FortiAuthenticator - OCI Deployment Guide

Version 6.1.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

March 28, 2020
FortiAuthenticator 6.1.0 OCI Deployment Guide
23-610-621026-20200328

TABLE OF CONTENTS

About FortiAuthenticator on OCI

Overview

FortiAuthenticator is designed specifically to provide authentication services for firewalls, SSL and IPsec VPNs, wireless access points, switches, routers, and servers. FortiAuthenticator includes Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAPv3) server authentication methods, and Security Assertion Markup Language (SAML), which is used for exchanging authentication and authorization data between an Identity Provider (IdP) and a Service Provider (SP). Authentication servers are an important part of an enterprise network, controlling access to protected network assets, and tracking user activity to comply with security policies.

FortiAuthenticator is not a firewall; it requires either a FortiGate-VM "virtual" or FortiGate "hardware" appliance to provide firewall-related services. Multiple FortiGate appliances can use a single FortiAuthenticator appliance for Fortinet Single Sign-On (FSSO) and other types of remote authentication, two-factor authentication, and FortiToken device management. This centralizes authentication and FortiToken maintenance.

FortiAuthenticator provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the Fortinet Single Sign-On (FSSO) Agent on a Windows Active Directory (AD) network.

OCI instance type support

FortiAuthenticator-VM supports the following OCI compute shapes. For up-to-date information on each instance type, see OCI Compute Shapes.

When selecting an instance type for your deployment, consider your use case for FortiAuthenticator and the requirements to support it.

Compute shape	OCPU	Max VNIC	FortiAuthenticator-VM license
VM.Standard2.1	1	2	FAC-VM-100-UG
VM.Standard2.2	2	2	FAC-VM-100-UG or FAC-VM-1000-UG
VM.Standard2.4	4	4	FAC-VM-100-UG, FAC-VM-1000-UG or FAC-VM-10000-UG
VM.Standard2.8	8	8	FAC-VM-10000-UG or FAC-VM-100000-UG
VM.Standard2.16	16	16	FAC-VM-100000-UG
VM.Standard2.24	24	24	FAC-VM-100000-UG
VM.Standard1.1	1	2	FAC-VM-100-UG
VM.Standard1.2	2	2	FAC-VM-100-UG or FAC-VM-1000-UG

Compute shape	OCPU	Max VNIC	FortiAuthenticator-VM license
VM.Standard1.4	4	4	FAC-VM-100-UG, FAC-VM-1000-UG or FAC-VM-10000-UG
VM.Standard1.8	8	8	FAC-VM-10000-UG or FAC-VM-100000-UG
VM.Standard1.16	16	16	FAC-VM-100000-UG

Licensing

FortiAuthenticator for OCI supports the bring your own license (BYOL) model.

Licenses can be obtained through any Fortinet partner. If you don't have a reseller partner, you can find a local Fortinet reseller partner by visiting the Find a Partner portal and performing a search in the following regions:

- Asia Pacific, Australia, and New Zealand
- EMEA (Europe, Middle East, and Africa)
- Latin America and Caribbean
- North America
- North America: US Federal

This license model is stackable, allowing you to expand your VM solution as your environment expands. For additional information on the FortiAuthenticator stackable license model, see the FortiAuthenticator datasheet.

Deploying FortiAuthenticator on OCI

Overview

This guide provides step-by-step instructions for successful deployment and initial configuration of FortiAuthenticator for OCI:

- Preparing for a deployment on page 6
- Creating an instance by importing an image on page 6
- Connecting to FortiAuthenticator-VM on page 15

Preparing for a deployment

The deployment section in this guide assumes that you have already created a Virtual Cloud Network (VCN) and relevant network resources, such as route tables and subnets. You must also configure a Security List so that you can access FortiAuthenticator over the Internet while closing unnecessary ports. At a minimum, you must open TCP port 443 and 22 to allow incoming access to the FortiAuthenticator management GUI and SSH console for initial configuration. See the *Ports and Protocols* document on the Fortinet Document Library.

You can obtain the deployment image, import the file into the OCI portal, and then launch the FortiAuthenticator-VM instance. See Creating an instance by importing an image on page 6.

Creating an instance by importing an image

This guide provides step-by-step instructions for successful deployment and initial configuration of FortiAuthenticator for OCI:

- Obtaining the deployment image and placing it in your bucket on page 6
- Importing the image on page 9
- Connecting to FortiAuthenticator-VM on page 15

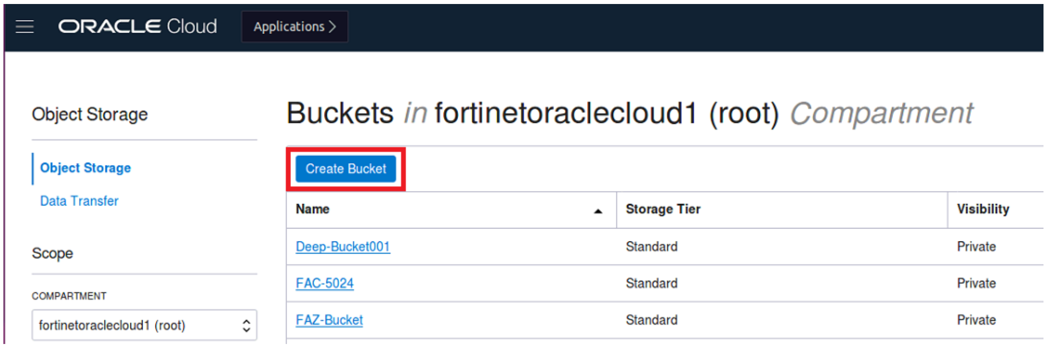
Obtaining the deployment image and placing it in your bucket

1. Go to https://support.fortinet.com.
2. In the top menu, navigate to *Download* > *Firmware Images*.
3. From the *Select Product dropdown* list, select *FortiAuthenticator*, then click the *Download* tab.
4. Navigate to the desired firmware release.

5. Download the *FAC_VM_OPCVX-buildXXXX-FORTINET.out.opc.zipfile*.

- *XXX* is the build number.
- Ensure the file name includes the OPC.

