FortiOS - OCI Cookbook

Version 6.2

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

December 08, 2020
FortiOS 6.2 OCI Cookbook
01-620-544730-20201208

TABLE OF CONTENTS

About FortiGate-VM for OCI

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate Next Generation Firewall (NGFW) technology delivers complete content and network protection. This solution is available for deployment on Oracle Cloud Infrastructure (OCI).

In addition to advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, features including application control, firewall, antivirus, IPS, web filter, and VPN work in concert to identify and mitigate the latest complex security threats.

FortiGate-VM for OCI supports active/passive high availability (HA) configuration with FortiGate-native unicast HA synchronization between the primary and secondary nodes. When the FortiGate-VM detects a failure, the passive firewall instance becomes active and uses OCI API calls to configure its interfaces/ports.

Highlights of FortiGate-VM for OCI include the following:

- Delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.
- IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- New Docker application control signatures protect your container environments from newly emerged security threats. See FortiGate-VM on a Docker environment.

Instance type support

You can deploy FortiGate for OCI as a virtual machine (VM), and supported instances are the standard types.

Supported instances may change without notice. For up-to-date information on each instance type, see the following:

- Virtual Machine Features
- Fortinet FortiGate-VM Next-Generation Firewall (NGFW) v5.6/v6.0 for OCI

Models

FortiGate-VM is available with different CPU and RAM sizes. You can deploy FortiGate-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 Order types on page 7.

1 OCPU is typically equivalent to 2 vCPU as mentioned in the Oracle Cloud Infrastructure Compute Classic FAQ.

Model name	vCPU	
	Minimum	Maximum
FG-VM02/02v/02s	1	2
FG-VM04/04v/04s	1	4
FG-VM08/08v/08s	1	8
FG-VM16/16v/16s	1	16
FG-VM32/32v/32s	1	32
FG-VMUL/ULv/ULs	1	Unlimited

The v-series and s-series do not support virtual domains (VDOMs) by default. To add VDOMs, you must separately purchase perpetual VDOM addition licenses. You can add and stack VDOMs up to the maximum supported number after initial deployment.

FortiOS 6.2.3 and later versions support the S-series licensing.

Generally there are RAM size restrictions to FortiGate BYOL licenses. However, these restrictions do not apply to OCI deployments. Any RAM size with certain CPU models are allowed. Licenses are based on the number of CPUs only.

Previously, platform-specific models such as FortiGate for OCI with an OCI-specific orderable menu existed. However, the common model now applies to all supported platforms.

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

The primary requirement for the provisioning of a virtual FortiGate may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, the options with a high number of interfaces tend to have high numbers of vCPUs.

The licensing for FortiGate-VM does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs indicated by the license does not restrict the FortiGate from working, regardless of how many vCPUs are included in the virtual instance. However, only the licensed number of vCPUs process traffic and management. The rest of the vCPUs are unused.

The following shows an example for FGT-VM08:

License	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	The FortiGate-VM uses eight vCPUs for traffic and management. It does not use the rest.	The FortiGate-VM uses eight vCPUs for traffic and management. It does not use the rest.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

Licensing

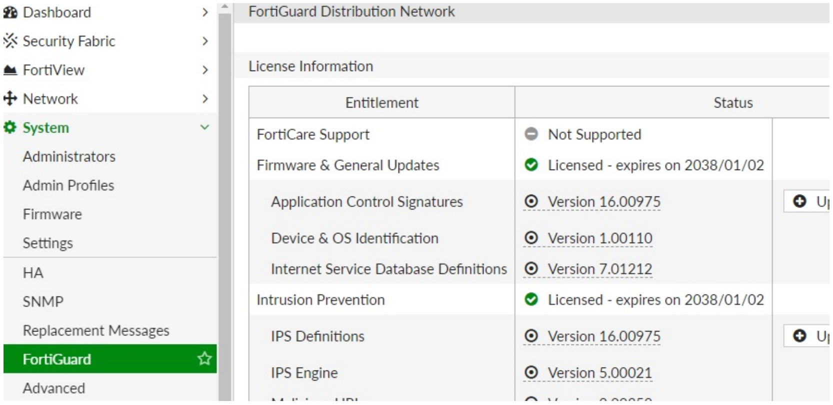
You must have a license to deploy FortiGate-VM for OCI. The following sections provide information on licensing FortiGate-VM for OCI:

Order types

OCI supports BYOL and PAYG licensing.

BYOL offers perpetual (normal series and v-series) and annual subscription (s-series, available starting Q4 2019) licensing as opposed to PAYG, which is an hourly subscription available with marketplace-listed products. BYOL licenses are available for purchase from resellers or your distributors, and prices are listed in the publicly available price list that is updated quarterly. 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.

When using a FortiGate-VM PAYG instance, the GUI may display expiry dates for FortiGuard services. However, these expiries are automatically extended for as long as the PAYG instance's lifespan. You do not need to be concerned about the expiry of FortiGuard services. For example, the following screenshot shows 2038/01/02.



Entitlement	Status	
FortiCare Support	Not Supported	
Firmware & General Updates	Licensed - expires on 2038/01/02	
Application Control Signatures	Version 16.00975	Up
Device & OS Identification	Version 1.00110	
Internet Service Database Definitions	Version 7.01212	
Intrusion Prevention	Licensed - expires on 2038/01/02	
IPS Definitions	Version 16.00975	Up
IPS Engine	Version 5.00021	

Creating a support account

FortiGate-VM for OCI supports BYOL and PAYG licensing models.

For BYOL, you typically order a combination of products and services, including support entitlement. PAYG includes support, for which you must contact Fortinet Support with your customer information.

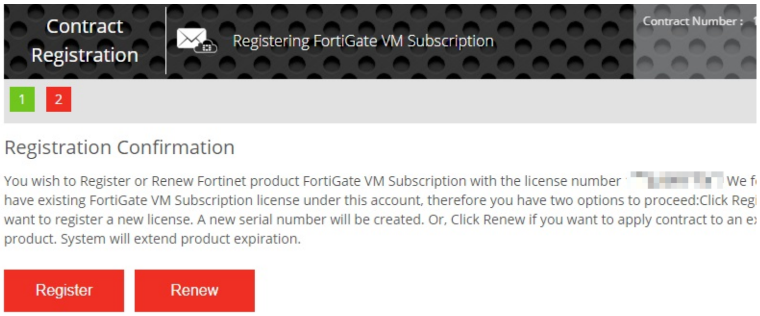
You must create a FortiCare support account and obtain a license to activate the product through the FortiCare support portal. If you have not activated the license, you will see the license upload screen when logging into the FortiGate-VM and cannot proceed to configure the FortiGate-VM. See Registering and downloading licenses on page 8.

Registering and downloading licenses

You can obtain licenses for the BYOL licensing model through any Fortinet partner. After you purchase a license or obtain an evaluation license (60-day term), you receive a PDF with an activation code.

To register and download a license:

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Go to *Asset* > *Register/Activate* to start the registration process.
3. In the *Specify Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.
4. If you register the S-series subscription model, the site prompts you to select one of the following:
   a. Click *Register* to newly register the code to acquire a new serial number with a new license file.
   b. Click *Renew* to renew and extend the licensed period on top of the existing serial number, so that all features on the VM node continue working uninterrupted upon license renewal.



Registration Confirmation

You wish to Register or Renew Fortinet product FortiGate VM Subscription with the license number [redacted] We f
have existing FortiGate VM Subscription license under this account, therefore you have two options to proceed:Click Regi
want to register a new license. A new serial number will be created. Or, Click Renew if you want to apply contract to an e
product. System will extend product expiration.

5. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiGate-VM. After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

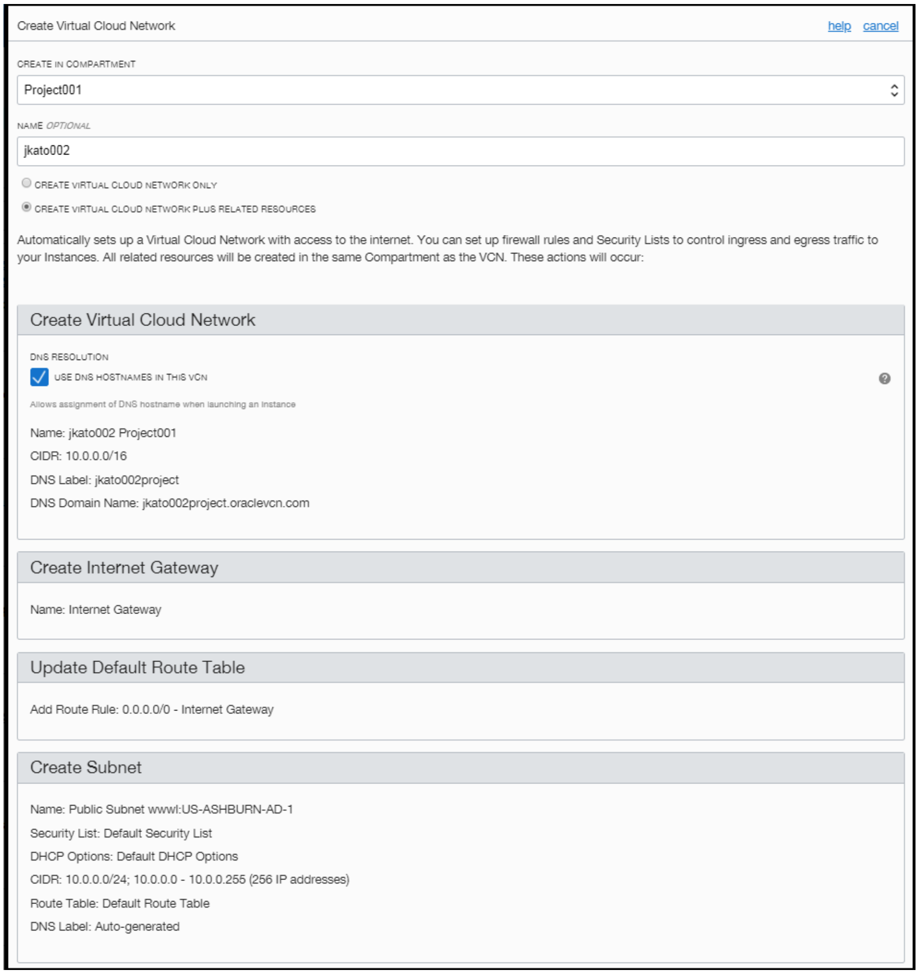
Single FortiGate-VM deployment

Deploying FortiGate-VM in paravirtualized or emulated mode

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

To create a VCN and public-facing subnets:

1. In OCI, go to *Networking* > *Virtual Cloud Networks*, and click *Create Virtual Cloud Network*.
2. In the *NAME* field, enter the VCN name. Then, select *CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES*. This allows you to create the Internet gateway, routing table, and subnet all together using Oracle default settings. If you intend to create each resource separately by specifying your own inputs, click *CREATE VIRTUAL CLOUD NETWORK ONLY*. This example uses the first choice.



Create Virtual Cloud Network

CREATE IN COMPARTMENT: Project001

NAME *OPTIONAL*: jkato002

○ CREATE VIRTUAL CLOUD NETWORK ONLY

● CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES

Automatically sets up a Virtual Cloud Network with access to the internet. You can set up firewall rules and Security Lists to control ingress and egress traffic to your Instances. All related resources will be created in the same Compartment as the VCN. These actions will occur:

Create Virtual Cloud Network

DNS RESOLUTION

☑ USE DNS HOSTNAMES IN THIS VCN

Allows assignment of DNS hostname when launching an instance

Name: jkato002 Project001

CIDR: 10.0.0.0/16

DNS Label: jkato002project

DNS Domain Name: jkato002project.oraclevcn.com

Create Internet Gateway

Name: Internet Gateway

Update Default Route Table

Add Route Rule: 0.0.0.0/0 - Internet Gateway

Create Subnet

Name: Public Subnet wwwl:US-ASHBURN-AD-1

Security List: Default Security List

DHCP Options: Default DHCP Options

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

Route Table: Default Route Table

DNS Label: Auto-generated

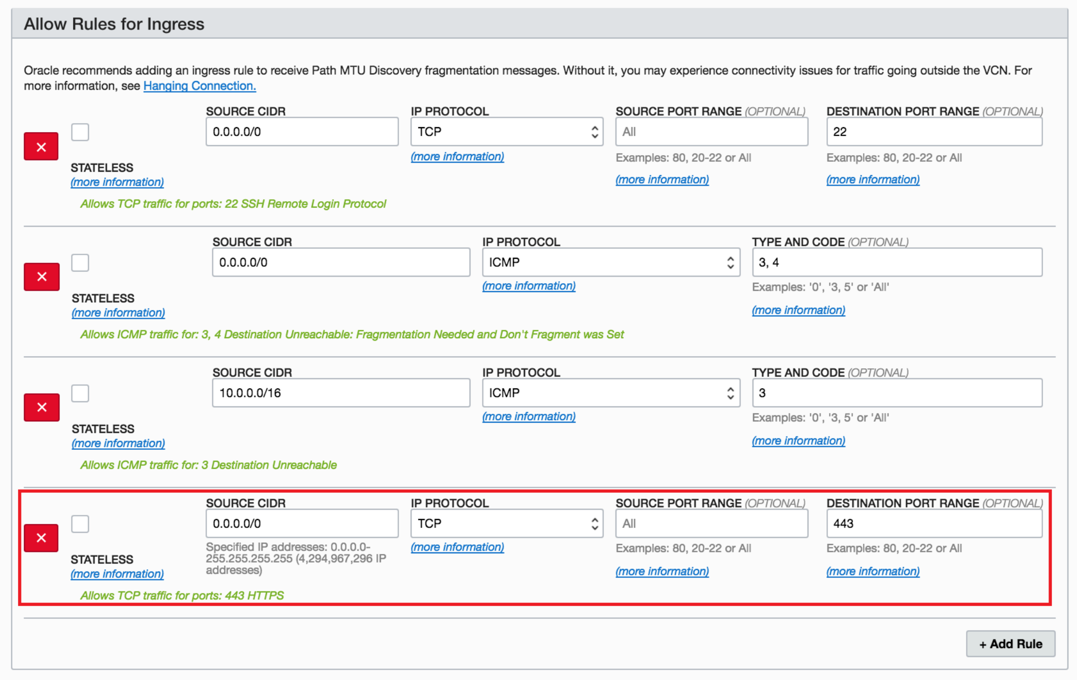
3. Click *Create Virtual Cloud Network* at the bottom of the screen.
   This configures the related resources. There are three subnets, each of which will belong to an AD. They can be defined as public-facing networks (connecting to the Internet). In this example, (1) is 10.0.x.x/24. You can access

the FortiGate over the Internet once it is deployed via HTTPS through the GUI management screen or via SSH.

Creating a security list

To create a security list:

1. Click *Default Security List* for the 10.0.0.0/24 subnet, which you defined as the network's public side. By default, port 22 is allowed.
2. Click *Edit all Rules* > *Add Rule*. Manually add a rule to allow TCP port 443.



Allow Rules for Ingress

Oracle recommends adding an ingress rule to receive Path MTU Discovery fragmentation messages. Without it, you may experience connectivity issues for traffic going outside the VCN. For more information, see Hanging Connection.

☐ STATELESS (more information) — SOURCE CIDR: 0.0.0.0/0 — IP PROTOCOL: TCP (more information) — SOURCE PORT RANGE (OPTIONAL): All, Examples: 80, 20-22 or All (more information) — DESTINATION PORT RANGE (OPTIONAL): 22, Examples: 80, 20-22 or All (more information)

Allows TCP traffic for ports: 22 SSH Remote Login Protocol

☐ STATELESS (more information) — SOURCE CIDR: 0.0.0.0/0 — IP PROTOCOL: ICMP (more information) — TYPE AND CODE (OPTIONAL): 3, 4, Examples: '0', '3, 5' or 'All' (more information)

Allows ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set

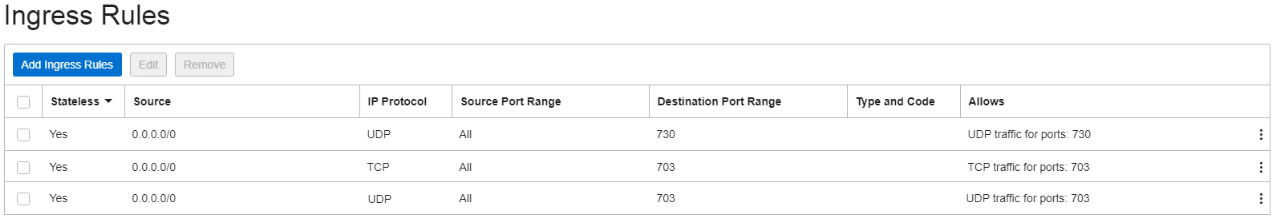
☐ STATELESS (more information) — SOURCE CIDR: 10.0.0.0/16 — IP PROTOCOL: ICMP (more information) — TYPE AND CODE (OPTIONAL): 3, Examples: '0', '3, 5' or 'All' (more information)

Allows ICMP traffic for: 3 Destination Unreachable

☐ STATELESS (more information) — 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 (more information) — SOURCE PORT RANGE (OPTIONAL): All, Examples: 80, 20-22 or All (more information) — DESTINATION PORT RANGE (OPTIONAL): 443, Examples: 80, 20-22 or All (more information)

Allows TCP traffic for ports: 443 HTTPS

For a full list of ports that you must allow for the FortiGate-VM instance, see FortiGate open ports. For example, for Heartbeat sync ports, the security list must have the following:



Ingress Rules

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

3. Click *Save Security List Rules*.

Creating a route table for the internal network

To create a route table for the internal network:

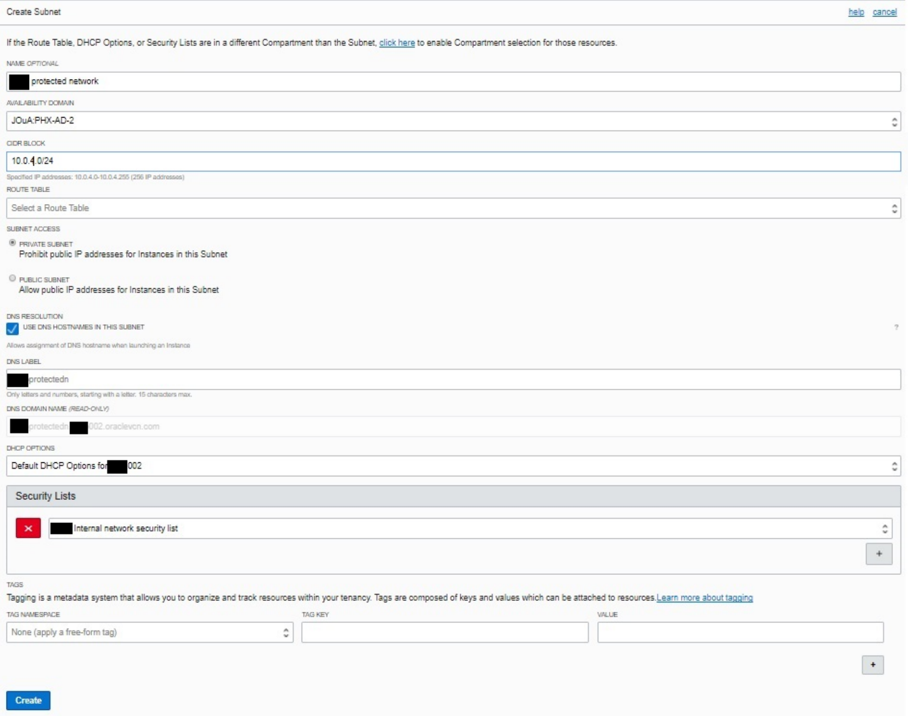
1. You must change the default gateway for the protected network and point it to the FortiGate-VM's second network interface. Go to *Route Tables* > *Create Route Table*.

2. For all destinations, choose *Internet Gateway* for now. You will change the configuration later. Click *Create Route Table*.

Creating an internal network subnet

To create an internal network subnet:

1. Create an internal protected network, where VMs will be placed under the FortiGate-VM's protection. Click *Create Subnet*.
2. Create the internal protected network in the AD where the FortiGate-VM is located. Choose the appropriate domain in use, then enter the internal subnet. The route table must be the one created earlier for the internal network. Under *SUBNET ACCESS*, select *PRIVATE SUBNET*. You can select any security list as desired. In the example, a security list that allows all protocols for any source and destination was selected. You must create the security list prior to this configuration.



Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, click here to enable Compartment selection for those resources.

NAME *OPTIONAL*: [redacted] protected network

AVAILABILITY DOMAIN: JOuA:PHX-AD-2

CIDR BLOCK: 10.0.4.0/24

Specified IP addresses: 10.0.4.0-10.0.4.255 (256 IP addresses)

ROUTE TABLE: Select a Route Table

SUBNET ACCESS

● PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

○ PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

☑ USE DNS HOSTNAMES IN THIS SUBNET

Allows assignment of DNS hostname when launching an Instance

DNS LABEL: [redacted]protectedn

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

DNS DOMAIN NAME *(READ-ONLY)*: [redacted]protectedn.[redacted]002.oraclevcn.com

DHCP OPTIONS: Default DHCP Options for [redacted]002

Security Lists: [redacted] Internal network security list

TAGS

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

TAG NAMESPACE: None (apply a free-form tag)

TAG KEY:

VALUE:

Creating a FortiGate-VM instance

There are two methods of creating the FortiGate-VM instance. Select one of the following methods:

- The first method consists of obtaining the deployment image file, importing the file into the OCI portal, then launching the FortiGate-VM instance. See Creating an instance by importing an image file on page 12.
- The second method consists of pointing to an available FortiGate-VM image on OCI instead of importing one. See Creating an instance by selecting an OCI partner image on page 15.

You can also add bootstrapping of FortiGate CLI commands and a BYOL license at the time of initial bootup as part of instance creation, as described in (Optional) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 18. This step is optional and can be included as part of either creation method.

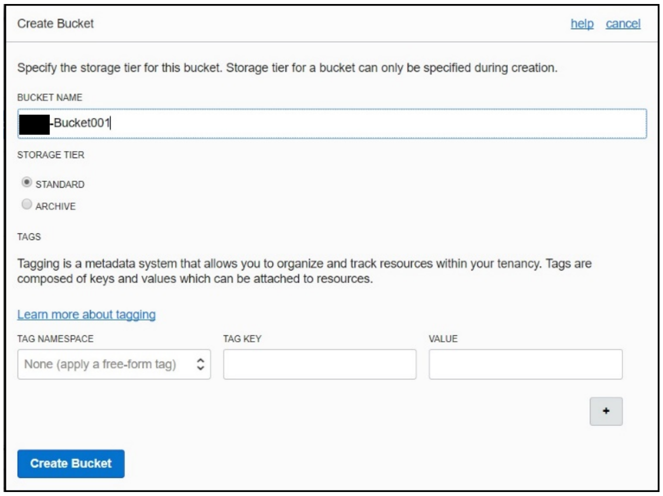
Once you have completed using either method to create a FortiGate-VM, continue to Attaching storage to the FortiGate-VM on page 19.

Creating an instance by importing an image file

To create a FortiGate-VM instance by importing an image file, follow these steps:

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

1. Obtain the deployment image file:
   - **a.** Go to Customer Service & Support. Go to *Download* > *VM Images* in the top menu.
   - **b.** In the *Select Product* dropdown list, select *FortiGate*.
   - **c.** In the *Select Platform* dropdown list, select *Oracle*.
   - **d.** Obtain the *FGT_VM64_OPC-vX-buildXXXX-FORTINET.out.OpenXen.zip* file. XXXX is the build number. Ensure that the file name includes OpenXen.
   - **e.** After downloading, unzip the file. You will find the *forties.qcow2* file, which is needed to deploy the FortiGate-VM on OCI.
2. In OCI, go to *Object Storage*, then click *Create Bucket* to create a standard storage bucket.
3. Configure the standard storage bucket as shown:



Create Bucket

Specify the storage tier for this bucket. Storage tier for a bucket can only be specified during creation.

BUCKET NAME: [redacted]-Bucket001

STORAGE TIER

● STANDARD

○ ARCHIVE

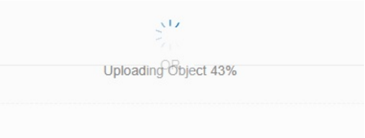
TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

Learn more about tagging

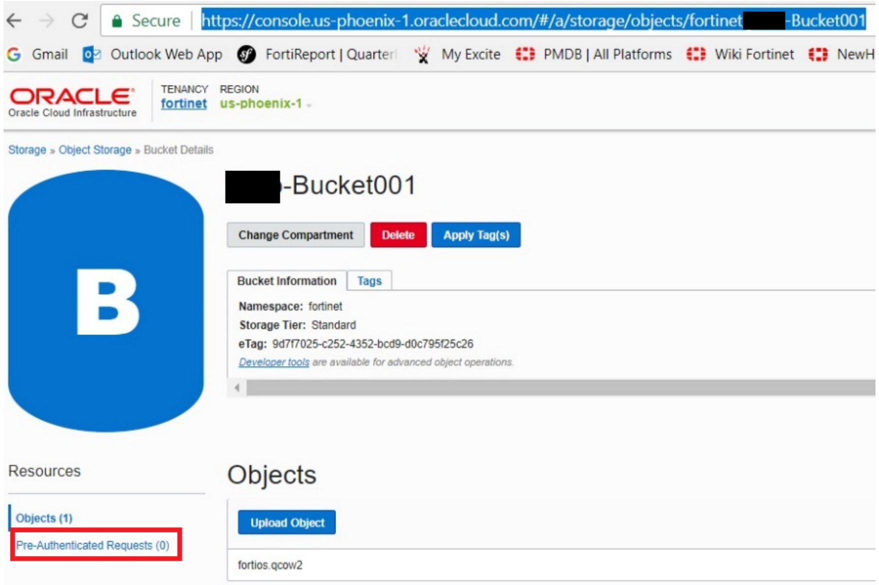
TAG NAMESPACE	TAG KEY	VALUE
None (apply a free-form tag)		

4. Select the bucket, then click *Upload Object* to upload the deployment image file *forties.qcow2*. The dialog shows the upload progress.



Uploading Object 43%

5. Once uploaded, the following screen appears. Click *Create Pre-Authenticated Requests*.



https://console.us-phoenix-1.oraclecloud.com/#/a/storage/objects/fortinet[redacted]-Bucket001

TENANCY fortinet REGION us-phoenix-1

[redacted]-Bucket001

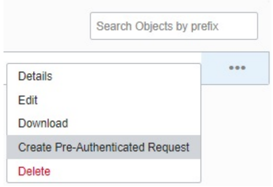
Namespace: fortinet

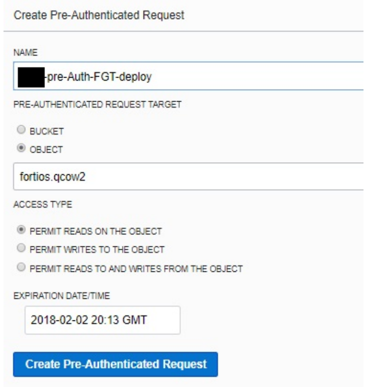
Storage Tier: Standard

eTag: 9d7f7025-c252-4352-bcd9-d0c795f25c26

Developer tools are available for advanced object operations.

fortios.qcow2





Create Pre-Authenticated Request

NAME

[redacted]-pre-Auth-FGT-deploy

PRE-AUTHENTICATED REQUEST TARGET

○ BUCKET

● OBJECT

fortios.qcow2

ACCESS TYPE

● PERMIT READS ON THE OBJECT

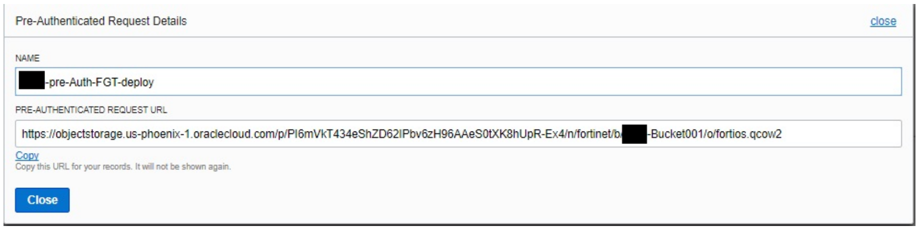
○ PERMIT WRITES TO THE OBJECT

○ PERMIT READS TO AND WRITES FROM THE OBJECT

EXPIRATION DATE/TIME

2018-02-02 20:13 GMT

6. Note down this URL. Further steps require it.



Pre-Authenticated Request Details

NAME

[redacted]-pre-Auth-FGT-deploy

PRE-AUTHENTICATED REQUEST URL

https://objectstorage.us-phoenix-1.oraclecloud.com/p/PI6mVkT434eShZD62IPbv6zH96AAeS0tXK8hUpR-Ex4/n/fortinet/b/[redacted]-Bucket001/o/fortios.qcow2

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

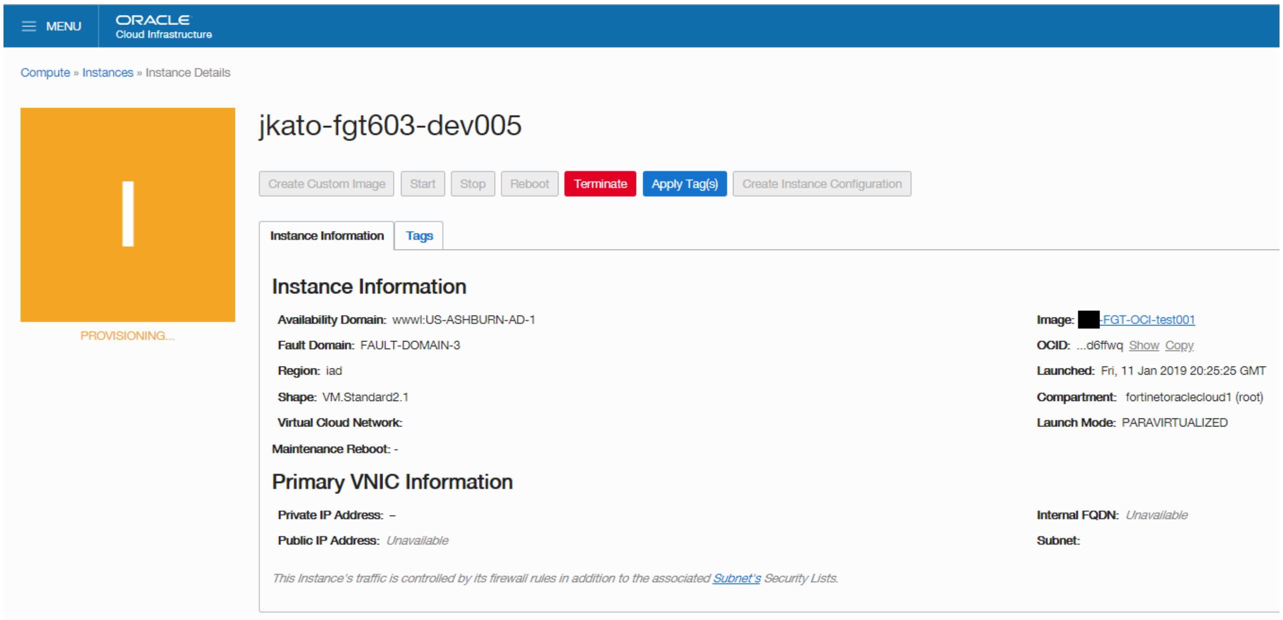
To import the image:

1. Go to *Compute* > *Custom Images*. Click *Import Image*.
2. In the *Import Image* dialog, complete the fields. In the *OBJECT STORAGE URL* field, enter the URL link obtained earlier and place it in your bucket.

3. Under *IMAGE TYPE*, select *QCOW2*.
4. Under *LAUNCH MODE*, select *PARAVIRTUALIZED MODE* or *EMULATED MODE*.
5. You have now imported the image. Wait until the *IMPORTING...* status changes to *AVAILABLE*.

To create the FortiGate-VM instance:

1. From the newly imported image, click *Create Instance*.
2. Configure the parameters:
   - a. In the *Name your instance* field, enter the desired name to identify the instance by.
   - b. Under *Select an availability domain for your instance*, select the desired domain.
   - c. Under *Choose instance type*, select *Virtual Machine*.
   - d. Under *Choose instance shape*, select one of the supported instance shapes. Currently, FortiGate-VM supports the Standard1 and Standard2 instance families.
   - e. In the *Virtual cloud network* field, select a network to launch the instance.
   - f. In the *Subnet* field, select a subnet on the Internet-facing side of the network.
   - g. Click *Show Advanced Options*.
   - h. On the *Management* tab, if you want to add bootstrapping of FortiGate CLI commands and a BYOL license, follow the instructions in (Optional) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 18, then copy and paste all of the text content (CLI commands and license) under *User Data*. Modify the text as needed.
   - i. On the *Networking* tab, in the *Private IP address* field, specify a static IP address within the selected subnet.
   - j. Ensure *Assign public IP address* is selected so you can access the FortiGate-VM over the Internet. You can disable this once you have configured everything as desired.
   - k. In the *Hostname* field, enter the desired name.
3. Click *Create*. Wait until the *PROVISIONING…* status changes to *RUNNING*. You can also check the FortiGate's public IP address in this screen once it becomes available.



jkato-fgt603-dev005

Instance Information

Availability Domain: wwwl:US-ASHBURN-AD-1
Fault Domain: FAULT-DOMAIN-3
Region: iad
Shape: VM.Standard2.1
Virtual Cloud Network:
Maintenance Reboot: -

Image: [redacted]-FGT-OCI-test001
OCID: ...d6ffwq Show Copy
Launched: Fri, 11 Jan 2019 20:25:25 GMT
Compartment: fortinetoraclecloud1 (root)
Launch Mode: PARAVIRTUALIZED

Primary VNIC Information

Private IP Address: –
Public IP Address: *Unavailable*

Internal FQDN: *Unavailable*
Subnet:

This Instance's traffic is controlled by its firewall rules in addition to the associated Subnet's Security Lists.

