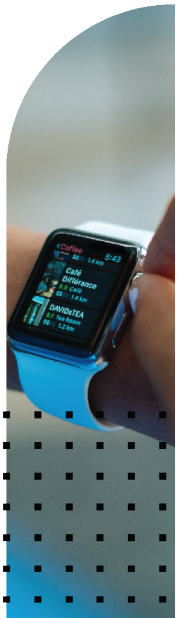
OCI Administration Guide

FortiAnalyzer 7.0



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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

September 23, 2022
FortiAnalyzer 7.0 OCI Administration Guide
05-700-704762-20220923

TABLE OF CONTENTS

About FortiAnalyzer for OCI **4**
Instance type support 4
Models 5
Licensing 5
Order types 5
Creating a support account 5
Registering and downloading licenses 6
Deploying FortiAnalyzer on OCI **7**
Creating an instance by importing the image file 7
Obtaining the deployment image file and placing it in your bucket 7
Importing the Image 9
Launching the FortiAnalyzer instance 11
Creating an instance by selecting an OCI partner image 13
Connecting to the FortiAnalyzer-VM 14
Adding a Disk to the FortiAnalyzer-VM for Logging 16
Change log **18**

About FortiAnalyzer for OCI

FortiAnalyzer-VM for OCI delivers centralized logging, analytics, and reporting features. As an OCI VM instance, FortiAnalyzer allows you to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location to get a simplified, consolidated view of your security position. In addition, you will have detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of security breaches.

Highlights of FortiAnalyzer for OCI include the following:

- Graphical summary reports provide network-wide reporting of events, activities, and trends occurring on FortiAnalyzers and third-party devices.
- Network event correlation enables IT administrators to quickly identify and react to security threats across the network.
- Scalable performance and capacity supports thousands of FortiAnalyzers and can dynamically scale storage based on retention and compliance requirements.
- Choice of standalone, collector, or analyzer mode allows deployment of individual instances or optimization for specific operations, such as store and forward or analytics.
- Seamless integration with the Fortinet product portfolio enables tight integration to allow FortiAnalyzer resources to be managed from FortiGate or FortiManager user interfaces.

Instance type support

FortiAnalyzer for OCI can be deployed as “Virtual Machine” and supported instances are the “Standard” types.

FortiAnalyzer has a minimum requirement of 4 vCPU and 8GB of RAM on an instance.
1 OCPU equates to 2 vCPUs. Ensure that you meet the requirements for your license.

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

- OCI: Compute Shapes
- Fortinet FortiAnalyzer-VM Centralized Logging/Reporting

The following shows supported instance shapes for FortiAnalyzer on OCI:

Specialty and previous generation

Instance shape	OCPU	RAM (GB)
VM.Standard2.2	2	30
VM.Standard2.4	4	60
VM.Standard2.8	8	120

Instance shape	OCPU	RAM (GB)
VM.Standard2.16	16	240
VM.Standard2.24	24	320

Models

FortiAnalyzer-VM is licensed based on the amount of logging per day and storage capacity. Refer to price lists and order SKUs available through your resellers/distributors. These are also referred to as bring your own license (BYOL) models.

FortiAnalyzer-VM can be deployed using different CPU and RAM sizes and launched on various private and public cloud platforms.

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

Licensing

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

- Order types on page 5
- Creating a support account on page 5
- Registering and downloading licenses on page 6

Order types

On OCI, there is only one license type: Bring Your Own License (BYOL). There is no Pay As You Go/On-Demand license available to purchase for FortiAnalyzer-VM for OCI.

BYOL is annual perpetual 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.

Creating a support account

FortiAnalyzer-VM for OCI supports BYOL licensing models.

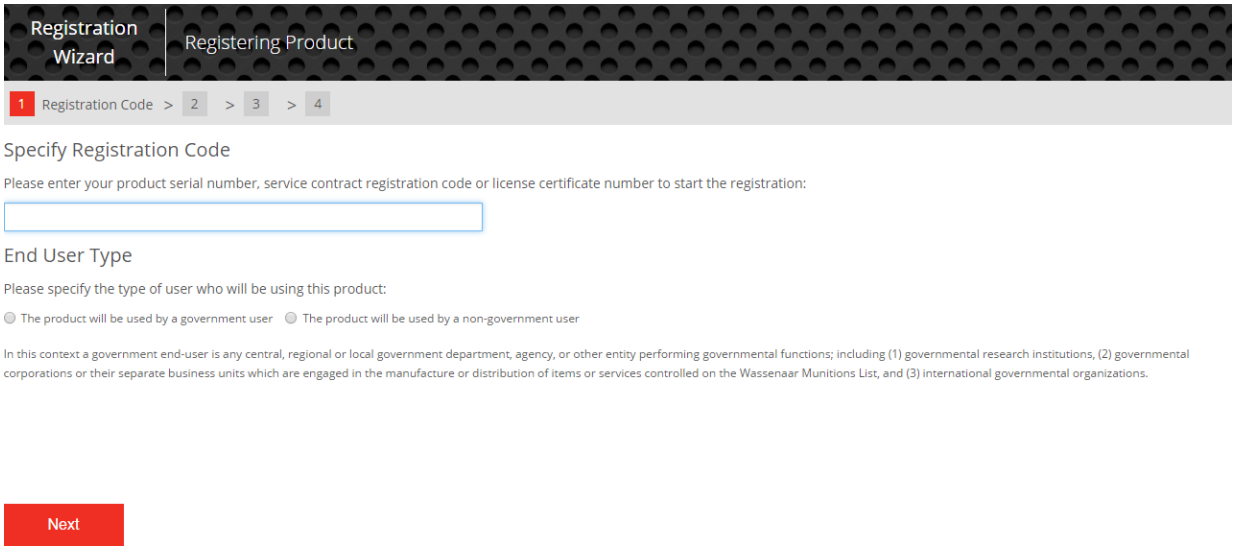
For BYOL, you typically order a combination of products and services, including support entitlement.