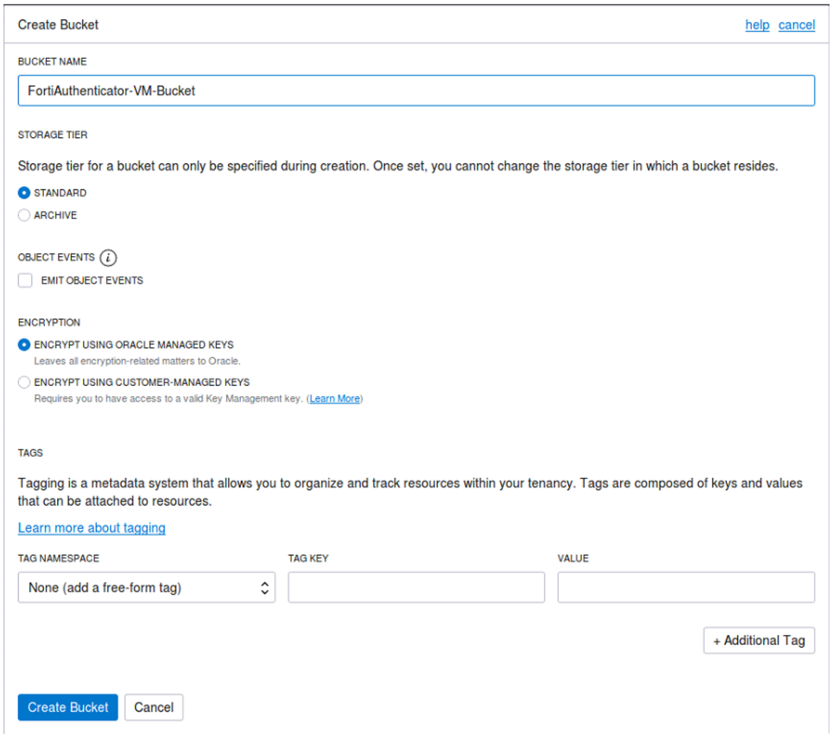
6. After you extract the zip the file, locate the *fackvm.qcow2* file.
   You will need this file to deploy FortiAuthenticator on OCI.
7. In OCI, go to Core *Infrastructure* > *Object Storage* > *Object Storage*.
8. Click *Create Bucket* to create a standard storage bucket.



Buckets *in* fortinetoraclecloud1 (root) *Compartment*

Name	Storage Tier	Visibility
Deep-Bucket001	Standard	Private
FAC-5024	Standard	Private
FAZ-Bucket	Standard	Private

9. In the *Bucket Name* field, name the bucket, then click *Create Bucket*.



Create Bucket

BUCKET NAME

FortiAuthenticator-VM-Bucket

STORAGE TIER

Storage tier for a bucket can only be specified during creation. Once set, you cannot change the storage tier in which a bucket resides.

● STANDARD

○ ARCHIVE

OBJECT EVENTS

□ EMIT OBJECT EVENTS

ENCRYPTION

● ENCRYPT USING ORACLE MANAGED KEYS
Leaves all encryption-related matters to Oracle.

○ ENCRYPT USING CUSTOMER-MANAGED KEYS
Requires you to have access to a valid Key Management key. (Learn More)

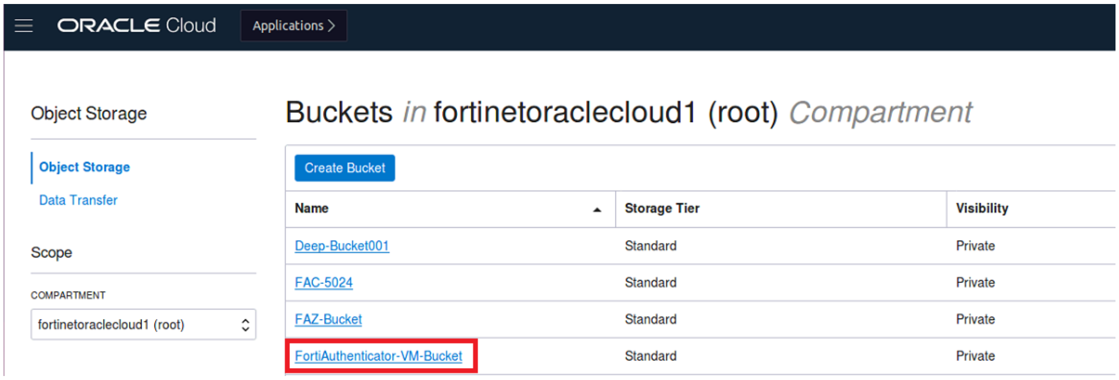
TAGS

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)		

10. Click the name of the bucket you created to edit it.

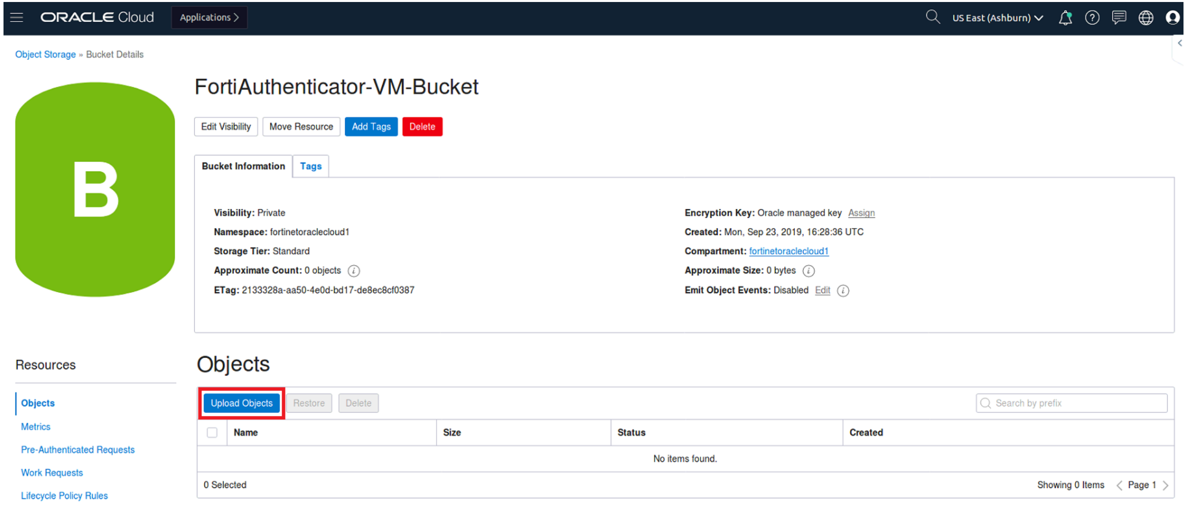


Buckets *in* fortinetoraclecloud1 (root) *Compartment*

Create Bucket

Name	Storage Tier	Visibility
Deep-Bucket001	Standard	Private
FAC-5024	Standard	Private
FAZ-Bucket	Standard	Private
FortiAuthenticator-VM-Bucket	Standard	Private

11. Click *Upload Objects*.



FortiAuthenticator-VM-Bucket

Visibility: Private
Namespace: fortinetoraclecloud1
Storage Tier: Standard
Approximate Count: 0 objects
ETag: 2133328a-aa50-4e0d-bd17-de8ec8cf0387

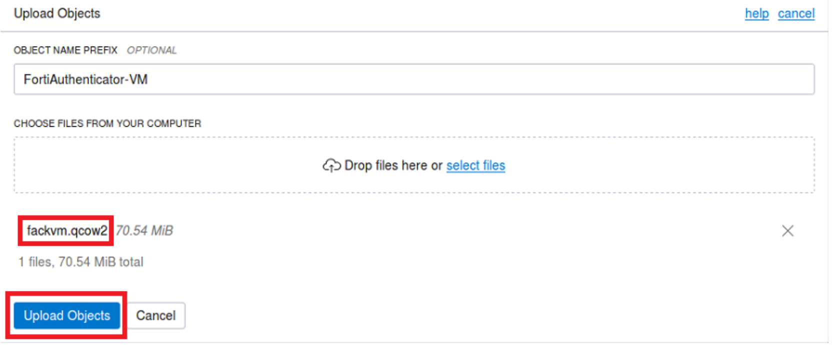
Encryption Key: Oracle managed key Assign
Created: Mon, Sep 23, 2019, 16:28:36 UTC
Compartment: fortinetoraclecloud1
Approximate Size: 0 bytes
Emit Object Events: Disabled Edit

Objects

□	Name	Size	Status	Created
		No items found.		

