480 MB/s (480 KB/s/GB)

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 encryption key. How do I manage my own encryption keys?

Attachment type

Attachment type: ISCSI

□ Require CHAP credentials

Device path

/dev/oracleoci/oraclevdb

Access type

● 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.

Attach Cancel

  iii. Click *Attach*.

n. **(Optional)** Add bootstrapping of FortiProxy CLI commands and a BYOL license at the time of initial bootup as part of instance creation:

i. At the bottom of the page, click *Show Advanced Options*.

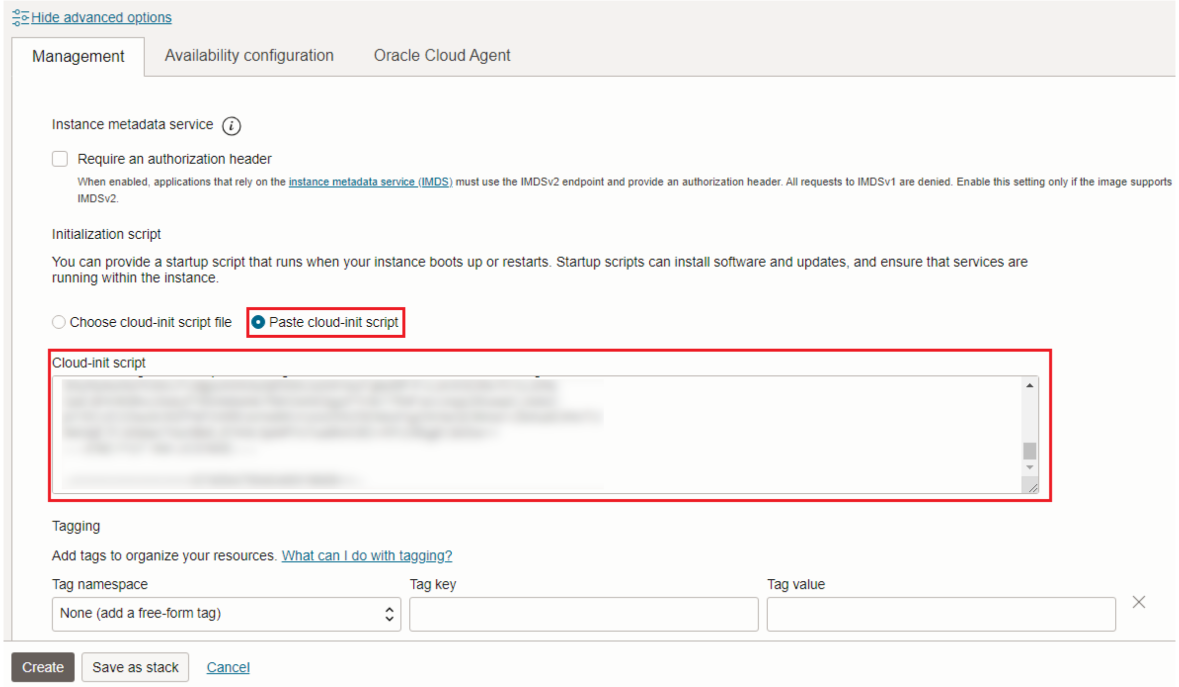
ii. On the *Management* tab, select *Paste cloud-ini script*.

iii. Customize the following sample code (in MIME format) according to your needs.

- Replace the `config system global` commands with your own set of CLI commands as needed. The timezone is set to GMT-9 Alaska in the sample code.
- Replace the license string with the license file content that you download from Customer Service & Support after registering your product code.

```
Content-Type: multipart/mixed; boundary="===============0740947994048919689=="
MIME-Version: 1.0

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config"

config system global
 set timezone 03
end

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license"

-----BEGIN FPX VM LICENSE-----
Replace with your own license file
-----END FPX VM LICENSE-----
```

iv. In the *Cloud-init script* field, enter your custom version of the sample code (including the CLI commands and your license) from the previous step.



Hide advanced options

Management | Availability configuration | Oracle Cloud Agent

Instance metadata service ⓘ

☐ Require an authorization header

When enabled, applications that rely on the instance metadata service (IMDS) must use the IMDSv2 endpoint and provide an authorization header. All requests to IMDSv1 are denied. Enable this setting only if the image supports IMDSv2.

Initialization script

You can provide a startup script that runs when your instance boots up or restarts. Startup scripts can install software and updates, and ensure that services are running within the instance.

○ Choose cloud-init script file ● Paste cloud-init script

Cloud-init script

[redacted]

Tagging

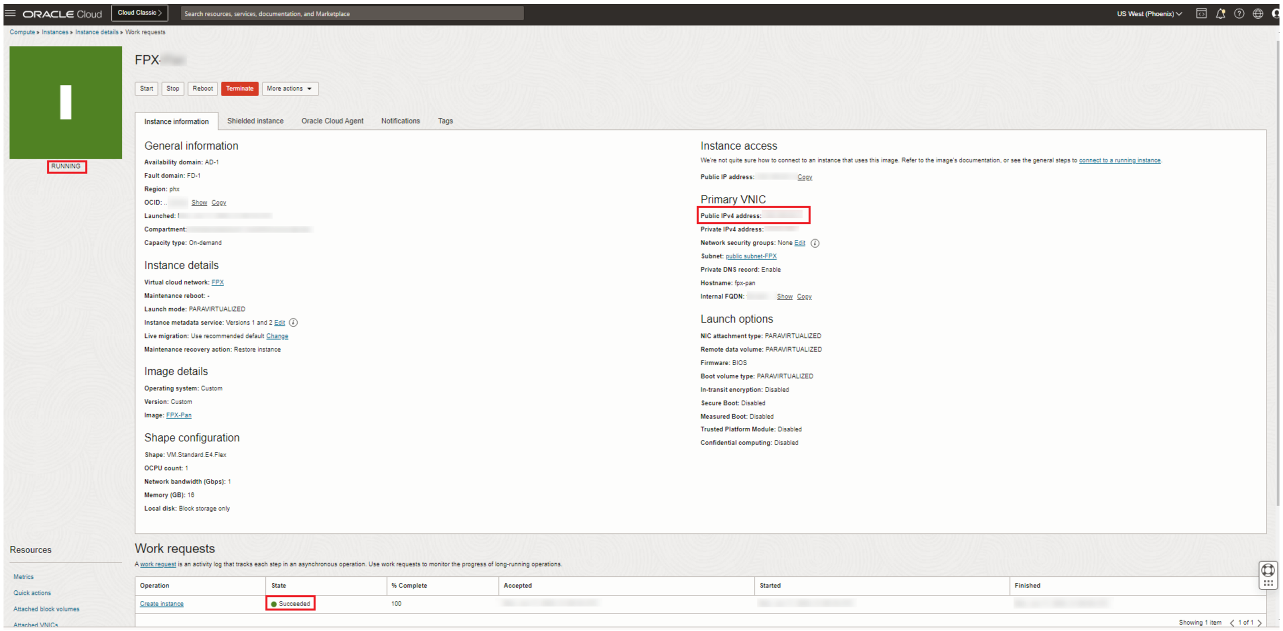
Add tags to organize your resources. What can I do with tagging?