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 FortiAnalyzer and cannot proceed to configure the FortiAnalyzer. See Registering and downloading licenses on page 6.

Registering and downloading licenses

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

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Go to *Asset* > *Register/Renew* 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. Enter your details in the other fields as required.
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 FortiAnalyzer-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 FortiAnalyzer-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

Deploying FortiAnalyzer on OCI

The deployment step mentioned in this guide assumes that you have already created a VCN and relevant network resources such as route tables and subnets. You must also configure a Security List so that you can access FortiAnalyzer over the Internet while closing unnecessary ports. See below:

- Creating a Virtual Cloud Network and Public-Facing Subnets
- Creating a Security List

You will at least need to open TCP port 443 to allow incoming access to FortiAnalyzer's management GUI console (or port 22 for SSH if you are familiar with the FortiAnalyzer command line interface) for initial configuration. See FortiAnalyzer open ports.

There are two methods for creating an instance. Select one of the following methods:

- The first method consists of obtaining the deployment image, importing the file into the OCI portal, then launching the FortiAnalyzer-VM instance. See Creating an instance by importing the image file on page 7
- The second method consists of pointing to an available FortiAnalyzer-VM image on OCI instead of importing one. See Creating an instance by selecting an OCI partner image on page 13

Creating an instance by importing the image file

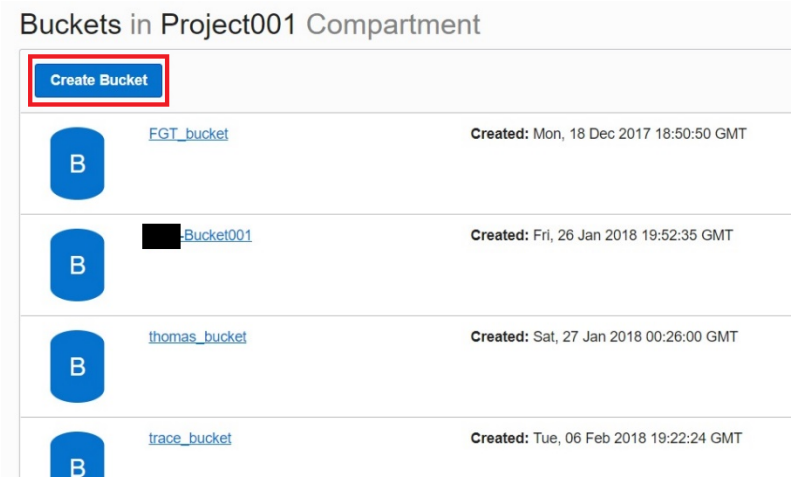
To create a FortiAnalyzer-VM instance by importing an image file, follow these steps:

1. Obtaining the deployment image file and placing it in your bucket on page 7
2. Importing the Image on page 9
3. Launching the FortiAnalyzer instance on page 11

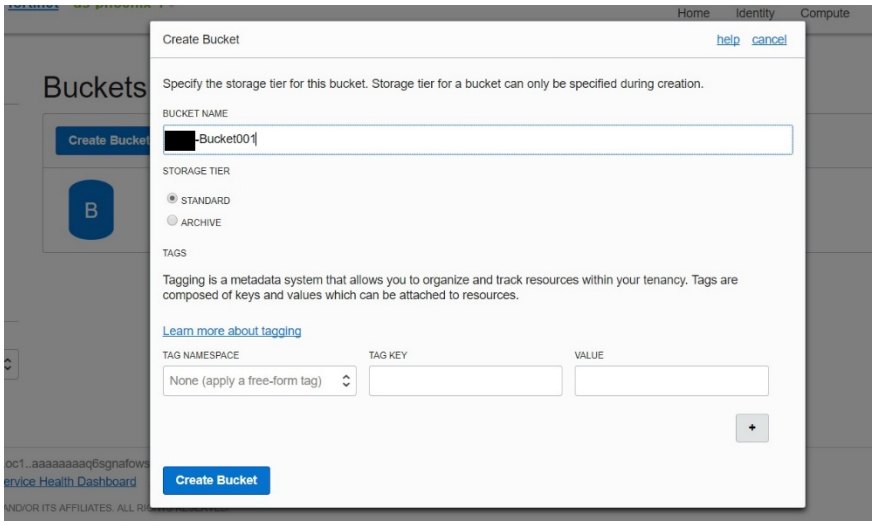
Obtaining the deployment image file and placing it in your bucket

1. Go to https://support.fortinet.com. Navigate to *Download* > *VM Images* in the top menu.
2. In the *Select Product* dropdown list, select *FortiAnalyzer*.
3. In the *Select Platform* dropdown list, select *Oracle*.
4. Obtain the *FAZ_VM64_OPC-vX-buildXXXX-FORTINET.out.OpenXen.zip* file. XXXX is the build number. Ensure the file name includes OpenXen.
5. After downloading, unzip the file. You will find the *faz.qcow2* file, which is needed to deploy the FortiAnalyzer on OCI.