0 Selected   Showing 0 Items Page 1

12. Upload the objects:
    a. (Optional) Edit the *Object Name Prefix*.
    b. Upload the deployment image *fackvm.qcow2* file that you downloaded.
    c. Click *Upload Objects*.



OBJECT NAME PREFIX *OPTIONAL*

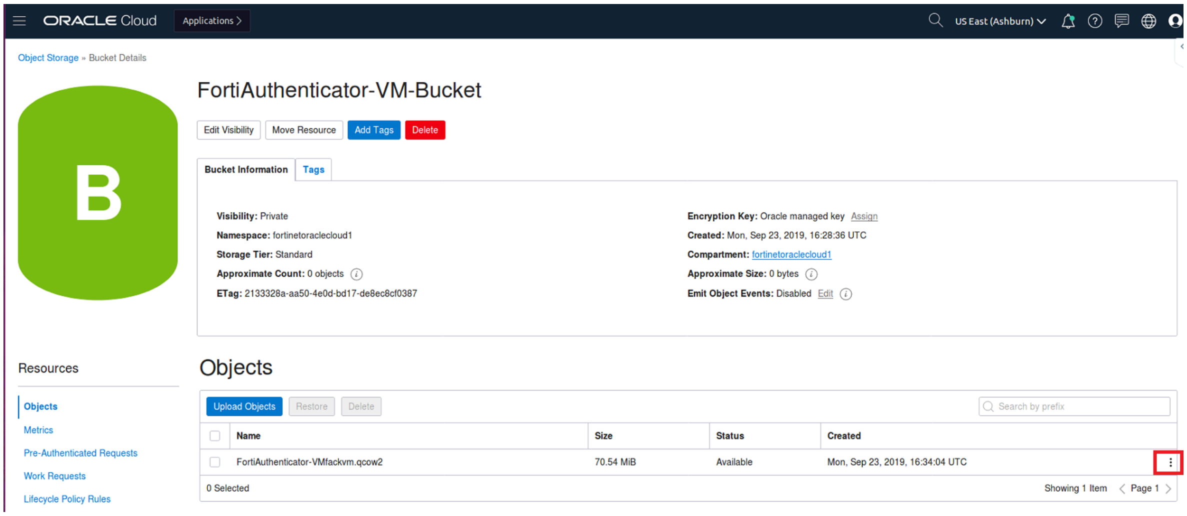
FortiAuthenticator-VM

CHOOSE FILES FROM YOUR COMPUTER

fackvm.qcow2 *70.54 MiB*

1 files, 70.54 MiB total

13. Select *View Object Details* for the newly uploaded object.



FortiAuthenticator-VM-Bucket

Visibility: Private
Namespace: fortinetoraclecloud1
Storage Tier: Standard
Approximate Count: 0 objects
ETag: 2133328a-aa50-4e0d-bd17-de8ec8cf0387

Encryption Key: Oracle managed key Assign
Created: Mon, Sep 23, 2019, 16:28:36 UTC
Compartment: fortinetoraclecloud1
Approximate Size: 0 bytes
Emit Object Events: Disabled Edit

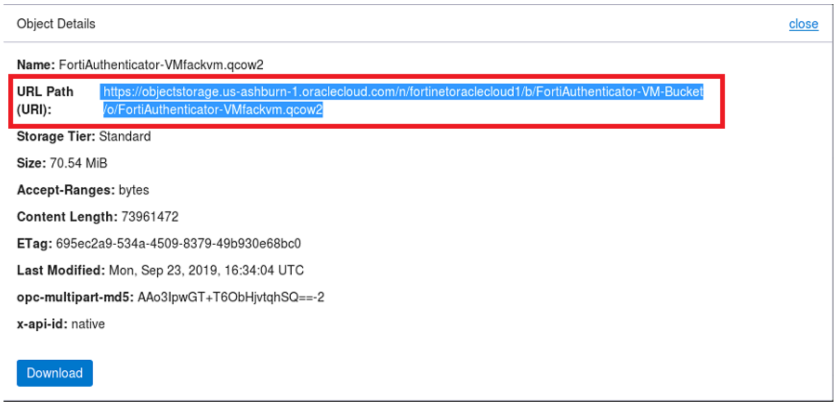
Objects

Name	Size	Status	Created
FortiAuthenticator-VMfackvm.qcow2	70.54 MiB	Available	Mon, Sep 23, 2019, 16:34:04 UTC

0 Selected   Showing 1 Item   Page 1

14. Save the URI of the object.

This file is required in a subsequent step.

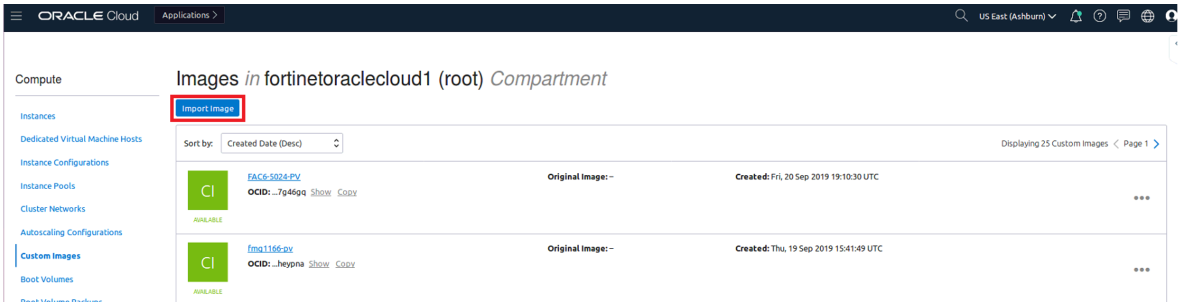


Object Details

Name: FortiAuthenticator-VMfackvm.qcow2
URL Path (URI): https://objectstorage.us-ashburn-1.oraclecloud.com/n/fortinetoraclecloud1/b/FortiAuthenticator-VM-Bucket/o/FortiAuthenticator-VMfackvm.qcow2
Storage Tier: Standard
Size: 70.54 MiB
Accept-Ranges: bytes
Content Length: 73961472
ETag: 695ec2a9-534a-4509-8379-49b930e68bc0
Last Modified: Mon, Sep 23, 2019, 16:34:04 UTC
opc-multipart-md5: AAo3IpwGT+T6ObHjvtqhSQ==-2
x-api-id: native