Tag namespace	Tag key	Tag value
None (add a free-form tag)		

Create | Save as stack | Cancel

3. Click *Create*. Wait until the *PROVISIONING…* status changes to *RUNNING* and verify that the *Create instance* operation status changes to *Succeeded*.

   You can also check the FortiProxy's public IP address in this screen once it becomes available.



ORACLE Cloud
Cloud Classic >
Search resources, services, documentation, and Marketplace
US West (Phoenix)
Compute » Instances » Instance details » Work requests

FPX[redacted]

RUNNING

Start | Stop | Reboot | Terminate | More actions

Instance information | Shielded instance | Oracle Cloud Agent | Notifications | Tags

General information

Availability domain: AD-1
Fault domain: FD-1
Region: phx
OCID: [redacted] Show Copy
Launched: [redacted]
Compartment: [redacted]
Capacity type: On-demand

Instance details

Virtual cloud network: FPX
Maintenance reboot: -
Launch mode: PARAVIRTUALIZED
Instance metadata service: Versions 1 and 2 Edit
Live migration: Use recommended default Change
Maintenance recovery action: Restore instance

Image details

Operating system: Custom
Version: Custom
Image: FPX-Pan

Shape configuration

Shape: VM.Standard.E4.Flex
OCPU count: 1
Network bandwidth (Gbps): 1
Memory (GB): 16
Local disk: Block storage only

Instance access

We're not quite sure how to connect to an instance that uses this image. Refer to the image's documentation, or see the general steps to connect to a running instance.

Public IP address: [redacted] Copy

Primary VNIC

Public IPv4 address: [redacted]
Private IPv4 address: [redacted]
Network security groups: None Edit
Subnet: public subnet-FPX
Private DNS record: Enable
Hostname: fpx-pan
Internal FQDN: [redacted] Show Copy

Launch options

NIC attachment type: PARAVIRTUALIZED
Remote data volume: PARAVIRTUALIZED
Firmware: BIOS
Boot volume type: PARAVIRTUALIZED
In-transit encryption: Disabled
Secure Boot: Disabled
Measured Boot: Disabled
Trusted Platform Module: Disabled
Confidential computing: Disabled

Work requests

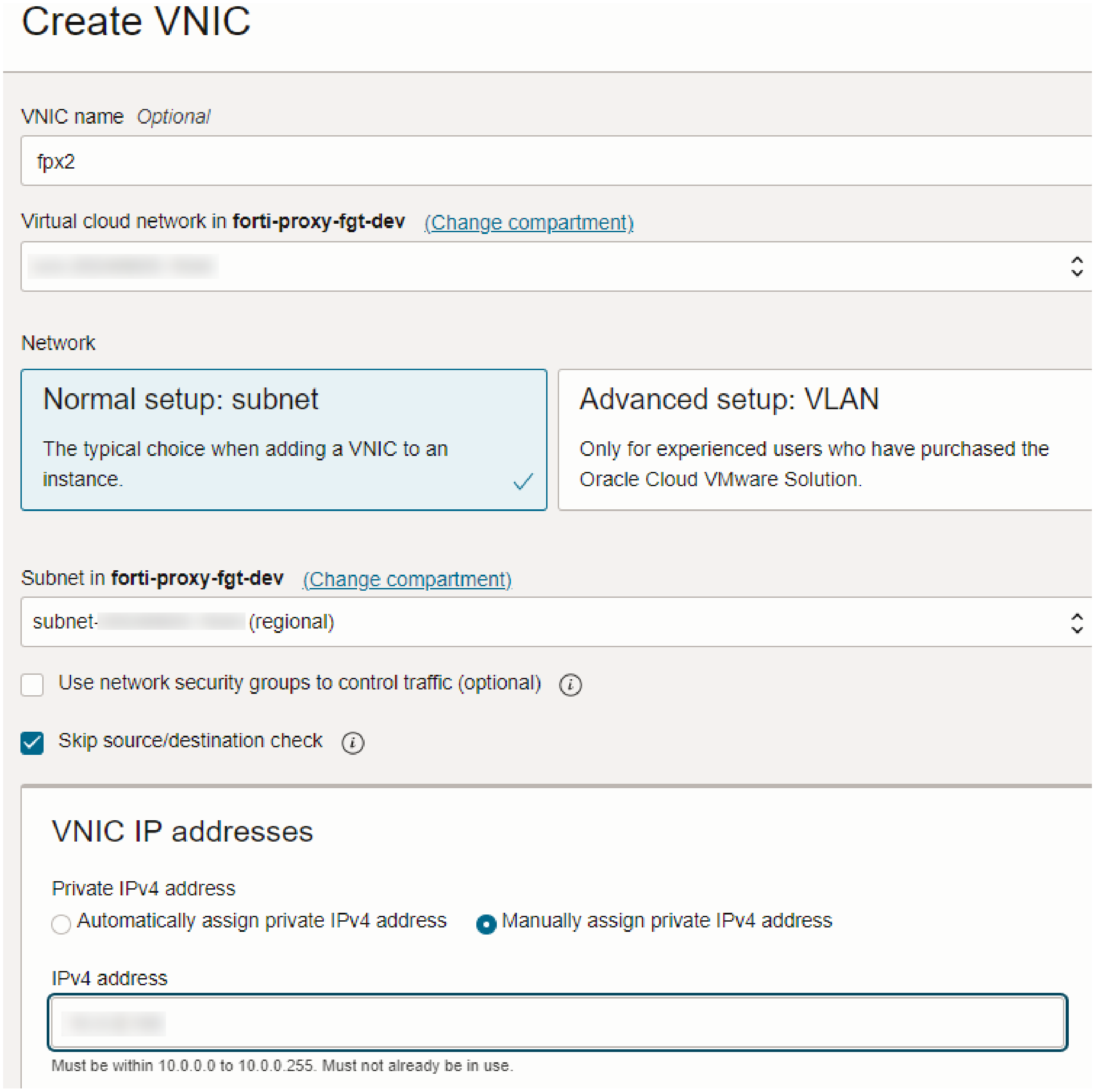
A work request is an activity log that tracks each step in an asynchronous operation. Use work requests to monitor the progress of long-running operations.