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

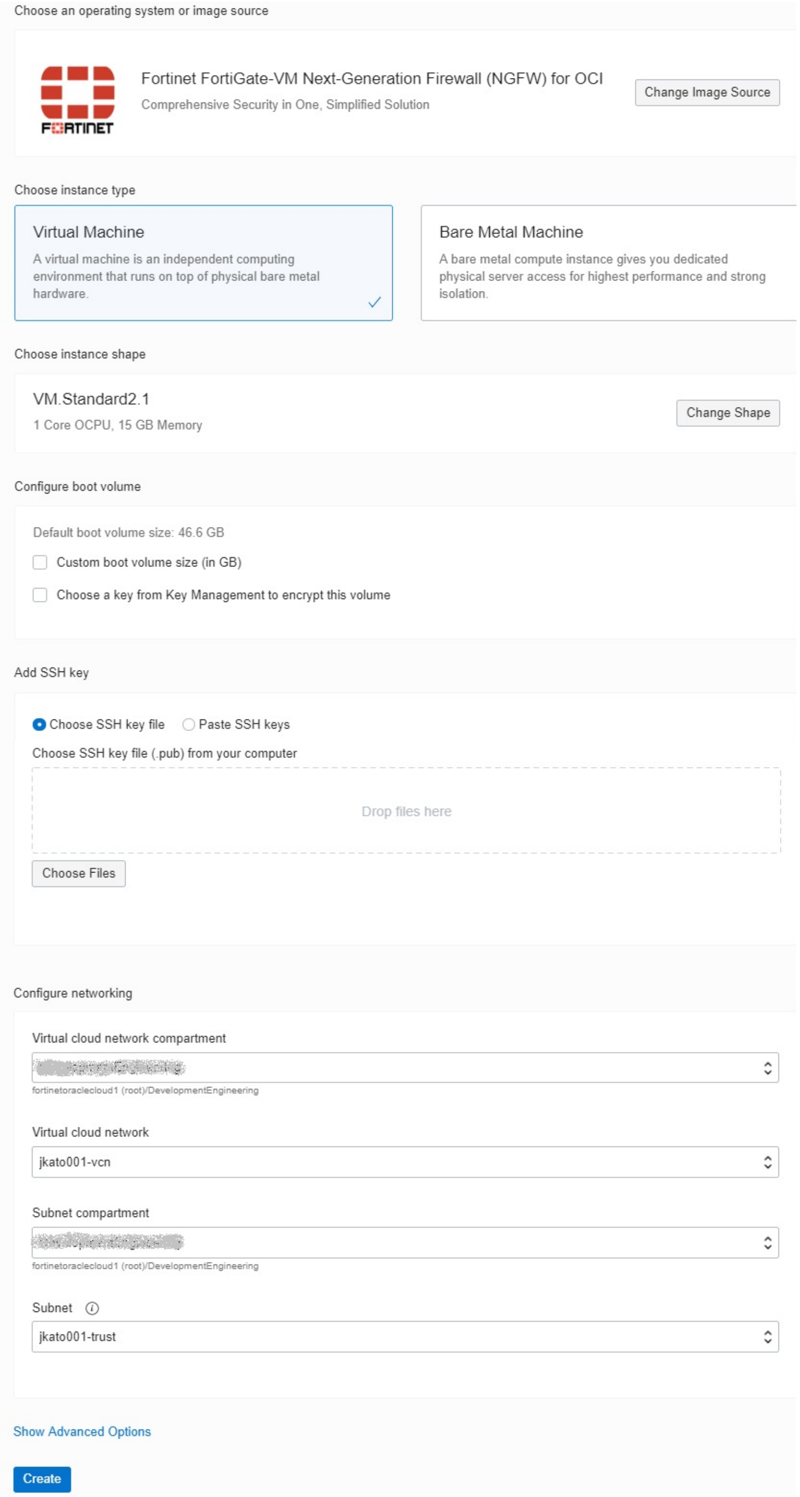
Creating an instance by selecting an OCI partner image

This section describes an alternative method of deploying a single FortiGate-VM instance. OCI's partner image catalog lists FortiGate deployment images. You can create the instance by pointing to an available image instead of importing one yourself.

To create an instance by selecting an OCI partner image:

1. In OCI, click *Create Instance*.
2. Name the instance as desired.
3. Under *Choose an operating system or image source*, click *Change Image Source*.
4. In the *Browse All Images* window, go to the *Partner Images* tab. Select the FortiGate app, then select an image/build from the *Image build* dropdown list. Select the checkbox at the bottom of the window to confirm that you have read and agree to the terms of use, then click *Select Image*.
5. Configure the parameters as follows:
   a. Under *Choose instance shape*, select one of the supported instance shapes.
   b. Under *Configure boot volume* and *Add SSH key*, keep the default values.

c. Under *Configure networking*, configure the options as required.



Choose an operating system or image source

Fortinet FortiGate-VM Next-Generation Firewall (NGFW) for OCI

Comprehensive Security in One, Simplified Solution

Choose instance type

Virtual Machine ✓

A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

Bare Metal Machine

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

Choose instance shape

VM.Standard2.1

1 Core OCPU, 15 GB Memory

Configure boot volume

Default boot volume size: 46.6 GB

□ Custom boot volume size (in GB)

□ Choose a key from Key Management to encrypt this volume

Add SSH key

● Choose SSH key file ○ Paste SSH keys

Choose SSH key file (.pub) from your computer

Drop files here

Configure networking

Virtual cloud network compartment

[redacted]

fortinetoraclecloud1 (root)/DevelopmentEngineering

Virtual cloud network

jkato001-vcn

Subnet compartment

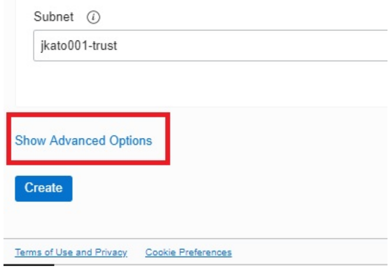
[redacted]

fortinetoraclecloud1 (root)/DevelopmentEngineering

Subnet ⓘ

jkato001-trust

d. Click *Show Advanced Options*.



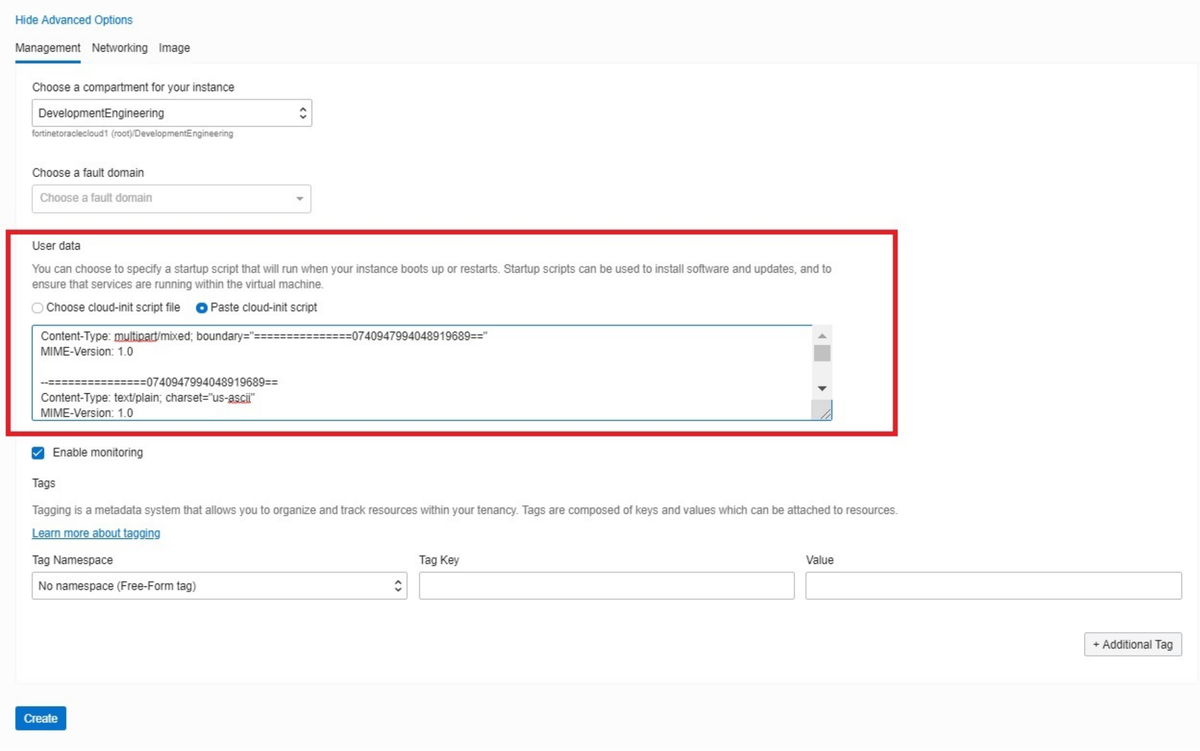
Subnet ⓘ

jkato001-trust

Show Advanced Options

Create

e. On the *Management* tab, if you want to add bootstrapping of FortiGate CLI commands and a BYOL license, follow the instructions in (Optional) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 18, then copy and paste all of the text content (CLI commands and license) under *User Data*. Modify the text as needed.



Hide Advanced Options

Management Networking Image

Choose a compartment for your instance

DevelopmentEngineering

fortinetoraclecloud1 (root)/DevelopmentEngineering

Choose a fault domain

Choose a fault domain

User data

You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine.

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

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

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
```

☑ Enable monitoring

Tags

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

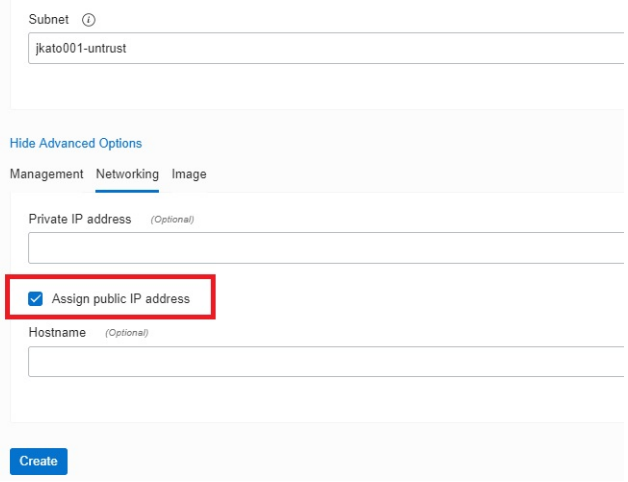
Learn more about tagging

Tag Namespace	Tag Key	Value
No namespace (Free-Form tag)		

+ Additional Tag

Create

f. On the *Networking* tab, ensure that *Assign public IP address* is enabled.



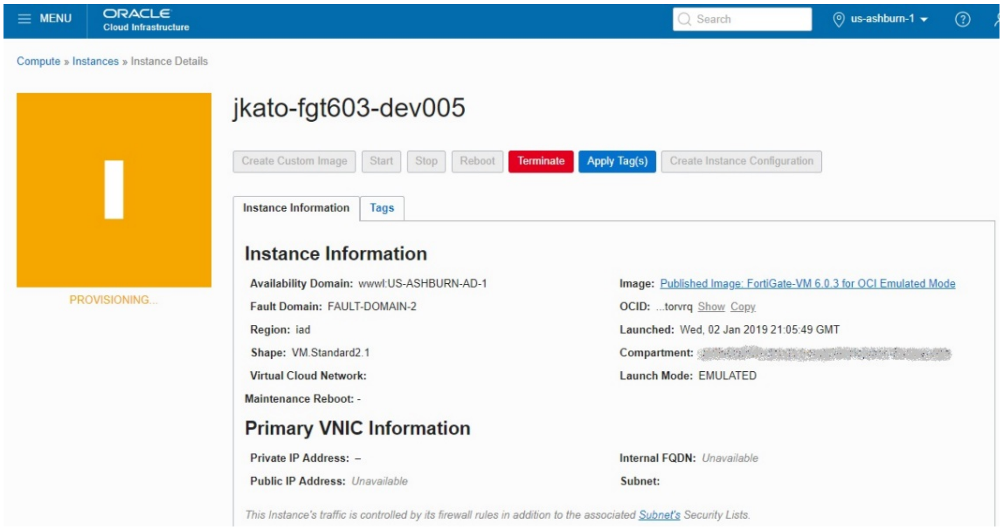
Subnet: jkato001-untrust

Private IP address (Optional)

☑ Assign public IP address

Hostname (Optional)

6. Click *Create*. This deploys the FortiGate-VM instance.



jkato-fgt603-dev005

Instance Information

Availability Domain: wwwl:US-ASHBURN-AD-1
Fault Domain: FAULT-DOMAIN-2
Region: iad
Shape: VM.Standard2.1
Virtual Cloud Network:
Maintenance Reboot: -

Image: Published Image: FortiGate-VM 6.0.3 for OCI Emulated Mode
OCID: ...torvrq Show Copy
Launched: Wed, 02 Jan 2019 21:05:49 GMT
Compartment: [redacted]
Launch Mode: EMULATED

Primary VNIC Information

Private IP Address: –
Public IP Address: *Unavailable*

Internal FQDN: *Unavailable*
Subnet:

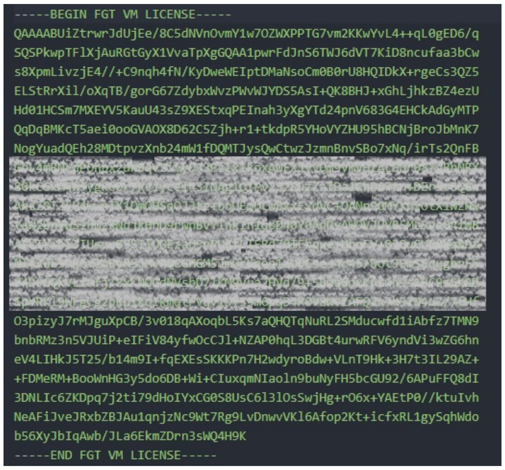
This Instance's traffic is controlled by its firewall rules in addition to the associated Subnet's Security Lists.

(Optional) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup

This section explains how to add bootstrapping of FortiGate CLI commands and a BYOL license at the time of initial bootup as part of instance creation on the OCI GUI console.

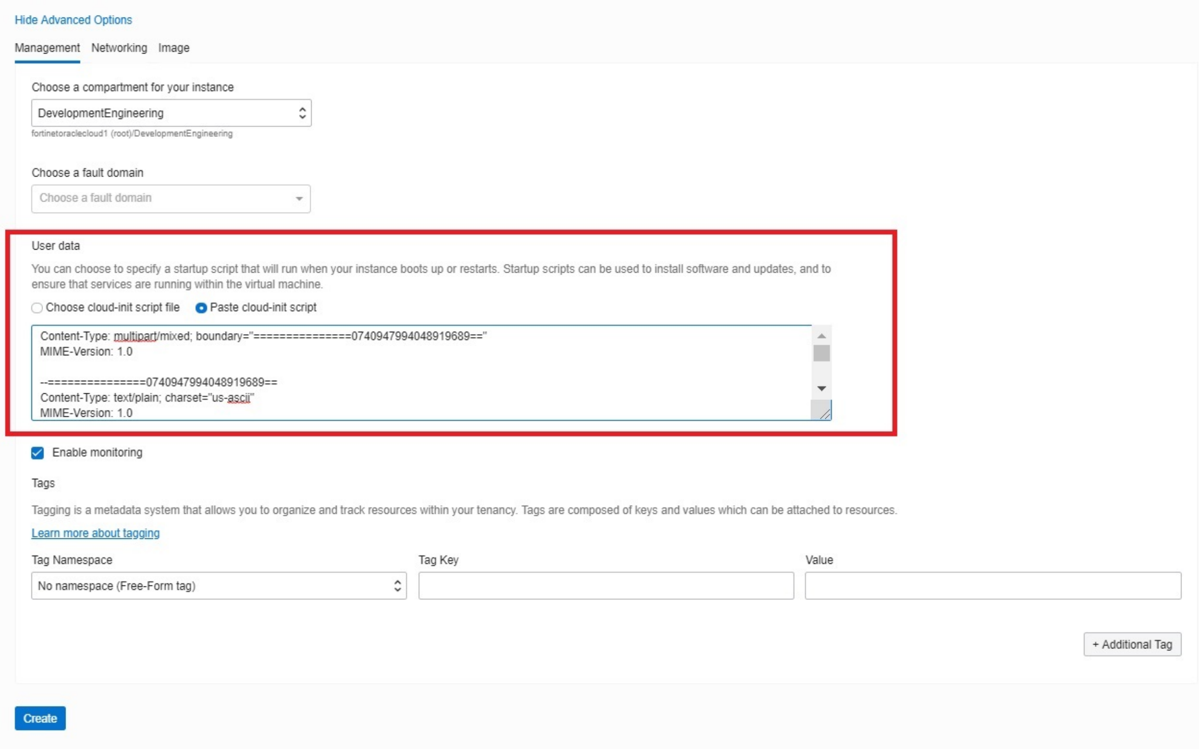
1. Refer to sample text content available on GitHub. This content is in MIME format.
2. This example uses the following CLI commands:
```
config system global
   set timezone 03
end
```
This example CLI sets the timezone as GMT-9 Alaska. You can replace these lines with your own set of CLI commands.
3. Download a FortiGate-VM license file from Customer Service & Support after registering your product code. In the sample text found in step 1, find the following lines:
```
20 -----BEGIN FGT VM LICENSE-----
21 Replace with your own
22 -----END FGT VM LICENSE-----
```

Replace these lines with the license file content. FortiGate-VM license content resembles the following:



```
-----BEGIN FGT VM LICENSE-----
QAAAABUiZtrwrJdUjEe/8C5dNVnOvmY1w7OZWXPPTG7vm2KKwYvL4++qL0gED6/q
SQSPkwpTFlXjAuRGtGyX1VvaTpXgGQAA1pwrFdJnS6TWJ6dVT7KiD8ncufaa3bCw
s8XpmLivzjE4//+C9nqh4fN/KyDweWEIptDMaNsoCm0B0rU8HQIDkX+rgeCs3QZ5
ELStRrXil/oXqTB/gorG67ZdybxWvzPWvWJYDS5AsI+QK8BHJ+xGhLjhkzBZ4ezU
Hd01HCSm7MXEYV5KauU43sZ9XEStxqPEInah3yXgYTd24pnV683G4EHCkAdGyMTP
QqDqBMKcT5aei0ooGVAOX8D62C5Zjh+r1+tkdpR5YHoVYZHU95hBCNjBroJbMnK7
NogYuadQEh28MDtpvzXnb24mW1fDQMTJysQwCtwzJzmnBnvSBo7xNq/irTs2QnFB
[redacted]
O3pizyJ7rMJguXpCB/3v018qAXoqbL5Ks7aQHQTqNuRL2SMducwfd1iAbfz7TMN9
bnbRMz3n5VJUiP+eIFiV84yfwOcCJl+NZAP0hqL3DGBt4urwRFV6yndVi3wZG6hn
eV4LIHkJ5T25/b14m9I+fqEXEsSKKKPn7H2wdyroBdw+VLnT9Hk+3H7t3IL29AZ+
+FDMeRM+BooWnHG3y5do6DB+Wi+CIuxqmNIaoln9buNyFH5bcGU92/6APuFFQ8dI
3DNLIc6ZKDpq7j2ti79dHoIYxCG0S8UsC6l3lOsSwjHg+rO6x+YAEtP0//ktuIvh
NeAFiJveJRxbZBJAu1qnjzNc9Wt7Rg9LvDnwvVKl6Afop2Kt+icfxRL1gySqhWdo
b56XyJbIqAwb/JLa6EkmZDrn3sWQ4H9K
-----END FGT VM LICENSE-----
```

You will copy and paste this content into the OCI GUI during instance creation in *Advanced Options* > *Management* > *User data*. See steps 2h in To create the FortiGate-VM instance: on page 14 or 5e in Creating an instance by selecting an OCI partner image on page 15.



Choose a compartment for your instance

DevelopmentEngineering

fortinetoraclecloud1 (root)/DevelopmentEngineering

Choose a fault domain

Choose a fault domain

User data

You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine.

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

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

--===============0740947994048919689==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
```

☑ Enable monitoring

Tags

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

Learn more about tagging

Tag Namespace	Tag Key	Value
No namespace (Free-Form tag)		

Attaching storage to the FortiGate-VM

To attach storage to the FortiGate-VM:

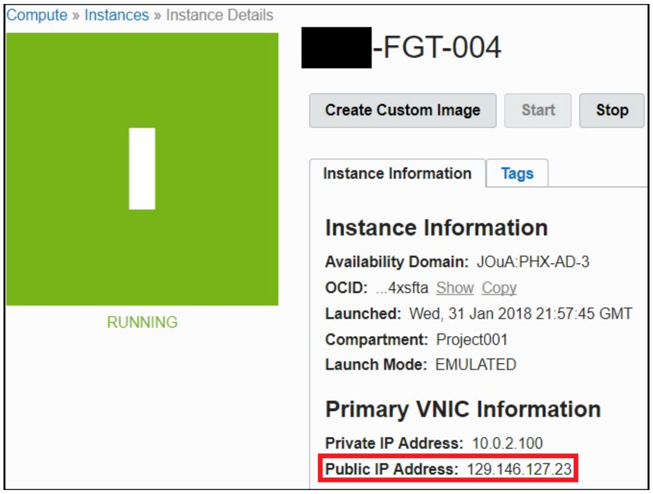
1. Go to *Storage* > *Block Volumes* > *Create Block Volume*.
2. Enter a unique name, choose the AD, then specify the size to around 50 GB. Click *Create Block Volume*. This provisions the volume.

3. Once provisioned, return to the FortiGate-VM instance. Click *Attach Block Volume*.
4. Under *Choose how you want to attach your block volume*, select *EMULATED*.
5. After attaching the block volume, ensure you reboot the FortiGate-VM instance.

Accessing the FortiGate-VM

To access the FortiGate-VM:

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



[redacted]-FGT-004

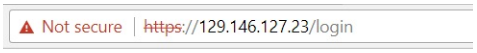
Instance Information

Availability Domain: JOuA:PHX-AD-3
OCID: ...4xsfta Show Copy
Launched: Wed, 31 Jan 2018 21:57:45 GMT
Compartment: Project001
Launch Mode: EMULATED

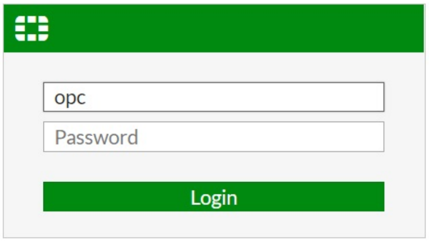
Primary VNIC Information

Private IP Address: 10.0.2.100
Public IP Address: 129.146.127.23

2. In a browser, go to *https://<public_IP_address>*.



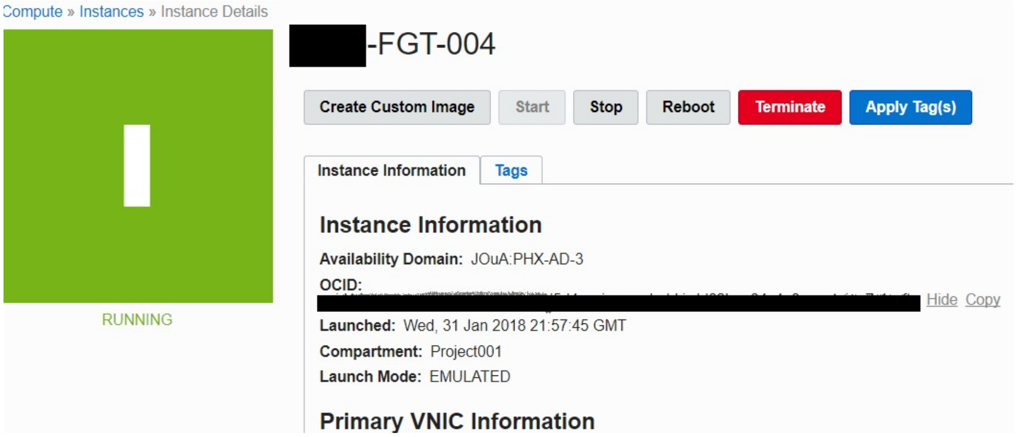
⚠ Not secure | ~~https~~://129.146.127.23/login



opc

Password

The default username is “opc” for FortiOS 5.6.x, 6.0.0, and 6.0.1, and “admin” for FortiOS 6.0.2 and later versions for new installations. For upgrades (such as from FortiOS 6.0.1 to 6.0.2), the exiting opc user is kept. The default password is the OCID. You can find the OCID as shown:



Compute » Instances » Instance Details

[redacted]-FGT-004

Instance Information

Availability Domain: JOuA:PHX-AD-3

OCID: [redacted] Hide Copy

Launched: Wed, 31 Jan 2018 21:57:45 GMT

Compartment: Project001

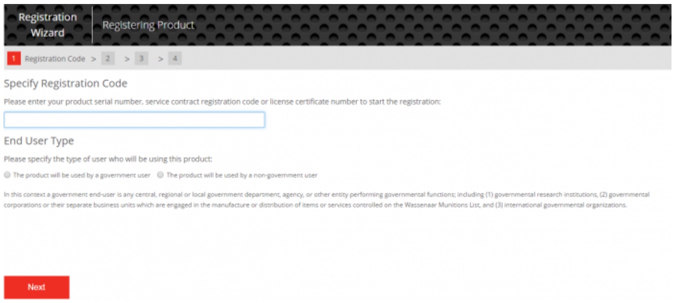
Launch Mode: EMULATED

Primary VNIC Information

3. Once logged in, FortiOS prompts for a license file. You can obtain licenses through any Fortinet partner. If you do not have a partner, contact Fortinet for assistance in purchasing a license. After you purchase a license or obtain an evaluation license (60-day term), you receive a PDF with an activation code. Go to Customer Service & Support and create a new account or log in with an existing account.

> If you added a license by following the instructions in (Optional) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 18, the system displays the dashboard instead of a license upload window, since the license is already activated.

4. Go to *Asset* > *Register/Activate* to start the registration process. In the *Specify Registration Code* field, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.



Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration:

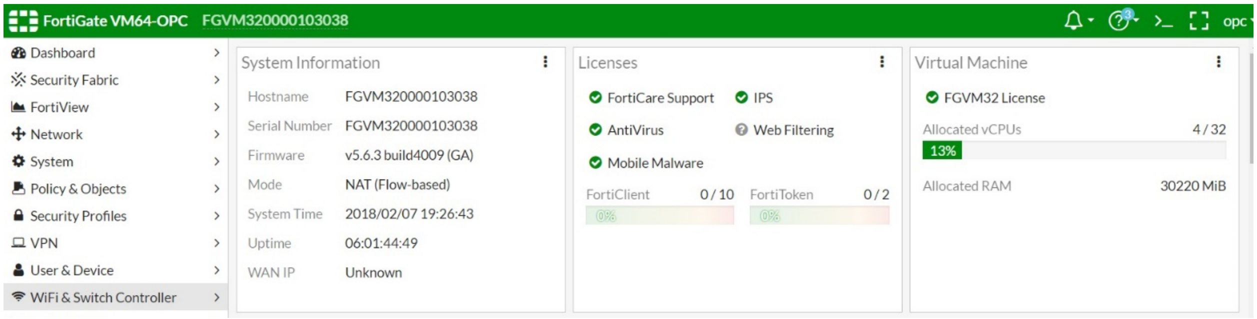
End User Type

Please specify the type of user who will be using this product:

○ The product will be used by a government user ○ The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

5. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license to activate the FortiGate.
6. After registering a license, Fortinet servers may take 30-45 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate, if you get an error that the license is invalid, wait 30 minutes and try again. You should now be able to see the FortiGate GUI console.



System Information

Hostname	FGVM320000103038
Serial Number	FGVM320000103038
Firmware	v5.6.3 build4009 (GA)
Mode	NAT (Flow-based)
System Time	2018/02/07 19:26:43
Uptime	06:01:44:49
WAN IP	Unknown

Licenses

✓ FortiCare Support ✓ IPS

✓ AntiVirus ? Web Filtering

✓ Mobile Malware

FortiClient 0 / 10 0%

FortiToken 0 / 2 0%

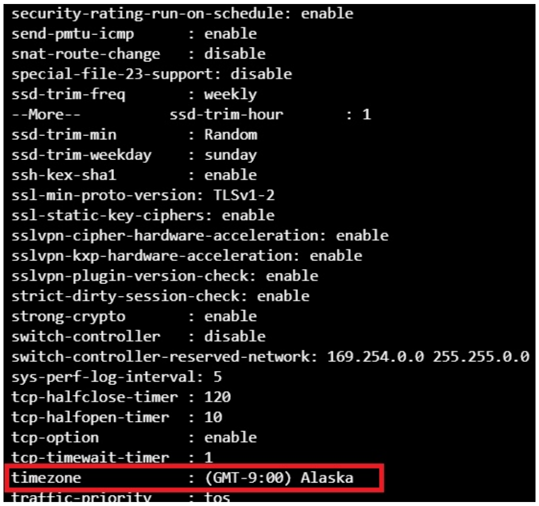
Virtual Machine

✓ FGVM32 License

Allocated vCPUs 4 / 32 13%

Allocated RAM 30220 MiB

7. If you followed the instructions in (Optional) Bootstrapping FortiGate-VM on the OCI GUI at initial bootup on page 18, you can check if the command was successful. Open the CLI console and enter `diag debug cloudinit show`. If the cloud-init was run successfully, the CLI shows `Finish running script` with no errors.
8. Check the timezone by running `config system global` and `get` commands.



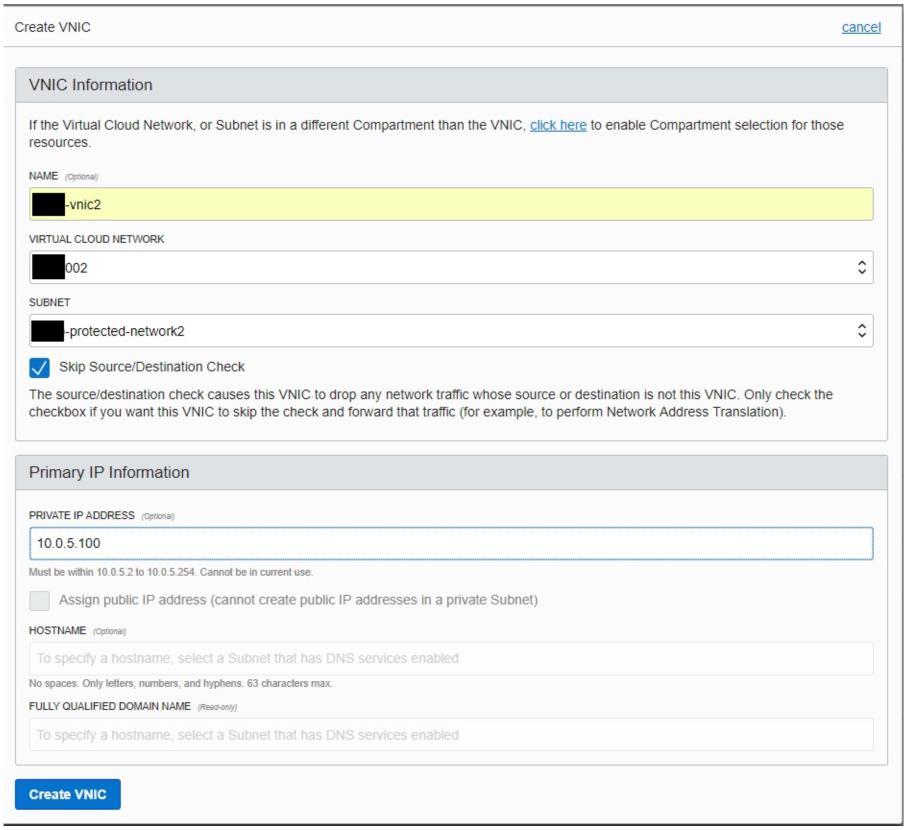
```
security-rating-run-on-schedule: enable
send-pmtu-icmp      : enable
snat-route-change   : disable
special-file-23-support: disable
ssd-trim-freq       : weekly
--More--          ssd-trim-hour       : 1
ssd-trim-min        : Random
ssd-trim-weekday    : sunday
ssh-kex-sha1        : enable
ssl-min-proto-version: 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
```

The timezone was changed to Alaska as expected, meaning that the bootstrapping CLI command was successful.

Creating the second virtual network interface (VNIC)

To create the second VNIC:

1. In the FortiGate-VM instance, click *Attached VNICs* > *Create VNIC*.
2. Create the VNIC by specifying the name, VNC, and internal subnet created earlier. Ensure that *Skip Source/Destination Check* is selected.. Enter an IP address and click *Create VNIC*. You now have the second network interface attached to the FortiGate-VM.



Create VNIC cancel

VNIC Information

If the Virtual Cloud Network, or Subnet is in a different Compartment than the VNIC, click here to enable Compartment selection for those resources.

NAME (Optional): [redacted]-vnic2

VIRTUAL CLOUD NETWORK: [redacted]002

SUBNET: [redacted]-protected-network2

☑ Skip Source/Destination Check

The source/destination check causes this VNIC to drop any network traffic whose source or destination is not this VNIC. Only check the checkbox if you want this VNIC to skip the check and forward that traffic (for example, to perform Network Address Translation).