Importing the image

1. In OCI, go to *Core Infrastructure* > *Compute* > *Custom Images*, and click *Import Image.*



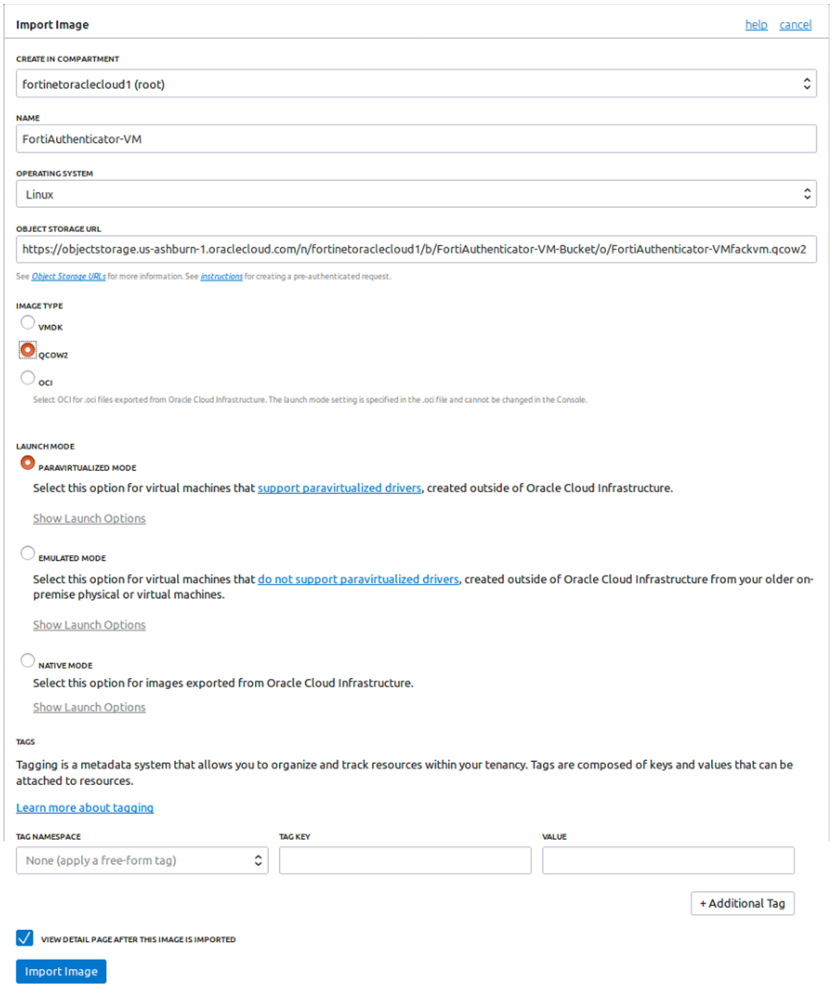
Images *in* fortinetoraclecloud1 (root) *Compartment*

Sort by: Created Date (Desc)   Displaying 25 Custom Images Page 1

FAC6-5024-PV
OCID: ...7g46gq Show Copy
Original Image: –
Created: Fri, 20 Sep 2019 19:10:30 UTC

fmg1166-pv
OCID: ...heypna Show Copy
Original Image: –
Created: Thu, 19 Sep 2019 15:41:49 UTC

2. On the *Import Image* page:
   a. *Name* the image.
   b. Set the *Image Type* to *QCOW2*.
   c. Set the *Launch Mode* to *Paravirtualized Mode*.
   d. Click *Import Image* and wait for the image status to become *Available*.



Import Image

CREATE IN COMPARTMENT
fortinetoraclecloud1 (root)

NAME
FortiAuthenticator-VM

OPERATING SYSTEM
Linux

OBJECT STORAGE URL
https://objectstorage.us-ashburn-1.oraclecloud.com/n/fortinetoraclecloud1/b/FortiAuthenticator-VM-Bucket/o/FortiAuthenticator-VMfackvm.qcow2

See *Object Storage URLs* for more information. See *instructions* for creating a pre-authenticated request.

IMAGE TYPE

○ VMDK
● QCOW2
○ OCI

Select OCI for .oci files exported from Oracle Cloud Infrastructure. The launch mode setting is specified in the .oci file and cannot be changed in the Console.

LAUNCH MODE

● PARAVIRTUALIZED MODE

Select this option for virtual machines that support paravirtualized drivers, created outside of Oracle Cloud Infrastructure.

Show Launch Options

○ EMULATED MODE

Select this option for virtual machines that do not support paravirtualized drivers, created outside of Oracle Cloud Infrastructure from your older on-premise physical or virtual machines.

Show Launch Options

○ NATIVE MODE

Select this option for images exported from Oracle Cloud Infrastructure.

Show Launch Options

TAGS

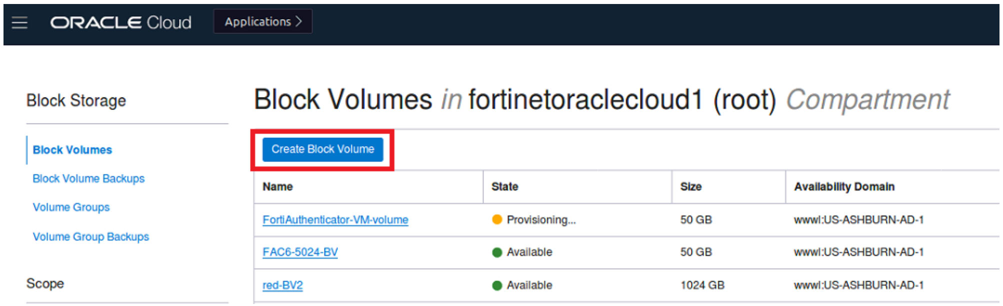
Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

Learn more about tagging

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

☑ VIEW DETAIL PAGE AFTER THIS IMAGE IS IMPORTED

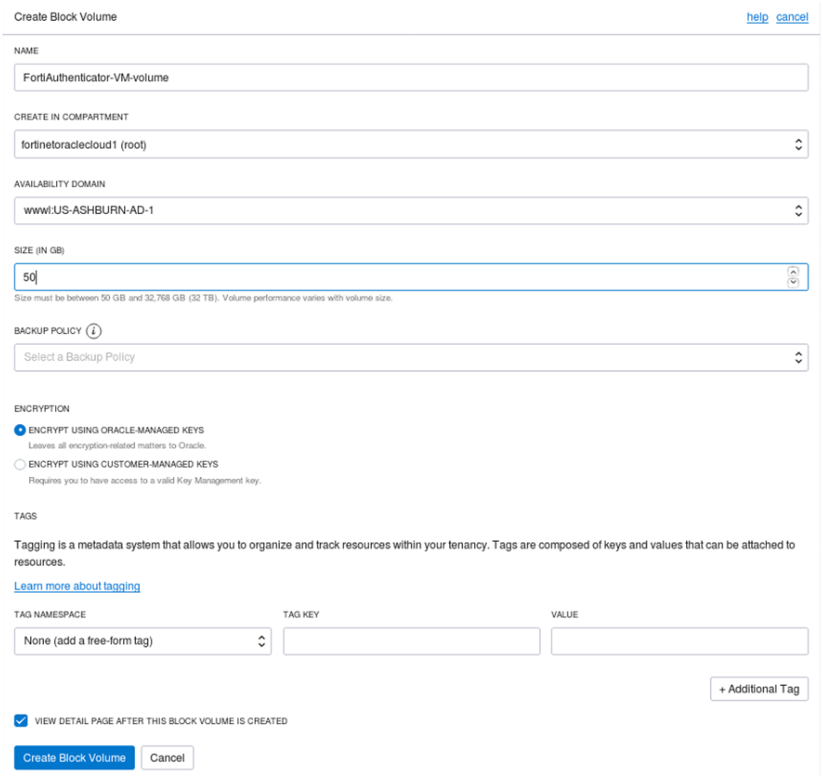
3. Go to *Core Infrastructure >Block Storage > Block Volumes*, and click *Create Block Volume*.