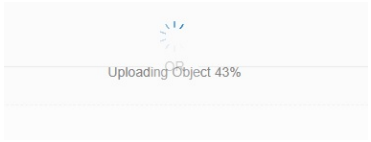
6. In OCI, go to *Storage* > *Object Storage*, then click *Create Bucket* to create a standard storage bucket.



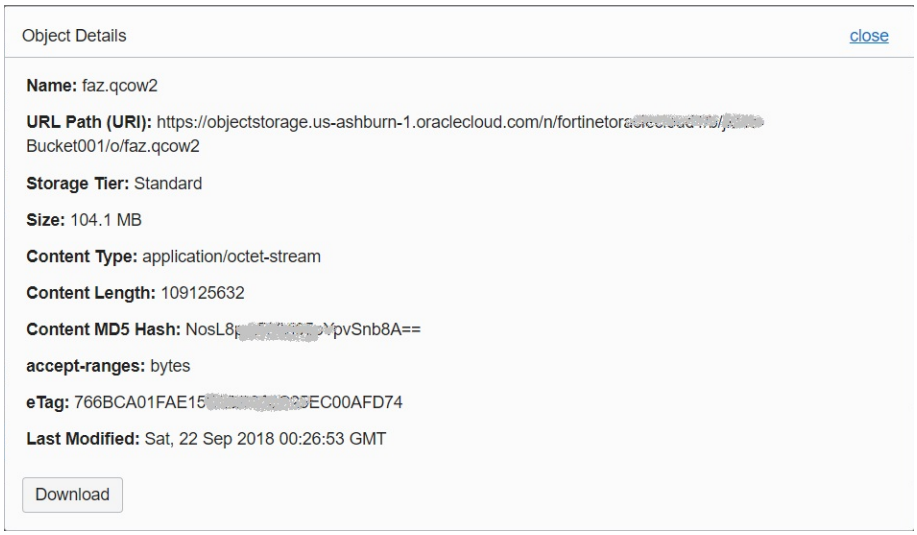
7. Select the bucket, then upload the deployment image file *faz.qcow2*.



8. Click *Upload Object*. The dialog shows the upload progress.



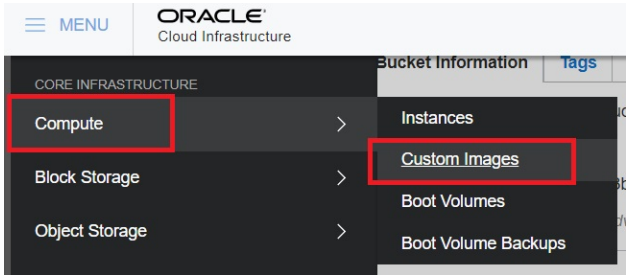
9. Once uploaded, the following screen appears. Click *Detail* on the image that you just uploaded. You can see the URL path to access the image.



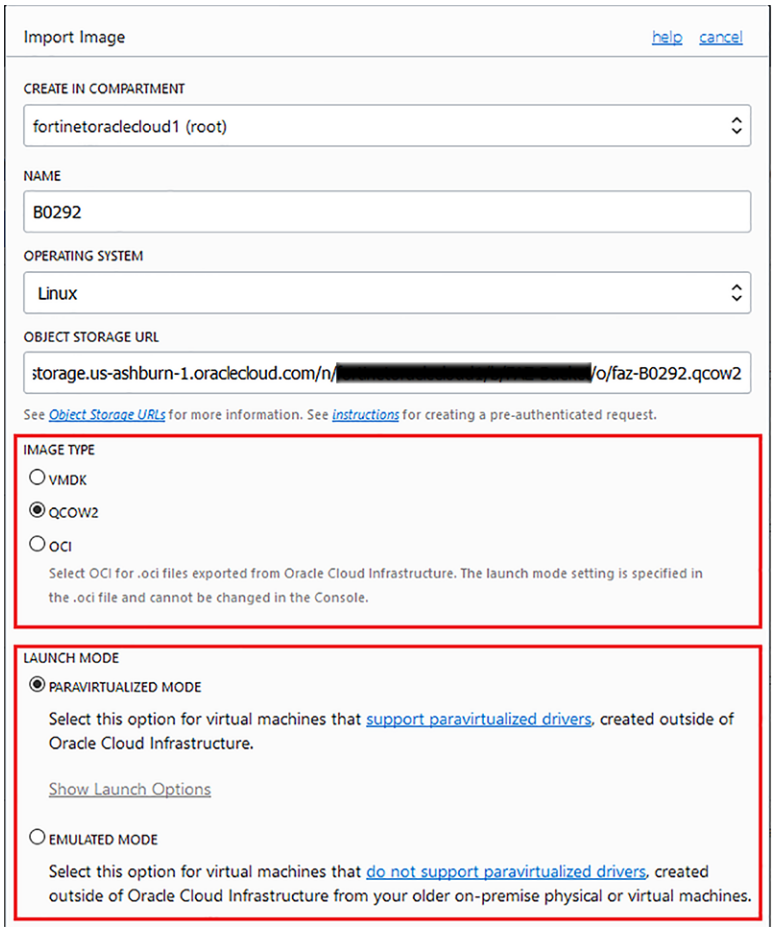
10. Note down this URL. It will be needed in further steps.