Primary IP Information

PRIVATE IP ADDRESS (Optional): 10.0.5.100

Must be within 10.0.5.2 to 10.0.5.254. Cannot be in current use.

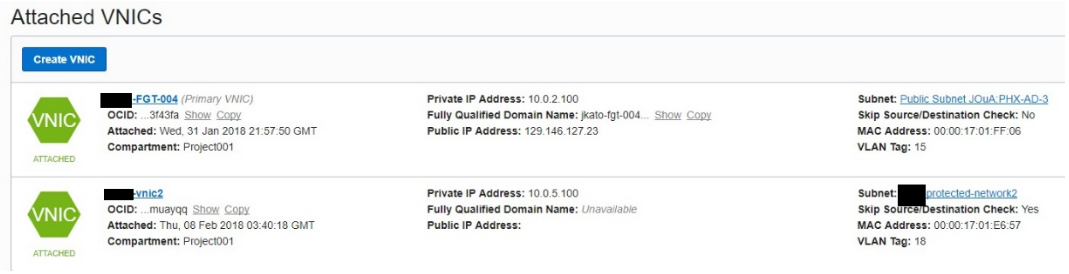
☐ Assign public IP address (cannot create public IP addresses in a private Subnet)

HOSTNAME (Optional): To specify a hostname, select a Subnet that has DNS services enabled

No spaces. Only letters, numbers, and hyphens. 63 characters max.

FULLY QUALIFIED DOMAIN NAME (Read-only): To specify a hostname, select a Subnet that has DNS services enabled

Create VNIC



Attached VNICs

Create VNIC

[redacted]-FGT-004 *(Primary VNIC)*
OCID: ...3f43fa Show Copy
Attached: Wed, 31 Jan 2018 21:57:50 GMT
Compartment: Project001
ATTACHED

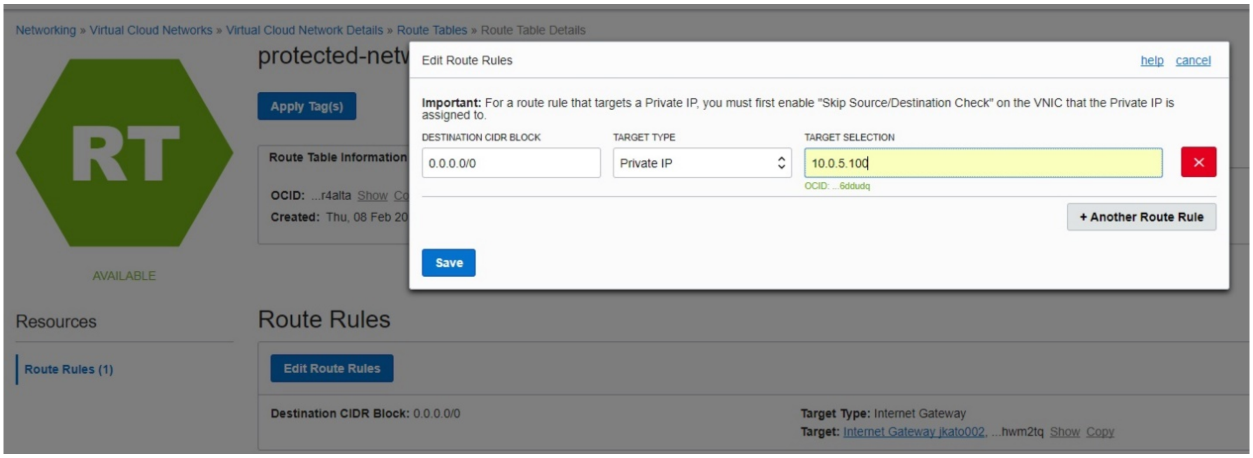
Private IP Address: 10.0.2.100
Fully Qualified Domain Name: jkato-fgt-004... Show Copy
Public IP Address: 129.146.127.23

Subnet: Public Subnet JOuA:PHX-AD-3
Skip Source/Destination Check: No
MAC Address: 00:00:17:01:FF:06
VLAN Tag: 15

[redacted]-vnic2
OCID: ...muayqq Show Copy
Attached: Thu, 08 Feb 2018 03:40:18 GMT
Compartment: Project001
ATTACHED

Private IP Address: 10.0.5.100
Fully Qualified Domain Name: *Unavailable*
Public IP Address:

Subnet: [redacted]protected-network2
Skip Source/Destination Check: Yes
MAC Address: 00:00:17:01:E6:57
VLAN Tag: 18



Networking » Virtual Cloud Networks » Virtual Cloud Network Details » Route Tables » Route Table Details

protected-netv

Apply Tag(s)

Route Table Information
OCID: ...r4alta Show Co
Created: Thu, 08 Feb 20

AVAILABLE

Edit Route Rules help cancel

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.

DESTINATION CIDR BLOCK: 0.0.0.0/0
TARGET TYPE: Private IP
TARGET SELECTION: 10.0.5.100
OCID: ...6ddudq

+ Another Route Rule

Save

Resources

Route Rules (1)

Route Rules

Edit Route Rules

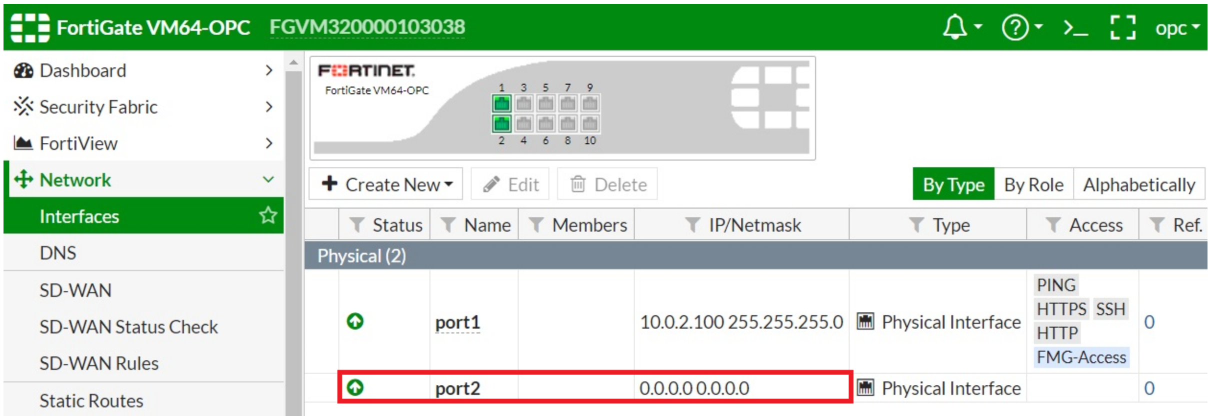
Destination CIDR Block: 0.0.0.0/0

Target Type: Internet Gateway
Target: Internet Gateway jkato002, ...hwm2tq Show Copy

Configuring the second VNIC on the FortiGate-VM

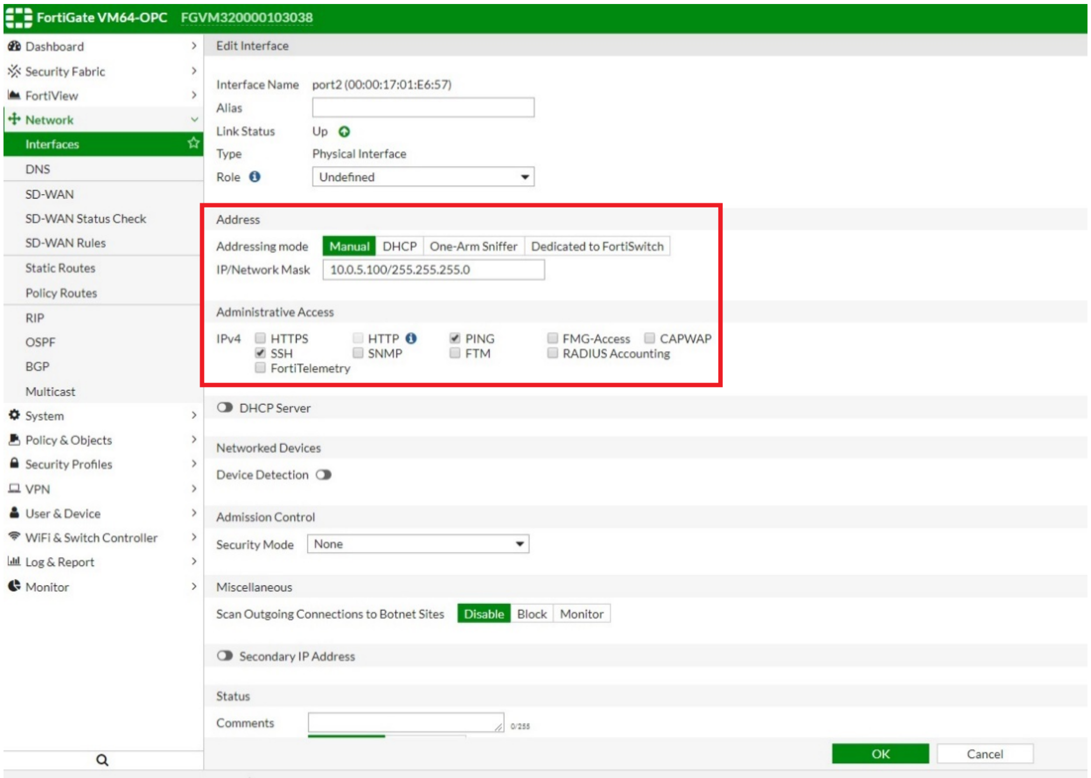
To configure the second VNIC on the FortiGate-VM:

1. After attaching the second VNIC to the FortiGate-VM, ensure you reboot, then log into the FortiGate-VM. Log into the GUI console and go to *Network* > *Interfaces*. You now see two ports, but the second port is not configured with an IP address. Manually configure the same IP address specified on OCI.



Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (2)						
●	port1		10.0.2.100 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
●	port2		0.0.0.0 0.0.0.0	Physical Interface		0

2. Select port2, then click *Edit*. Manually enter the IP address and netmask. Allow administrative access to PING, SSH, and so on as desired. Click *OK*.



Edit Interface

Interface Name: port2 (00:00:17:01:E6:57)
Alias:
Link Status: Up
Type: Physical Interface
Role: Undefined

Address

Addressing mode: [✓ Manual] DHCP One-Arm Sniffer Dedicated to FortiSwitch
IP/Network Mask: 10.0.5.100/255.255.255.0

Administrative Access

IPv4: □ HTTPS ☑ SSH □ FortiTelemetry □ HTTP □ SNMP ☑ PING □ FTM □ FMG-Access □ RADIUS Accounting □ CAPWAP

DHCP Server

Networked Devices

Device Detection

Admission Control

Security Mode: None

Miscellaneous

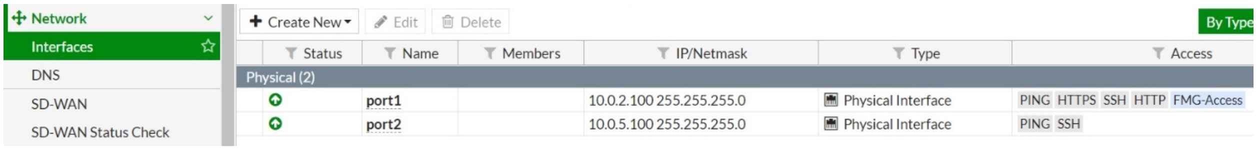
Scan Outgoing Connections to Botnet Sites: [✓ Disable] Block Monitor

Secondary IP Address

Status

Comments: 0/255

You now have two network interfaces configured.

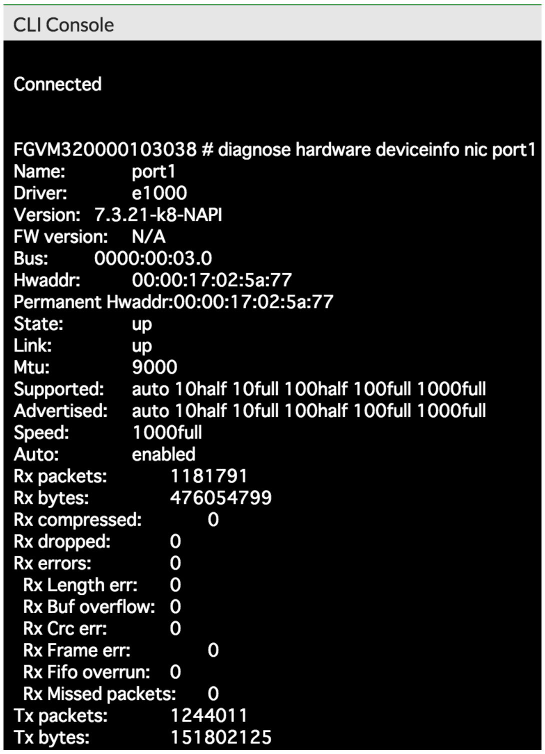


Status	Name	Members	IP/Netmask	Type	Access
Physical (2)					
●	port1		10.0.2.100 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access
●	port2		10.0.5.100 255.255.255.0	Physical Interface	PING SSH

Enabling jumbo frame on the second VNIC

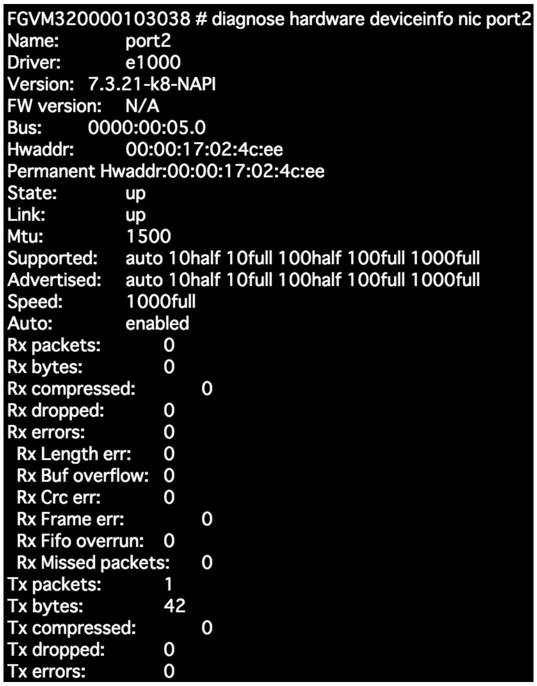
By default, the first VNIC port1 is enabled for jumbo frame. You must configure the same on the newly added VNIC port2. For jumbo frame support, refer to the following KB note.

If you look at the VNIC information in the CLI, MTU is set to 9000 by default.


CLI Console

```
Connected

FGVM320000103038 # diagnose hardware deviceinfo nic port1
Name:           port1
Driver:         e1000
Version:   7.3.21-k8-NAPI
FW version:     N/A
Bus:       0000:00:03.0
Hwaddr:         00:00:17:02:5a:77
Permanent Hwaddr:00:00:17:02:5a:77
State:          up
Link:           up
Mtu:            9000
Supported:      auto 10half 10full 100half 100full 1000full
Advertised:     auto 10half 10full 100half 100full 1000full
Speed:          1000full
Auto:           enabled
Rx packets:          1181791
Rx bytes:            476054799
Rx compressed:            0
Rx dropped:          0
Rx errors:           0
  Rx Length err:     0
  Rx Buf overflow:   0
  Rx Crc err:        0
  Rx Frame err:           0
  Rx Fifo overrun:   0
  Rx Missed packets:      0
Tx packets:          1244011
Tx bytes:            151802125
```

After adding the second VNIC in the previous step, it is not set with the jumbo frame by default. As you can see, the MTU is set to 1500.

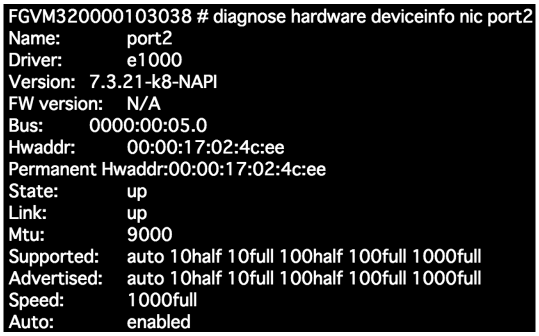


```
FGVM320000103038 # diagnose hardware deviceinfo nic port2
Name:           port2
Driver:         e1000
Version:   7.3.21-k8-NAPI
FW version:     N/A
Bus:       0000:00:05.0
Hwaddr:         00:00:17:02:4c:ee
Permanent Hwaddr:00:00:17:02:4c:ee
State:          up
Link:           up
Mtu:            1500
Supported:      auto 10half 10full 100half 100full 1000full
Advertised:     auto 10half 10full 100half 100full 1000full
Speed:          1000full
Auto:           enabled
Rx packets:          0
Rx bytes:            0
Rx compressed:            0
Rx dropped:          0
Rx errors:           0
  Rx Length err:     0
  Rx Buf overflow:   0
  Rx Crc err:        0
  Rx Frame err:           0
  Rx Fifo overrun:   0
  Rx Missed packets:      0
Tx packets:          1
Tx bytes:            42
Tx compressed:            0
Tx dropped:          0
Tx errors:           0
```

Run the following CLI commands to change the MTU size on port2. See Interface MTU packet size.

```
config system interface
   edit port2
      set mtu-override enable
      set mtu 9000
end
```

Check if the MTU changed as expected.



```
FGVM320000103038 # diagnose hardware deviceinfo nic port2
Name:           port2
Driver:         e1000
Version:   7.3.21-k8-NAPI
FW version:     N/A
Bus:       0000:00:05.0
Hwaddr:         00:00:17:02:4c:ee
Permanent Hwaddr:00:00:17:02:4c:ee
State:          up
Link:           up
Mtu:            9000
Supported:      auto 10half 10full 100half 100full 1000full
Advertised:     auto 10half 10full 100half 100full 1000full
Speed:          1000full
Auto:           enabled
```

Changing the protected network's default route

Once you have created the VNIC with the private IP address, it is available for you to select it as the default gateway in the route table configuration. Go to the route tables and edit the route rules for the internal network subnet. For all destinations, select *Private IP* as the *Target Type*, and enter the FortiGate-VM's second VNIC’s private IP address.

Deploying a native mode FortiGate-VM on OCI

This guide demonstrates how to launch a native mode FortiGate-VM on OCI. This deployment consists of the following steps:

1. Create a native mode FGT-VM64-OPC custom image.
2. Create a FGT-VM64-OPC instance with the native mode custom image.
3. Attach a hard disk to the FGT-VM64-OPC with iSCSI mode.
4. Run diagnose commands.

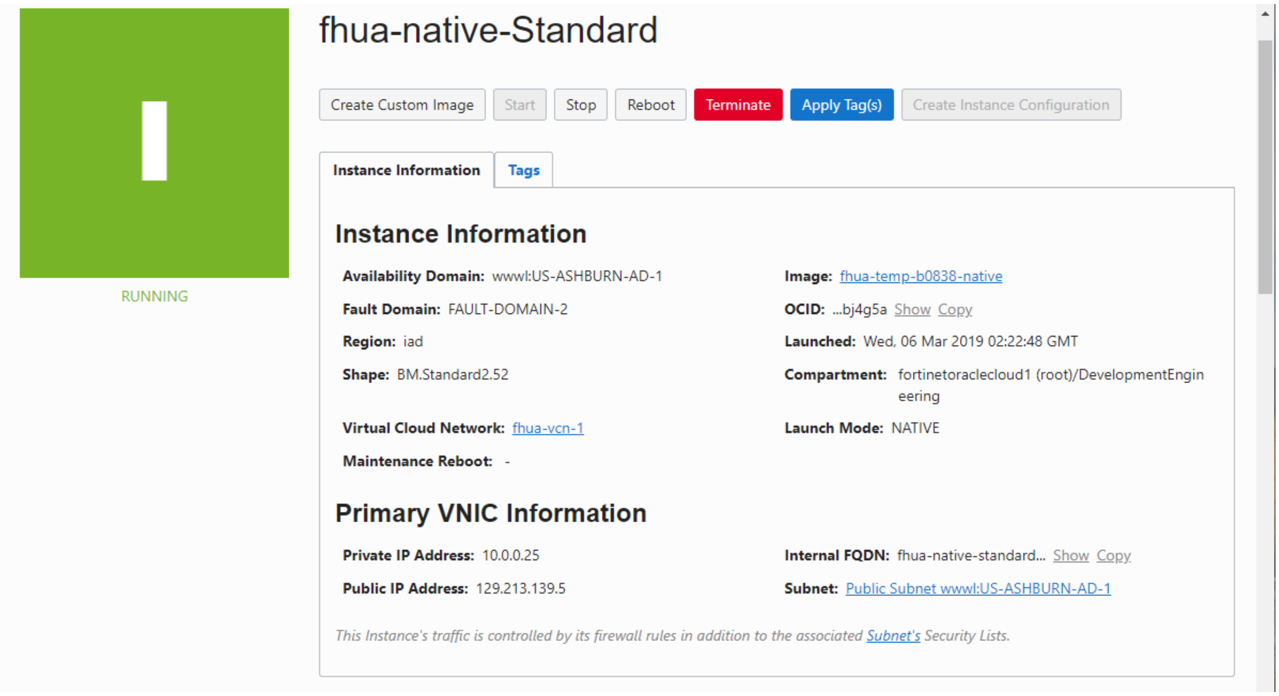
To create a native mode FortiGate-VM custom image:

1. Obtain the deployment image file and upload the forties.qcow2 file to OCI object storage as described in To obtain the deployment image file and place it in your bucket: on page 12. Obtain the file URL path.
2. Import the image:
   a. Go to *Compute* > *Custom Images*. Click *Import Image*.
   b. In the *Import Image* dialog, complete the fields. In the *OBJECT STORAGE URL* field, enter the URL link obtained in step 1.
   c. Under *OPERATING SYSTEM*, select *Linux*.
   d. Under *IMAGE TYPE*, select *QCOW2*.
   e. Under *LAUNCH MODE*, select *NATIVE MODE*.
   f. Click *Import Image*. After some time, the FortiGate for OCI custom image becomes available on OCI.

To create a FortiGate-VM instance with the native mode custom image:

1. Log into the OCI web portal. Go to *Compute* > *Instances* > *Create Instance*.
2. Configure the FortiGate-VM instance:
   a. In the *Name your instance* field, enter the desired name for your FortiGate-VM instance.
   b. Select an availability domain (AD) for your instance.
   c. Under *Choose an operating system or image source*, select the image source as the image created in the previous step.
   d. Under *Choose instance type*, select *Virtual Machine* or *Bare Metal Machine*.
   e. Under *Choose instance shape*, select *Change Shape* and select the instance shape.
   f. Under *Configure networking*, select your virtual cloud network and subnet.
   g. Leave the *Configure boot volume* options at their default values. You can also add an SSH key file if desired.
3. Click *Create*. After a few minutes, the instance is ready and running. You can access the FortiGate-VM with your SSH key or using the username "admin" and the OCID as the password.

4. Go to the *Instance Information* tab for the FortiGate-VM. Verify that the instance's *Launch Mode* displays as *NATIVE*.



fhua-native-Standard

Instance Information

Availability Domain: wwwl:US-ASHBURN-AD-1

Fault Domain: FAULT-DOMAIN-2

Region: iad

Shape: BM.Standard2.52

Virtual Cloud Network: fhua-vcn-1

Maintenance Reboot: -

Image: fhua-temp-b0838-native

OCID: ...bj4g5a Show Copy

Launched: Wed, 06 Mar 2019 02:22:48 GMT

Compartment: fortinetoraclecloud1 (root)/DevelopmentEngineering

Launch Mode: NATIVE

Primary VNIC Information

Private IP Address: 10.0.0.25

Public IP Address: 129.213.139.5

Internal FQDN: fhua-native-standard... Show Copy

Subnet: Public Subnet wwwl:US-ASHBURN-AD-1

This Instance's traffic is controlled by its firewall rules in addition to the associated Subnet's Security Lists.

To attach a hard disk to the FortiGate-VM with ISCSI mode:

1. From the navigation bar, click *Attach Block Volume*.
2. Under *Choose how you want to attach your block volume*, select *ISCSI*.
3. Leave *ACCESS* at the default value, *READ/WRITE*.
4. Configure other options as desired.
5. Click *Attach*. After a few minutes, the *Instance Information* page shows that the block volume was attached.
6. Under *Attached Block Volumes*, go to the block volume entry, and click *iSCSI Commands & Information*. You can find this iSCSCI's IP address and IQN here.
7. Log into the FortiGate and run the following commands to configure the iSCSI hard disk:

```
config system iscsi
   edit "Demo-iSCSI-HD"
      set ip 169.254.2.4 set iqn "iqn.2015-12.com.oracleiaas:debf5040-260a-4a28-a00e-
            da172baa6698"
   next
end
```

8. Run the `d hardware deviceinfo disk` command to ensure that the second hard drive (50.0 GiB) is attached. The output should look like the following:

```
Disk SYSTEM(boot) 46.6GiB type: ISCSI [IET Controller] dev: /dev/sda
   partition 123.0MiB, 62.0MiB free mounted: Y label: dev: /dev/sda1(boot) start: 2048
   partition 1.7GiB, 1.7GiB free mounted: Y label: dev: /dev/sda2(boot) start: 264192
   partition ref: 3 127.0MiB, 86.0MiB free mounted: N label: dev: /dev/sda3 start:
         3932160
Disk Virtual-Disk ref: 32 50.0GiB type: ISCSI [IET Controller] dev: /dev/sdc
   partition ref: 33 49.2GiB, 48.9GiB free mounted: N label: LOGUSEDX6FFE3A65 dev:
         /dev/sdc1 start: 2048
Total available disks: 2 Max SSD disks: 8 Available storage disks: 1
```

To run diagnose commands:

1. Run the following commands to configure the ISCSI disk:
```
config system iscsi
   edit "i1"
      set ip class_ip
      set iqn string
   next
end
```
2. Run the `execute iscsi logout <iscis-disk-name>` command to disconnect the ISCSI disk.
3. Run the `execute iscsi login <iscis-disk-name>` command to connect the ISCSI disk.

Deploying FortiGate-VM via the marketplace

To deploy FortiGate-VM via the marketplace:

1. Go to *Compute* > *Instances*. Click *Create Instance*.
2. Enter the desired instance name.
3. For *Choose an operating system or image source*, click *Change Image Source*, then *Partner Images* > *FortiGate Next Gen Firewall (BYOL)*.
4. Select the desired instance shape. If this instance will be part of an HA topology, select a shape with at least four OCPU.
5. Select the desired VCN and subnet, then click *Create*.

A newly created FortiGate-VM only has one VNIC. To configure a second VNIC, see Creating the second virtual network interface (VNIC) on page 22 and Configuring the second VNIC on the FortiGate-VM on page 24.

HA for FortiGate-VM on OCI

Deploying FortiGate-VM HA on OCI within one AD

FortiGate active-passive HA

FortiGate's native active-passive HA feature (without using an OCI supplementary mechanism such as a load balancer) can be configured with two FortiGate-VM instances: one acting as the primary node and the other as the secondary node, both located in the same AD. This guide refers to the primary and secondary nodes as FortiGate A and FortiGate B, respectively. This is called "unicast HA" and is specific to cloud environments, including OCI, to be compliant to their network restrictions in comparison to an equivalent feature that physical FortiGates provided. The FortiGate-VMs run heartbeats between dedicated ports and synchronize OS 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 FortiGate-VM. Sessions are also synchronized at the time of failover.

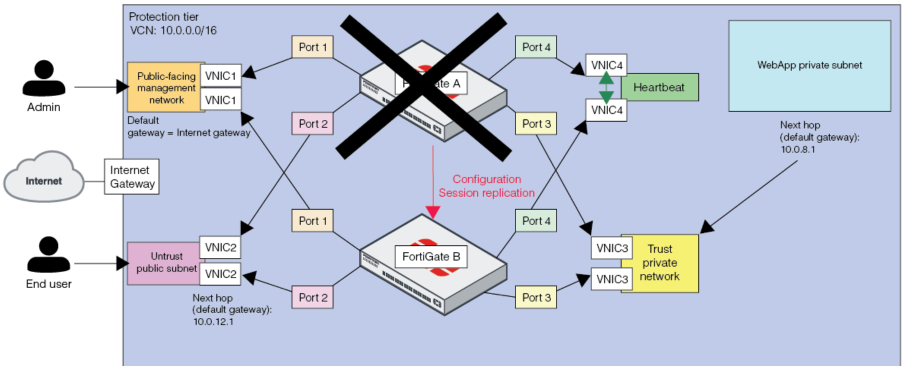
Using the latest version of FortiGate-VM is always recommended.

When deploying a FortiGate-VM HA cluster, choose a compute VM shape that supports four or more vNICs for each FortiGate-VM instance.

Two FortiGate-VM instances must be the same compute VM shape.

Deploying and configuring FortiGate active-passive HA

For this HA deployment, you can manually configure two FortiGate-VM instances after deployment on OCI using CLI commands, or run Terraform scripts. Your deployment will have different IP addresses than in the diagram.



FortiGate A

Component	IP address
Port 1	Public IP: 129.213.x.x Primary private IP: 10.0.0.3
Port 2	Public IP: 129.213.x.x Port IP: 10.0.12.3 = OCI vNIC's secondary IP
Port 3	Port IP: 10.0.8.10 Secondary private IP: 10.0.8.11
Port 4	Primary private IP: 10.0.10.3

FortiGate B

Component	IP address
Port 1	Public IP: 129.213.x.x Primary private IP: 10.0.0.4
Port 2	Public IP: 129.213.x.x When FortiGate A fails, its port 2's secondary IP address, 10.0.12.3, moves to FortiGate B's port 2. Therefore, the public IP address that is paired with the secondary private IP address also moves.
Port 3	Port IP: 10.0.8.12 When FortiGate A fails, its port 3's secondary IP address, 10.0.8.11, moves to FortiGate B's port 3.
Port 4	Primary private IP: 10.0.10.4

Subnets

Subnet	IP address
Heartbeat	10.0.10.0/24
Trust private subnet	10.0.8.10/24
Untrust public subnet	10.0.12.0/24
Public-facing management network	10.0.0.0/24
WebApp private subnet	10.0.201.0/24

Unlike other public clouds, on OCI, you must configure port 1 as the management interface. The other ports are interchangeable. Locating each port in a different subnet is considered best practice. DNS must work with port 1 to resolve OCI's API endpoint URLs at the time of HA failover.

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

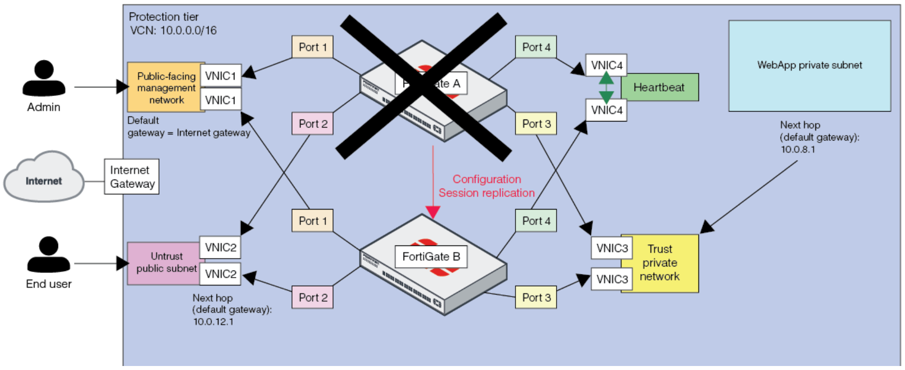
Checking the prerequisites

To deploy and configure the FortiGate-VM as an A-P HA solution, you need the following items:

- OCI account to operate in OCI compute portal
- Availability to accommodate required OCI resources
  - See Service Limits.
  - VCN with five subnets
  - Three public IP addresses
    - One for traffic to/through the active (primary) FortiGate-VM
    - Two for management access to each FortiGate-VM
  - All IP addresses must be static, not DHCP.
  - Two FortiGate-VM instances
    - You must deploy the two nodes in the same AD and under the same VCN.
    - Each FortiGate-VM must have at least four network interfaces. See Compute Shapes.
- Two valid FortiGate-VM BYOL licenses. See Licensing on page 7.
- The following summarizes minimum sufficient IAM roles for this deployment:
  - 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 subnets in tenancy
  - Allow dynamic-group <group_name> to manage private-ips in tenancy
  - Allow dynamic-group <group_name> to manage public-ips in tenancy
  - Allow dynamic-group <group_name> to manage route-tables in tenancy
  - To define simpler roles, use the following:
    - 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 manage virtual-network-family in tenancy

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

Reviewing the network topology



FortiGate A

Component	IP address
Port 1	Public IP: 129.213.x.x Primary private IP: 10.0.0.3
Port 2	Public IP: 129.213.x.x Port IP: 10.0.12.3 = OCI vNIC's secondary IP
Port 3	Port IP: 10.0.8.10 Secondary private IP: 10.0.8.11
Port 4	Primary private IP: 10.0.10.3

FortiGate B

Component	IP address
Port 1	Public IP: 129.213.x.x Primary private IP: 10.0.0.4
Port 2	Public IP: 129.213.x.x When FortiGate A fails, its port 2's secondary IP address, 10.0.12.3, moves to FortiGate B's port 2. Therefore, the public IP address that is paired with the secondary private IP address also moves.
Port 3	Port IP: 10.0.8.12 When FortiGate A fails, its port 3's secondary IP address, 10.0.8.11, moves to FortiGate B's port 3.
Port 4	Primary private IP: 10.0.10.4

Subnets

Subnet	IP address
Heartbeat	10.0.10.0/24
Trust private subnet	10.0.8.10/24
Untrust public subnet	10.0.12.0/24
Public-facing management network	10.0.0.0/24
WebApp private subnet	10.0.201.0/24

A recommended installation requires four network interfaces per FortiGate-VM node. In addition to inbound and outbound data interfaces, two interfaces are used for internal operations: management and heartbeat. Ensure you choose OCI VM instance sizes that can equip four network interfaces.