Block Volumes *in* fortinetoraclecloud1 (root) *Compartment*

Name	State	Size	Availability Domain
FortiAuthenticator-VM-volume	● Provisioning...	50 GB	wwwI:US-ASHBURN-AD-1
FAC6-5024-BV	● Available	50 GB	wwwI:US-ASHBURN-AD-1
red-BV2	● Available	1024 GB	wwwI:US-ASHBURN-AD-1

4. On the *Create Block Volume* page:
   a. *Name* the volume.
   b. Set the block volume *Size (in GB)*.
      The FortiAuthenticator-VM is able to run using the minimum 50 GB size, but a larger storage size may be desirable depending on how long of a log history must be preserved and how much activity the VM instance will be subject to.
   c. Click *Create Block Volume*.



Create Block Volume

NAME
FortiAuthenticator-VM-volume

CREATE IN COMPARTMENT
fortinetoraclecloud1 (root)

AVAILABILITY DOMAIN
wwwl:US-ASHBURN-AD-1

SIZE (IN GB)
50
Size must be between 50 GB and 32,768 GB (32 TB). Volume performance varies with volume size.

BACKUP POLICY
Select a Backup Policy

ENCRYPTION
● ENCRYPT USING ORACLE-MANAGED KEYS
Leaves all encryption-related matters to Oracle.
○ ENCRYPT USING CUSTOMER-MANAGED KEYS
Requires you to have access to a valid Key Management key.

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.

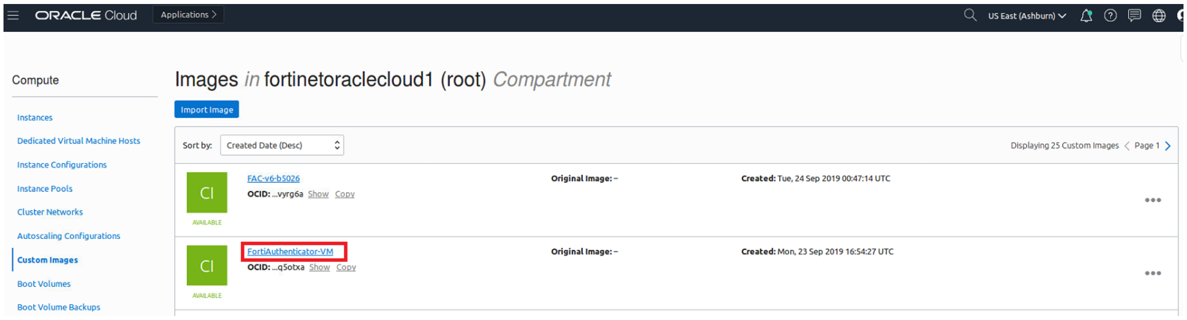
Learn more about tagging

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

☑ VIEW DETAIL PAGE AFTER THIS BLOCK VOLUME IS CREATED

Launching the FortiAuthenticator-VM instance

1. In OCI go to *Core Infrastructure* > *Compute* > *Custom Images*, and click the previously imported image. See Importing the image on page 9.



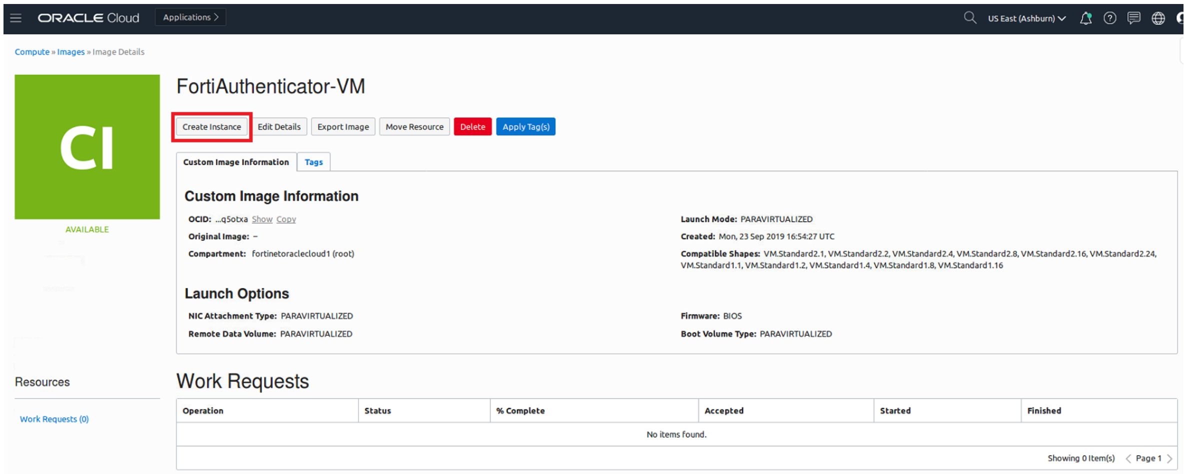
Images *in* fortinetoraclecloud1 (root) *Compartment*

Sort by: Created Date (Desc)

Displaying 25 Custom Images Page 1

CI AVAILABLE	FAC-v6-b5026 **OCID:** ...vyrg6a Show Copy	**Original Image:** –	**Created:** Tue, 24 Sep 2019 00:47:14 UTC
CI AVAILABLE	FortiAuthenticator-VM **OCID:** ...q5otxa Show Copy	**Original Image:** –	**Created:** Mon, 23 Sep 2019 16:54:27 UTC

2. Click *Create Instance*.



FortiAuthenticator-VM

Custom Image Information

OCID: ...q5otxa Show Copy

Original Image: –

Compartment: fortinetoraclecloud1 (root)