Operation	State	% Complete	Accepted	Started	Finished
Create instance	● Succeeded	100	[redacted]	[redacted]	[redacted]

Showing 1 item < 1 of 1 >

   Refer to Accessing the FortiProxy-VM on page 24 for details about how to access the FortiProxy-VM instance.

4. Configure three extra VNICs for the FortiProxy-VM instance by repeating the following steps for each VNIC:
   a. In the FortiProxy-VM instance details page, click *Attached VNICs* > *Create VNIC*.
   b. Create the virtual network interface by specifying the name, VNC, and the subnet created earlier.



Create VNIC

VNIC name *Optional*

fpx2

Virtual cloud network in **forti-proxy-fgt-dev** (Change compartment)

[redacted]

Network

Normal setup: subnet ✓
The typical choice when adding a VNIC to an instance.

Advanced setup: VLAN
Only for experienced users who have purchased the Oracle Cloud VMware Solution.

Subnet in **forti-proxy-fgt-dev** (Change compartment)

subnet-[redacted] (regional)

□ Use network security groups to control traffic (optional) ⓘ

☑ Skip source/destination check ⓘ

VNIC IP addresses

Private IPv4 address

○ Automatically assign private IPv4 address ● Manually assign private IPv4 address

IPv4 address

[redacted]

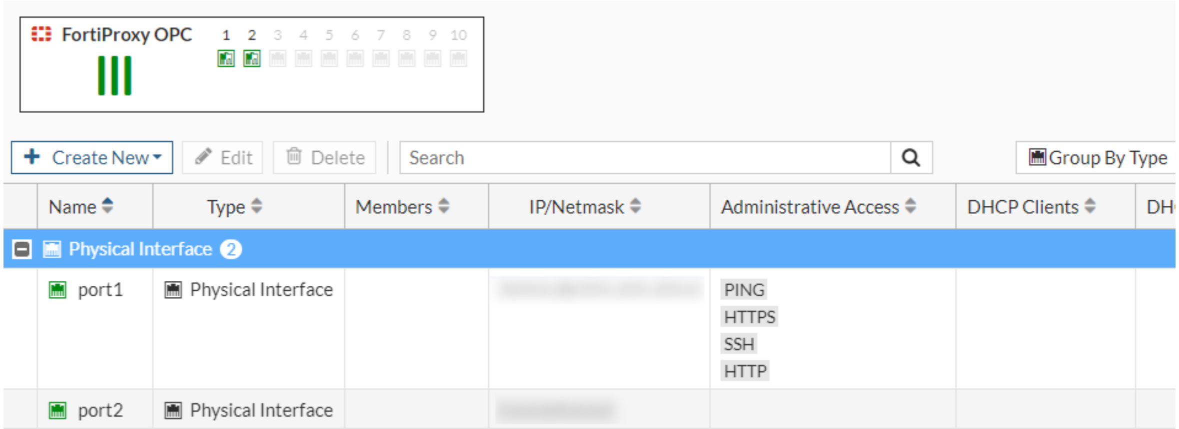
Must be within 10.0.0.0 to 10.0.0.255. Must not already be in use.

c. Select *Skip Source/Destination Check*. Enter an IP address, and click *Save changes*.
The network interface is attached to the FortiProxy-VM.

d. Configure the VNIC in FortiProxy:

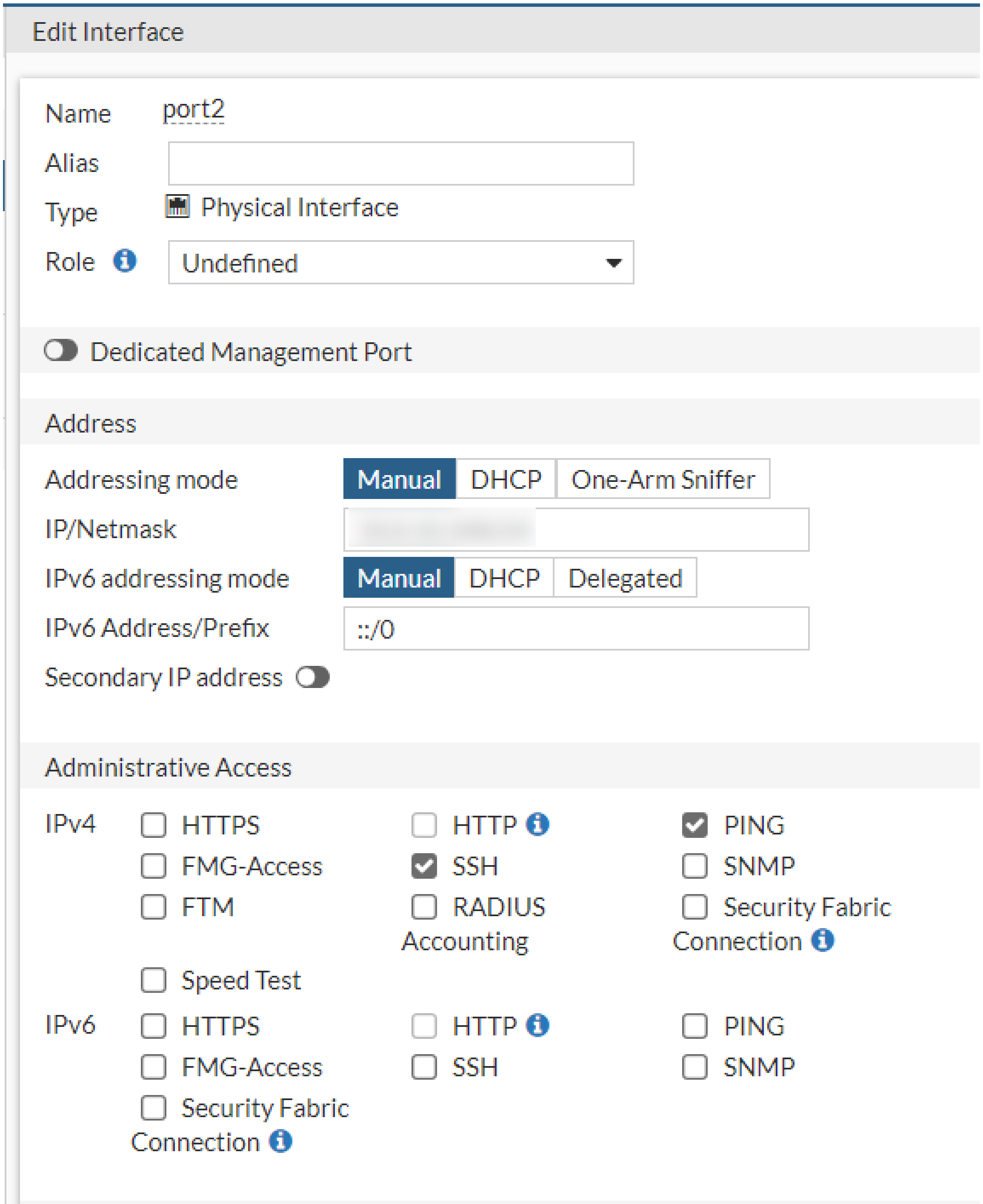
i. Reboot the FortiProxy-VM instance and then log into the GUI console.

ii. In *Network* > *Interfaces*, select the corresponding port (such as port2) and then click *Edit*.



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DH
Physical Interface 2						
port1	Physical Interface		[redacted]	PING HTTPS SSH HTTP		
port2	Physical Interface		[redacted]			

iii. Specify the IP address and netmask as defined in OCIfor the port. Allow administrative access to PING, SSH, and so on as desired. Click *OK*.



Edit Interface

Name	port2
Alias	
Type	Physical Interface
Role	Undefined

○ Dedicated Management Port

Address

Addressing mode	[✓ Manual] DHCP One-Arm Sniffer
IP/Netmask	[redacted]
IPv6 addressing mode	[✓ Manual] DHCP Delegated
IPv6 Address/Prefix	::/0
Secondary IP address	○

Administrative Access

IPv4	□ HTTPS	□ HTTP	☑ PING
	□ FMG-Access	☑ SSH	□ SNMP
	□ FTM	□ RADIUS Accounting	□ Security Fabric Connection
	□ Speed Test		
IPv6	□ HTTPS	□ HTTP	□ PING
	□ FMG-Access	□ SSH	□ SNMP
	□ Security Fabric Connection		

e. Repeat the steps above to create the remaining two interfaces for the FortiProxy-VM instance.

5. Repeat the previous steps to create another FortiProxy-VM instance with four VNICs.

6. Configure route tables:

   a. Go to OCI console, go to *Networking* > *Virtual Cloud Networks* > *Route Tables*.

   b. Configure an internal routing table, setting the default gateway as FPX-A-AD1 NIC2's primary IP address (10.0.12.21). Two subnets, net12-internal and net22-internal, will use this routing table.

c. Configure an external routing table, setting the default gateway as this VCN's Internet gateway. The remaining six subnets use this routing table.

Configuring the OCI HA interfaces

OCI recommends leaving VM NIC interfaces set to DHCP to avoid potential misaligned configurations. However, when configuring an NVA, you need to ignore this recommendation and ensure that the IP addresses correspond with those intended so that the configurations match as required.

In the case of HA, OCI API calls enable the failover through the OCI Fabric connector only for IP addresses configured as secondary in the OCI VNIC. You must configure the FortiProxy-VMs with the correct static IP addresses for proper failover between the two instances. Moreover, API calls initiated from within a VCN must be made by a primary interface with a public address with DNS properly configured.

Fortinet recommends that you perform interface IP address and route configuration via the console as you may lose connection to the instance during the process.

FPX-A

port1

The primary VNIC associated with the FortiProxy NVA must have a primary IP address with a corresponding public IP address, and so needs to be configured in a public subnet. This is used as a management interface and also the interface from which API calls are made. You assign this in the HA configuration. Make sure the FortiProxy-VM port 1 configuration matches the interface's OCI configuration.

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.0.14.21 255.255.255.0
      set allowaccess ping https ssh http fgfm
      set description "management"
      set mtu-override enable
      set mtu 9000
   next
end
```

port2

This example uses port2 as the public/WAN-facing interface.

```
config system interface
   edit "port2"
   set vdom "root"
      set ip 10.0.11.21 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "untrust"
      set secondary-IP enable
      set mtu-override enable
      set mtu 9000
   next
end
```

port3

This example configures port3 as the private port, which the configuration uses to connect to internal resources on local subnets, peered VCNs, and so on. However, as aforementioned, FortiProxy does not use the primary IP address. You must still attach the VNIC to the instance with the primary IP address. However, the configuration is synced from the primary FortiProxy.

```
config system interface
   edit "port3"
      set vdom "root"
      set ip 10.0.12.21 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "trusted"
      set mtu-override enable
      set mtu 9000
   next
end
```

Enabling *Skip Source/Destination Check* for the VNIC is recommended.

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.