Importing the Image

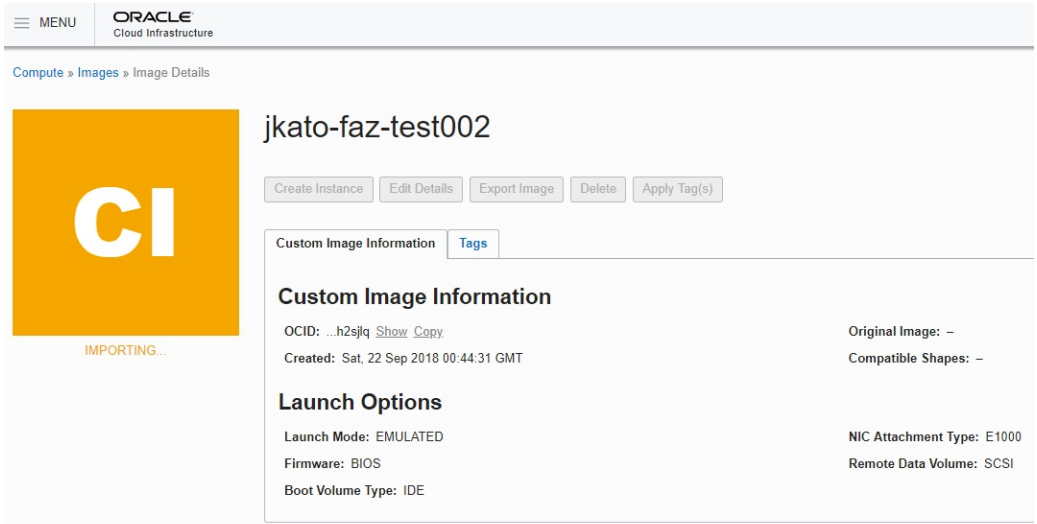
1. Navigate to *Compute* > *Custom Images*.



2. Click *Import Image*. Complete the fields. In the *OBJECT STORAGE URL* field, enter the URL link obtained in Obtaining the deployment image file and placing it in your bucket on page 7.

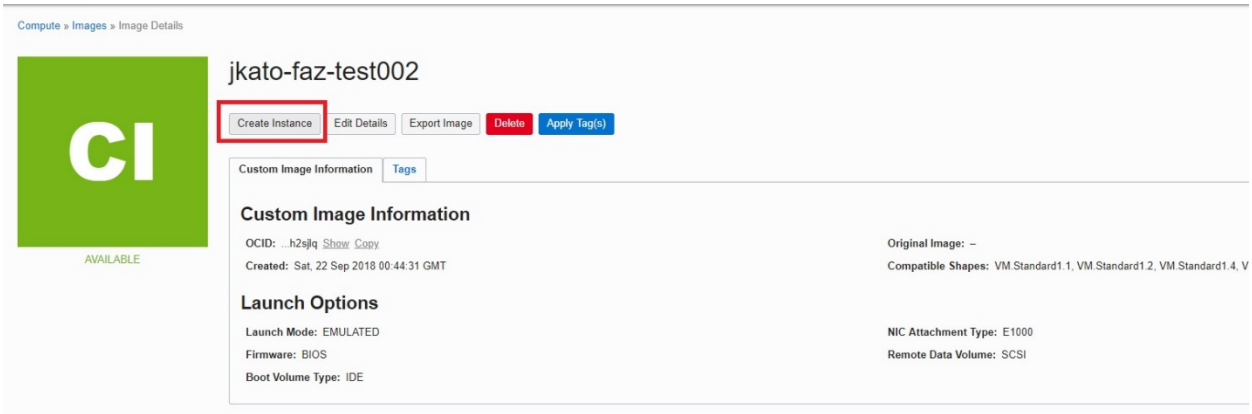


3. Under *IMAGE TYPE*, select *QCOW2*.
4. Under *LAUNCH MODE*, select *PARAVIRTUALIZED MODE* or *EMULATED MODE*. Native mode is not supported.
5. Click *Import Image*.
6. You have now imported the image. Wait until the *Importing...* status changes to *Available*. After the change, navigate to the image.