The table describes the usage of each port. Port1 and 2 are on public (or untrusted) subnets, and public IP addresses are allocated to them.

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. FortiGate 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 FortiGate nodes. This is unicast communication. This heartbeat interface has its dedicated "hbdev" VDOM and cannot be used for any other purpose.

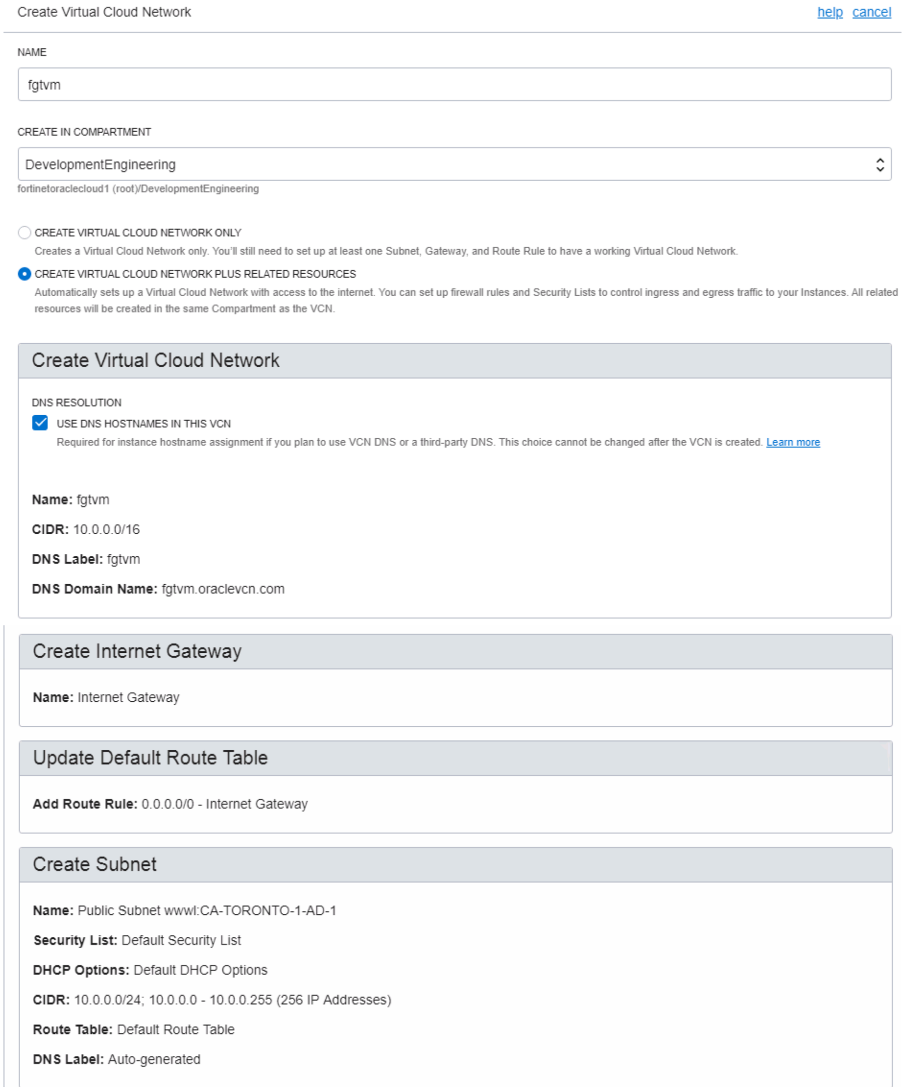
You must configure port 1 as the management interface. The other ports are interchangeable. The best practice is to locate each port in a different subnet.

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 same-AD HA topology

To create a VCN and public-facing subnets:

1. In OCI, go to *Networking* > *Virtual Cloud Networks*, and click *Create Virtual Cloud Network*.
2. In the *NAME* field, enter the VCN name. Then, select *CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES*. This allows you to create the Internet gateway, routing table, and subnet all together using Oracle default settings. If you intend to create each resource separately by specifying your own inputs, click *CREATE VIRTUAL CLOUD NETWORK ONLY*. This example uses the first choice.



Create Virtual Cloud Network

NAME

fgtvm

CREATE IN COMPARTMENT

DevelopmentEngineering

fortinetoraclecloud1 (root)/DevelopmentEngineering

○ CREATE VIRTUAL CLOUD NETWORK ONLY

Creates a Virtual Cloud Network only. You'll still need to set up at least one Subnet, Gateway, and Route Rule to have a working Virtual Cloud Network.

● CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES

Automatically sets up a Virtual Cloud Network with access to the internet. You can set up firewall rules and Security Lists to control ingress and egress traffic to your Instances. All related resources will be created in the same Compartment as the VCN.

Create Virtual Cloud Network

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

Name: fgtvm

CIDR: 10.0.0.0/16

DNS Label: fgtvm

DNS Domain Name: fgtvm.oraclevcn.com

Create Internet Gateway

Name: Internet Gateway

Update Default Route Table

Add Route Rule: 0.0.0.0/0 - Internet Gateway

Create Subnet

Name: Public Subnet wwwl:CA-TORONTO-1-AD-1

Security List: Default Security List

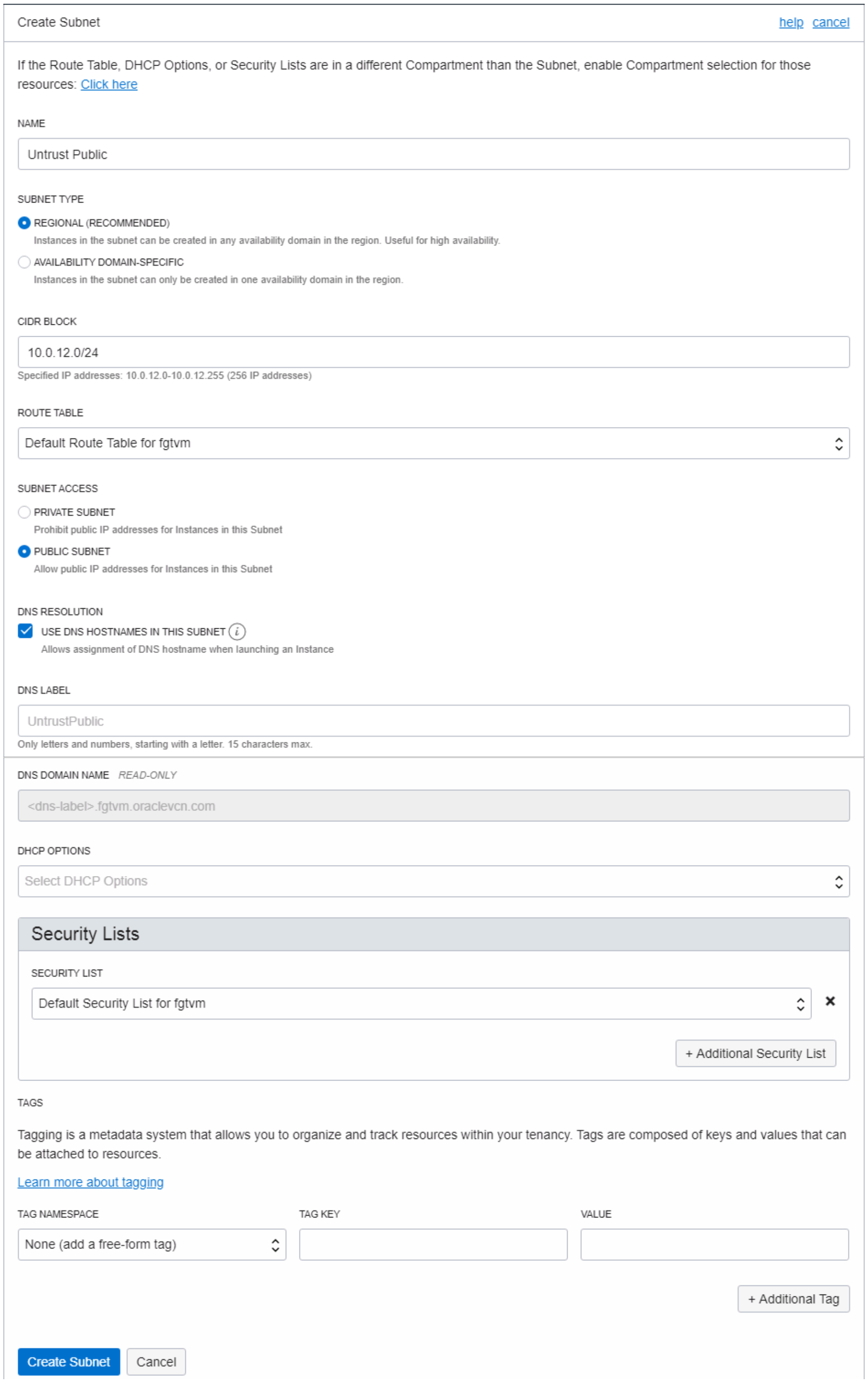
DHCP Options: Default DHCP Options

CIDR: 10.0.0.0/24; 10.0.0.0 - 10.0.0.255 (256 IP Addresses)

Route Table: Default Route Table

DNS Label: Auto-generated

3. Click *Create Virtual Cloud Network* at the bottom of the screen, then click *Close*.
   This configures the related resources.
4. Create the other subnets:
   a. Go to *Networking* > *Virtual Cloud Networks*. Click the name of the previously created VCN, then click *Create Subnet*.
   b. For *Subnet Type*, select *Regional*.
   c. For *Subnet Access*, select *Private* or *Public Subnet* as desired. The screenshot shows the configuration for the public subnet.



Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: Click here

NAME

Untrust Public

SUBNET TYPE

● REGIONAL (RECOMMENDED)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

○ AVAILABILITY DOMAIN-SPECIFIC
Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK

10.0.12.0/24

Specified IP addresses: 10.0.12.0-10.0.12.255 (256 IP addresses)

ROUTE TABLE

Default Route Table for fgtvm

SUBNET ACCESS

○ PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

● PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

☑ USE DNS HOSTNAMES IN THIS SUBNET
Allows assignment of DNS hostname when launching an Instance

DNS LABEL

UntrustPublic

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

DNS DOMAIN NAME *READ-ONLY*

<dns-label>.fgtvm.oraclevcn.com

DHCP OPTIONS

Select DHCP Options

Security Lists

SECURITY LIST

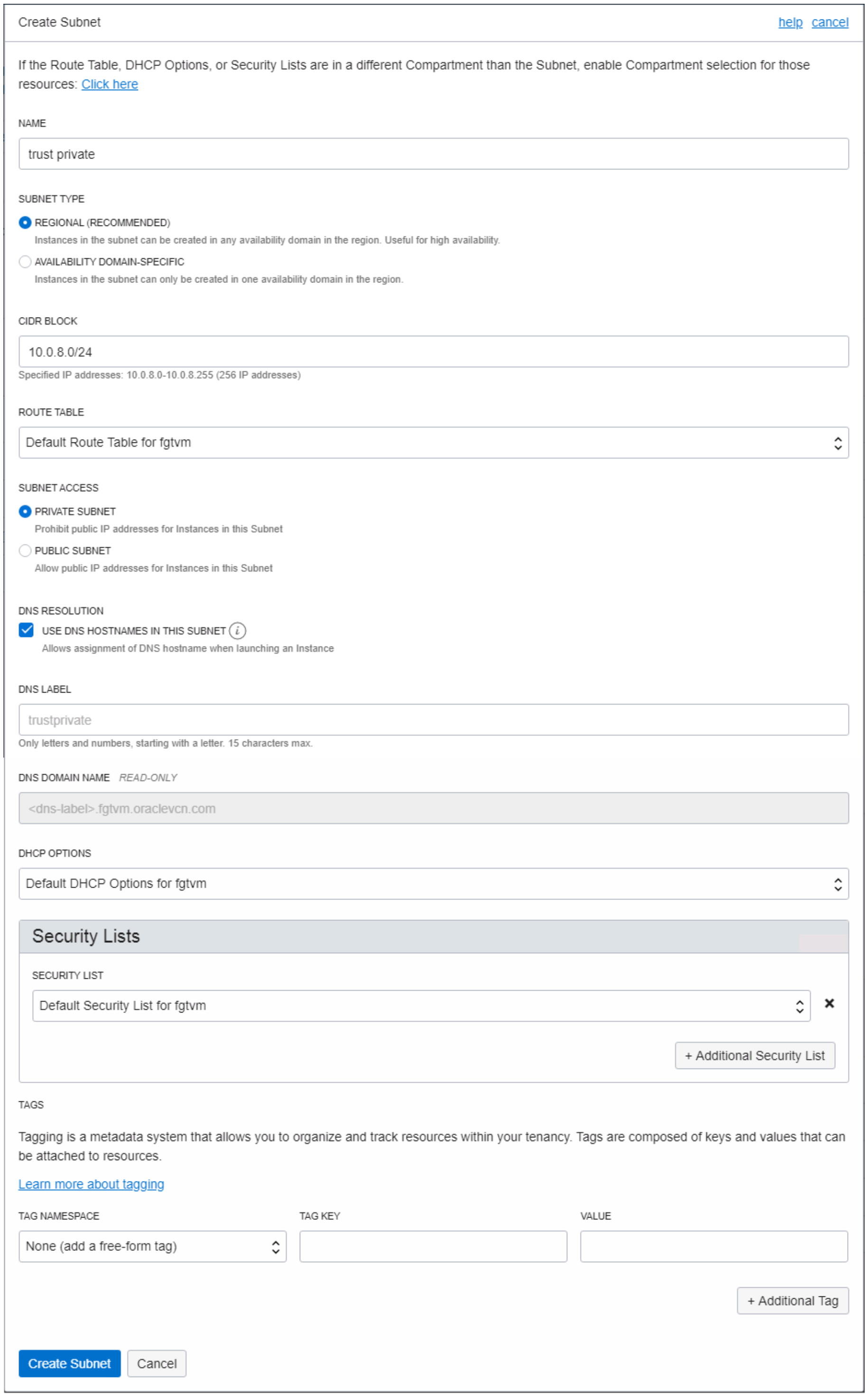
Default Security List for fgtvm

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		



Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: Click here

NAME: trust private

SUBNET TYPE

● REGIONAL (RECOMMENDED)
Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

○ AVAILABILITY DOMAIN-SPECIFIC
Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK: 10.0.8.0/24
Specified IP addresses: 10.0.8.0-10.0.8.255 (256 IP addresses)

ROUTE TABLE: Default Route Table for fgtvm

SUBNET ACCESS

● PRIVATE SUBNET
Prohibit public IP addresses for Instances in this Subnet

○ PUBLIC SUBNET
Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

☑ USE DNS HOSTNAMES IN THIS SUBNET
Allows assignment of DNS hostname when launching an Instance

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

DNS DOMAIN NAME *READ-ONLY*: <dns-label>.fgtvm.oraclevcn.com

DHCP OPTIONS: Default DHCP Options for fgtvm

Security Lists

SECURITY LIST: Default Security List for fgtvm

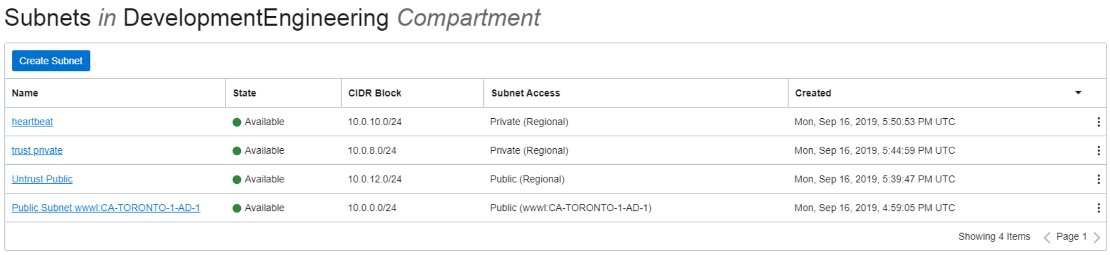
TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		

d. Repeat to create a minimum of four subnets for HA setup. The following shows an example of the minimum requirement:



Subnets *in* DevelopmentEngineering *Compartment*

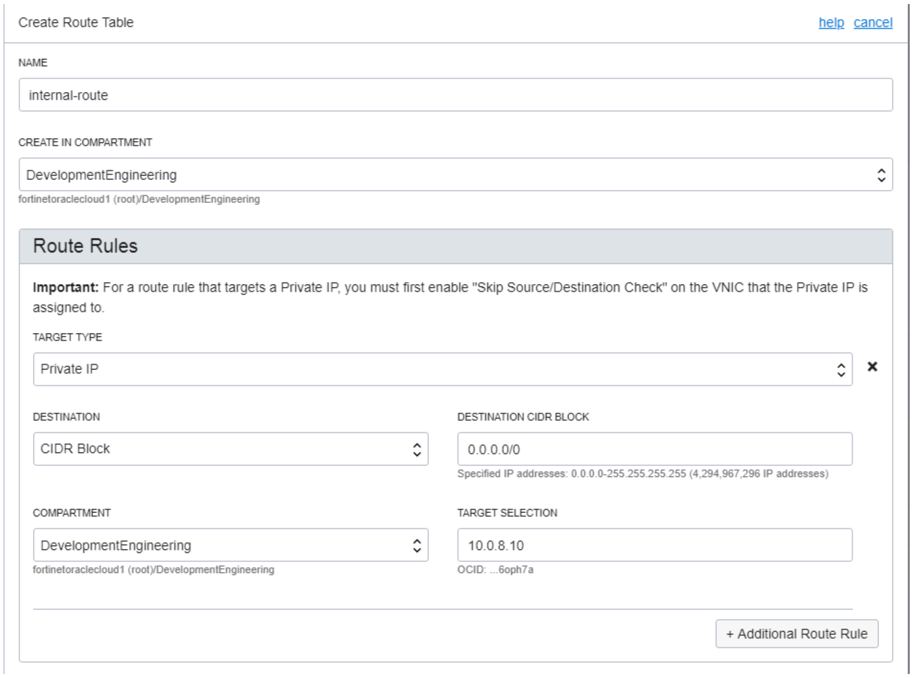
Create Subnet

Name	State	CIDR Block	Subnet Access	Created
heartbeat	● Available	10.0.10.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:50:53 PM UTC
trust private	● Available	10.0.8.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:44:59 PM UTC
Untrust Public	● Available	10.0.12.0/24	Public (Regional)	Mon, Sep 16, 2019, 5:39:47 PM UTC
Public Subnet wwwl:CA-TORONTO-1-AD-1	● Available	10.0.0.0/24	Public (wwwl:CA-TORONTO-1-AD-1)	Mon, Sep 16, 2019, 4:59:05 PM UTC

Showing 4 Items   Page 1

Deploying the FortiGate-VM

1. Set up the OCI VCN environment. See Creating a VCN for same-AD HA topology on page 33.
2. Deploy FortiGate-VMs in the environment for an active-passive configuration. See Creating a FortiGate-VM instance on page 11. To deploy FortiGate-VM from the marketplace, see Deploying FortiGate-VM via the marketplace on page 29.
3. Configure extra VNICs for the FortiGate-VM. You must ensure there are at least four network interfaces configured for each instance. See Checking the prerequisites on page 31. To create an extra VNIC, see Creating the second virtual network interface (VNIC) on page 22. To configure the extra VNIC, see Configuring the second VNIC on the FortiGate-VM on page 24.
4. Update route rules to point to the internal/trust private IP address on the active FortiGate. It is recommended to create a separate route table for the internal/trust subnet:
   a. Go to *Networking > Virtual Cloud Networks > <VCN used> > Route Tables*, then click *Create Route Table*.
   b. Specify the route table to point to the internal/trust private IP address on the active FortiGate:



Create Route Table   help   cancel

NAME

internal-route

CREATE IN COMPARTMENT

DevelopmentEngineering

fortinetoraclecloud1 (root)/DevelopmentEngineering

Route Rules

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.

TARGET TYPE

Private IP

DESTINATION

CIDR Block

DESTINATION CIDR BLOCK

0.0.0.0/0

Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

COMPARTMENT

DevelopmentEngineering

fortinetoraclecloud1 (root)/DevelopmentEngineering

TARGET SELECTION

10.0.8.10

OCID: ...6oph7a

+ Additional Route Rule

   c. Go to *Networking > Virtual Cloud Networks > <VCN used>*. Edit the desired subnet.
   d. Under *Route Table*, update the configuration to the newly created route table.

Configuring the OCI HA interfaces

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

In the case of HA, it is necessary that the FortiGate-VMs have the correct IP information statically configured in order to provide proper failover between the two devices.

OCI API calls enable the failover mentioned above through the OCI Fabric connector, but only for IP addresses configured as secondary in the OCI VNIC configuration.

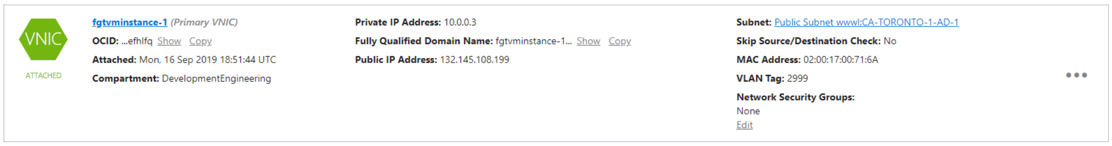
Also, OCI API calls, if initiated from within a VCN, must be made by a primary interface with a public address with DNS properly configured. Thus, the network configuration for OCI HA will be unique and very specific.

You may lose connection to the instance during interface IP address and route configuration. It is therefore recommended to perform this configuration via the console.

Primary FortiGate

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address, and so needs to be configured in a public subnet. This will be used as a management interface and also the interface from which API calls are made (this will be assigned in the HA configuration). See this interface's OCI configuration, then the corresponding FortiGate-VM configuration.



fgtvminstance-1 *(Primary VNIC)*
OCID: ...efhlfq Show Copy
Attached: Mon, 16 Sep 2019 18:51:44 UTC
Compartment: DevelopmentEngineering

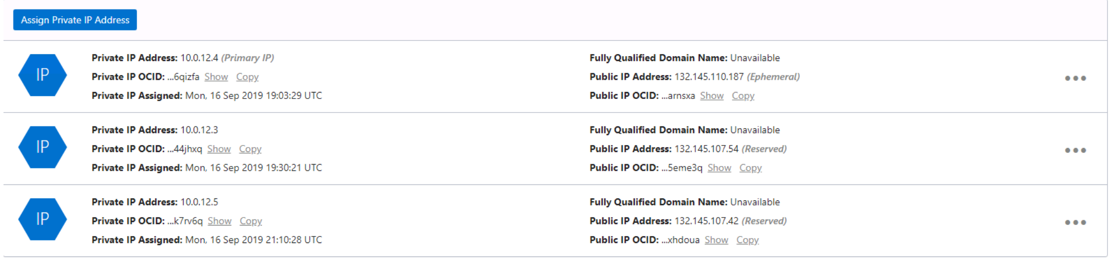
Private IP Address: 10.0.0.3
Fully Qualified Domain Name: fgtvminstance-1... Show Copy
Public IP Address: 132.145.108.199

Subnet: Public Subnet wwwl:CA-TORONTO-1-AD-1
Skip Source/Destination Check: No
MAC Address: 02:00:17:00:71:6A
VLAN Tag: 2999
Network Security Groups:
None
Edit

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.0.0.3 255.255.255.0
      set allowaccess ping https ssh http fgfm
      set description "management"
      set mtu-override enable
      set mtu 9000
   next
end
```

port2

Beyond port1 (also the primary VNIC), interface order is arbitrary and can be rearranged. In this example, port2 is assumed to be a public/WAN-facing interface. The following FortiGate configuration does not use the primary IP address for its interface IP address. Instead, it uses the non-primary private IP address, as shown. This is because the primary IP address is not relocatable to the secondary FortiGate in the event of HA failover. In this example, the FortiGate uses only 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 FortiGate. Therefore, if any extra non-primary private IP addresses are used in the setup, these IP addresses must be referenced explicitly in the interface configuration by enabling secondary IP addresses.



Private IP Address: 10.0.12.4 *(Primary IP)*
Private IP OCID: ...6qizfa Show Copy
Private IP Assigned: Mon, 16 Sep 2019 19:03:29 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: 132.145.110.187 *(Ephemeral)*
Public IP OCID: ...arnsxa Show Copy

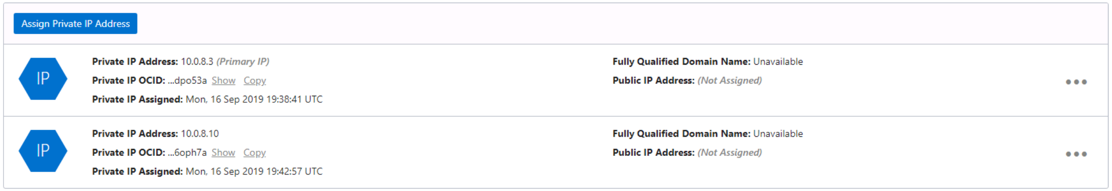
Private IP Address: 10.0.12.3
Private IP OCID: ...44jhxq Show Copy
Private IP Assigned: Mon, 16 Sep 2019 19:30:21 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: 132.145.107.54 *(Reserved)*
Public IP OCID: ...5eme3q Show Copy

Private IP Address: 10.0.12.5
Private IP OCID: ...k7rv6q Show Copy
Private IP Assigned: Mon, 16 Sep 2019 21:10:28 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: 132.145.107.42 *(Reserved)*
Public IP OCID: ...xhdoua Show Copy

```
config system interface
   edit "port2"
   set vdom "root"
      set ip 10.0.12.3 255.255.255.0
      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 internal port, which is used to connect to internal resources on local subnets, peered VCNs, and so on. However, as mentioned earlier, FortiGate 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 FortiGate.



Private IP Address: 10.0.8.3 *(Primary IP)*
Private IP OCID: ...dpo53a Show Copy
Private IP Assigned: Mon, 16 Sep 2019 19:38:41 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

Private IP Address: 10.0.8.10
Private IP OCID: ...6oph7a Show Copy
Private IP Assigned: Mon, 16 Sep 2019 19:42:57 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

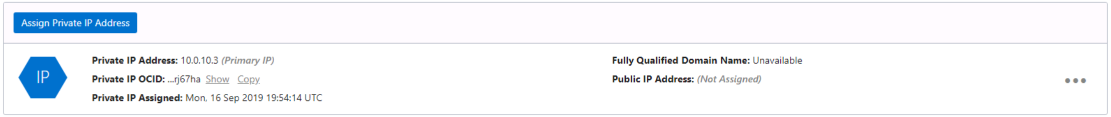
```
config system interface
   edit "port3"
      set vdom "root"
      set ip 10.0.8.10 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "trusted"
      set mtu-override enable
      set mtu 9000
   next
```

```
end
```

It is recommended to enable *Skip Source/Destination Check* for the VNIC.

port4

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



Private IP Address: 10.0.10.3 *(Primary IP)*
Private IP OCID: ...rj67ha
Private IP Assigned: Mon, 16 Sep 2019 19:54:14 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

```
config system interface
   edit "port4"
      set vdom "root"
      set ip 10.0.10.3 255.255.255.0
      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 FortiGate needs a route assigned to know how to get to them. Typically, these will be connected via the internal 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 FortiGate 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 no default route will be configured through DHCP, you must also add this default route. In FortiOS, if no destination is set, the default route of 0.0.0.0/0 is assumed. Therefore, the 2 configuration is the default route.

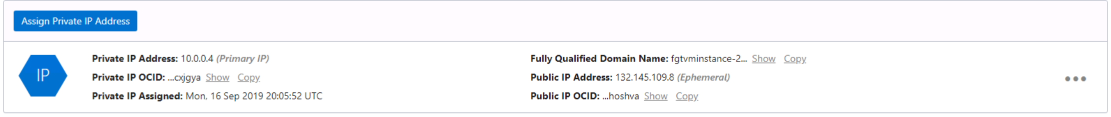
```
config router static
   edit 2
      set gateway 10.0.12.1
      set device "port2"
   next
   edit 3
      set dst 10.0.0.0 255.0.0.0
      set gateway 10.0.8.1
      set device "port3"
   next
end
```

Secondary FortiGate

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

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address, and so needs to be configured in a public subnet. This will be used as a management interface and also the interface from which API calls are made (this will be assigned in the HA configuration). See this interface's OCI configuration, then the corresponding FortiGate-VM configuration.



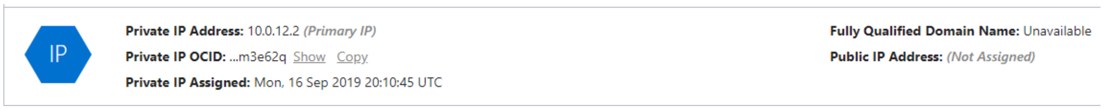
Private IP Address: 10.0.0.4 *(Primary IP)*
Private IP OCID: ...cxjgya Show Copy
Private IP Assigned: Mon, 16 Sep 2019 20:05:52 UTC

Fully Qualified Domain Name: fgtvminstance-2... Show Copy
Public IP Address: 132.145.109.8 *(Ephemeral)*
Public IP OCID: ...hoshva Show Copy

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.0.0.4 255.255.255.0
      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 FortiGate syncs the configuration from the primary unit.

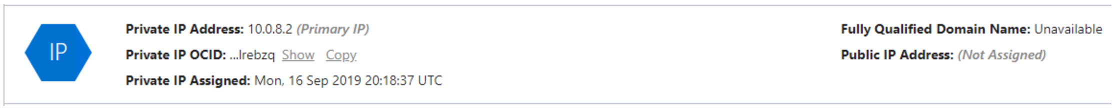


Private IP Address: 10.0.12.2 *(Primary IP)*
Private IP OCID: ...m3e62q Show Copy
Private IP Assigned: Mon, 16 Sep 2019 20:10:45 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

port3

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

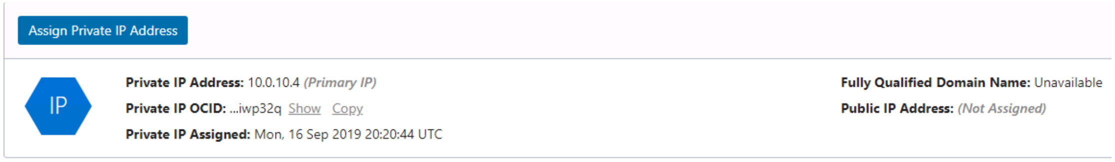


Private IP Address: 10.0.8.2 *(Primary IP)*
Private IP OCID: ...lrebzq Show Copy
Private IP Assigned: Mon, 16 Sep 2019 20:18:37 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

port4

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



Private IP Address: 10.0.10.4 *(Primary IP)*
Private IP OCID: ...iwp32q Show Copy
Private IP Assigned: Mon, 16 Sep 2019 20:20:44 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

```
config system interface
   edit "port4"
      set vdom "root"
```

```
        set ip 10.0.10.4 255.255.255.0
        set allowaccess ping https ssh fgfm
        set description "heartbeat"
    next
end
```

Initial Fabric connector configuration

First, you must configure a Fabric connector in FortiOS. This step is required to call APIs to OCI during HA failover.

Follow the steps in Certificate-based Security Fabric connector integration on page 74. Ensure you can successfully call APIs to OCI by referring to Troubleshooting OCI Fabric connector on page 81.

You must ensure that HA status is enabled for the Fabric connector:

```
config system sdn-connector
    edit "oci"
        set type oci
        set ha-status enable
    next
end
```

You must then configure A-P HA settings by using CLI commands on the GUI or via SSH.

Using a custom certificate

OCI requires a mechanism to append a certain signature/credential in making API requests. Currently FortiGate uses a certificate to do so. You must specify a certificate on the FortiGate for OCI when configuring A-P HA. The certificate calls APIs to OCI. In the previous deployment step, you used a built-in FortiGate certificate called "Fortinet_Factory".

For greater security, OCI recommends rotating the security element periodically. You may want to change the default certificate 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.

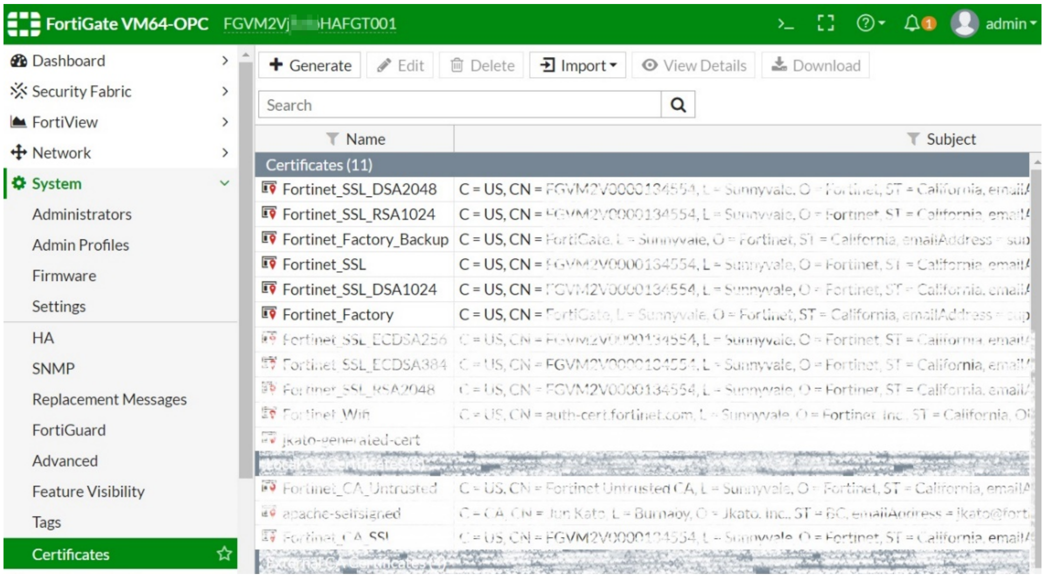
This section explains how to replace the certificate. This example uses a self-signed certificate that you created for your organization outside of the FortiGate. For details about the certificates that OCI requires, see Request Signatures.

You need three files:

- Certificate file (for use on the FortiGate)
- Key file (for use on the FortiGate)
- PEM file (for use on OCI)

The signing algorithm must be RSA SHA-256. In this example, you have used an RSA-2048-bit key to create a certificate.

1. Import your custom certificate to the primary FortiGate. There is no need to do the same on the secondary unit, as A-P HA enables a feature called configuration synchronization, where the certificate is automatically applied to the secondary unit with the FortiOS configuration:
    a. Log into the primary FortiGate and go to *System* > *Certificates*. The list of available FortiGate certificates displays.

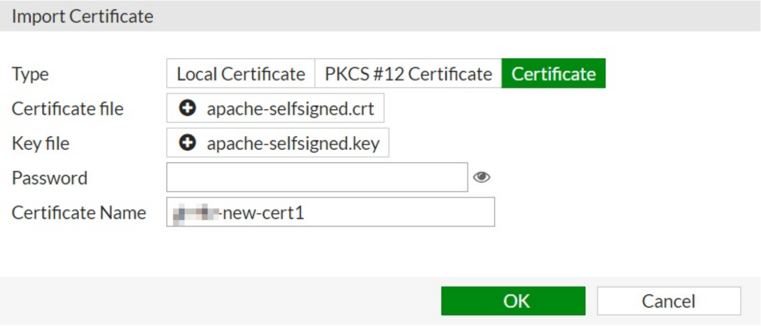


Name	Subject
Certificates (11)	
Fortinet_SSL_DSA2048	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
Fortinet_SSL_RSA1024	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
Fortinet_Factory_Backup	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = sup
Fortinet_SSL	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
Fortinet_SSL_DSA1024	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
Fortinet_Factory	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = sup
Fortinet_SSL_ECDSA256	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
Fortinet_SSL_ECDSA384	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
Fortinet_SSL_RSA2048	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet Inc., ST = California, O
jkato-generated-cert	
Local CA Certificates (3)	
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, email
apache-selfsigned	C = CA, CN = Jun Kato, L = Burnaby, O = Jkato. Inc., ST = BC, emailAddress = jkato@fort
Fortinet_CA_SSL	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = California, email
External CA Certificates ([illegible])	

b. Have a pair of the certificate and key files ready on the PC.

c. Click *Import* > *Local Certificate*. In the *Import Certificate* panel, for *Type*, select *Certificate*.

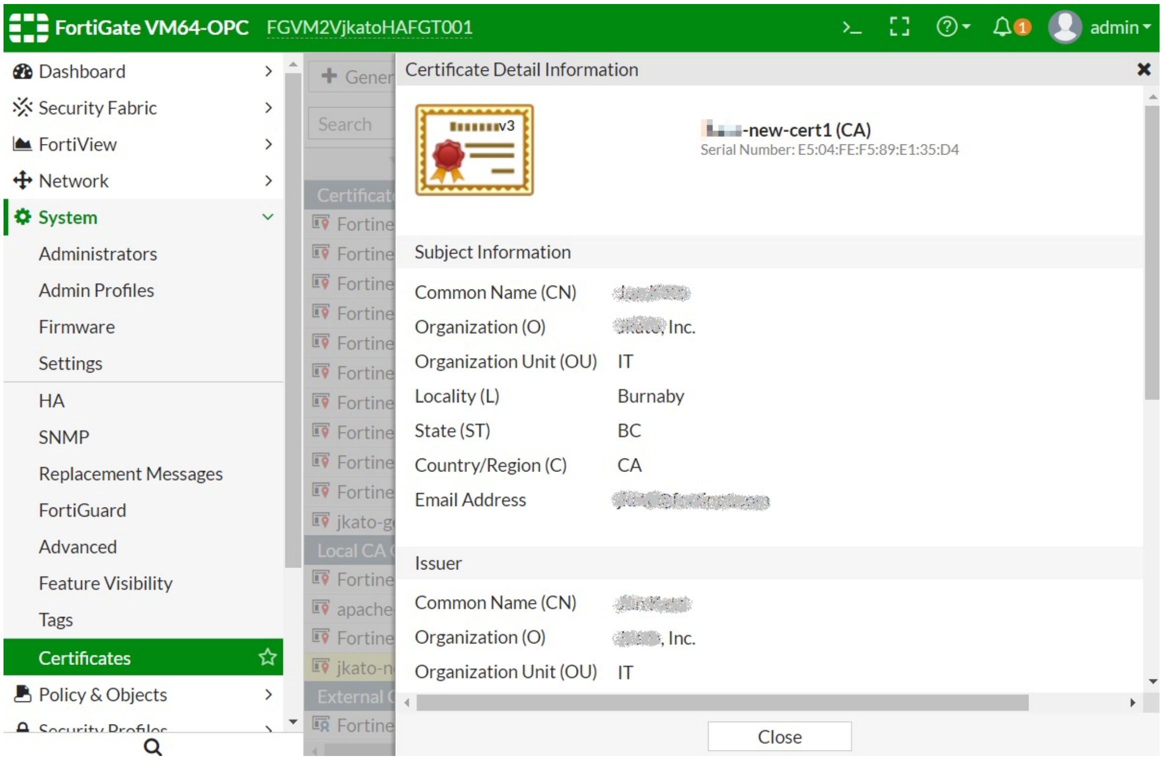
d. Upload the pair of certificate and key files. In this example, the file names are apache-selfsigned.crt and apache-selfsigned.key, respectively. Enter the password if any, and name the certificate as desired. Click *OK*.



Import Certificate

Type	Local Certificate / PKCS #12 Certificate / **Certificate**
Certificate file	apache-selfsigned.crt
Key file	apache-selfsigned.key
Password	
Certificate Name	[redacted]-new-cert1

e. The certificate displays on the screen. Double-click to show certificate detail.



Certificate Detail Information

[redacted]-new-cert1 (CA)
Serial Number: E5:04:FE:F5:89:E1:35:D4

Subject Information

Common Name (CN)	[redacted]
Organization (O)	[redacted], Inc.
Organization Unit (OU)	IT
Locality (L)	Burnaby
State (ST)	BC
Country/Region (C)	CA
Email Address	[redacted]

Issuer

Common Name (CN)	[redacted]
Organization (O)	[redacted], Inc.
Organization Unit (OU)	IT

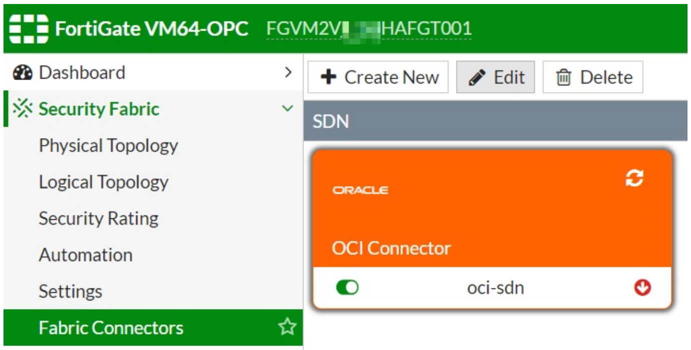
Close

2. Edit the OCI Fabric connector created earlier. You can do this via the GUI or the CLI.

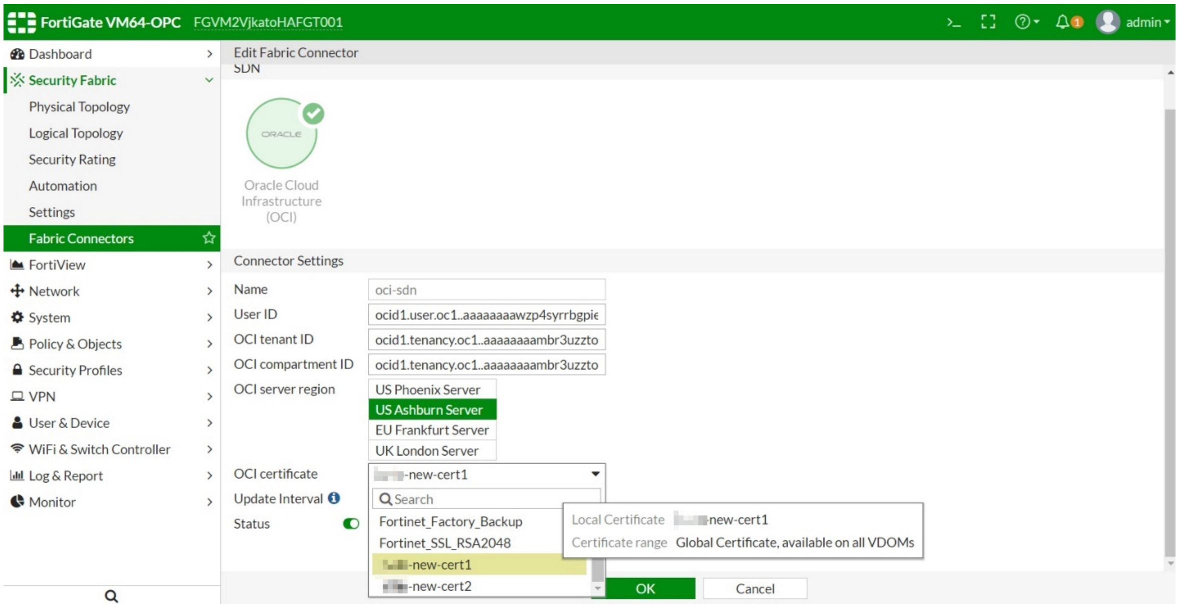
a. To edit the Fabric connector via the GUI, do the following:

i. Go to *Security Fabric > Fabric Connectors*.

ii. Select the Fabric connector, then click *Edit*.



iii. From the *OCI certificate* dropdown list, select the newly created certificate.



FortiGate VM64-OPC FGVM2VjkatoHAFGT001

Edit Fabric Connector

SDN

Oracle Cloud Infrastructure (OCI)

Connector Settings

- Name: oci-sdn
- User ID: ocid1.user.oc1..aaaaaaaawzp4syrrbgpie
- OCI tenant ID: ocid1.tenancy.oc1..aaaaaaaambr3uzzto
- OCI compartment ID: ocid1.tenancy.oc1..aaaaaaaambr3uzzto
- OCI server region: US Phoenix Server / US Ashburn Server (selected) / EU Frankfurt Server / UK London Server
- OCI certificate: [redacted]-new-cert1
- Update Interval
- Status

Certificate dropdown: Search; Fortinet_Factory_Backup; Fortinet_SSL_RSA2048; [redacted]-new-cert1; [redacted]-new-cert2

Local Certificate: [redacted]new-cert1
Certificate range: Global Certificate, available on all VDOMs

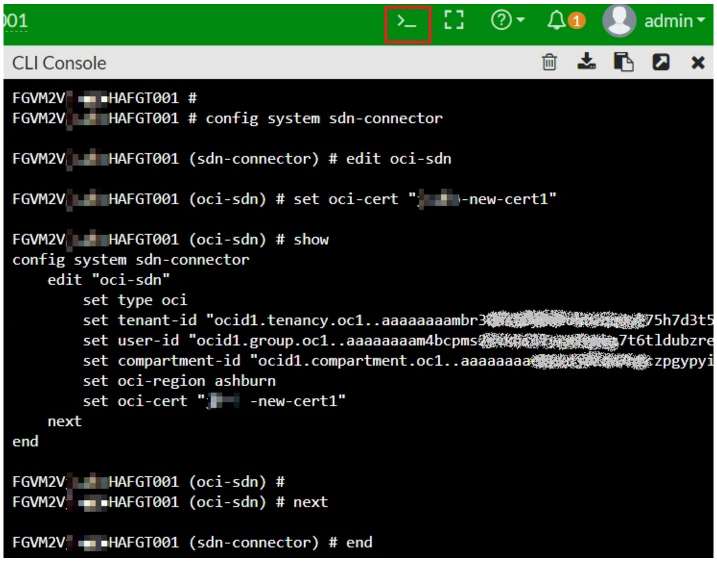
iv. Click *OK*.

b. To edit the Fabric connector via the CLI, do the following:

i. Open the CLI console in the FortiGate-VM management console.

ii. Enter CLI commands as follows to point to the new certificate. The `show` command shows what is currently configured. `next` and `end` save the configuration and returns to the original indentation with which you started. Replace `oci-sdn` with the name you configured for your Fabric connector, and enter the desired certificate name. The example certificate name is jkato-new-cert1.

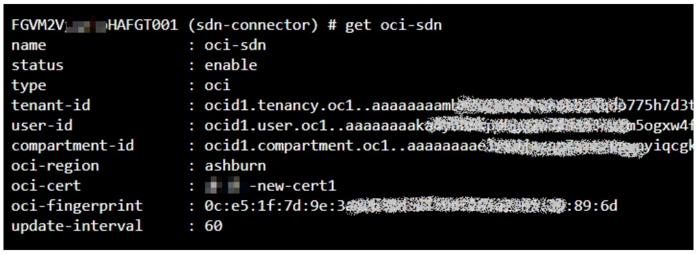
```
config system sdn-connector
   edit oci-sdn
      set oci-cert “your_certificate_name”
   next
end
```



CLI Console

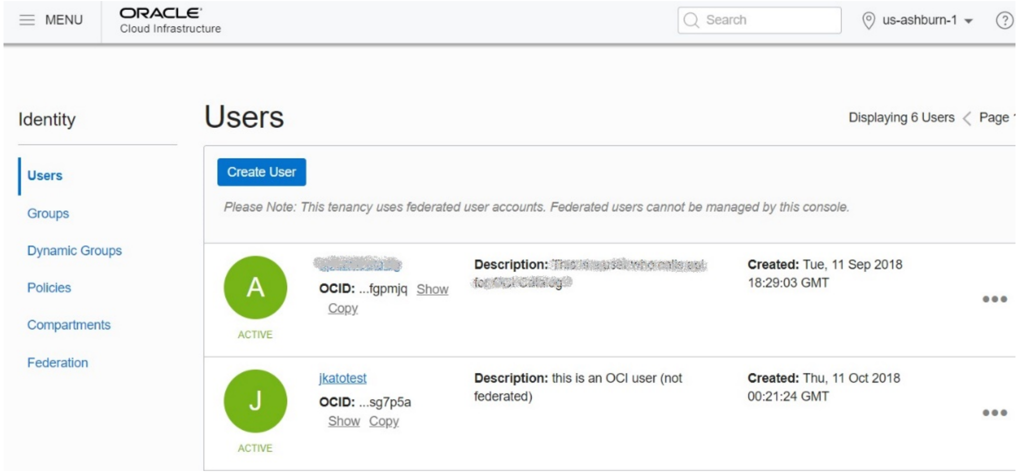
```
FGVM2V[redacted]HAFGT001 #
FGVM2V[redacted]HAFGT001 # config system sdn-connector

FGVM2V[redacted]HAFGT001 (sdn-connector) # edit oci-sdn

FGVM2V[redacted]HAFGT001 (oci-sdn) # set oci-cert "[redacted]-new-cert1"

FGVM2V[redacted]HAFGT001 (oci-sdn) # show
config system sdn-connector
    edit "oci-sdn"
        set type oci
        set tenant-id "ocid1.tenancy.oc1..aaaaaaaambr3[redacted]75h7d3t5
        set user-id "ocid1.group.oc1..aaaaaaaam4bcpms[redacted]7t6tldubzre
        set compartment-id "ocid1.compartment.oc1..aaaaaaaa[redacted]zpgypyi
        set oci-region ashburn
        set oci-cert "[redacted] -new-cert1"
    next
end

FGVM2V[redacted]HAFGT001 (oci-sdn) #
FGVM2V[redacted]HAFGT001 (oci-sdn) # next

FGVM2V[redacted]HAFGT001 (sdn-connector) # end
```

You can see the configuration by running `get OCI_connector_name`.



```
FGVM2V[redacted]HAFGT001 (sdn-connector) # get oci-sdn
name                : oci-sdn
status              : enable
type                : oci
tenant-id           : ocid1.tenancy.oc1..aaaaaaaam[redacted]775h7d3t
user-id             : ocid1.user.oc1..aaaaaaaaka[redacted]m5ogxw4t
compartment-id      : ocid1.compartment.oc1..aaaaaaaae[redacted]yiqcgk
oci-region          : ashburn
oci-cert            : [redacted] -new-cert1
oci-fingerprint     : 0c:e5:1f:7d:9e:3[redacted]:89:6d
update-interval     : 60
```

3. Next, you must add a new fingerprint for the user based on the new certificate's PEM. Log into the OCI compute portal and locate the user, which you specified with *user-id* above.



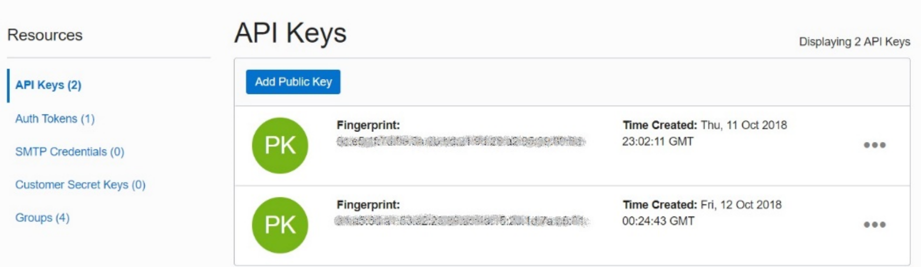
Users

Displaying 6 Users Page

Please Note: This tenancy uses federated user accounts. Federated users cannot be managed by this console.

A ACTIVE	[redacted] **OCID:** ...fgpmjq Show Copy	**Description:** [redacted]	**Created:** Tue, 11 Sep 2018 18:29:03 GMT
J ACTIVE	jkatotest **OCID:** ...sg7p5a Show Copy	**Description:** this is an OCI user (not federated)	**Created:** Thu, 11 Oct 2018 00:21:24 GMT

a. Select the user and go to API Keys. Click *Add Public Key*.

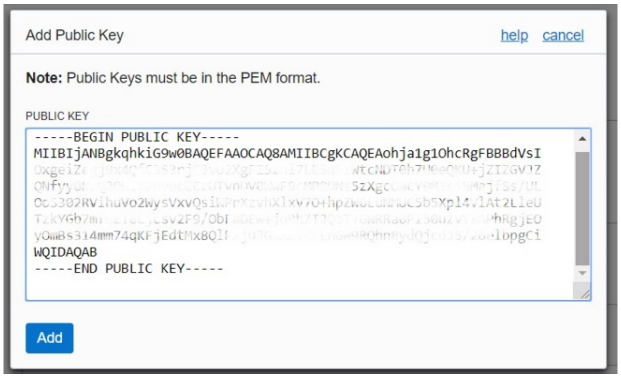


API Keys

Displaying 2 API Keys

PK	**Fingerprint:** [redacted]	**Time Created:** Thu, 11 Oct 2018 23:02:11 GMT
PK	**Fingerprint:** [redacted]	**Time Created:** Fri, 12 Oct 2018 00:24:43 GMT

b. Copy and paste the content of the PEM key. Click *Add*.

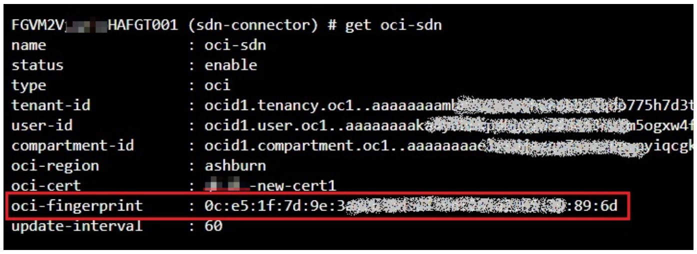


Note: Public Keys must be in the PEM format.

PUBLIC KEY

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAohja1g1OhcRgFBBBdVsI
[redacted]
WQIDAQAB
-----END PUBLIC KEY-----
```

You should see that a new fingerprint has been added. You can also see the fingerprint in the CLI by running the `get OCI_connector_name` command.



```
FGVM2V[redacted]HAFGT001 (sdn-connector) # get oci-sdn
name                : oci-sdn
status              : enable
type                : oci
tenant-id           : ocid1.tenancy.oc1..aaaaaaaam[redacted]o775h7d3t
user-id             : ocid1.user.oc1..aaaaaaaak[redacted]m5ogxw4f
compartment-id      : ocid1.compartment.oc1..aaaaaaaae[redacted]yiqcgk
oci-region          : ashburn
oci-cert            : [redacted]-new-cert1
oci-fingerprint     : 0c:e5:1f:7d:9e:3[redacted]:89:6d
update-interval     : 60
```

4. Check if you can successfully make API calls by referring to Troubleshooting OCI Fabric connector on page 81.

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 port 1, as OCI allows only port 1 for metadata access.
- When setting priority on FortiGate B, set the priority to 100 (lower than FortiGate 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 FortiGate B, which has port4 IP address 10.0.10.4 in the example. When setting FortiGate B's configuration, specify FortiGate A's port4 IP address, which is 10.0.10.3.

The following is the primary FortiGate 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 10.0.10.4
end
```

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

The following is the secondary FortiGate 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 10.0.10.3
end
```

Troubleshooting

To validate your HA configuration sync you can issue:

```
diagnose sys ha checksum show
```

OCI components in FortiOS come with their own daemon, including debug output. This can be invoked with:

```
diagnose debug application ocid -99
```

You can display diagnose commands with:

```
diagnose test application ocid -1
1. show HA stats
2. SDN api test
3. HA api test
4. filter list test
99. restart
```

You can verify that the following `diagnose` command works for the ocid daemon:

On FortiGate A:

```
diag test application ocid 1
ocid stats:
master: 1
```

On FortiGate B:

```
diag test application ocid 1
ocid stats:
master: 0
```

`SDN api test` is practical to see whether your sdn-connector configuration can successfully authenticate and issue commands to OCI Management.

Running `HA api test` on production environments is not recommended. This may lead your cluster to a mixed state. Use it only to see whether ocid daemon successfully sends failover commands to OCI Management.

If you have performed any modifications to your CLI configuration, restart your ocid daemon by running the following commands:

```
diag test application ocid 99
ocid start
```

By default, all configuration between firewalls is synchronized. Since some settings, especially NAT, are node-specific, you may want to disable synchronization.

```
config system ha
   set sync-config disable
end
```

During a successful HA failover event, the secondary FortiGate-VM takes over the private IP address from the active unit to the passive unit. The following shows the sample debug output in this scenario:

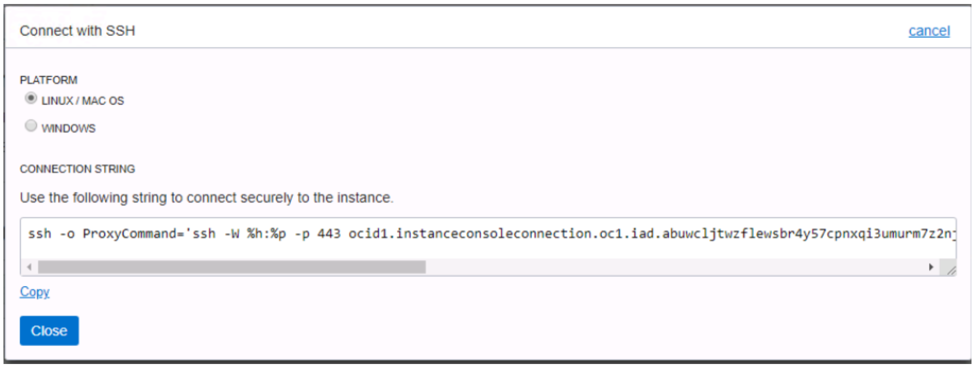
```
FGVM8VTM19000449 # diag debug enable
FGVM8VTM19000449 # diag debug application ocid -1
Debug messages will be on for 30 minutes.
FGVM8VTM19000449 # HA event
Become HA master
ocid collect vnics info for instance fgtvminstance-2
vnic id(1/4): ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljraiheu5bqvg5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a
vnic id(2/4): ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljrhxf63fvlacjnyl6del3vzo42g5cjyvlczvosxuc5dtn4zqrnwdsa
vnic id(3/4): ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljr3hmbq675vbgjbuwn2aywjhonqmwb5slxjitwy4pyw3fipa2wzwpq
vnic id(4/4): ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljruyxpzi4db2tjet45gix3qauwwgnvf3pbsjcvbd337rgr7ygyy4ka
ocid fail over private ip: 10.0.12.3
private ip 10.0.12.3 is attached in remote instance
attaching private ip 10.0.12.3 to local vnic (ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljraiheu5bqvg5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a)
updating private ip with data: {"vnicId": "ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljraiheu5bqvg5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a"}
moving private ip 10.0.12.3 to local successfully
ocid fail over private ip: 10.0.12.5
private ip 10.0.12.5 is attached in remote instance
attaching private ip 10.0.12.5 to local vnic (ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljraiheu5bqvg5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a)
updating private ip with data: {"vnicId": "ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljraiheu5bqvg5riy4rsngg2lm6z766glghhlneqjld3gcpquuhlv5a"}
moving private ip 10.0.12.5 to local successfully
ocid fail over private ip: 10.0.8.10
private ip 10.0.8.10 is attached in remote instance
attaching private ip 10.0.8.10 to local vnic (ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljr3hmbq675vbgjbuwn2aywjhonqmwb5slxjitwy4pyw3fipa2wzwpq)
updating private ip with data: {"vnicId": "ocid1.vnic.oc1.ca-toronto-
     1.ab2g6ljr3hmbq675vbgjbuwn2aywjhonqmwb5slxjitwy4pyw3fipa2wzwpq"}
moving private ip 10.0.8.10 to local successfully
```

To access FortiOS via the console:

If the instance is malfunctioning, you can attempt access to the instance via the console for troubleshooting.

1. Create the console connection for an instance:
   a. In the OCI console, go to *Core Infrastructure* > *Compute* > *Instances*. Select the desired instance name.
   b. Go to *Resources* > *Console Connections*. Click *Create Console Connection*.
   c. Specify the public key (.pub) portion for the SSH key. You can browse to a public key file on your computer or paste your public key into the text field. Then, click *Create Console Connection*. When the console connection has been created and is available, the status changes to *ACTIVE*.

2. Connect to FortiOS via the console using OpenSSH on macOS or Linux:
   a. Click the *Actions* icon, then click *Connect with SSH*.
   b. In the *Connect with SSH* dialog, click *Copy* to copy the string to your clipboard.



Use the following string to connect securely to the instance.

```
ssh -o ProxyCommand='ssh -W %h:%p -p 443 ocid1.instanceconsoleconnection.oc1.iad.abuwcljtwzflewsbr4y57cpnxqi3umurm7z2n
```

   c. Use the string to connect to the FortiGate-VM instance. Ensure that you specify the correct SSH key and use –i:

```
ssh -i id_rsa -o ProxyCommand='ssh -i id_rsa -W %h:%p -p 443 …..
```

Deploying FortiGate-VM 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 FortiGate NIC and attaches to the new primary FortiGate NIC.
- Route next hop updates to point to the new primary FortiGate NIC's primary private IP address.
- System interfaces, static route configurations, and sessions do not sync between FortiGates when deployed between multiple ADs. They do sync when deploying within one AD.

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

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

Checking the prerequisites

To deploy and configure the FortiGate-VM as an A-P HA solution, you need the following items:

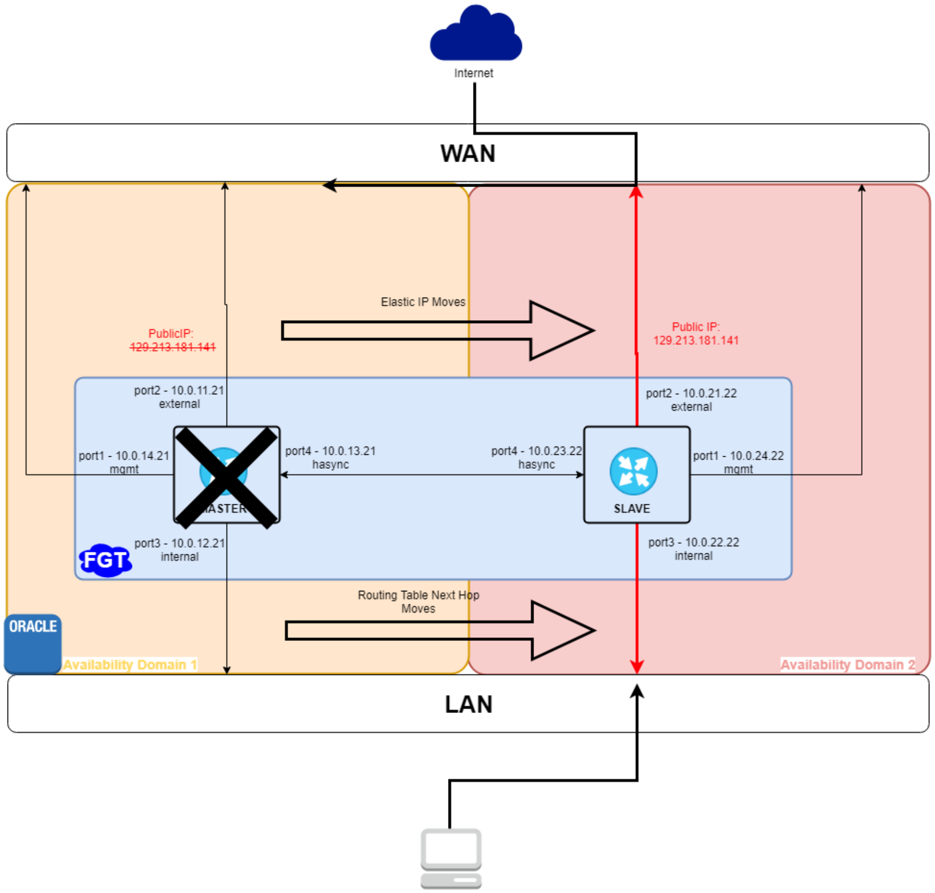
- OCI account to operate in OCI compute portal
- Availability to accommodate required OCI resources
  - See Service Limits.
  - VCN with eight subnets located in two different ADs for management, external, internal, and heartbeat purposes.

    - Three public IP addresses
    - All IP addresses must be static, not DHCP.
    - Two FortiGate-VM instances
- Two valid FortiGate-VM BYOL licenses. See Licensing on page 7
- The following summarizes minimum sufficient IAM roles for this deployment:
    - 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 subnets in tenancy
    - Allow dynamic-group <group_name> to manage private-ips in tenancy
    - Allow dynamic-group <group_name> to manage public-ips in tenancy
    - Allow dynamic-group <group_name> to manage route-tables in tenancy
    - To define simpler roles, use the following:
        - 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 manage virtual-network-family in tenancy

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

Reviewing the network topology

Failover Event



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

Port	OCI primary IP address	Subnet
Port 1	10.0.14.21	10.0.14.0/24 EIP1
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 FGT-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	OCI primary IP address	Subnet
Port 4	10.0.23.22	10.0.23.0/24

Configuring the OCI VCN

To configure the OCI VCN:

1. In the OCI console, go to *Networking* > *Virtual Cloud Networks* > *Subnets*.
2. 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.

3. Go to *Route Tables*.
4. Configure an internal routing table, setting the default gateway as FGT-A-AD1 NIC2's primary IP address (10.0.12.21). You can create this routing table after configuring NIC2 on FGT-A-AD1. Two subnets, net12-internal and net22-internal, use this routing table.
5. Configure an external routing table, setting the default gateway as this VCN's Internet gateway. The remaining six subnets use this routing table.

Deploying the FortiGate-VM

1. Prepare your OCI environment as detailed in Configuring the OCI VCN on page 52 if you do not have one yet.
2. To take advantage of A-P HA, you need four VNICs (port1 to port4) on each FortiGate-VM that constitutes an A-P HA cluster. Configure all required network interfaces (OCI VNICs and FortiGate-VM network interface configuration) that support A-P HA. You must choose an OCI instance type that supports at least four VNICs.
3. Ensure you configure the security list on each subnet for egress and ingress interfaces appropriately. It is particularly important that the management interfaces have egress Internet access for API calls to the OCI metadata server.
4. Ensure that you attached four NICs to each FortiGate and that you assigned the static private IP address.

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. If using SSH, the FortiGate may lose connection due to routing table changes, so configuring HA via the GUI is recommended.