```
config system interface
   edit "port4"
      set vdom "root"
      set ip 10.0.13.21 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "heartbeat"
      set mtu-override enable
      set mtu 9000
   next
end
```

FPX-B

For FPX-B, you do not need to configure port2 or port3 as these configurations should sync from FPX-A.

port1

The primary VNIC associated with the FortiProxy NVA must have a primary IP address with a corresponding public IP address, and so must be configured in a public subnet. This is used as a management interface and also the interface from which API calls are made. You assign this in the HA configuration. Make sure the FortiProxy-VM port 1 configuration matches the interface's OCI configuration.

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.0.24.22 255.255.255.0
      set allowaccess ping https ssh http fgfm
      set description "management"
      set mtu-override enable
      set mtu 9000
   next
end
```

port2

You must attach the VNIC to the instance with the primary IP address. However, the FortiProxy syncs the configuration from FPX-A.

port3

You must attach the VNIC to the instance with the primary IP address. However, the FortiProxy syncs the configuration from FPX-A.

port4

This example uses port4 as the HA interface for heartbeat and configuration synchronization. As such, it only needs a single private IP address.

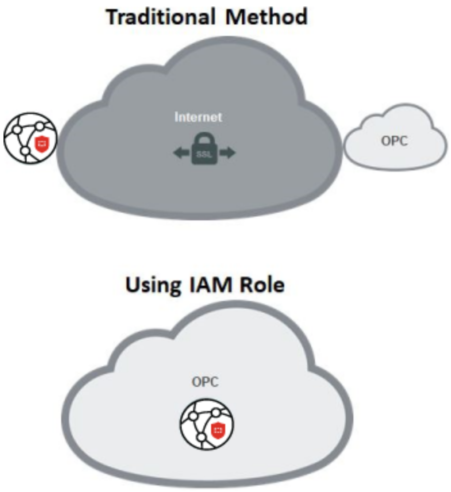
```
config system interface
   edit "port4"
      set vdom "root"
      set ip 10.0.23.22 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "heartbeat"
   next
end
```

Configuring an OCI SND connector

To allow calling APIs to OCI during HA failover, you must configure an OCI SDN connector with HA enabled. The OCI SDN connector can be certificate-based or IAM role-based based on the authentication type:

- A certificate-based OCI SDN connector uses traditional certificate authentication from the FortiProxy-VM to OCI over TCP/IP.
- An IAM-role based OCI SDN connector uses IAM roles to control the permissions to grant to the FortiProxy instance so that the instance can implicitly access metadata information and communicate to the SDN connector on its own private internal network without further authentication.

The following topology compares the two authentication types of the OCI SDN connector:



Creating an OCI SDN connector using certificates

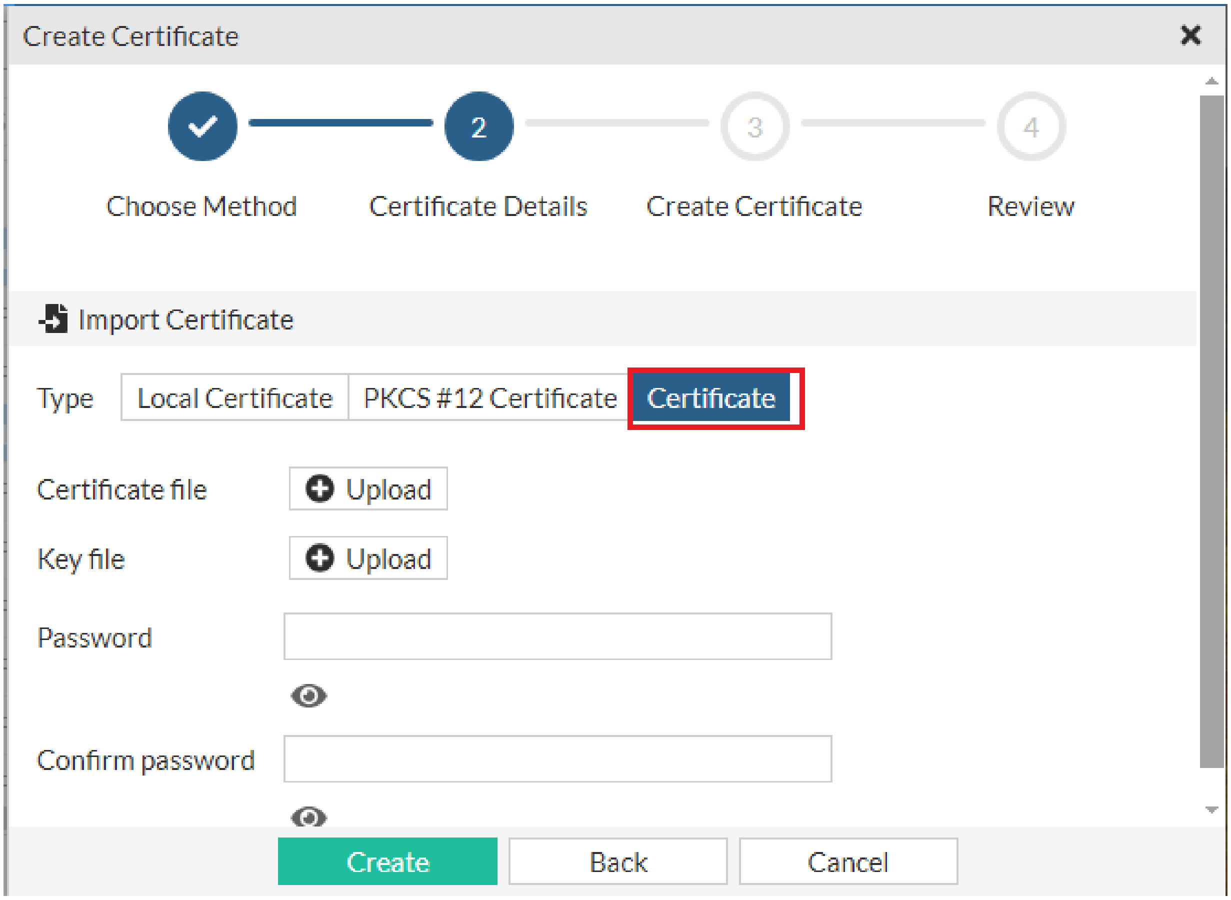
Use the `config system sdn-connector` command to configure a certificate-based OCI SDN connector in FortiProxy. Make sure HA is enabled.