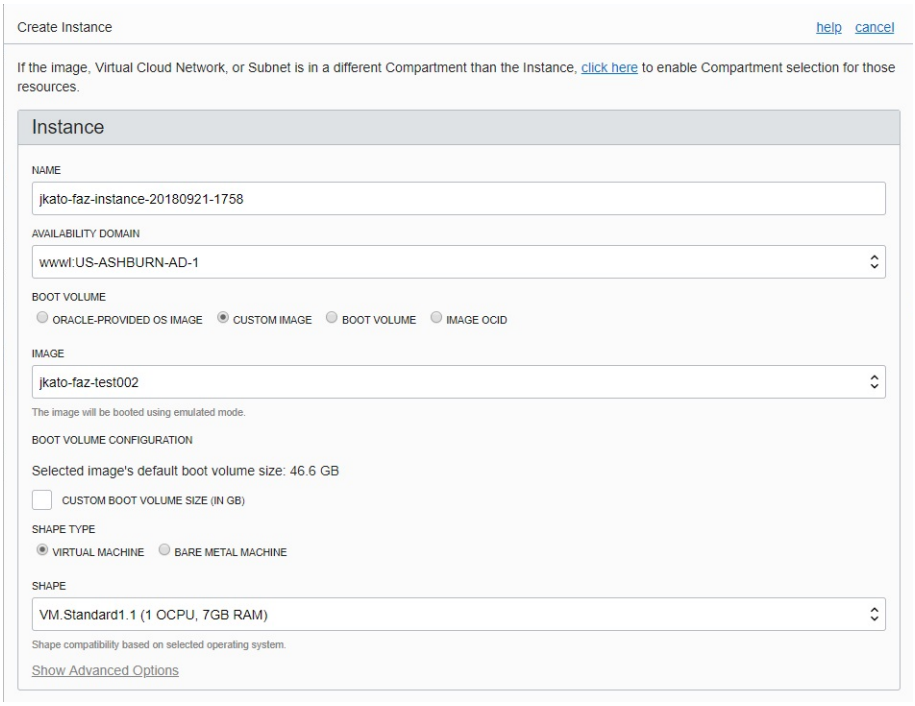


Launching the FortiAnalyzer instance

1. Click *Create Instance*.

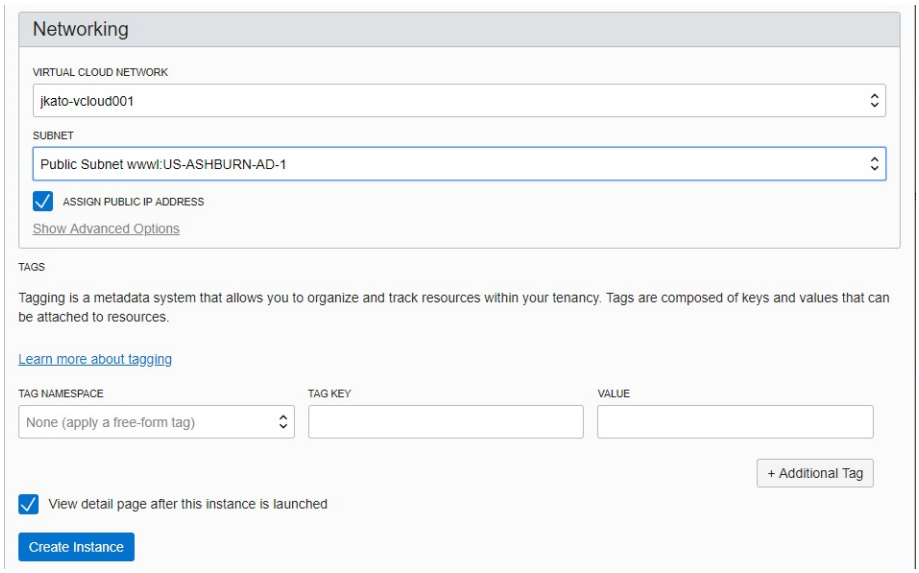


2. In the *NAME* field, enter the desired name to identify the instance by.



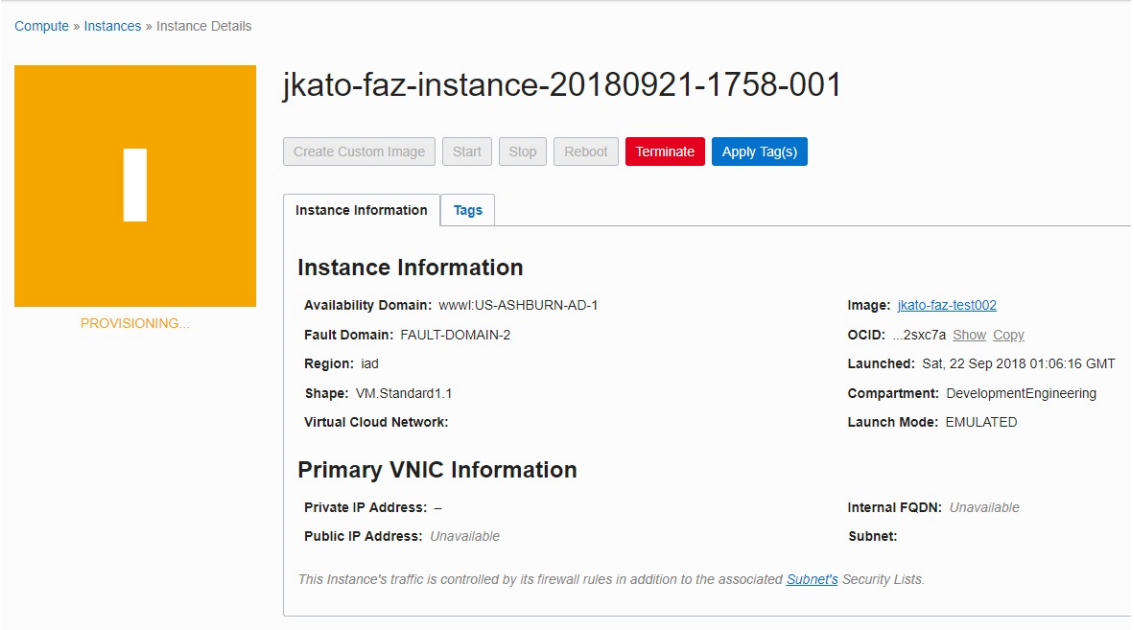
3. In the *AVAILABILITY DOMAIN* field, select the desired domain.
4. Under *IMAGE SOURCE*, select *CUSTOM IMAGE*, then select the image you imported earlier.
5. Under *SHAPE TYPE*, select *VIRTUAL MACHINE*.
6. In the *SHAPE FIELD*, select one of the following supported instance shapes. Other instance shapes are not supported:
   a. VM.Standard1.1
   b. VM.Standard1.2
   c. VM.Standard1.4
   d. VM.Standard1.8
   e. VM.Standard1.16
7. In the *VIRTUAL CLOUD NETWORK* field, select a network to launch the instance.