Launch Mode: PARAVIRTUALIZED

Created: Mon, 23 Sep 2019 16:54:27 UTC

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

Launch Options

NIC Attachment Type: PARAVIRTUALIZED

Remote Data Volume: PARAVIRTUALIZED

Firmware: BIOS

Boot Volume Type: PARAVIRTUALIZED

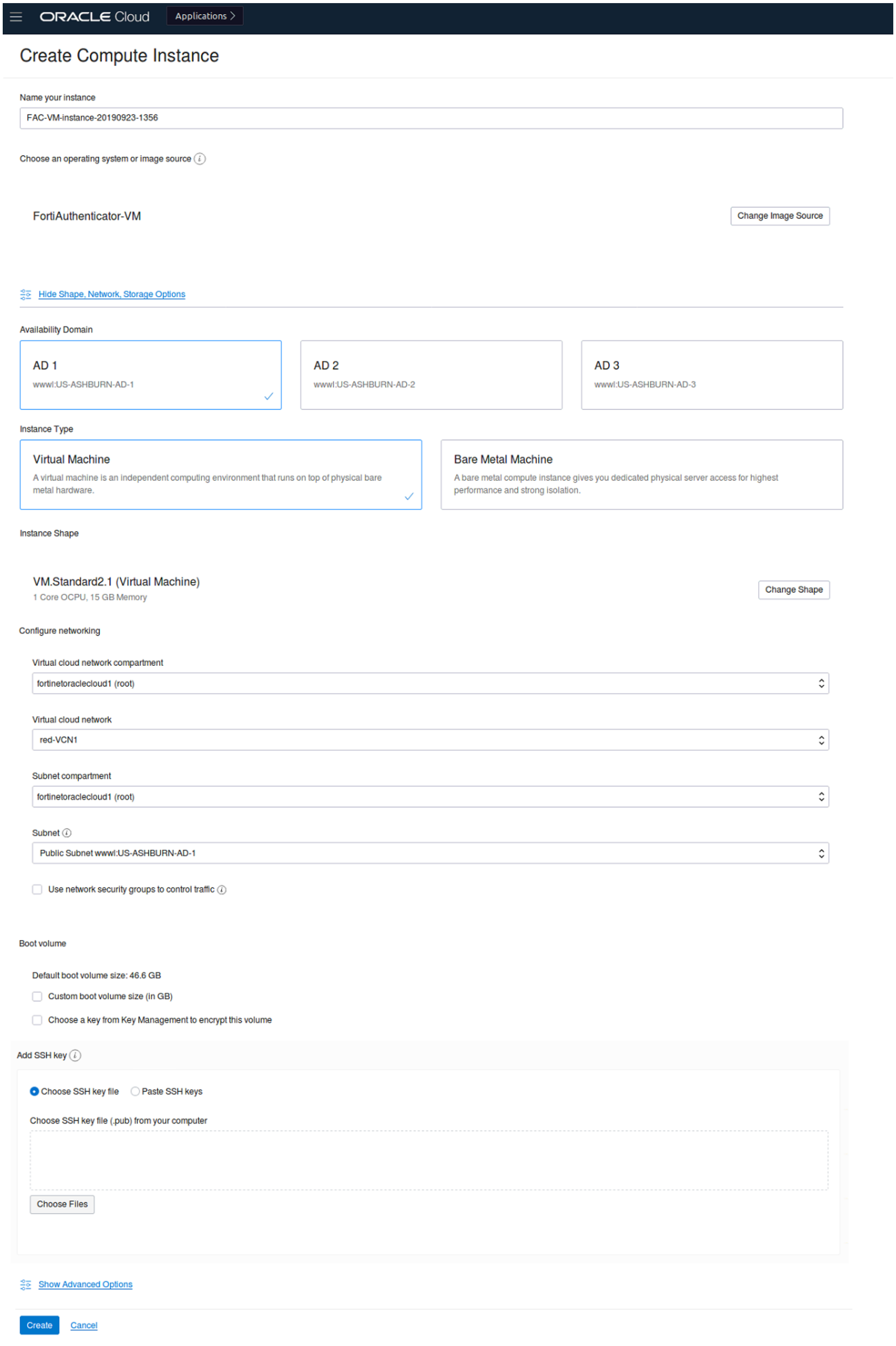
Work Requests

Operation	Status	% Complete	Accepted	Started	Finished
No items found.					

Showing 0 Item(s) < Page 1 >

3. On the *Create Compute Instance* page:
    a. In the *Name your instance* field, name the instance.
    b. In the *Configure networking* section, configure the network.

The *Subnet* must be a public network reachable using an SSH client and web browser.



Create Compute Instance

Name your instance: FAC-VM-instance-20190923-1356

Choose an operating system or image source: FortiAuthenticator-VM

Availability Domain

- AD 1 — wwwl:US-ASHBURN-AD-1 ✓
- AD 2 — wwwl:US-ASHBURN-AD-2
- AD 3 — wwwl:US-ASHBURN-AD-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.

Instance Shape

VM.Standard2.1 (Virtual Machine)
1 Core OCPU, 15 GB Memory

Configure networking

Virtual cloud network compartment: fortinetoraclecloud1 (root)

Virtual cloud network: red-VCN1

Subnet compartment: fortinetoraclecloud1 (root)

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

□ Use network security groups to control traffic

Boot volume

Default boot volume size: 46.6 GB

□ Custom boot volume size (in GB)

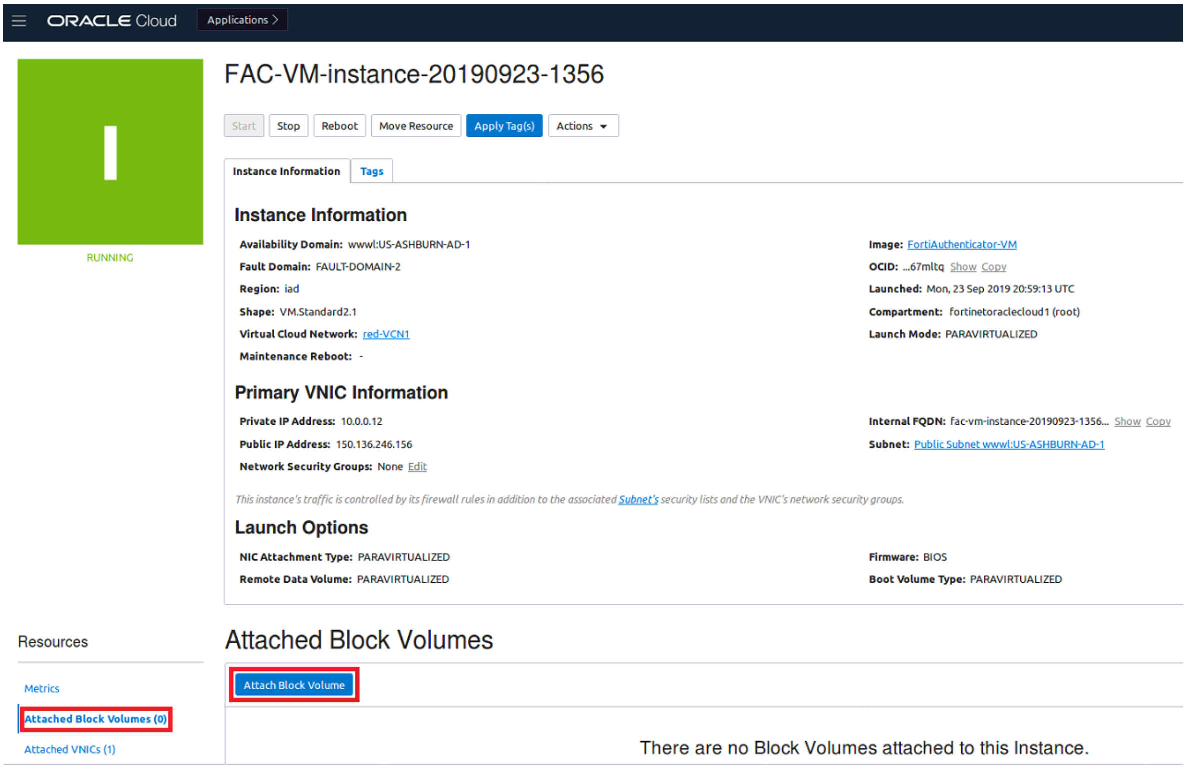
□ Choose a key from Key Management to encrypt this volume

Add SSH key

● Choose SSH key file ○ Paste SSH keys

Choose SSH key file (.pub) from your computer

4. Once the instance is *Running*:
   a. From the side-menu, select *Attached Block Volumes (0)*.
   b. Click *Attach Block*.