- For `user-id`, specify the OCID of an OCI user that belongs to the administrator group with the following minimum privileges:
  - Allow dynamic-group <group_name> to read compartments in tenancy
  - Allow dynamic-group <group_name> to read instances in tenancy
  - Allow dynamic-group <group_name> to read vnic-attachments in tenancy
  - Allow dynamic-group <group_name> to read private-ips in tenancy
  - Allow dynamic-group <group_name> to read public-ips in tenancy
  - Allow group <group_name> to manage private-ips in tenancy
  - Allow group <group_name> to manage public-ips in tenancy
  - Allow group <group_name> to manage vnics in tenancy
- For `oci-cert`, you can specify the built-in FortiProxy certificate called "Fortinet_Factory" or a custom certificate. To use a custom certificate, you need a certificate file and key file for use on the FortiProxy and a PEM file for use on OCI. The signing algorithm must be RSA SHA-256. For details about the certificates that OCI requires, see Request Signatures.

You may want to switch from the default certificate to a custom one after some time, or if you have multiple sets of A-P HA clusters, you may want to use a different certificate for each cluster initially.

To configure the OCI SND connector to use a custom certificate:

a. Import the certificate to the primary FortiProxy (see Import a local certificate and image below). The secondary FortiProxy will then synchronize the configuration and use the same certificate.



b. Add an API key for the OCI user using the custom certificate's PEM. See the OCI documentation for detailed instructions.

c. Reference the custom certificate in the `oci-cert` option when configuring the OCI SDN connector.

Creating an OCI SDN connector using IAM roles

To configure an OCI SDN connector using IAM roles, complete the following steps:

1. Configure an IAM role on OCI:
   a. In OCI, go to *Compute* > *Instances*, and select the desired FortiProxy-VM instance.
   b. On the *Instance Details* page, note the instance's OCID.
   c. Open the OPC menu and go to *Identity* > *Dynamic Groups*. Create a dynamic group with rules that allow instances that match the FortiProxy-VM's instance ID. Use the syntax "ALL {instance.id ='instanceID'}" when creating the rule. To include multiple instances in the dynamic group, create multiple rules.
   d. Go to *Identity* > *Policies*. Create a policy that allows the dynamic group to manage the environment. This allows the instance referenced in the dynamic group to query metadata and move resources around if the SDN connector is used for HA. In the *STATEMENT* field, use the syntax "Allow dynamic-group <group-name> to manage all-resources in TENANCY".
2. Configure an IAM role-based OCI SDN connector using the `config system sdn-connector` command in FortiProxy. Make sure HA is enabled.

   For `user-id`, specify the OCID of an OCI user that belongs to the administrator group with the following minimum privileges:

- Allow dynamic-group <group_name> to read compartments in tenancy
- Allow dynamic-group <group_name> to read instances in tenancy
- Allow dynamic-group <group_name> to read vnic-attachments in tenancy
- Allow dynamic-group <group_name> to read private-ips in tenancy
- Allow dynamic-group <group_name> to read public-ips in tenancy
- Allow group <group_name> to manage private-ips in tenancy
- Allow group <group_name> to manage public-ips in tenancy
- Allow group <group_name> to manage vnics in tenancy

Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

You can also use resource tags to further control the API calls, as follows:

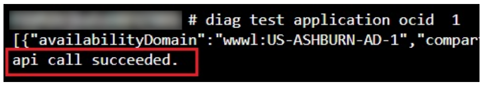
- Allow dynamic-group <group_name> to manage private-ips in tenancy
- Allow dynamic-group <group_name> to manage public-ips in tenancy where any { target.resource.tag.<namespace>.<tag key>= 'value'}
- Allow dynamic-group <group_name> to manage vnics in tenancy where any { target.resource.tag.<namespace>.<tag key>= 'value'}

- If you have security concerns about the policy allowing the dynamic group access to the entire environment, follow the concept of least privileges detailed in the OPC documentation. For example, if you are not using the SDN connector for failover and instead are using it for querying, you can assign the dynamic group read-only permissions.
- Actual role configurations may differ depending on your environments. Check with your company's public cloud administrators for more details.

Troubleshooting SDN connector configuration issues

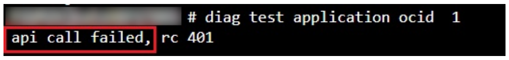
In case of issues with connector configuration, try the following methods to troubleshoot:

- Ensure the SDN connector is connected to OCIby running the `diagnose sys sdn status` command. The output should display that the SDN connector has a connected status.
- Ensure you can successfully call APIs to OCI by running `diagnose test application ocid 1`. The following shows an example of a successful configuration:

  ```
  [redacted] # diag test application ocid  1
  [{"availabilityDomain":"wwwl:US-ASHBURN-AD-1","compar
  api call succeeded.
  ```

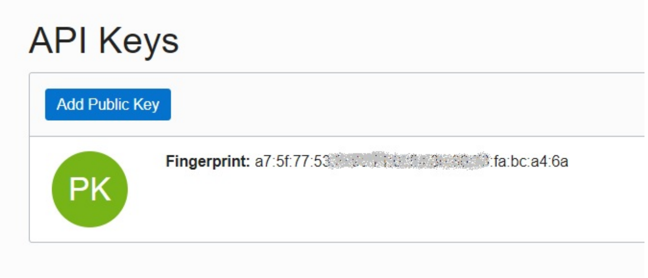
  The following shows an example of a failed configuration:

  ```
  [redacted] # diag test application ocid  1
  api call failed, rc 401
  ```

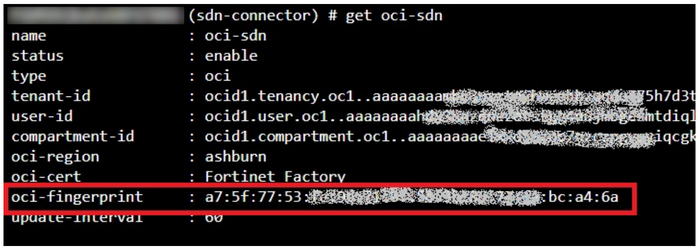
- Check the following to see if you made other unexpected changes:
  - Tenant ID
  - User ID
  - Compartment ID

- Does the specified OCI user belong to the Administrator group on the OCI portal?
- Does the fingerprint on the OCI portal match the one that the specified user has on the FortiProxy-VM? If you change the certificate, its corresponding fingerprint must be updated or added to the OCI user on the OCI portal. In the earlier example, the fingerprint on the OCI portal and the SDN connector settings match.