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

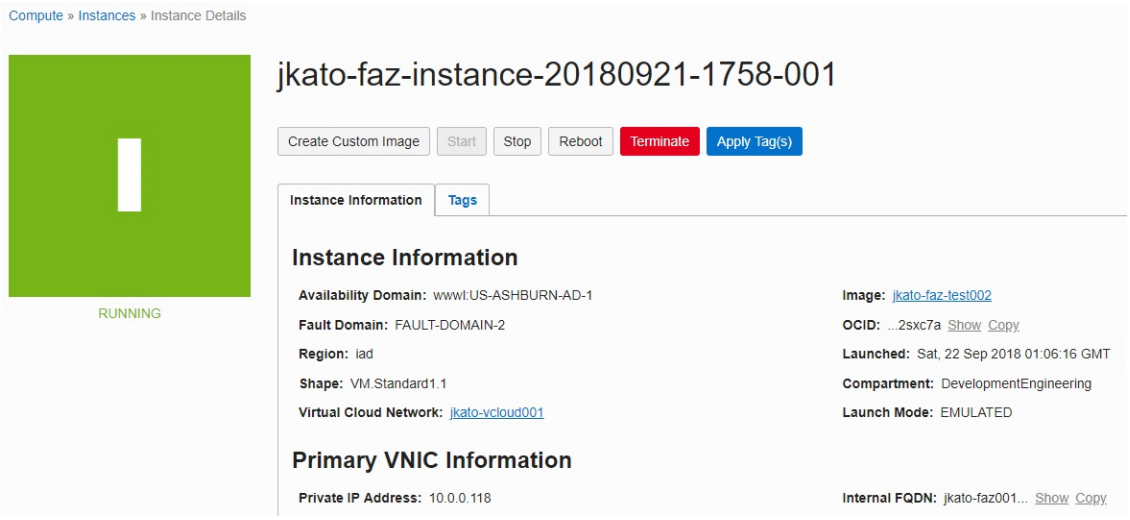


9. Ensure *ASSIGN PUBLIC IP ADDRESS* is selected so you can access the FortiAnalyzer over the Internet. This can be disabled once everything has been configured as desired.
10. Click *HIDE ADVANCED OPTIONS*.
11. In the *PRIVATE IP ADDRESS* field, specify a static IP address within the selected subnet.
12. In the *HOSTNAME* field, enter the desired name.

13. Click *Create Instance*. Wait until the *PROVISIONING…* status changes to *RUNNING*. You can also check the FortiAnalyzer's public IP address in this screen once it becomes available.



At this stage, FortiAnalyzer deployment is not complete. You also need to add a storage volume as a system log disk and attach it to the FortiAnalyzer instance once it starts running.



Creating an instance by selecting an OCI partner image

FortiAnalyzer deployment images are listed on OCI's partner image catalog. You can create the instance by pointing to an available image instead of importing one yourself.

1. In OCI, go to *Compute* > *Instances*.
2. Select the appropriate compartment from the dropdown menu on the left.
3. Click *Create Instance*.
4. Name the instance as desired.
5. Under *Choose an operating system or image source*, click *Change Image Source*.