FAC-VM-instance-20190923-1356

Instance Information

Availability Domain: wwwl:US-ASHBURN-AD-1
Fault Domain: FAULT-DOMAIN-2
Region: iad
Shape: VM.Standard2.1
Virtual Cloud Network: red-VCN1
Maintenance Reboot: -
Image: FortiAuthenticator-VM
OCID: ...67mltq Show Copy
Launched: Mon, 23 Sep 2019 20:59:13 UTC
Compartment: fortinetoraclecloud1 (root)
Launch Mode: PARAVIRTUALIZED

Primary VNIC Information

Private IP Address: 10.0.0.12
Public IP Address: 150.136.246.156
Network Security Groups: None Edit
Internal FQDN: fac-vm-instance-20190923-1356... 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 and the VNIC's network security groups.

Launch Options

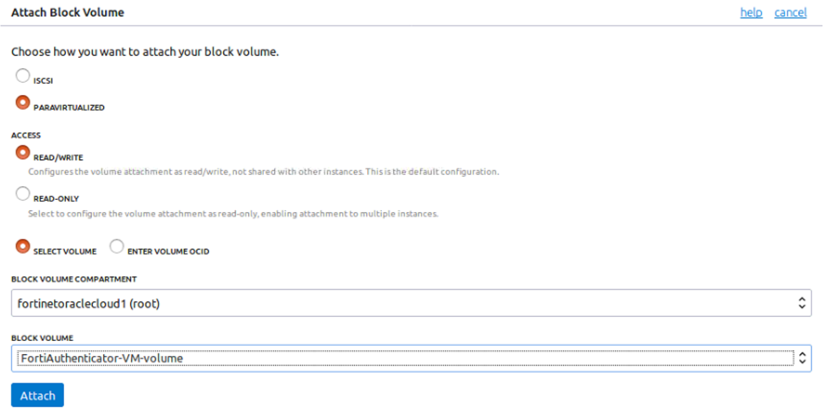
NIC Attachment Type: PARAVIRTUALIZED
Remote Data Volume: PARAVIRTUALIZED
Firmware: BIOS
Boot Volume Type: PARAVIRTUALIZED

Attached Block Volumes

There are no Block Volumes attached to this Instance.

5. On the *Attach Block Volume* page, select the following options, and click *Attach*:

- *PARAVIRTUALIZED*
- *READ/WRITE*
- The previously created *BLOCK VOLUME*



Attach Block Volume

Choose how you want to attach your block volume.

○ ISCSI
● PARAVIRTUALIZED

ACCESS

● READ/WRITE
Configures the volume attachment as read/write, not shared with other instances. This is the default configuration.

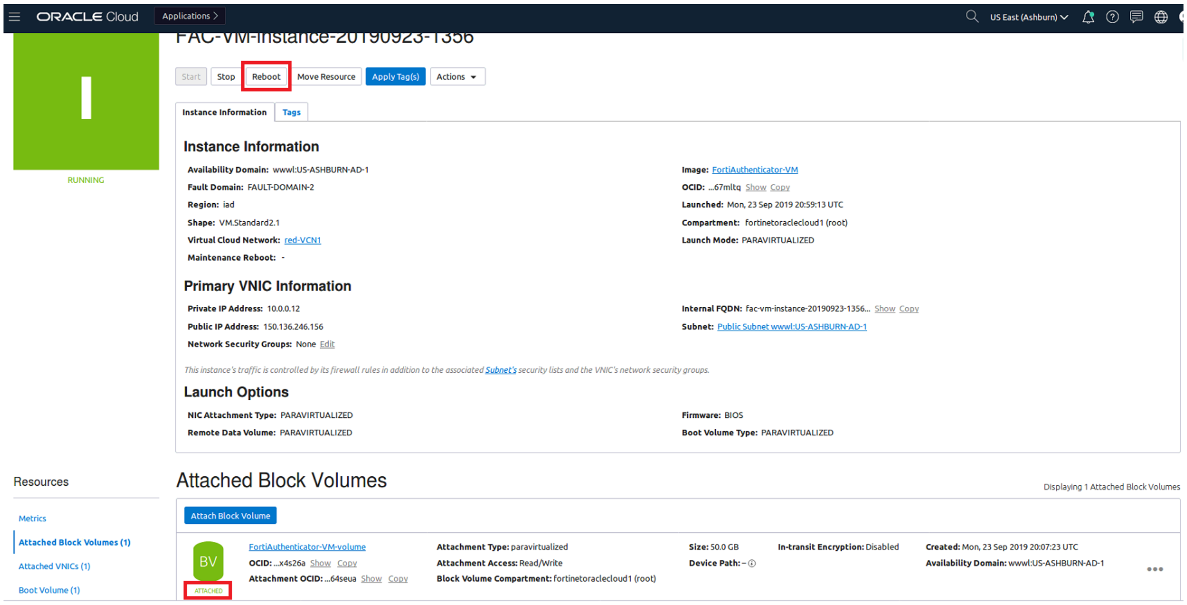
○ READ-ONLY
Select to configure the volume attachment as read-only, enabling attachment to multiple instances.

● SELECT VOLUME ○ ENTER VOLUME OCID

BLOCK VOLUME COMPARTMENT
fortinetoraclecloud1 (root)

BLOCK VOLUME
FortiAuthenticator-VM-volume

6. Wait for the block volume to reach the *Attached* state, then click *Reboot* to restart the FortiAuthenticator-VM.



FAC-VM-instance-20190923-1356

Instance Information

Availability Domain: wwwl:US-ASHBURN-AD-1
Fault Domain: FAULT-DOMAIN-2
Region: iad
Shape: VM.Standard2.1
Virtual Cloud Network: red-VCN1
Maintenance Reboot: -
Image: FortiAuthenticator-VM
OCID: ...67mltq Show Copy
Launched: Mon, 23 Sep 2019 20:59:13 UTC
Compartment: fortinetoraclecloud1 (root)
Launch Mode: PARAVIRTUALIZED

Primary VNIC Information

Private IP Address: 10.0.0.12
Public IP Address: 150.136.246.156
Network Security Groups: None Edit
Internal FQDN: fac-vm-instance-20190923-1356... 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 and the VNIC's network security groups.