To configure the HA interfaces on FGT-A-AD1:

```
config system interface
   edit "port1"
         set mode static
         set ip 10.0.14.21 255.255.255.0
         set allowaccess ping https ssh snmp http
      next
   edit "port2"
      set ip 10.0.11.21 255.255.255.0
      set allowaccess ping https ssh snmp http
   next
   edit "port3"
      set ip 10.0.12.21 255.255.255.0
      set allowaccess ping https ssh snmp http
   next
   edit "port4"
      set ip 10.0.13.21 255.255.255.0
      set allowaccess ping https ssh snmp http
   next
end
```

To configure the HA interfaces on FGT-B-AD2:

```
config system interface
   edit "port1"
      set mode static
      set ip 10.0.24.22 255.255.255.0
      set allowaccess ping https ssh snmp http
   next
   edit "port2"
      set ip 10.0.21.22 255.255.255.0
      set allowaccess ping https ssh snmp http
   next
   edit "port3"
      set ip 10.0.22.22 255.255.255.0
      set allowaccess ping https ssh snmp http
   next
   edit "port4"
      set ip 10.0.23.22 255.255.255.0
      set allowaccess ping https ssh snmp http
   next
end
```

To configure the routing tables on FGT-A-AD1:

```
config router static
   edit 1
      set gateway 10.0.11.1
      set device "port2"
   next
   edit 2
      set dst 10.0.22.0 255.255.255.0
      set gateway 10.0.12.1
      set device "port3"
   next
end
```

To configure the routing tables on FGT-B-AD2:

```
config router static
   edit 1
      set gateway 10.0.21.1
      set device "port2"
   next
   edit 2
      set dst 10.0.12.0 255.255.255.0
      set gateway 10.0.22.1
      set device "port3"
   next
end
```

To configure the OCI Fabric connector on FGT-A-AD1 and FGT-B-AD2:

```
config system sdn-connector
   edit "FGT-OCI-SDN"
      set type oci
      set use-metadata-iam disable
      set ha-status enable
      set tenant-id
           "ocid1.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a"
      set user-id
           "ocid1.user.oc1..aaaaaaaakgeja4xkdvgfcsfyctpj5gxwjlogq4iv3l673wsaljbfluegzh3q"
      set compartment-id
           "ocid1.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a"
      set oci-region "us-ashburn-1"
      set oci-cert "Fortinet_Factory"
   next
end
```

The Fabric connector settings are the same on both FortiGates. Ensure that you imported the oci-cert public key as an OCI user API key. You can print the certificate public key in the FortiOS CLI with the `diagnose oci pubkey` command.

To configure the firewall policy on FGT-A-AD1 and FGT-B-AD2:

```
config firewall policy
   edit 1
      set srcintf "port3"
      set dstintf "port2"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set nat enable
   next
end
```

To configure HA settings on FGT-A-AD1:

```
config system ha
   set group-name "ha-cross-ad"
   set mode a-p
   set hbdev "port4" 50
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port1"
         set gateway 10.0.14.1
      next
   end
   set unicast-hb enable
   set unicast-hb-peerip 10.0.23.22
end
```

To configure HA settings on FGT-B-AD2:

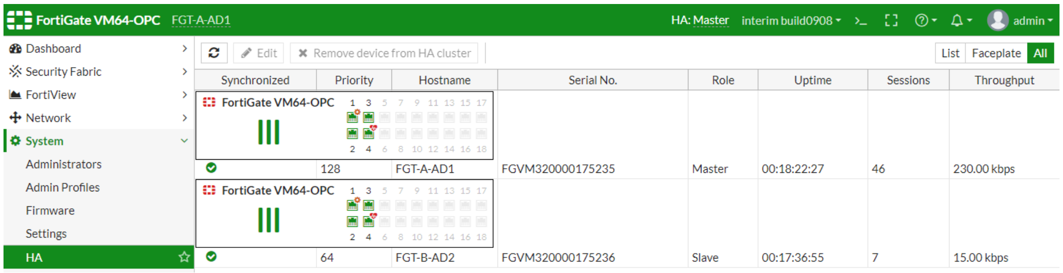
You must set the FGT-B HA priority to a value lower than FGT-A's priority level. The node with the lower priority level is determined as the secondary node.

```
config system ha
   set group-name "ha-cross-ad"
   set mode a-p
   set hbdev "port4" 50
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port1"
         set gateway 10.0.24.1
      next
   end
   set priority 64
   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 FortiOS on the primary FortiGate, go to *System > HA*. Check that the HA status is synchronized.



Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
✓	128	FGT-A-AD1	FGVM320000175235	Master	00:18:22:27	46	230.00 kbps
✓	64	FGT-B-AD2	FGVM320000175236	Slave	00:17:36:55	7	15.00 kbps

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 FGT-A-AD1, the current primary node.
3. Shut down FGT-A-AD1.
4. Verify that FGT-B-AD2 becomes the primary FortiGate.

5. Use an API call to verify that the internal routing table's next hop changed from FGT-A-AD1's internal NIC address (10.0.12.21) to FGT-B-AD2's internal NIC address (10.0.22.22) and that the EIP address attached to FGT-A-AD1's external NIC reattached to FGT-B-AD2's external NIC. You can also use the following diagnose command:

```
FGT-B-AD2 # d deb app ocid -1
Debug messages will be on for 30 minutes.

FGT-B-AD2 # d deb en

FGT-B-AD2 # 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 FGT-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: FGT-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 FGT-B-AD2, the new primary node.

Deploying FortiGate-VM HA on OCI between multiple ADs using a regional VCN

This deployment process consists of the following steps:

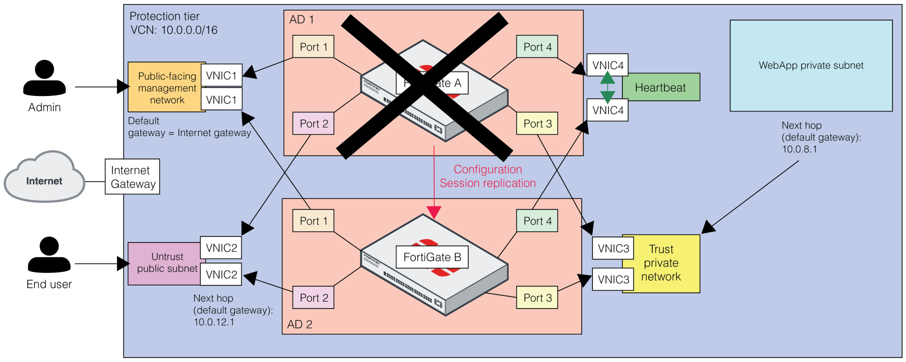
Checking the prerequisites

To deploy and configure the FortiGate-VM as an A-P HA solution, you need the following items:

- OCI account to operate in OCI compute portal
- Availability to accommodate required OCI resources
  - See Service Limits.
  - VCN with five subnets
  - Three public IP addresses
    - One for traffic to/through the active (primary) FortiGate-VM
    - Two for management access to each FortiGate-VM
  - All IP addresses must be static, not DHCP.
  - Two FortiGate-VM instances
    - You must deploy the two nodes in different ADs and under the same VCN.
    - Each FortiGate-VM must have at least four network interfaces. See Compute Shapes.
- Two valid FortiGate-VM BYOL licenses. See Licensing on page 7.
- The following summarizes minimum sufficient IAM roles for this deployment:
  - 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 subnets in tenancy
  - Allow dynamic-group <group_name> to manage private-ips in tenancy
  - Allow dynamic-group <group_name> to manage public-ips in tenancy
  - Allow dynamic-group <group_name> to manage route-tables in tenancy
  - To define simpler roles, use the following:
    - 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 manage virtual-network-family in tenancy

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

Reviewing the network topology



FortiGate A

Component	IP address
Port 1	Public IP: 129.146.x.x Primary private IP: 10.0.13.3
Port 2	Public IP: 129.146.x.x Port IP: 10.0.12.6 = OCI vNIC's secondary IP
Port 3	Port IP: 10.0.8.3 Secondary private IP: 10.0.8.10
Port 4	Primary private IP: 10.0.10.3

FortiGate B

Component	IP address
Port 1	Public IP: 129.146.x.x Primary private IP: 10.0.13.4
Port 2	Public IP: 129.146.x.x When FortiGate A fails, its port 2's secondary IP address, 10.0.12.6, moves to FortiGate B's port 2. Therefore, the public IP address that is paired with the secondary private IP address also moves.
Port 3	Port IP: 10.0.8.12 When FortiGate A fails, its port 3's secondary IP address, 10.0.8.10, moves to FortiGate B's port 3.
Port 4	Primary private IP: 10.0.10.4

Subnets

Subnet	IP address
Heartbeat	10.0.10.0/24
Trust private subnet	10.0.8.10/24
Untrust public subnet	10.0.12.0/24
Public-facing management network	10.0.0.0/24
WebApp private subnet	10.0.201.0/24

A recommended installation requires four network interfaces per FortiGate-VM node. In addition to inbound and outbound data interfaces, two interfaces are used for internal operations: management and heartbeat. Ensure you choose OCI VM instance sizes that can equip four network interfaces.

The table describes the usage of each port. Port1 and 2 are on public (or untrusted) subnets, and public IP addresses are allocated to them.

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.
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. FortiGate 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 FortiGate nodes. This is unicast communication. This heartbeat interface has its dedicated "hbdev" VDOM and cannot be used for any other purpose.

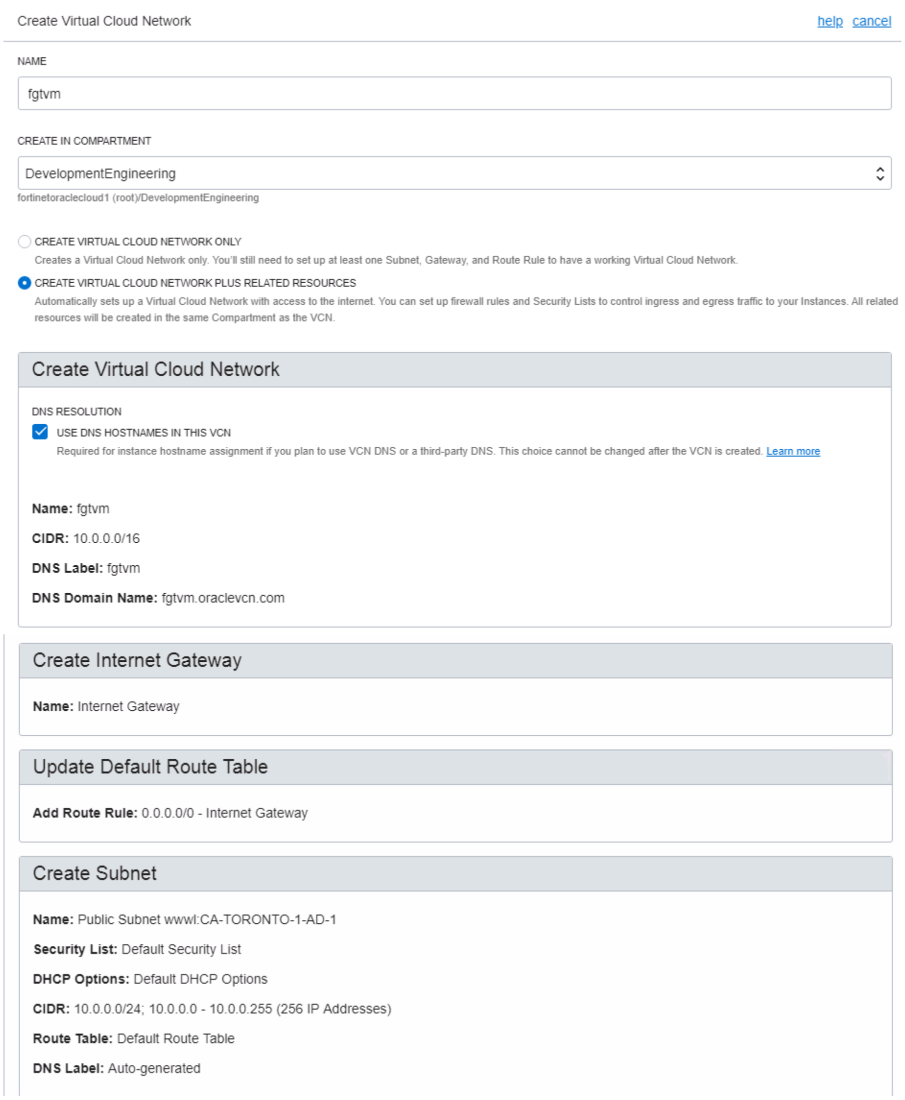
You must configure port 1 as the management interface. The other ports are interchangeable. The best practice is to locate each port in a different subnet.

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 multiple-AD HA topology

To create a VCN and public-facing subnets:

1. In OCI, go to *Networking* > *Virtual Cloud Networks*, and click *Create Virtual Cloud Network*.
2. In the *NAME* field, enter the VCN name. Then, select *CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES*. This allows you to create the Internet gateway, routing table, and subnet all together using Oracle default settings. If you intend to create each resource separately by specifying your own inputs, click *CREATE VIRTUAL CLOUD NETWORK ONLY*. This example uses the first choice.



Create Virtual Cloud Network

NAME

fgtvm

CREATE IN COMPARTMENT

DevelopmentEngineering

fortinetoraclecloud1 (root)/DevelopmentEngineering

○ CREATE VIRTUAL CLOUD NETWORK ONLY

Creates a Virtual Cloud Network only. You'll still need to set up at least one Subnet, Gateway, and Route Rule to have a working Virtual Cloud Network.

● CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES

Automatically sets up a Virtual Cloud Network with access to the internet. You can set up firewall rules and Security Lists to control ingress and egress traffic to your Instances. All related resources will be created in the same Compartment as the VCN.

Create Virtual Cloud Network

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

Name: fgtvm

CIDR: 10.0.0.0/16

DNS Label: fgtvm

DNS Domain Name: fgtvm.oraclevcn.com

Create Internet Gateway

Name: Internet Gateway

Update Default Route Table

Add Route Rule: 0.0.0.0/0 - Internet Gateway

Create Subnet

Name: Public Subnet wwwl:CA-TORONTO-1-AD-1

Security List: Default Security List

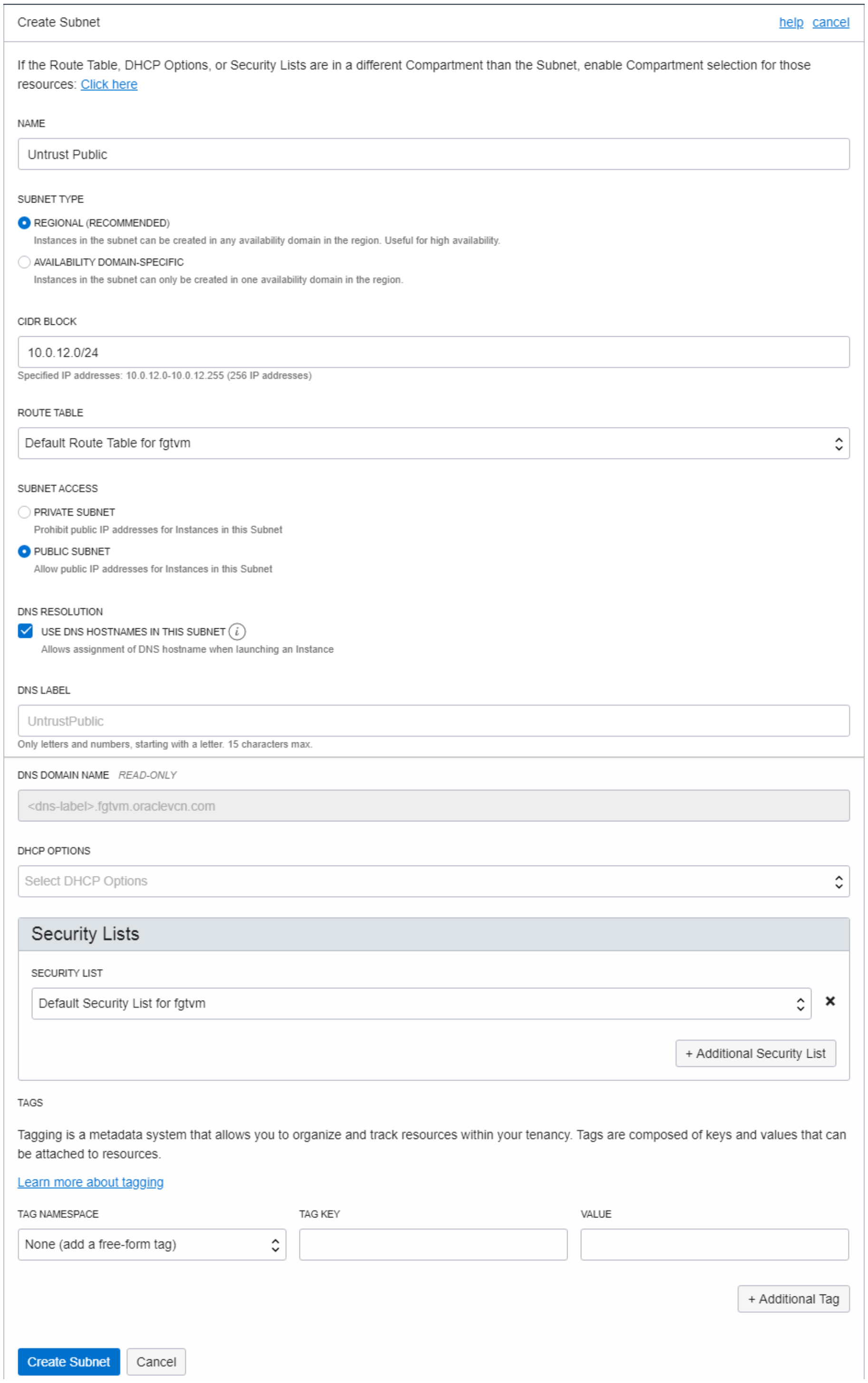
DHCP Options: Default DHCP Options

CIDR: 10.0.0.0/24; 10.0.0.0 - 10.0.0.255 (256 IP Addresses)

Route Table: Default Route Table

DNS Label: Auto-generated

3. Click *Create Virtual Cloud Network* at the bottom of the screen, then click *Close*.
   This configures the related resources.
4. Create the other subnets:
   a. Go to *Networking* > *Virtual Cloud Networks*. Click the name of the previously created VCN, then click *Create Subnet*.
   b. For *Subnet Type*, select *Regional*.
   c. For *Subnet Access*, select *Private* or *Public Subnet* as desired. The screenshot shows the configuration for the public subnet.



Create Subnet

help cancel

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: Click here

NAME

Untrust Public

SUBNET TYPE

● REGIONAL (RECOMMENDED)

Instances in the subnet can be created in any availability domain in the region. Useful for high availability.

○ AVAILABILITY DOMAIN-SPECIFIC

Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK

10.0.12.0/24

Specified IP addresses: 10.0.12.0-10.0.12.255 (256 IP addresses)

ROUTE TABLE

Default Route Table for fgtvm

SUBNET ACCESS

○ PRIVATE SUBNET

Prohibit public IP addresses for Instances in this Subnet

● PUBLIC SUBNET

Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

☑ USE DNS HOSTNAMES IN THIS SUBNET

Allows assignment of DNS hostname when launching an Instance

DNS LABEL

UntrustPublic

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

DNS DOMAIN NAME *READ-ONLY*

<dns-label>.fgtvm.oraclevcn.com

DHCP OPTIONS

Select DHCP Options

Security Lists

SECURITY LIST

Default Security List for fgtvm

+ Additional Security List

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

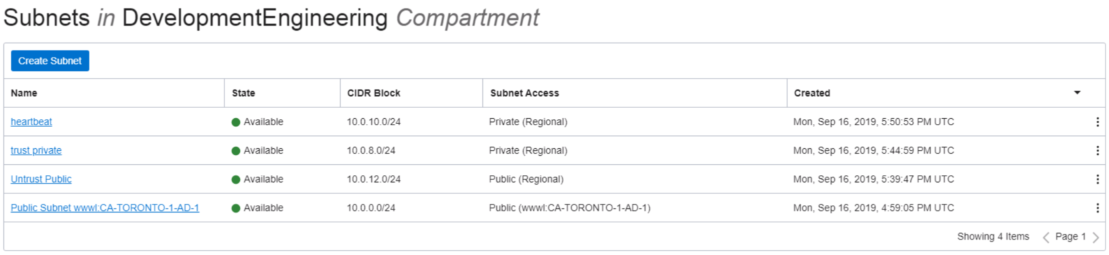
Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		

+ Additional Tag

Create Subnet Cancel

d. Repeat to create a minimum of four subnets for HA setup. The following shows an example of the minimum requirement:



Subnets *in* DevelopmentEngineering *Compartment*

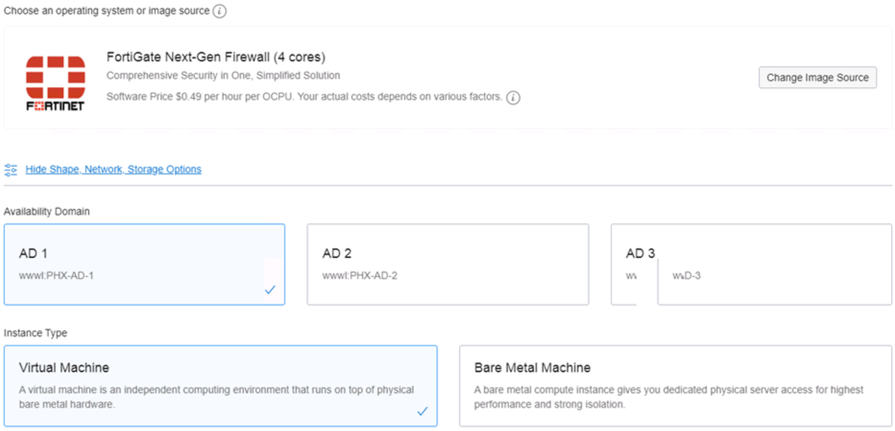
Create Subnet

Name	State	CIDR Block	Subnet Access	Created
heartbeat	● Available	10.0.10.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:50:53 PM UTC
trust private	● Available	10.0.8.0/24	Private (Regional)	Mon, Sep 16, 2019, 5:44:59 PM UTC
Untrust Public	● Available	10.0.12.0/24	Public (Regional)	Mon, Sep 16, 2019, 5:39:47 PM UTC
Public Subnet wwwl:CA-TORONTO-1-AD-1	● Available	10.0.0.0/24	Public (wwwl:CA-TORONTO-1-AD-1)	Mon, Sep 16, 2019, 4:59:05 PM UTC

Showing 4 Items Page 1

Deploying the FortiGate-VM

1. Set up the OCI VCN environment. See Creating a VCN for multiple-AD HA topology on page 60.
2. Deploy FortiGate-VMs in the environment for an active-passive configuration. See Creating a FortiGate-VM instance on page 11. To deploy FortiGate-VM from the marketplace, see Deploying FortiGate-VM via the marketplace on page 29. You must select different ADs when creating the Compute instances:



Choose an operating system or image source

FortiGate Next-Gen Firewall (4 cores)

Comprehensive Security in One, Simplified Solution

Software Price $0.49 per hour per OCPU. Your actual costs depends on various factors.

Change Image Source

Hide Shape, Network, Storage Options

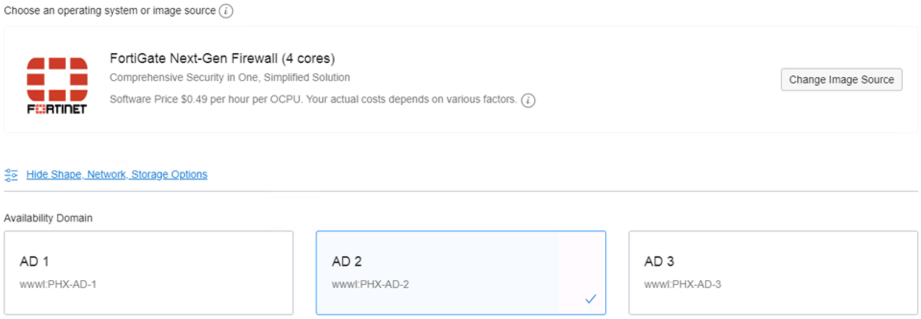
Availability Domain

AD 1 ✓ wwwl:PHX-AD-1 | AD 2 wwwl:PHX-AD-2 | AD 3 w\ w\D-3

Instance Type

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

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



Choose an operating system or image source

FortiGate Next-Gen Firewall (4 cores)

Comprehensive Security in One, Simplified Solution

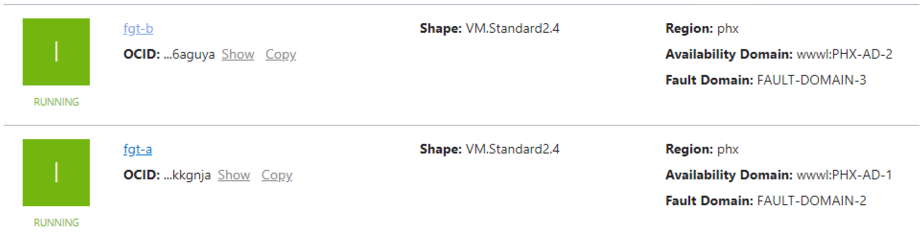
Software Price $0.49 per hour per OCPU. Your actual costs depends on various factors.

Change Image Source

Hide Shape, Network, Storage Options

Availability Domain

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



fgt-b — RUNNING

OCID: ...6aguya Show Copy

Shape: VM.Standard2.4

Region: phx

Availability Domain: wwwl:PHX-AD-2

Fault Domain: FAULT-DOMAIN-3

fgt-a — RUNNING

OCID: ...kkgnja Show Copy

Shape: VM.Standard2.4

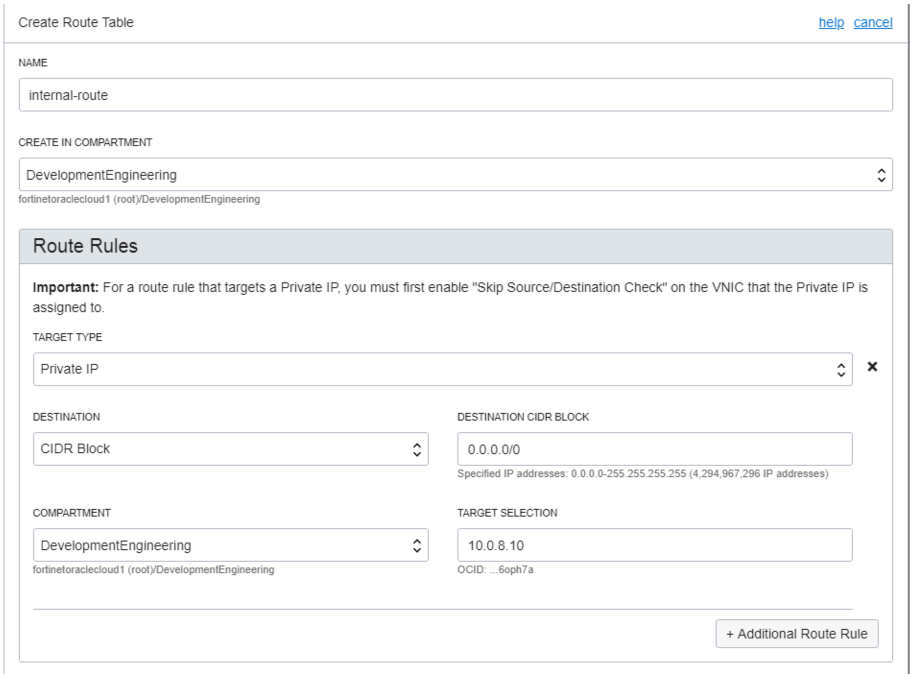
Region: phx

Availability Domain: wwwl:PHX-AD-1

Fault Domain: FAULT-DOMAIN-2

3. Configure extra VNICs for the FortiGate-VM. You must ensure there are at least four network interfaces configured for each instance. See Checking the prerequisites on page 31. To create an extra VNIC, see Creating the second virtual network interface (VNIC) on page 22. To configure the extra VNIC, see Configuring the second VNIC on the FortiGate-VM on page 24.

4. Update route rules to point to the internal/trust private IP address on the active FortiGate. It is recommended to create a separate route table for the internal/trust subnet:
   a. Go to *Networking* > *Virtual Cloud Networks* > *<VCN used>* > *Route Tables*, then click *Create Route Table*.
   b. Specify the route table to point to the internal/trust private IP address on the active FortiGate:



Create Route Table

NAME
internal-route

CREATE IN COMPARTMENT
DevelopmentEngineering
fortinetoraclecloud1 (root)/DevelopmentEngineering

Route Rules

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.

TARGET TYPE
Private IP

DESTINATION
CIDR Block

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

COMPARTMENT
DevelopmentEngineering
fortinetoraclecloud1 (root)/DevelopmentEngineering

TARGET SELECTION
10.0.8.10
OCID: ...6oph7a

   c. Go to *Networking* > *Virtual Cloud Networks* > *<VCN used>*. Edit the desired subnet.
   d. Under *Route Table*, update the configuration to the newly created route table.

Configuring the OCI HA interfaces

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

In the case of HA, it is necessary that the FortiGate-VMs have the correct IP information statically configured in order to provide proper failover between the two devices.

OCI API calls enable the failover mentioned above through the OCI Fabric connector, but only for IP addresses configured as secondary in the OCI VNIC configuration.

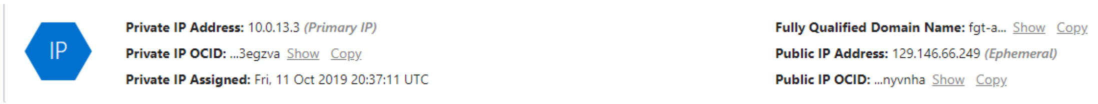
Also, OCI API calls, if initiated from within a VCN, must be made by a primary interface with a public address. Thus, the network configuration for OCI HA will be unique and very specific.

You may lose connection to the instance during interface IP address and route configuration. It is therefore recommended to perform this configuration via the console.

Primary FortiGate

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address configured in a public subnet. This will be used as a management interface and also the interface from which API calls are made (this will be assigned in the HA configuration). See this interface's OCI configuration, then the corresponding FortiGate-VM configuration.



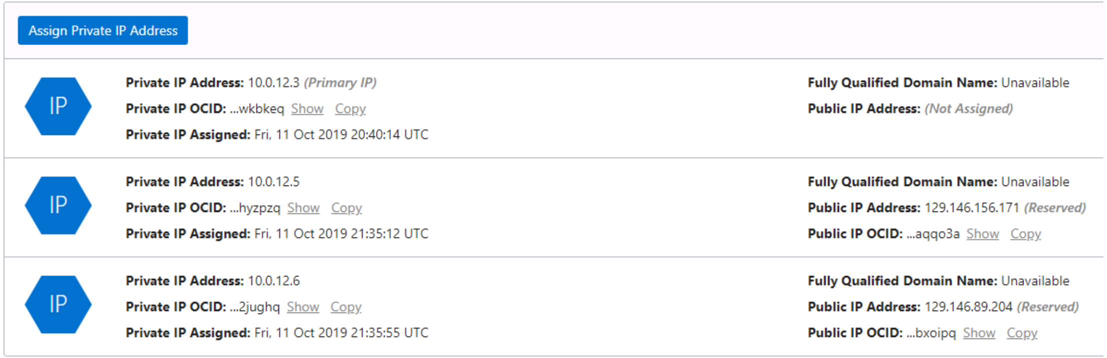
Private IP Address: 10.0.13.3 *(Primary IP)*
Private IP OCID: ...3egzva Show Copy
Private IP Assigned: Fri, 11 Oct 2019 20:37:11 UTC

Fully Qualified Domain Name: fgt-a... Show Copy
Public IP Address: 129.146.66.249 *(Ephemeral)*
Public IP OCID: ...nyvnha Show Copy

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.0.13.3 255.255.255.0
      set allowaccess ping https ssh http fgfm
      set description "management"
      set mtu-override enable
      set mtu 9000
   next
end
```

port2

In this example, port2 is assumed to be a public/WAN-facing interface. The following FortiGate configuration does not use the primary IP address for its interface IP address. Instead, it uses the non-primary private IP address, as shown. This is because the primary IP address is not relocatable to the secondary FortiGate in the event of HA failover. In this example, the FortiGate uses only 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 FortiGate. Therefore, if any extra non-primary private IP addresses are used in the setup, these IP addresses must be referenced explicitly in the interface configuration by enabling secondary IP addresses.



Private IP Address: 10.0.12.3 *(Primary IP)*
Private IP OCID: ...wkbkeq Show Copy
Private IP Assigned: Fri, 11 Oct 2019 20:40:14 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

Private IP Address: 10.0.12.5
Private IP OCID: ...hyzpzq Show Copy
Private IP Assigned: Fri, 11 Oct 2019 21:35:12 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: 129.146.156.171 *(Reserved)*
Public IP OCID: ...aqqo3a Show Copy

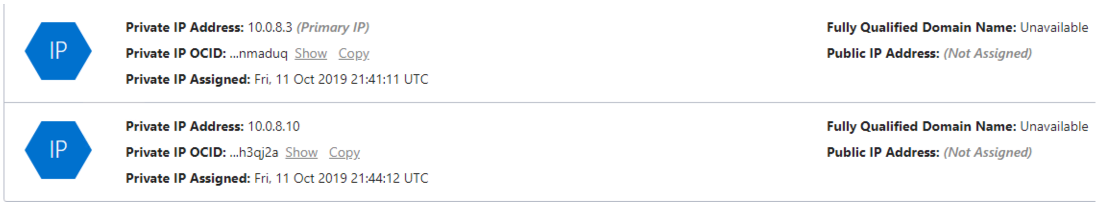
Private IP Address: 10.0.12.6
Private IP OCID: ...2jughq Show Copy
Private IP Assigned: Fri, 11 Oct 2019 21:35:55 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: 129.146.89.204 *(Reserved)*
Public IP OCID: ...bxoipq Show Copy

```
config system interface
   edit "port2"
   set vdom "root"
      set ip 10.0.12.5 255.255.255.0
      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 10.0.12.6 255.255.255.0
            set allowaccess ping https ssh fgfm
         next
      end
   next
end
```

port3

This example configures port3 as the internal port, which is used to connect to internal resources on local subnets, peered VCNs, and so on. However, as mentioned earlier, FortiGate does not use the primary IP address.



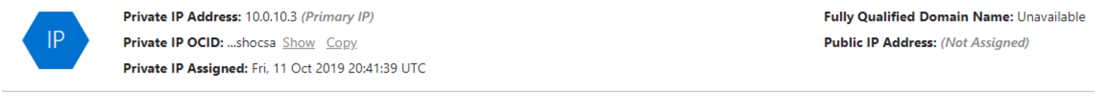
Private IP Address: 10.0.8.3 *(Primary IP)*
Private IP OCID: ...nmaduq Show Copy
Private IP Assigned: Fri, 11 Oct 2019 21:41:11 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

Private IP Address: 10.0.8.10
Private IP OCID: ...h3qj2a Show Copy
Private IP Assigned: Fri, 11 Oct 2019 21:44:12 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

```
config system interface
   edit "port3"
      set vdom "root"
      set ip 10.0.8.10 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "trusted"
      set mtu-override enable
      set mtu 9000
   next
end
```

port4

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



Private IP Address: 10.0.10.3 *(Primary IP)*
Private IP OCID: ...shocsa Show Copy
Private IP Assigned: Fri, 11 Oct 2019 20:41:39 UTC
Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

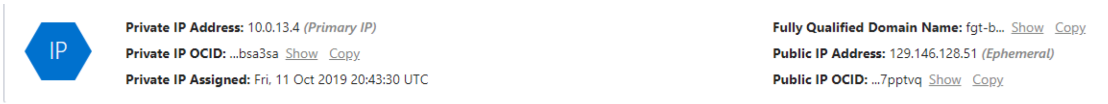
```
config system interface
   edit "port4"
      set vdom "root"
      set ip 10.0.10.3 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "heartbeat"
      set mtu-override enable
      set mtu 9000
   next
end
```

Secondary FortiGate

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

port1

The primary VNIC associated with the FortiGate NVA must have a primary IP address with a corresponding public IP address, and so needs to be configured in a public subnet. This will be used as a management interface and also the interface from which API calls are made (this will be assigned in the HA configuration).



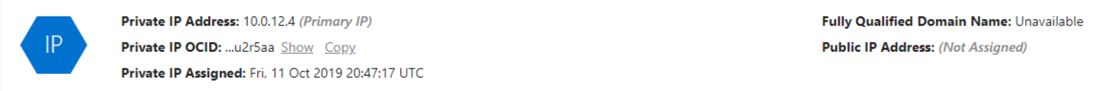
Private IP Address: 10.0.13.4 *(Primary IP)*
Private IP OCID: ...bsa3sa Show Copy
Private IP Assigned: Fri, 11 Oct 2019 20:43:30 UTC

Fully Qualified Domain Name: fgt-b... Show Copy
Public IP Address: 129.146.128.51 *(Ephemeral)*
Public IP OCID: ...7pptvq Show Copy

```
config system interface
   edit "port1"
      set vdom "root"
      set ip 10.0.13.4 255.255.255.0
      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 FortiGate syncs the configuration from the primary unit.