API Keys

Fingerprint: a7:5f:77:53[redacted]:fa:bc:a4:6a



```
[redacted] (sdn-connector) # get oci-sdn
name                : oci-sdn
status              : enable
type                : oci
tenant-id           : ocid1.tenancy.oc1..aaaaaaaa[redacted]5h7d3t
user-id             : ocid1.user.oc1..aaaaaaaah[redacted]mtdiql
compartment-id      : ocid1.compartment.oc1..aaaaaaaae[redacted]iqcgk
oci-region          : ashburn
oci-cert            : Fortinet Factory
oci-fingerprint     : a7:5f:77:53[redacted]:bc:a4:6a
update-interval     : 60
```

- Does the OCI security list on the Internet-facing subnet allow proper outgoing access from the FortiProxy?

Configuring active-passive HA

This step shows you how to configure A-P HA settings by using CLI commands on the GUI or via SSH.

In the commands, note the following:

- Port4 is the hbdev port used for heartbeat connection.
- For the management interface, you must use port1, as OCI allows only port 1 for metadata access.
- When setting priority on FPX-B, set the priority to 100 (lower than FPX-A's priority level). The node with the lower priority level is determined as the secondary node.
- When setting the unicast heartbeat peer IP address (the last command), this is the IP address on the peer, which in the example is FPX-B, which has port4 IP address 10.0.23.22 in the example. When setting FPX-B's configuration, specify FPX-A's port4 IP address, which is 10.0.13.21.

The following is the primary FortiProxy configuration:

```
config system ha
   set group-id 30
   set group-name "ha-cluster"
   set mode a-p
   set hbdev "port4" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port1"
         set gateway 10.0.14.1
      next
   end
   set override disable
   set priority 200
   set unicast-hb enable
   set unicast-hb-peerip 10.0.23.22
end
```

Once configuration is complete, exit the CLI or SSH session.

The following is the secondary FortiProxy configuration:

```
config system ha
   set group-id 30
   set group-name "ha-cluster"
   set mode a-p
   set hbdev "port4" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port1"
         set gateway 10.0.24.1
      next
   end
   set override disable
   set priority 100
   set unicast-hb enable
   set unicast-hb-peerip 10.0.13.21
end
```

Checking the HA status and function

To check the HA status and function:

1. In FortiProxy on the primary FortiProxy, go to *System* > *HA*. Check that the HA status is synchronized.
2. Create one PC in the internal subnet located in AD1, and another PC in the internal subnet located in AD2. Verify that both PCs can access the Internet via FPX-A-AD1, the current primary node.
3. Shut down FPX-A-AD1.
4. Verify that FPX-B-AD2 becomes the primary FortiProxy.
5. Use an API call to verify that the internal routing table's next hop changed from FPX-A-AD1's internal NIC address (10.0.12.21) to FPX-B-AD2's internal NIC address (10.0.22.22) and that the EIP address attached to FPX-A-AD1's external NIC reattached to FPX-B-AD2's external NIC. You can also use the following diagnose command:

   ```
   # d deb app ocid -1
   Debug messages will be on for 30 minutes.

   # d deb en

   # HA event
   Become HA master mode 2
   Getting oci meta-token
   ```

```
ocid api url: https://auth.us-ashburn-1.oraclecloud.com/v1/x509
ocid collect public ip from OCI
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/publicIps?compartmentId=ocid1.tenancy.oc1..aaaaaaaambr3u
zztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a&scope=REGION&lifetime=RESERVED&limi
t=1000
ocid collect vnics info for instance FPX-B
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/vnicAttachments?compartmentId=ocid1.tenancy.oc1..aaaaaaa
ambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a&instanceId=ocid1.instance.oc1
.iad.abuwcljsdd24ejpo2pvzdtoltfvuil4ss6w2md7k6gc66xzt222546ygc7la
vnic id(1/4):
ocid1.vnic.oc1.iad.abuwcljs76qzu6gmevtzpvl2xpaih3cq6atcvyxbvywezp2rwhdlk6xfhvza
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljs76qzu6gmevt
zpvl2xpaih3cq6atcvyxbvywezp2rwhdlk6xfhvza
vnic id(2/4):
ocid1.vnic.oc1.iad.abuwcljsdka5z6qukwhaeemg5uxn4zqiaksp3gqyezdisxcvvveczcy2di5a
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljsdka5z6qukwh
aeemg5uxn4zqiaksp3gqyezdisxcvvveczcy2di5a
vnic id(3/4):
ocid1.vnic.oc1.iad.abuwcljsoict6e4i3rr4vzl25ogims22b26khe2kroywwdre5ybuvmxqjswq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljsoict6e4i3rr
4vzl25ogims22b26khe2kroywwdre5ybuvmxqjswq
vnic id(4/4):
ocid1.vnic.oc1.iad.abuwcljs72l3az24q4ellxxde7533bcvz6tebfdzzmi2henh4acwrpl5kjbq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljs72l3az24q4e
llxxde7533bcvz6tebfdzzmi2henh4acwrpl5kjbq
instance: FPX-B
    vnic: 10.0.24.22(129.213.188.144)
    vnic: 10.0.21.22
    vnic: 10.0.22.22
    vnic: 10.0.23.22
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/subnets/ocid1.subnet.oc1.iad.aaaaaaaaz5htioi34gbwpm4ib6t
54lhdsmwlp6gpwygo4joy2zqhtc4jzswq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/subnets?compartmentId=ocid1.tenancy.oc1..aaaaaaaambr3uzz
toyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a&vcnId=ocid1.vcn.oc1.iad.aaaaaaaa5dfd4
ud7pceb5uykemraiddojlgk3qsibvm2sectfvmpeuta73ha
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocid1.subnet.oc
1.iad.aaaaaaaajjdbd62mq2kqfy7ncjada5i4pvnfyuuwrwqri763illanlyh3y3a
ocid api url: https://iaas.us-ashburn-
```

```
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocid1.subnet.oc
1.iad.aaaaaaaaz5htioi34gbwpm4ib6t54lhdsmwlp6gpwygo4joy2zqhtc4jzswq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocid1.subnet.oc
1.iad.aaaaaaaagypiubrwowu4cy3khyo23uxqcnrftdizqzmbrdwpx2qoxediub2q
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocid1.subnet.oc
1.iad.aaaaaaaalk3n5o74urfjbg5q77owicsahhc34fjdsmlyq5r7auuzpbhknj7a
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocid1.subnet.oc
1.iad.aaaaaaaaep4y5zoaotwpjlyrxtvucrkshappytdw2ktdw5kwpplykg2h57ya
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?ipAddress=10.0.13.21&subnetId=ocid1.subnet.oc
1.iad.aaaaaaaafn3wl6kuh5fbaqsggfezgxkhqagduo2lxw6my5wb4hrywd7s73fq
ocid found peer heart beat ip 10.0.13.21 in subnet net13-heartbeat
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/vnicAttachments?compartmentId=ocid1.tenancy.oc1..aaaaaaa
ambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a&vnicId=ocid1.vnic.oc1.iad.abu
wcljtqtujnevzbifkcvv6c4itt3xmrn6gr57qps2v2w7ccwfrijrdmkhq
ocid collect vnics info for peer instance
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/vnicAttachments?compartmentId=ocid1.tenancy.oc1..aaaaaaa
ambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a&instanceId=ocid1.instance.oc1
.iad.abuwcljt5zkznwtdirurbeqhpeuh5ktcizg2srdn6segjebphejscoj2y6la
vnic id(1/4):
ocid1.vnic.oc1.iad.abuwcljtqtujnevzbifkcvv6c4itt3xmrn6gr57qps2v2w7ccwfrijrdmkhq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljtqtujnevzbif
kcvv6c4itt3xmrn6gr57qps2v2w7ccwfrijrdmkhq
vnic id(2/4):
ocid1.vnic.oc1.iad.abuwcljt5aj42rcy6yrpmfmhem7wiboiargdlvdfnskg5jkqc426gukhavdq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljt5aj42rcy6yr
pmfmhem7wiboiargdlvdfnskg5jkqc426gukhavdq
vnic id(3/4):
ocid1.vnic.oc1.iad.abuwcljtzdqf5rhpvcbhzm7gxgvmzu5xm34eo6kiaxtea5l5f4qwhskw6nbq
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljtzdqf5rhpvcb
hzm7gxgvmzu5xm34eo6kiaxtea5l5f4qwhskw6nbq
vnic id(4/4):
ocid1.vnic.oc1.iad.abuwcljtpw6tkr3jevqd52b3sg4f5rkzqoyd4zegimdqkqa4ualwe5cnat4q
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/privateIps?vnicId=ocid1.vnic.oc1.iad.abuwcljtpw6tkr3jevq
d52b3sg4f5rkzqoyd4zegimdqkqa4ualwe5cnat4q
instance:
    vnic: 10.0.14.21(129.213.181.141)
    vnic: 10.0.11.21(129.213.191.163)
    vnic: 10.0.12.21
    vnic: 10.0.13.21
checking ip: 10.0.21.22 in port2
ocid failover public ip 129.213.191.163 from 10.0.11.21 to 10.0.21.22
ocid updating public ip 129.213.191.163 with data: {"privateIpId":
"ocid1.privateip.oc1.iad.abuwcljsvgcf5narv2qgmbc5djv43qci6heja3lxamtch24qhp5vzizwbs
na"}
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/publicIps/ocid1.publicip.oc1.iad.aaaaaaaaucxuvfvi2tyl222
ib4mcluori5fofovq2lqkowy7eikwhaaijdnq
ocid assigned public ip 129.213.191.163 to private ip 10.0.21.22 successfully
checking ip: 10.0.22.22 in port3
ocid collect route table info from vcn
ocid1.vcn.oc1.iad.aaaaaaaa5dfd4ud7pceb5uykemraiddojlgk3qsibvm2sectfvmpeuta73ha
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/routeTables?compartmentId=ocid1.tenancy.oc1..aaaaaaaambr
3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a&vcnId=ocid1.vcn.oc1.iad.aaaaaaaa5
dfd4ud7pceb5uykemraiddojlgk3qsibvm2sectfvmpeuta73ha
route table: rtb-internal
    rule: 0.0.0.0/0, next hop: 10.0.12.21
ocid update next hop from 10.0.12.21 to 10.0.22.22 in route table rtb-internal
ocid updating route table rtb-internal with data: {"routeRules": [{"destination":
"0.0.0.0/0", "destinationType": "CIDR_BLOCK", "networkEntityId":
"ocid1.privateip.oc1.iad.abuwcljstkyb7gvv5lyrf3ugb4mqbmmugijl6zpcbtr2cht4tsggqlq6e4
fq"}]}
ocid api url: https://iaas.us-ashburn-
1.oraclecloud.com/20160918/routeTables/ocid1.routetable.oc1.iad.aaaaaaaapxqqkjnznvk
qvhcbghotxzfzy7umjgg4jtg7z6o2s5dcmjsmmmta
ocid update route table rtb-internal successfully
HA event
```

6. Log into both PCs created in step 2. Verify that each PC can access the Internet via FPX-B-AD2, the new primary node.

www.fortinet.com