Launch Options

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

Attached Block Volumes

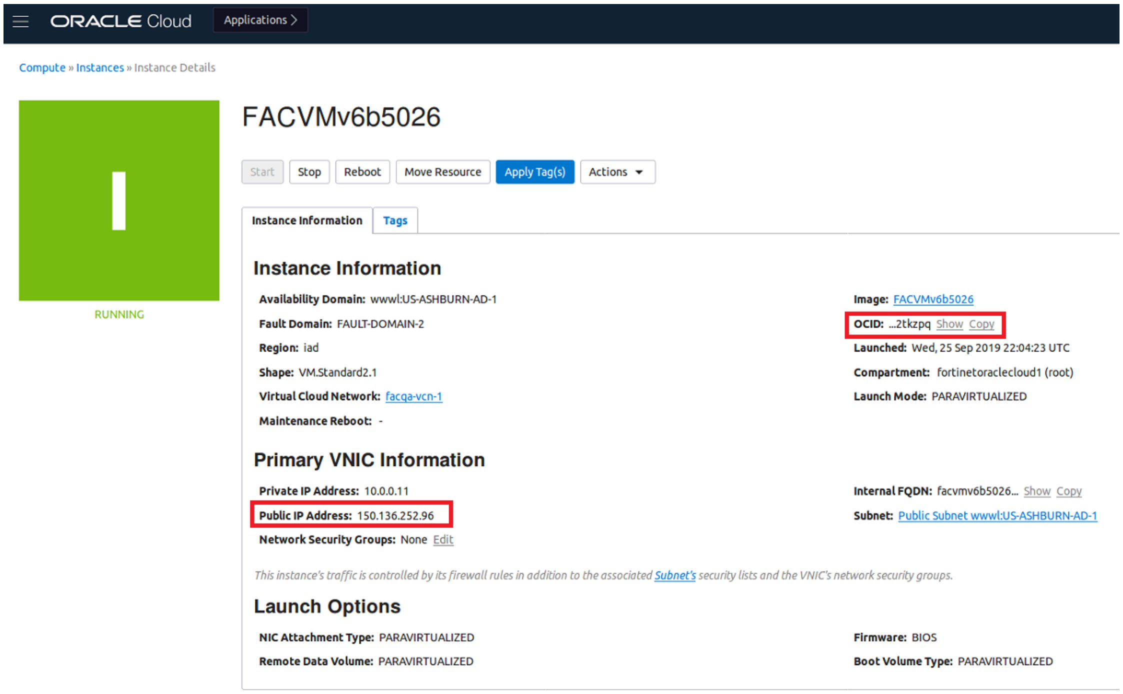
Displaying 1 Attached Block Volumes

FortiAuthenticator-VM-volume
OCID: ...x4s26a Show Copy
Attachment OCID: ...64seua Show Copy
Attachment Type: paravirtualized
Attachment Access: Read/Write
Block Volume Compartment: fortinetoraclecloud1 (root)
Size: 50.0 GB
Device Path: –
In-transit Encryption: Disabled
Created: Mon, 23 Sep 2019 20:07:23 UTC
Availability Domain: wwwl:US-ASHBURN-AD-1

Connecting to FortiAuthenticator-VM

To access the GUI console of the FortiAuthenticator-VM, log in to its CLI console via SSH, and then connect the public IP address assigned to the instance.

1. On OCI, go to *Core Infrastructure* > *Compute* > *Instances*, and click the name of the FortiAuthenticator-VM instance that is running.
2. Copy the *Public IP Address* and *OCID*.



FACVMv6b5026

Instance Information

Availability Domain: wwwl:US-ASHBURN-AD-1
Fault Domain: FAULT-DOMAIN-2
Region: iad
Shape: VM.Standard2.1
Virtual Cloud Network: facqa-vcn-1
Maintenance Reboot: -
Image: FACVMv6b5026
OCID: ...2tkzpq Show Copy
Launched: Wed, 25 Sep 2019 22:04:23 UTC
Compartment: fortinetoraclecloud1 (root)
Launch Mode: PARAVIRTUALIZED

Primary VNIC Information

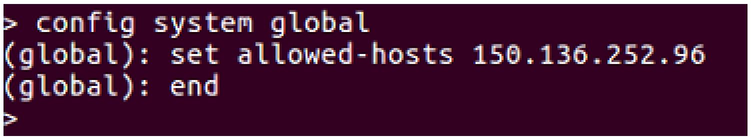
Private IP Address: 10.0.0.11
Public IP Address: 150.136.252.96
Network Security Groups: None Edit
Internal FQDN: facvmv6b5026... Show Copy
Subnet: Public Subnet wwwl:US-ASHBURN-AD-1

This instance's traffic is controlled by its firewall rules in addition to the associated Subnet's security lists and the VNIC's network security groups.

Launch Options

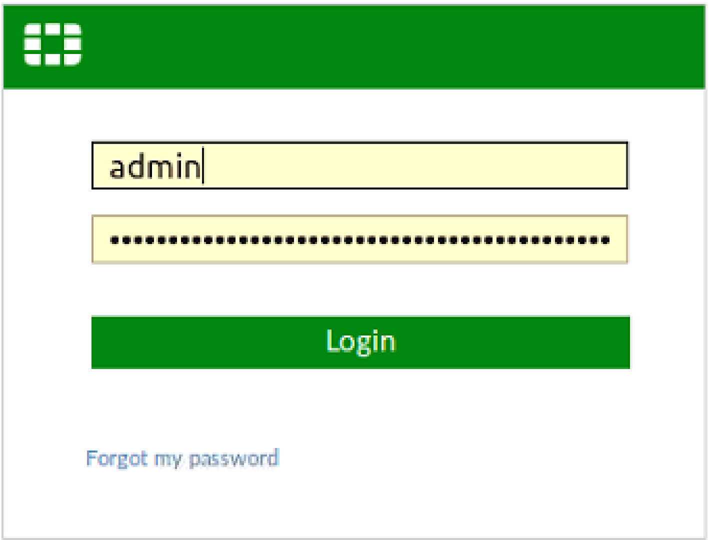
NIC Attachment Type: PARAVIRTUALIZED
Remote Data Volume: PARAVIRTUALIZED
Firmware: BIOS
Boot Volume Type: PARAVIRTUALIZED

3. Connect to the public IP address using an SSH client.
   a. Log in with *admin* as the username and the *OCID* as the password.
   b. Using the CLI, add the public IP address to the `allowed-hosts`. For example:



```
> config system global
(global): set allowed-hosts 150.136.252.96
(global): end
>
```

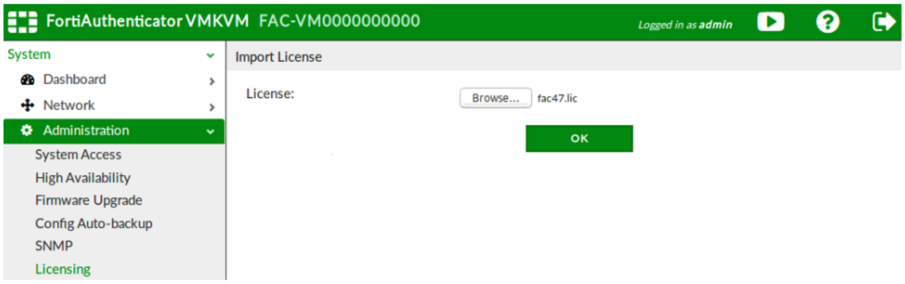
4. In a browser, go to *https://<Public IP Address>*.
   The browser will display a certificate error message, because the default FortiAuthenticator certificate is self-signed and not recognized by browsers.
   You can proceed past this message.
5. Log in with *admin* as the username and the *OCID* as the password.



admin

••

6. Go to *System* > *Administration* > *Licensing*.
7. Click *Browse*, and select your purchased FortiAuthenticator-VM license file.



License: fac47.lic

8. Click *OK*.
   The FortiAuthenticator-VM instance is ready to use after the automatic reboot.