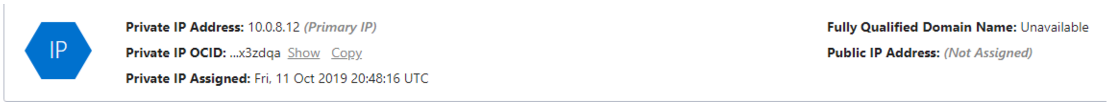


Private IP Address: 10.0.12.4 *(Primary IP)*
Private IP OCID: ...u2r5aa Show Copy
Private IP Assigned: Fri, 11 Oct 2019 20:47:17 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

port3

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

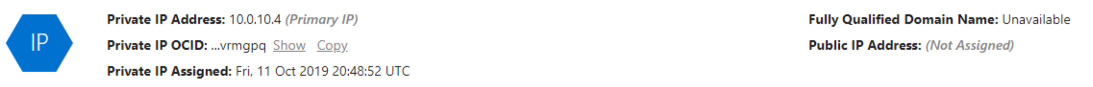


Private IP Address: 10.0.8.12 *(Primary IP)*
Private IP OCID: ...x3zdqa Show Copy
Private IP Assigned: Fri, 11 Oct 2019 20:48:16 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

port4

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



Private IP Address: 10.0.10.4 *(Primary IP)*
Private IP OCID: ...vrmgpq Show Copy
Private IP Assigned: Fri, 11 Oct 2019 20:48:52 UTC

Fully Qualified Domain Name: Unavailable
Public IP Address: *(Not Assigned)*

```
config system interface
```

```
   edit "port4"
      set vdom "root"
      set ip 10.0.10.4 255.255.255.0
      set allowaccess ping https ssh fgfm
      set description "heartbeat"
   next
end
```

Initial Fabric connector configuration

First, you must configure a Fabric connector in FortiOS. This step is required to call APIs to OCI during HA failover.

Follow the steps in Certificate-based Security Fabric connector integration on page 74. Ensure you can successfully call APIs to OCI by referring to Troubleshooting OCI Fabric connector on page 81.

You must ensure that HA status is enabled for the Fabric connector:

```
config system sdn-connector
   edit "oci"
      set type oci
      set ha-status enable
   next
end
```

You must then configure A-P HA settings by using CLI commands on the GUI or via SSH.

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. Note the following:

In the commands, note the following:

- Port4 is the hbdev port used for heartbeat connection.
- For the management interface, you must use port 1, as OCI allows only port 1 for metadata access.
- When setting priority on FortiGate B, set the priority to 100 (lower than FortiGate 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 FortiGate B, which has port4 IP address 10.0.10.4 in the example. When setting FortiGate B's configuration, specify FortiGate A's port4 IP address, which is 10.0.10.3.

The following is the primary FortiGate 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 10.0.13.1
      next
   end
   set override disable
   set priority 200
   set unicast-hb enable
   set unicast-hb-peerip 10.0.10.4
end
```

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

The following is the secondary FortiGate 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 10.0.13.1
      next
   end
   set override disable
   set priority 100
   set unicast-hb enable
   set unicast-hb-peerip 10.0.10.3
end
```

Troubleshooting

See Troubleshooting on page 47.

Deploying FortiGate-VM using Terraform in the CLI

This section includes explanation of how to add bootstrapping of FortiGate CLI commands and a BYOL license at the time of initial bootup as part of a Terraform deployment.

See the corresponding files:

- Variables
- Config

To deploy FortiGate-VM using Terraform in the CLI:

1. See Deployment of a single FortiGate-VM on the Oracle Cloud Infrastructure (OCI).
2. Bootstrap the FortiGate-VM at initial bootup:
   a. Replace the following lines in config.conf with your own FortiOS CLI commands:

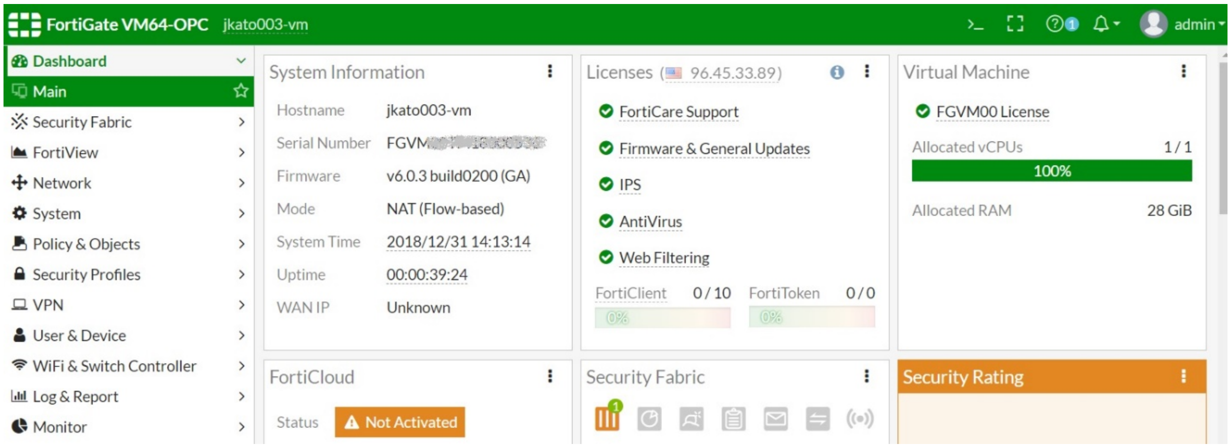
```
config system global
   set hostname OCI-Single
end
config system interface
   edit port1
      set alias untrust
   next
   edit port2
      set alias trust
      set mode static
      set ip ${port2_ip} ${port2_mask}
   next
end
```

   b. To bootstrap a FortiGate-VM license, obtain one from Customer Service & Support after registering your product code. Save the license file as licence.lic. FortiGate-VM license content resembles the following:

```
-----BEGIN FGT VM LICENSE-----
QAAAABUiZtrwrJdUjEe/8C5dNVnOvmY1w7OZWXPPTG7vm2KKwYvL4++qL0gED6/q
SQSPkwpTFlXjAuRGtGyX1VvaTpXgGQAA1pwrFdJnS6TWJ6dVT7KiD8ncufaa3bCw
s8XpmLivzjE4//+C9nqh4fN/KyDweWEIptDMaNsoCm0B0rU8HQIDkX+rgeCs3QZ5
ELStRrXil/oXqTB/gorG67ZdybxWvzPWvWJYDS5AsI+QK8BHJ+xGhLjhkzBZ4ezU
Hd01HCSm7MXEYV5KauU43sZ9XEStxqPEInah3yXgYTd24pnV683G4EHCkAdGyMTP
QqDqBMKcT5aei0ooGVAOX8D62C5Zjh+r1+tkdpR5YHoVYZHU95hBCNjBroJbMnK7
NogYuadQEh28MDtpvzXnb24mW1fDQMTJysQwCtwzJzmnBnvSBo7xNq/irTs2QnFB
[redacted]
O3pizyJ7rMJguXpCB/3v018qAXoqbL5Ks7aQHQTqNuRL2SMducwfd1iAbfz7TMN9
bnbRMz3n5VJUiP+eIFiV84yfwOcCJl+NZAP0hqL3DGBt4urwRFV6yndVi3wZG6hn
eV4LIHkJ5T25/b14m9I+fqEXEsSKKKPn7H2wdyroBdw+VLnT9Hk+3H7t3IL29AZ+
+FDMeRM+BooWnHG3y5do6DB+Wi+CIuxqmNIaoln9buNyFH5bcGU92/6APuFFQ8dI
3DNLIc6ZKDpq7j2ti79dHoIYxCG0S8UsC6l3lOsSwjHg+rO6x+YAEtP0//ktuIvh
NeAFiJveJRxbZBJAu1qnjzNc9Wt7Rg9LvDnwvVKl6Afop2Kt+icfxRL1gySqhWdo
b56XyJbIqAwb/JLa6EkmZDrn3sWQ4H9K
-----END FGT VM LICENSE-----
```

   c. Bootstrap the license file as described at the end of the following scripts: main and variables.
   d. Place the license.lic file in the same directory as the other Terraform definition files in your working directory so that the next step will parse and process it automatically.
   e. Run Terraform as described in Using Terraform to deploy a single FortiGate-VM on page 71.

f. After deployment, log into the FortiGate by accessing https://<IP_address> in your browser. The system displays the dashboard instead of a license upload window, since the license is already activated.



System Information

Hostname	jkato003-vm
Serial Number	FGVM[redacted]
Firmware	v6.0.3 build0200 (GA)
Mode	NAT (Flow-based)
System Time	2018/12/31 14:13:14
Uptime	00:00:39:24
WAN IP	Unknown

Licenses (96.45.33.89)

- ✓ FortiCare Support
- ✓ Firmware & General Updates
- ✓ IPS
- ✓ AntiVirus
- ✓ Web Filtering

FortiClient 0 / 10 0%   FortiToken 0 / 0 0%

Virtual Machine

✓ FGVM00 License

Allocated vCPUs 1 / 1 100%

Allocated RAM 28 GiB

FortiCloud

Status Not Activated

To see how bootstrapping went, check if the command was successfully run. Open the CLI console and enter `diag debug cloudinit show`.

If the cloud-init was run successfully, the CLI shows `Finish running script` with no errors.

Using Terraform to deploy a single FortiGate-VM

You can deploy FortiGate-VM using Terraform. In this example, OCI is a Terraform provider, and FortiGate is a Terraform consumer. For details about Terraform, see Introduction to Terraform.

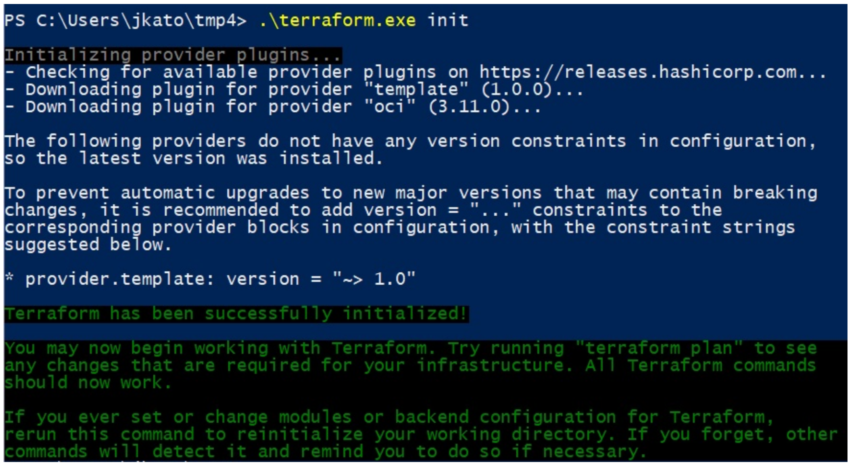
Before using Terraform to deploy a FortiGate-VM, ensure the following prerequisites are met:

1. See Getting Started with the Terraform Provider.
2. Prepare a PEM key file for the user to authenticate themselves with the OCI platform.
3. Upload the FortiGate-VM image to OCI where you plan to deploy the FortiGate-VM. See To obtain the deployment image file and place it in your bucket: on page 12.

The following lists the steps for deploying a FortiGate-VM using Terraform:

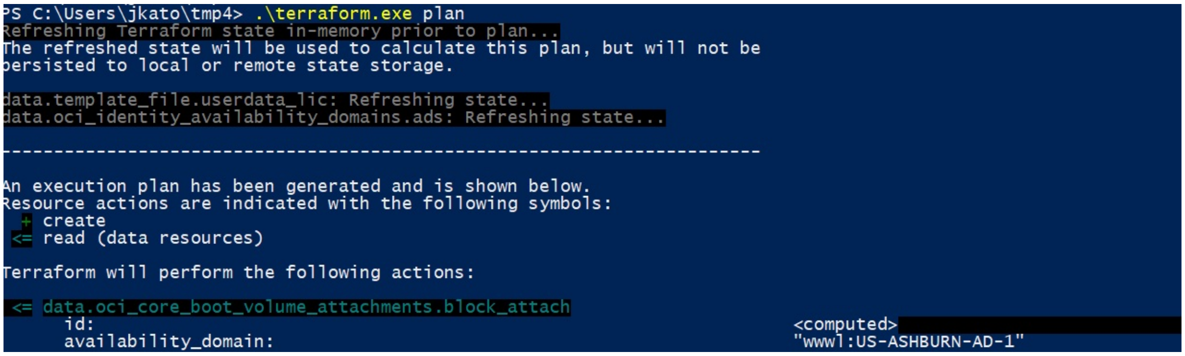
1. Prepare Terraform deployment files. There is a sample set of Terraform files available on GitHub. Clone or download the files in the Single-VM-BareMinimum-BYOL directory. This creates a new VCN.
2. Select your OS with the Terraform applications. See Terraform Downloads.
3. Edit the Terraform variables and config files to suit your environment:
    a. Change the OCI variables in the terraform.tfvars file. You must know the OCIDs of your tenant, compartment, user, and AD. If using Windows, you do not need to specify the C: drive in paths.
    b. Change the resource names in the block.tf, compute.tf, network.tf, and variables.tf files. You can modify resources including the following:
        i. FortiGate-VM hostname
        ii. VCN name
        iii. Network interface, subnet, volume names
        iv. Security list settings. Ensure you open port 443 to allow access to the FortiGate-VM.
        v. Disk size for the second drive. By default, this is 50 GB.
        vi. Network CIDRs

4. Run Terraform:
   a. Run `terraform.exe init` to initialize the Terraform environment.



```
PS C:\Users\jkato\tmp4> .\terraform.exe init

Initializing provider plugins...
- Checking for available provider plugins on https://releases.hashicorp.com...
- Downloading plugin for provider "template" (1.0.0)...
- Downloading plugin for provider "oci" (3.11.0)...

The following providers do not have any version constraints in configuration,
so the latest version was installed.

To prevent automatic upgrades to new major versions that may contain breaking
changes, it is recommended to add version = "..." constraints to the
corresponding provider blocks in configuration, with the constraint strings
suggested below.

* provider.template: version = "~> 1.0"

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```

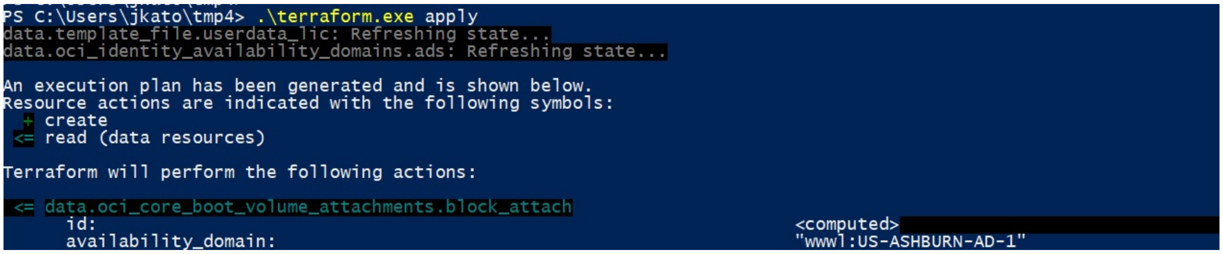
   b. Run `terraform.exe plan`.



```
PS C:\Users\jkato\tmp4> .\terraform.exe plan
Refreshing Terraform state in-memory prior to plan...
The refreshed state will be used to calculate this plan, but will not be
persisted to local or remote state storage.

data.template_file.userdata_lic: Refreshing state...
data.oci_identity_availability_domains.ads: Refreshing state...

------------------------------------------------------------------------

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
  + create
 <= read (data resources)

Terraform will perform the following actions:

 <= data.oci_core_boot_volume_attachments.block_attach
      id:                                                                <computed>
      availability_domain:                                               "wwwl:US-ASHBURN-AD-1"
```

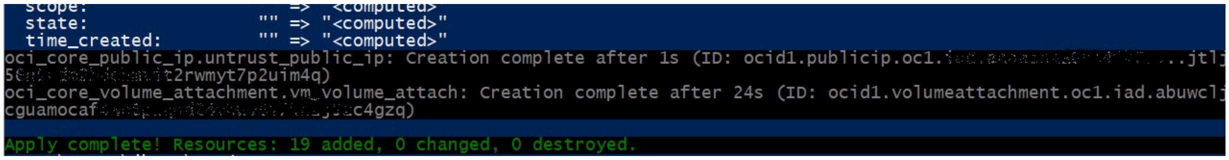
Check the output for newly creating resources. You can add "-out" and an output file to check the output in the file.

   c. Run `terraform.exe apply`.



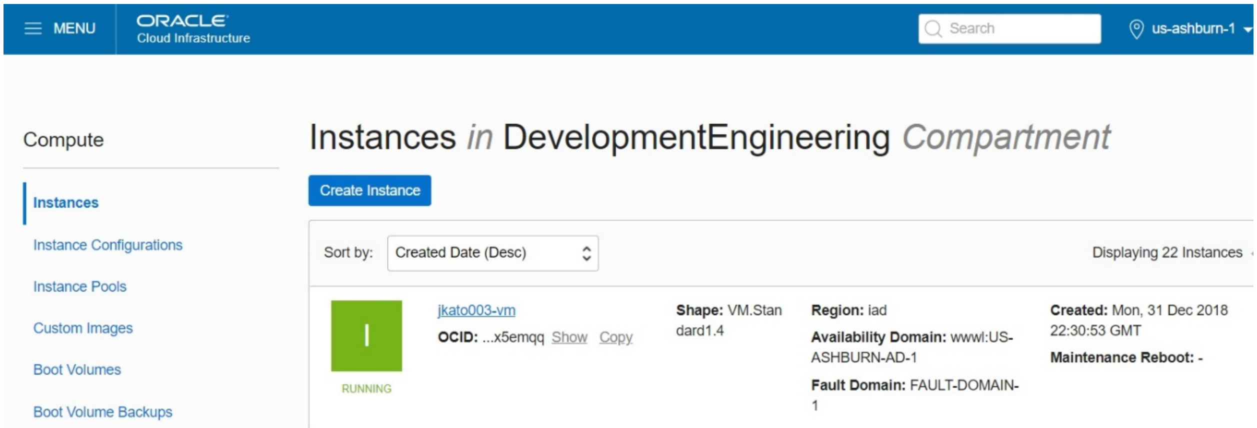
```
PS C:\Users\jkato\tmp4> .\terraform.exe apply
data.template_file.userdata_lic: Refreshing state...
data.oci_identity_availability_domains.ads: Refreshing state...

An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
  + create
 <= read (data resources)

Terraform will perform the following actions:

 <= data.oci_core_boot_volume_attachments.block_attach
      id:                                                                <computed>
      availability_domain:                                               "wwwl:US-ASHBURN-AD-1"
```

At the `Enter a value` prompt, enter `yes` to continue. Wait about ten minutes for the command to end.



```
  scope:                      =>  <computed>
  state:                   "" => "<computed>"
  time_created:            "" => "<computed>"
oci_core_public_ip.untrust_public_ip: Creation complete after 1s (ID: ocid1.publicip.oc1.[redacted]...jtlj
5[redacted]t2rwmyt7p2uim4q)
oci_core_volume_attachment.vm_volume_attach: Creation complete after 24s (ID: ocid1.volumeattachment.oc1.iad.abuwclj
cguamocaf[redacted]c4gzq)

Apply complete! Resources: 19 added, 0 changed, 0 destroyed.
```

5. In the OCI console, go to the newly created resources. The FortiGate-VM instances and VCN have been created.



Instances *in* DevelopmentEngineering *Compartment*

Sort by: Created Date (Desc)

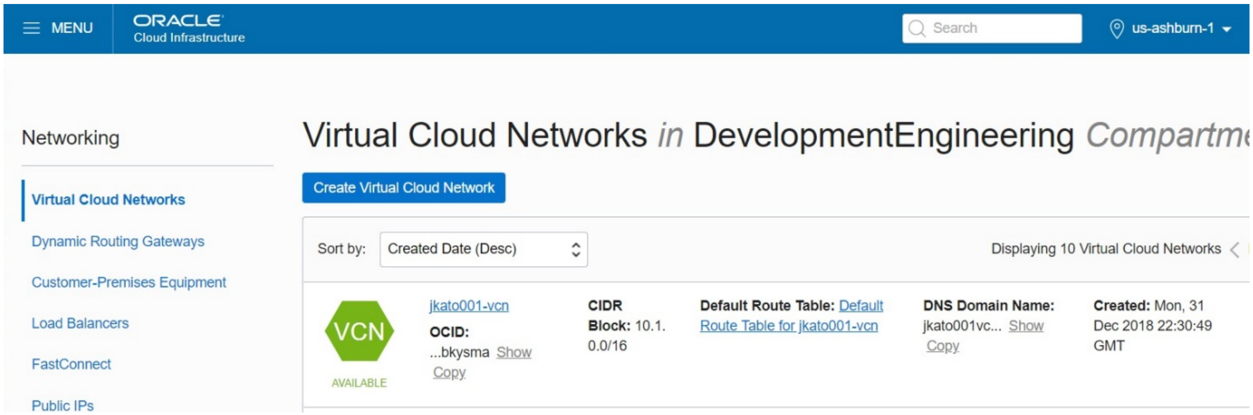
Displaying 22 Instances

jkato003-vm
OCID: ...x5emqq Show Copy

Shape: VM.Standard1.4

Region: iad
Availability Domain: wwwl:US-ASHBURN-AD-1
Fault Domain: FAULT-DOMAIN-1

Created: Mon, 31 Dec 2018 22:30:53 GMT
Maintenance Reboot: -



Virtual Cloud Networks *in* DevelopmentEngineering *Compartme*

Sort by: Created Date (Desc)

Displaying 10 Virtual Cloud Networks

jkato001-vcn
OCID: ...bkysma Show Copy

CIDR Block: 10.1.0.0/16

Default Route Table: Default Route Table for jkato001-vcn

DNS Domain Name: jkato001vc... Show Copy

Created: Mon, 31 Dec 2018 22:30:49 GMT

6. Connect to the FortiGate-VMs. See Accessing the FortiGate-VM on page 20.

Security Fabric connector integration with OCI

You can configure Security Fabric connector integration with OCI in one of the following ways:

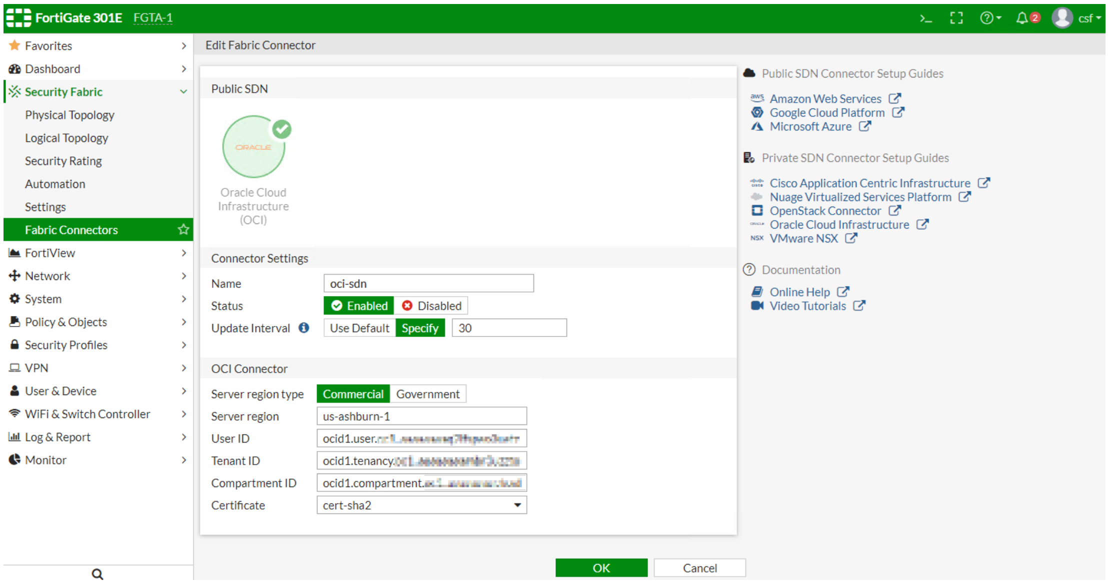
- Using certificates from the FortiGate-VM to OCI over TCP/IP. This is the more common method of configuring the integration. See Certificate-based Security Fabric connector integration on page 74.
- Using an IAM role provided by and configurable in the OCI environment. See Configuring an OCI Fabric connector using IAM roles on page 82.

Certificate-based Security Fabric connector integration

Configuring an OCI Fabric connector

To configure an OCI Fabric connector:

1. In FortiOS, go to *Security Fabric > Fabric Connectors*. Click *Create New*, then select *Oracle Cloud Infrastructure (OCI)*.



Edit Fabric Connector

Public SDN

Oracle Cloud Infrastructure (OCI)

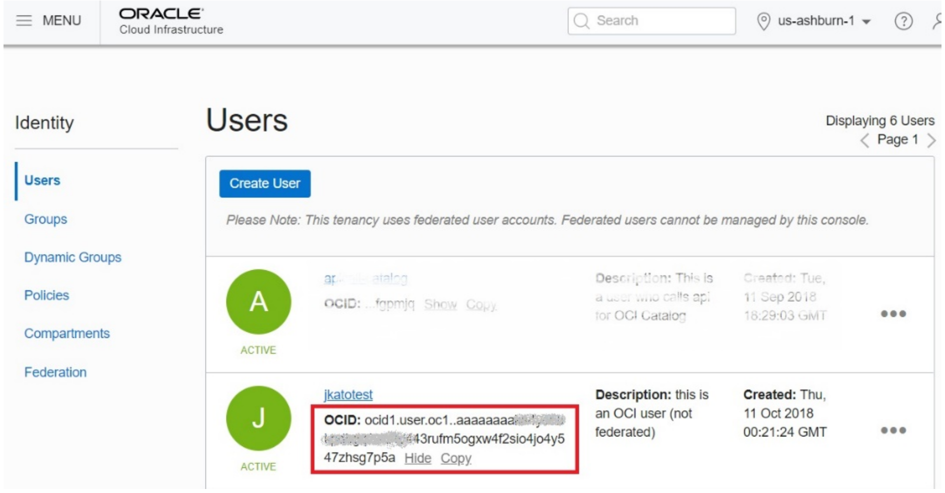
Connector Settings

Name	oci-sdn
Status	[✓ Enabled] Disabled
Update Interval	Use Default [✓ Specify] 30

OCI Connector

Server region type	[✓ Commercial] Government
Server region	us-ashburn-1
User ID	ocid1.user.[redacted]
Tenant ID	ocid1.tenancy.[redacted]
Compartment ID	ocid1.compartment.[redacted]
Certificate	cert-sha2

2. Configure the connector as follows:
   a. *Name*: Enter the desired connector name.
   b. *User ID*: Enter the OCID of the OCI user who belongs to the administrator group. You can find the OCID on the OCI portal as shown:



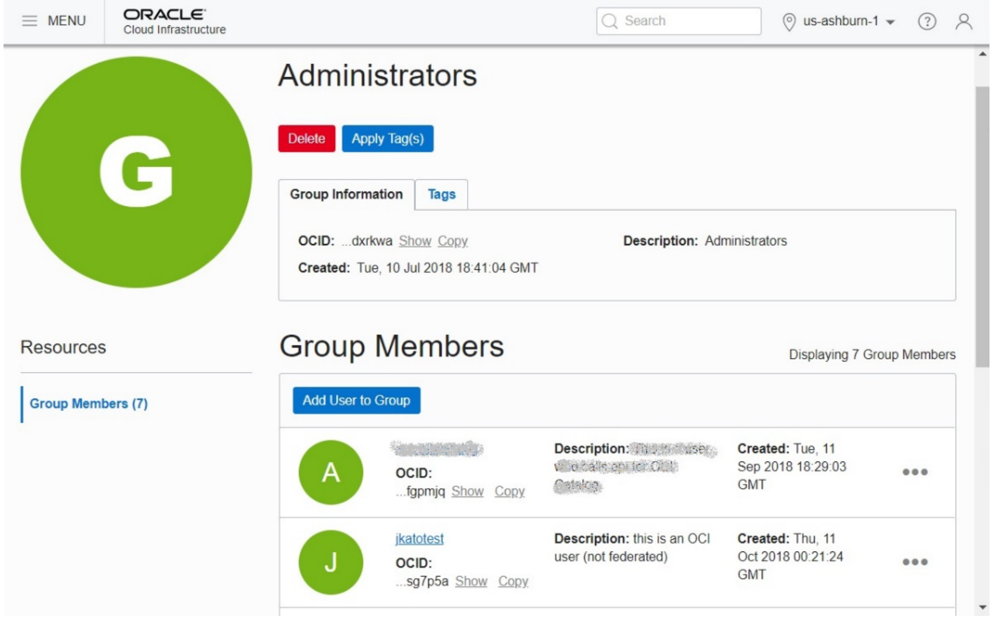
Users

Displaying 6 Users
Page 1

Please Note: This tenancy uses federated user accounts. Federated users cannot be managed by this console.

A ACTIVE	ap[redacted]atalog OCID: ...fgpmjq Show Copy	Description: This is a user who calls api for OCI Catalog	Created: Tue, 11 Sep 2018 18:29:03 GMT
J ACTIVE	jkatotest OCID: ocid1.user.oc1..aaaaaaaa[redacted]43rufm5ogxw4f2sio4jo4y547zhsg7p5a Hide Copy	Description: this is an OCI user (not federated)	Created: Thu, 11 Oct 2018 00:21:24 GMT

The user must be in the Administrators group on OCI.



Administrators

OCID: ...dxrkwa Show Copy

Description: Administrators

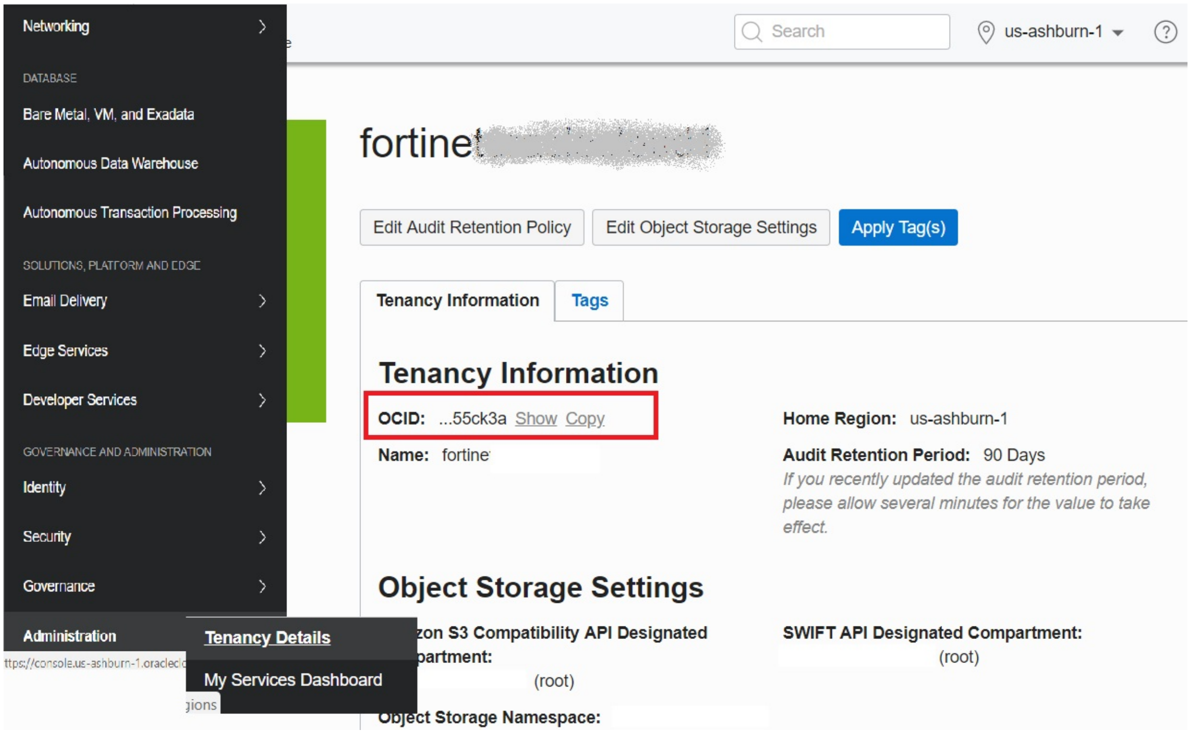
Created: Tue, 10 Jul 2018 18:41:04 GMT

Group Members

Displaying 7 Group Members

A	[redacted] OCID: ...fgpmjq Show Copy	Description: [redacted]	Created: Tue, 11 Sep 2018 18:29:03 GMT
J	jkatotest OCID: ...sg7p5a Show Copy	Description: this is an OCI user (not federated)	Created: Thu, 11 Oct 2018 00:21:24 GMT

c. *Tenant ID*: Enter the tenant's OCID. You can find this on the OCI portal as shown:


Networking
DATABASE
Bare Metal, VM, and Exadata
Autonomous Data Warehouse
Autonomous Transaction Processing
SOLUTIONS, PLATFORM AND EDGE
Email Delivery
Edge Services
Developer Services
GOVERNANCE AND ADMINISTRATION
Identity
Security
Governance
Administration
Tenancy Details
My Services Dashboard
Search
us-ashburn-1
Edit Audit Retention Policy
Edit Object Storage Settings
Apply Tag(s)
Tenancy Information
Tags

fortine[redacted]

Tenancy Information

OCID: ...55ck3a Show Copy

Name: fortine[redacted]

Home Region: us-ashburn-1

Audit Retention Period: 90 Days

If you recently updated the audit retention period, please allow several minutes for the value to take effect.

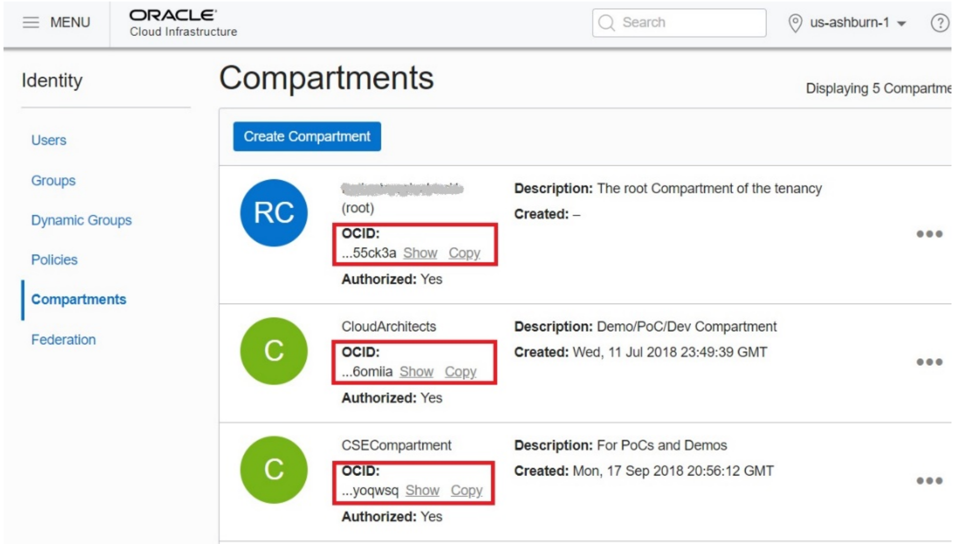
Object Storage Settings

...zon S3 Compatibility API Designated ...partment: (root)

SWIFT API Designated Compartment: (root)

Object Storage Namespace:

d. *Compartment ID*: Enter the compartment's OCID. If you have multiple compartments, choose the desired one. You can find this on the OCI portal as shown:



Compartments

Displaying 5 Compartme

[redacted] (root)
OCID: ...55ck3a Show Copy
Authorized: Yes
Description: The root Compartment of the tenancy
Created: –

CloudArchitects
OCID: ...6omiia Show Copy
Authorized: Yes
Description: Demo/PoC/Dev Compartment
Created: Wed, 11 Jul 2018 23:49:39 GMT

CSECompartment
OCID: ...yoqwsq Show Copy
Authorized: Yes
Description: For PoCs and Demos
Created: Mon, 17 Sep 2018 20:56:12 GMT

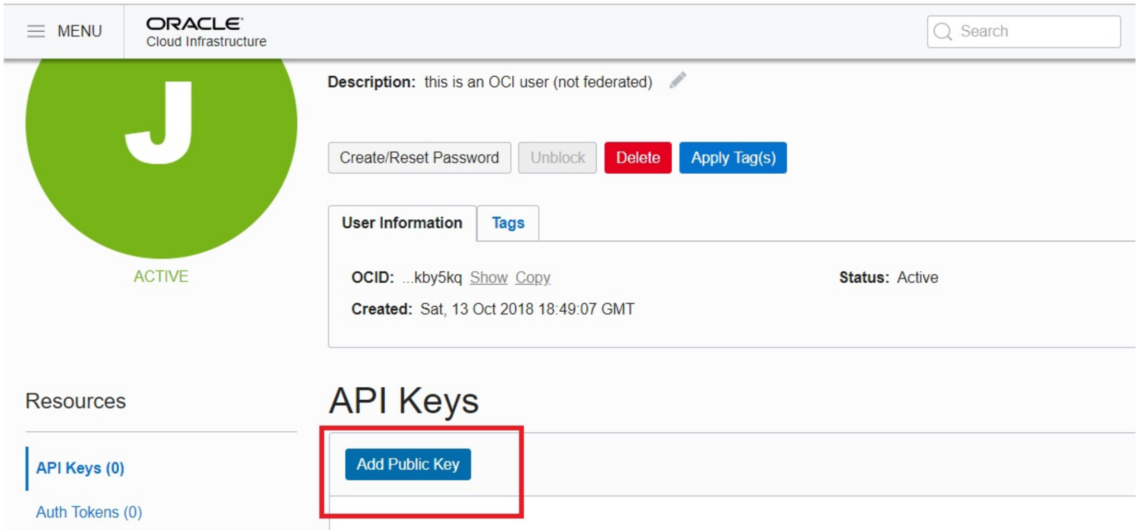
e. *OCI Region*: Choose the one currently in use.

f. For the *OCI Certificate* field, you must select a certificate that satisfies OCI key size limits. The minimum size is 2048 bits. Do one of the following:

   i. Select the built-in default certificate called Fortinet_Factory.

   ii. Follow steps 1-2 in Using a custom certificate on page 41 to configure a custom certificate.

3. At this stage, you must register the certificate's fingerprint to the specified OCI user.
   a. Go to the OCI user, then *API Keys* > *Add Public Key*.



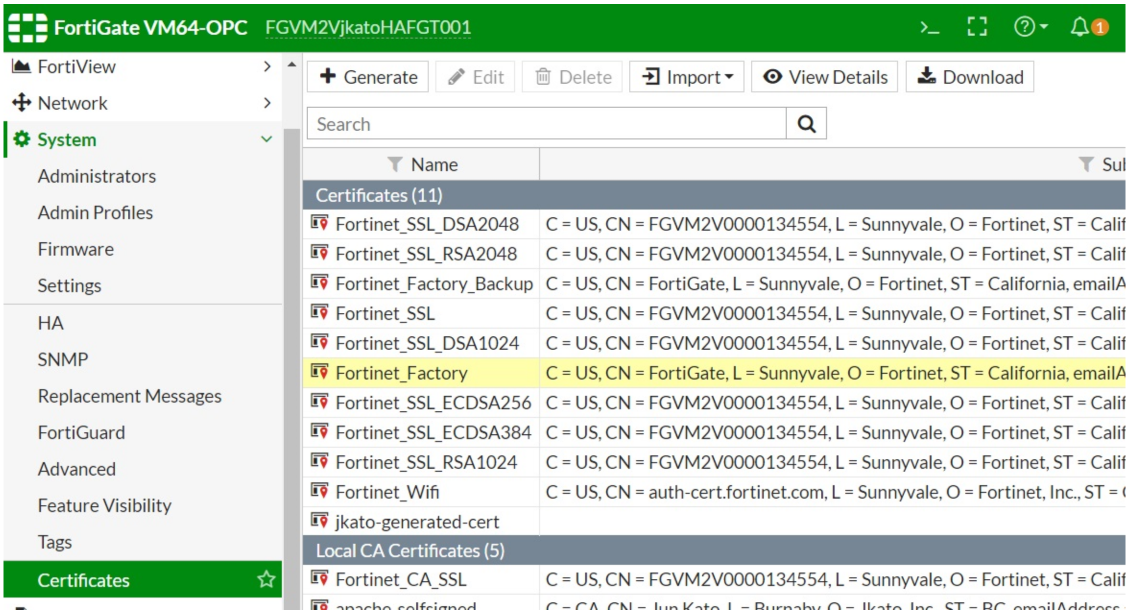
Description: this is an OCI user (not federated)

OCID: ...kby5kq

Status: Active

Created: Sat, 13 Oct 2018 18:49:07 GMT

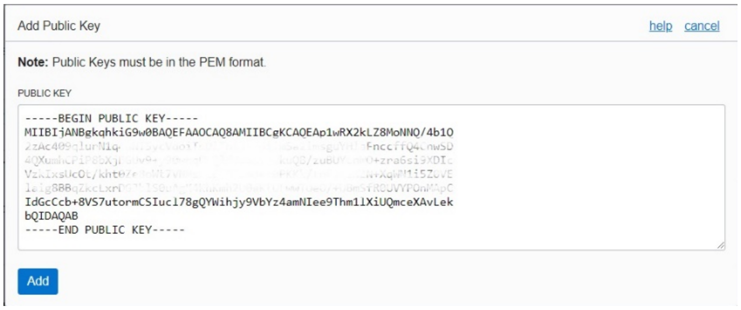
   b. If you selected the Fortinet_Factory certificate in step 2f, do the following:
      i. In FortiOS, go to *System* > *Certificate*. Select Fortinet_Factory, then click *Download*.



Name	Sul
Certificates (11)	
Fortinet_SSL_DSA2048	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
Fortinet_SSL_RSA2048	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
Fortinet_Factory_Backup	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailA
Fortinet_SSL	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
Fortinet_SSL_DSA1024	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
Fortinet_Factory	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailA
Fortinet_SSL_ECDSA256	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
Fortinet_SSL_ECDSA384	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
Fortinet_SSL_RSA1024	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, Inc., ST = (
jkato-generated-cert	
Local CA Certificates (5)	
Fortinet_CA_SSL	C = US, CN = FGVM2V0000134554, L = Sunnyvale, O = Fortinet, ST = Calif
apache-selfsigned	C = CA, CN = Jun Kato, L = Burnaby, O = Ikato Inc., ST = BC, emailAddress

      ii. You now have the Fortinet_Factory.cer file. Create a public key file in PEM format from it, using a freely available tool of your choice such as OpenSSL.

c. Copy and paste the content of the certificate PEM key file in the *Add Public Key* window in OCI. Click *Add*.



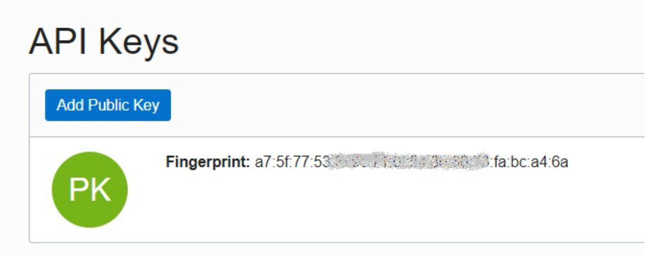
Add Public Key

Note: Public Keys must be in the PEM format.

PUBLIC KEY

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp1wRX2kLZ8MoNNQ/4b1Q
[redacted]
IdGcCcb+8VS7utormCSIucl78gQYWihjy9VbYz4amNIee9Thm1lXiUQmceXAvLek
bQIDAQAB
-----END PUBLIC KEY-----
```

d. You now see the fingerprint.



API Keys

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

You can configure the following for the fingerprint:

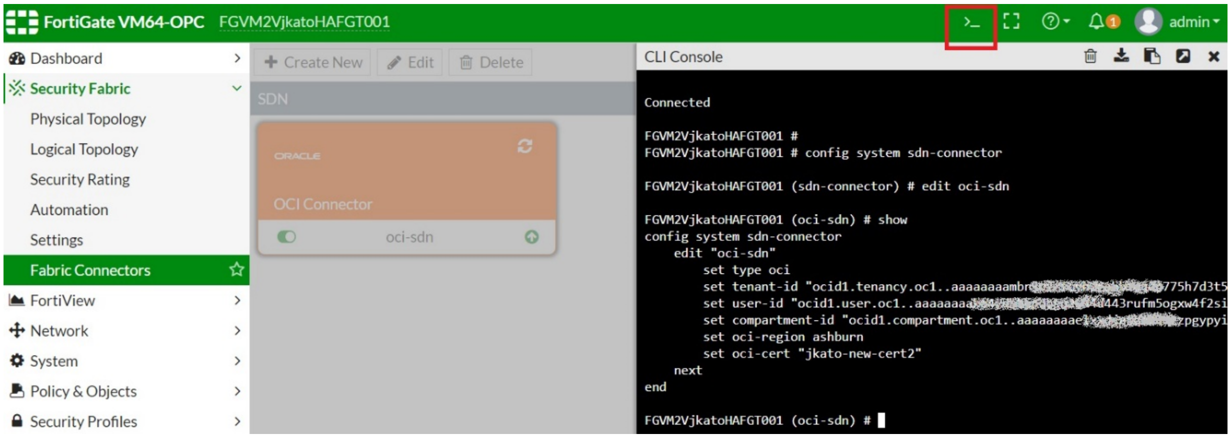
1. *Update Interval*: The default value is 60 seconds. You can change the value to between 1 and 3600 seconds.
2. *Status*: Green means that the connector is enabled. You can disable it at any time by toggling the switch.

e. Click *OK*.

You can also configure the Fabric connector using the CLI. Execute the following commands:

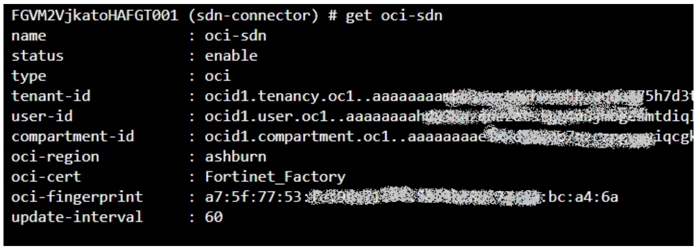
```
config system sdn-connector
   edit “<OCI connector name>”
```

The `show` command shows what is currently configured. To set each element, execute `set <element> <value>` and then `next end` saves the configuration and returns to the original indentation that you started with.



```
Connected

FGVM2VjkatoHAFGT001 #
FGVM2VjkatoHAFGT001 # config system sdn-connector

FGVM2VjkatoHAFGT001 (sdn-connector) # edit oci-sdn

FGVM2VjkatoHAFGT001 (oci-sdn) # show
config system sdn-connector
    edit "oci-sdn"
        set type oci
        set tenant-id "ocid1.tenancy.oc1..aaaaaaaambr[redacted]775h7d3t5
        set user-id "ocid1.user.oc1..aaaaaaaa[redacted]443rufm5ogxw4f2si
        set compartment-id "ocid1.compartment.oc1..aaaaaaaae[redacted]zpgypyi
        set oci-region ashburn
        set oci-cert "jkato-new-cert2"
    next
end

FGVM2VjkatoHAFGT001 (oci-sdn) # █
```

You can also see the configuration by running `get <OCI connector name>`. In this case, enter `get oci-sdn`.



```
FGVM2VjkatoHAFGT001 (sdn-connector) # get oci-sdn
name                : oci-sdn
status              : enable
type                : oci
tenant-id           : ocid1.tenancy.oc1..aaaaaaaam[redacted]5h7d3
user-id             : ocid1.user.oc1..aaaaaaaah[redacted]mtdiq
compartment-id      : ocid1.compartment.oc1..aaaaaaaae[redacted]iqcg
oci-region          : ashburn
oci-cert            : Fortinet_Factory
oci-fingerprint     : a7:5f:77:53:[redacted]:bc:a4:6a
update-interval     : 60
```

Creating an address

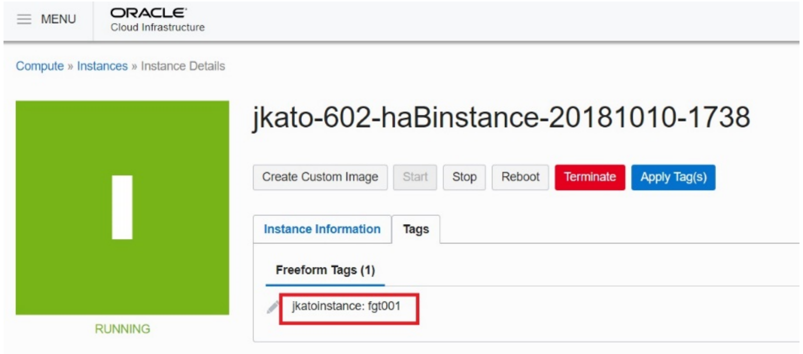
The next step is to create an address. You can do this via the GUI or the CLI. Either way, take note of the following:

- You will create an address which is used as an address group or single address to be used for source/destination of firewall policies. The address is based on IP addresses. The address contains IP addresses of OCI instances that are currently running.
- No matter what changes occur to the instances, the Fabric connector populates and updates the changes automatically based on the specified filtering condition so that administrators do not need to reconfigure the address content manually.
- Appropriate firewall policies using the address are applied to the instances that are members of it.

To create an address using the GUI:

1. Go to *Policy & Objects* > *Addresses*. Click *Create New* > *Address*.
2. Configure the address as described:
   a. *Name*: Enter the desired name.
   b. *Type*: Select *Fabric Connector Address*.
   c. *Fabric Connector Type*: Select *Oracle Cloud Infrastructure (OCI)*.
   d. *Filter*: The Fabric connector automatically populates and updates only IP addresses belonging to the specified filter that matches the condition. Currently, OCI connectors support the following filters:
      i. `'vm_name=<vm name>'`: This matches a VM instance name.
      ii. `'instance_id=<instance id>'`: This matches an instance OCID.
      iii. `'tag.<key>=<value>'`: This matches a freeform tag key and its value.
      iv. `'definedtag.<namespace>.<key>=<value>'`: This matches a tag namespace, tag key, and its value.

   In this example, let's use `'tag.<key>=<value>'`. You can configure tags on OCI:



   In this example, let's populate IP addresses of instances that have the "jkatoinstance" tag name with the "demomachine" value.

You can set filtering conditions using multiple entries with AND ("&") or OR ("|"). When both AND and OR are specified, AND is interpreted first, then OR.

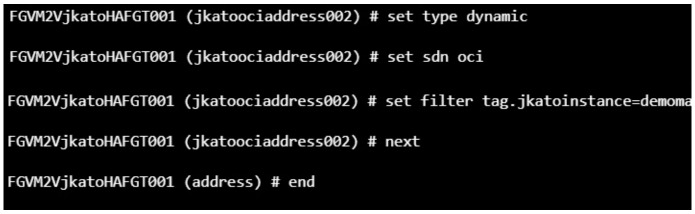
For example, you can enter "`tag.<key>=<value> & vm_name=<vm name>`". In this case, the Fabric connector populates and updates IP addresses of instances that match both the tag and VM name. Wildcards, such as asterisks, are not allowed in filter values.

3. Click *OK* after completing all required fields.
4. Ensure that you created the address by going to *Policy & Objects > Addresses*.
5. After a few minutes, the new address takes effect. Hover your cursor on the address to see a list of IP addresses and instances that have the tag key value "demomachine" as configured.

To create an address using the CLI:

1. Open the FortiOS CLI with admin credentials.
2. Enter `config firewall address`.
3. The prompt becomes the FortiGate-VM hostname and (address)$. Enter `edit <address_name>` to create an address. For example, if the address name is jkatoociaddress002, enter `edit jkatoociaddress002`.
4. Configure the address as a Fabric connector supporting element.
   a. Enter `set type dynamic`.
   b. Enter `set sdn oci`.
5. Configure the filter. The Fabric connector automatically populates and updates only IP addresses belonging to the specified filter that matches the condition. Currently, OCI connectors support the following filters:
   a. `'vm_name=<vm name>'`: This matches a VM instance name.
   b. `'tag.<key>=<value>'`: This matches a freeform tag key and its value.
   c. `'instance_id=<instance id>'`: This matches an instance OCID.
   d. `'definedtag.<namespace>.<key>=<value>'`: This matches a tag namespace, tag key, and its value.

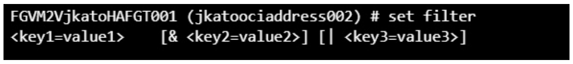
   In this example, let's use `'tag.<key>=<value>'`, populating IP addresses of instances that have the "jkatoinstance" tag name with the "demomachine" value. Enter `set filter tag.jkatoinstance=demomachine`. Entering `next end` saves the configuration and returns to the original indentation you started with.



```
FGVM2VjkatoHAFGT001 (jkatoociaddress002) # set type dynamic

FGVM2VjkatoHAFGT001 (jkatoociaddress002) # set sdn oci

FGVM2VjkatoHAFGT001 (jkatoociaddress002) # set filter tag.jkatoinstance=demoma

FGVM2VjkatoHAFGT001 (jkatoociaddress002) # next

FGVM2VjkatoHAFGT001 (address) # end
```

   You can set filtering conditions using multiple entries with AND ("&") or OR ("|"). When both AND and OR are specified, AND is interpreted first, then OR.

   You can check the syntax by entering `set filter ?`

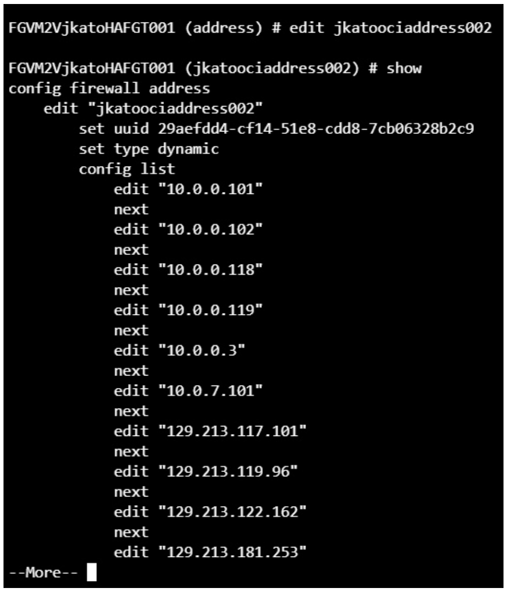


```
FGVM2VjkatoHAFGT001 (jkatoociaddress002) # set filter
<key1=value1>    [& <key2=value2>] [| <key3=value3>]
```

   For example, you can enter "`tag.<key>=<value> & vm_name=<vm name>`". In this case, the Fabric connector populates and updates IP addresses of instances that match both the tag and VM name. Wildcards, such as asterisks, are not allowed in filter values.

6. After a few minutes, the new address takes effect. Repeat steps 1-3, then enter `show`. You can see the list of IP

addresses that have been populated.



```
FGVM2VjkatoHAFGT001 (address) # edit jkatoociaddress002

FGVM2VjkatoHAFGT001 (jkatoociaddress002) # show
config firewall address
    edit "jkatoociaddress002"
        set uuid 29aefdd4-cf14-51e8-cdd8-7cb06328b2c9
        set type dynamic
        config list
            edit "10.0.0.101"
            next
            edit "10.0.0.102"
            next
            edit "10.0.0.118"
            next
            edit "10.0.0.119"
            next
            edit "10.0.0.3"
            next
            edit "10.0.7.101"
            next
            edit "129.213.117.101"
            next
            edit "129.213.119.96"
            next
            edit "129.213.122.162"
            next
            edit "129.213.181.253"
--More--
```

Creating a firewall policy

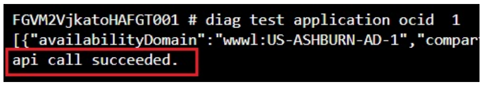
Finally, you can use this address to configure a firewall policy as a source or destination. The following operation is not Fabric connector-specific but shows a general way of creating a firewall policy in FortiOS.

You can use the GUI or CLI to create the firewall policy.

Go to *Policy & Objects* > *IPv4 Policy*, and create a firewall policy. Specify the created address as a source or destination.

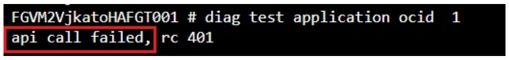
Troubleshooting OCI Fabric connector

You can check if API calls are made successfully by running `diag test application ocid 1`. The below shows an example of a successful configuration.



```
FGVM2VjkatoHAFGT001 # diag test application ocid  1
[{"availabilityDomain":"wwwl:US-ASHBURN-AD-1","compar
api call succeeded.
```

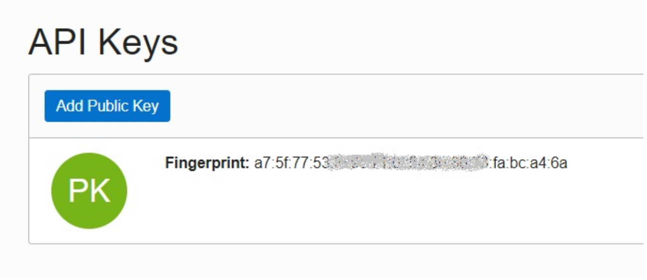
The below shows an example of a failed configuration.



```
FGVM2VjkatoHAFGT001 # diag test application ocid  1
api call failed, rc 401
```

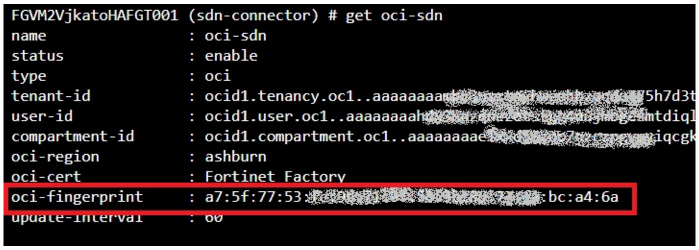
Check the following to see if you made other unexpected changes:

- 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 FortiGate-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 Fabric connector settings match.



API Keys

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



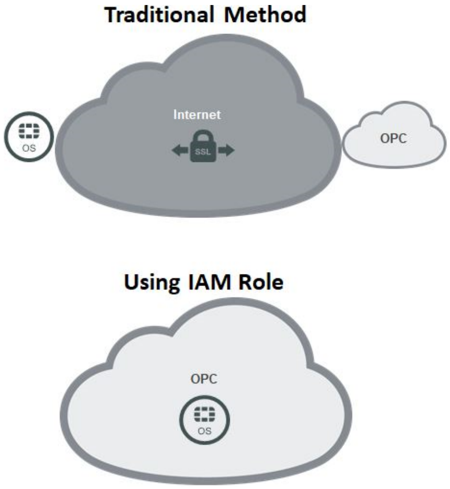
```
FGVM2VjkatoHAFGT001 (sdn-connector) # get oci-sdn
name                : oci-sdn
status              : enable
type                : oci
tenant-id           : ocid1.tenancy.oc1..aaaaaaaa[redacted]5h7d3t
user-id             : ocid1.user.oc1..aaaaaaaah[redacted]mtdiql
compartment-id      : ocid1.compartment.oc1..aaaaaaaae[redacted]iqcgk
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 FortiGate?

Configuring an OCI Fabric connector using IAM roles

This guide provides a sample configuration of an OCI Fabric connector using IAM roles instead of traditional authentication. Traditional authentication uses certificates from the FortiGate-VM to OCI over TCP/IP. Instead, this configuration uses the IAM role provided by and configurable in the OCI environment for authentication. The IAM role includes permissions that you can give to the instance, so that FortiOS can implicitly access metadata information and communicate to the Fabric connector on its own private internal network without further authentication.

The following shows the topology when using traditional authentication versus IAM roles:



Traditional Method

Using IAM Role

The following prerequisites must be met for this configuration:

- A FortiGate located on OCI
- Correct administrative permissions as an administrator on OCI over the FortiGate instance and the environment

- The following summarizes minimum sufficient IAM roles for this deployment:
  - 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
  - To define simpler roles, use the following:
    - 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 virtual-network-family in tenancy
  - For an HA setup, configure management permissions for virtual-network-family in tenancy:
    - Allow dynamic-group <group_name> to manage virtual-network-family in tenancy

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

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

1. Configure an IAM role on OCI.
2. Configure a Fabric connector in FortiOS.
3. Perform testing to ensure that the Fabric connector is connected to OCI.

To configure an IAM role on OCI:

1. In OCI, go to *Compute* > *Instances*, and select the desired FortiGate-VM instance.
2. On the *Instance Details* page, note the instance's OCID. In this example, the OCID is ocid1.instance.oc1.iad.abuwcljthhvsi7djktxkljr2pzjelkcj4pgozd46bnpcpt5pxcaj56mkurhq.
3. Open the OPC menu and go to *Identity* > *Dynamic Groups*. Create a dynamic group with rules that allow instances that match the FortiGate-VM's instance ID. Use the syntax "ALL {instance.id ='instanceID'}" when creating the rule. In this example, the configured rule is "ALL {instance.id = 'ocid1.instance.oc1.iad.abuwcljthhvsi7djktxkljr2pzjelkcj4pgozd46bnpcpt5pxcaj56mkurhq'}". If you have multiple instances to include in the dynamic group, create multiple rules for this dynamic group.
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 Fabric connector is used for HA. In the *STATEMENT* field, use the syntax "Allow dynamic-group <group-name> to manage all-resources in TENANCY".

To configure a Fabric connector in FortiOS:

To configure a Fabric connector in the FortiOS GUI, do the following:

1. In FortiOS, go to *Security Fabric* > *Fabric Connectors*.
2. Click *Create New* > *Oracle Cloud Infrastructure (OCI*).
3. Enable *Use metadata IAM*.
4. In the *Tenant ID* field, enter the FortiGate-VM's tenant ID.
5. In the *Compartment ID* field, enter the compartment's tenant ID. This may be the same as the tenant ID depending on your configuration.
6. Configure the other Fabric connector settings as required.

7. In *Security Fabric* > *Fabric Connectors*, ensure that the OCI connector has been created and is enabled and connected.

To configure a Fabric connector using the FortiOS CLI, run the following commands:

```
config system sdn-connector
   edit "oci-sdn-connector"
      set status enable
      set type oci
      set ha-status disable
      set tenant-id "<tenant ID>"
      set user-id ''
      set compartment-id "<compartment ID>"
      set oci-region phoenix
      set oci-cert ''
      set use-metadata-iam enable
      set update-interval 60
   next
end
```

To perform testing:

To ensure the Fabric connector is connected to OCI, run the `diagnose sys sdn status` command. The output should display that the Fabric connector has a connected status.

You can run the `diagnose debug application ocid -1` and `diagnose test application ocid` commands for further debugging.

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 Fabric connector for failover and instead are using it for querying, you can assign the dynamic group read-only permissions.

Oracle Kubernetes (OKE) Fabric connector

OCI Fabric connectors support dynamic address groups based on Oracle Kubernetes (OKE) filters. See the *FortiOS Cookbook*.

Change log

Date	Change Description
2019-03-28	Initial release.
2019-05-31	Added Deploying FortiGate-VM HA on OCI between multiple ADs on page 49.
2019-06-28	Added Oracle Kubernetes (OKE) Fabric connector on page 84.
2019-07-22	Updated Checking the prerequisites on page 31, Checking the prerequisites on page 49, and Configuring an OCI Fabric connector using IAM roles on page 82.
2019-09-17	Updated Deploying a native mode FortiGate-VM on OCI on page 27.
2019-09-18	Added Deploying FortiGate-VM via the marketplace on page 29 and Deploying FortiGate-VM using Terraform in OCI marketplace. Updated Deploying FortiGate-VM HA on OCI within one AD on page 30 sections.
2019-10-21	Added Deploying FortiGate-VM HA on OCI between multiple ADs using a regional VCN on page 58. Updated Configuring the OCI HA interfaces on page 37 and Creating a security list on page 10
2019-11-14	Updated About FortiGate-VM for OCI on page 5.
2019-11-29	Updated Models on page 5, Order types on page 7, and Creating a support account on page 7.
2019-12-13	Updated Using a custom certificate on page 41 and Configuring an OCI Fabric connector on page 74.
2020-02-05	Updated Deploying FortiGate-VM HA on OCI between multiple ADs on page 49.
2020-02-25	Updated Configuring an OCI Fabric connector using IAM roles on page 82.
2020-05-05	Updated Models on page 5 and Registering and downloading licenses on page 8.
2020-05-15	Updated Order types on page 7.
2020-06-30	Updated Deploying FortiGate-VM using Terraform and Deploying FortiGate-VM HA on OCI within one AD on page 30 subtopics.
2020-12-08	Updated Order types on page 7.