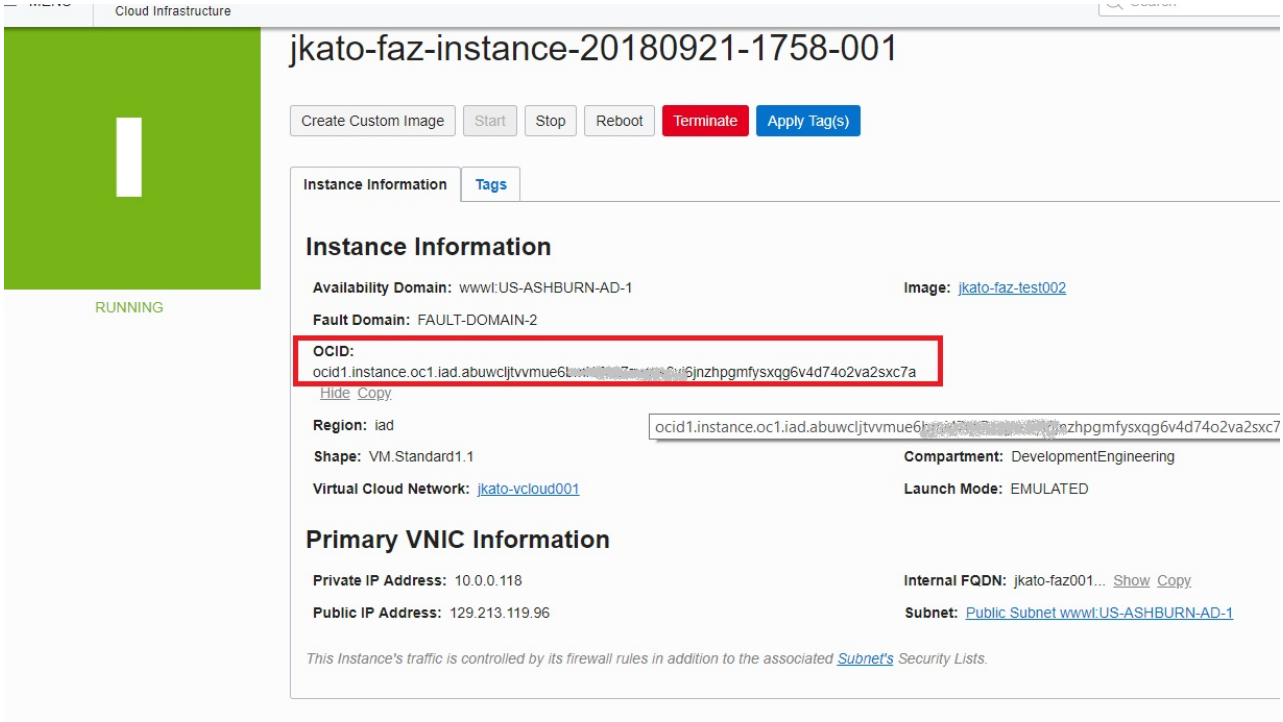
6. In the *Browse All Images* window, go to the *Partner Images* tab. Select the *Fortinet FortiAnalyzer-VM Centralized Logging/Reporting for OCI* app. Select the checkbox at the bottom of the window to confirm that you have read and agree to the terms of use, then click *Select Image*.
   You will return to the instance creation screen.
7. Configure the following settings:
   a. Under *Choose instance type*, select *Virtual Machine*.
   b. Under *Choose instance shape*, select one of the supported instance shapes.
   c. Under *Configure boot volume*, keep the default values.
   d. Under *Configure networking*, add your network configuration settings as desired.
8. Click *Create*. This deploys the FortiAnalyzer-VM instance.

Connecting to the FortiAnalyzer-VM

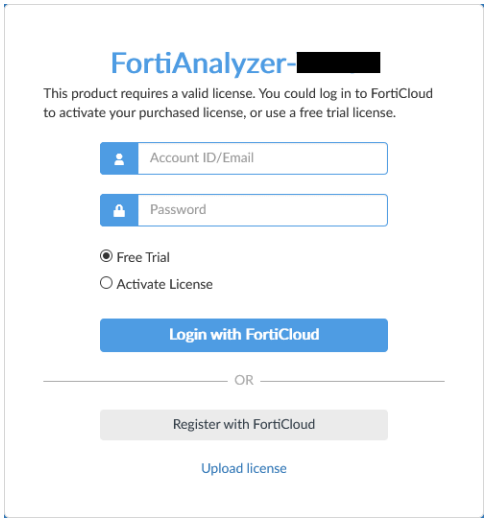
To connect to the FortiAnalyzer, you need your login credentials and the FortiAnalyzer-VM's public IPv4 address. In a web browser, use the public DNS IPv4 address as the URL: https://<public IPv4 address>. You will log in with the default username *admin* and the instance OCID as the password to configure your FortiAnalyzer-VM.

To activate a license for FortiAnalyzer VM:

1. Find the public IP address as shown below and copy the OCID.



2. Connect to the FortiAnalyzer using your browser.
   The login dialog box is displayed.



3. Take one of the following actions:

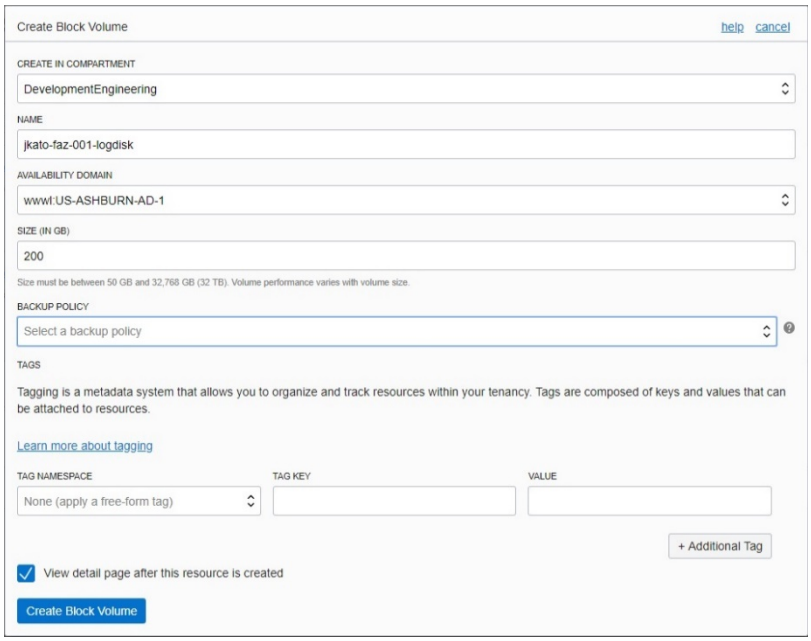
Action	Description
Free Trial	If a valid license is not associated with the account, you can start a free trial license. **1.** Select *Free Trial*, and click *Login with FortiCloud*. **2.** Use your FortiCloud account credentials to log in, or create a new account. FortiAnalyzer connects to FortiCloud to get the trial license. The system will restart to apply the trial license. **3.** Read and accept the license agreement. For more information, see the *FortiAnalyzer 7.0.0 VM Trial License Guide*.
Activate License	If you have a license file, you can activate it . **1.** Select *Activate License*, and click *Login with FortiCloud*. **2.** Use your FortiCloud account credentials to log in. FortiAnalyzer connects to FortiCloud, and the license agreement is displayed. **3.** Read and accept the license agreement.
Upload License	**1.** Click *Browse* to upload the license file, or drag it onto the field. **2.** Click *Upload*. After the license file is uploaded, the system will restart to verify it. This may take a few moments. To download the license file, go to the Fortinet Technical Support site (https://support.fortinet.com/), and use your FortiCloud credentials to log in. Go to *Asset Managmeent* > *Products* > *Product List*, then click the product serial number.

4. Once registration is complete, log into the FortiAnalyzer-VM with the username *admin* and the supplied temporary password.

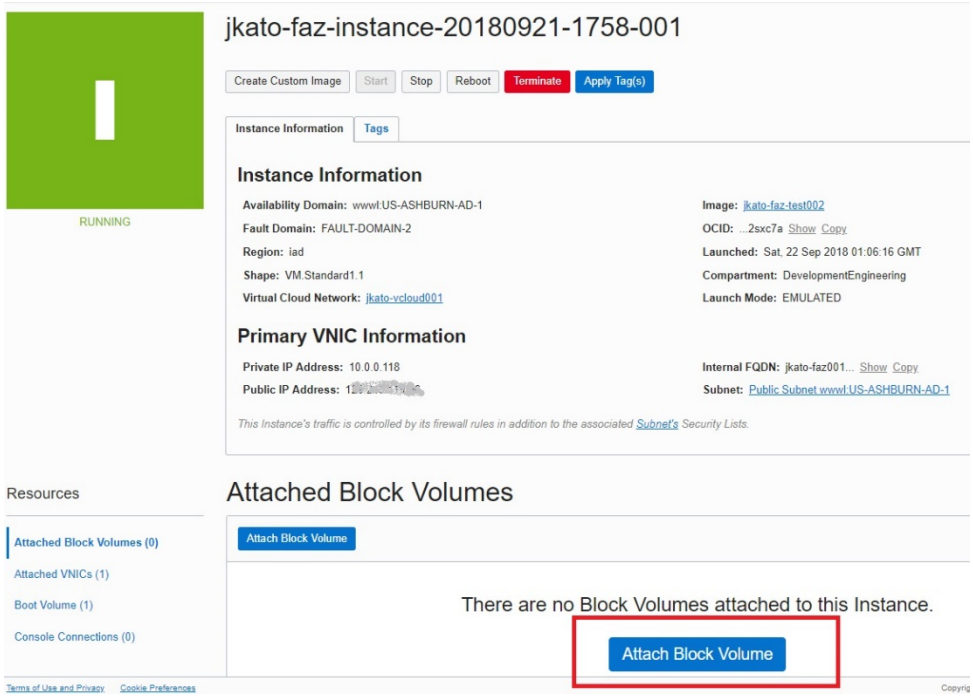
Adding a Disk to the FortiAnalyzer-VM for Logging

You must add another disk to FortiAnalyzer as a log disk.

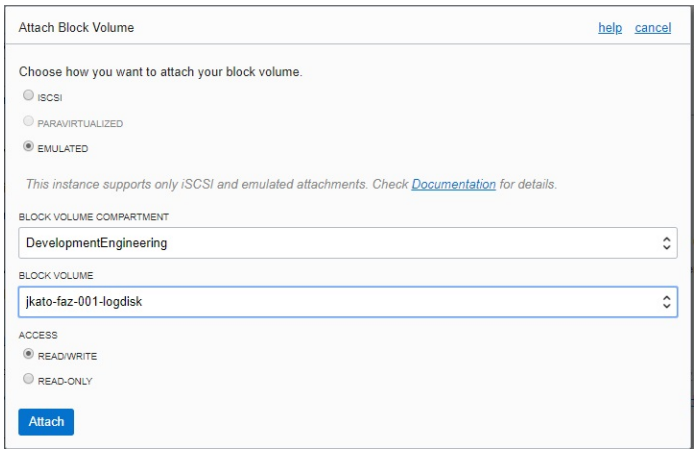
1. Click *Create Block Volume* and configure as shown below. The disk size depends on the ordered license. The example below uses 200 GB.



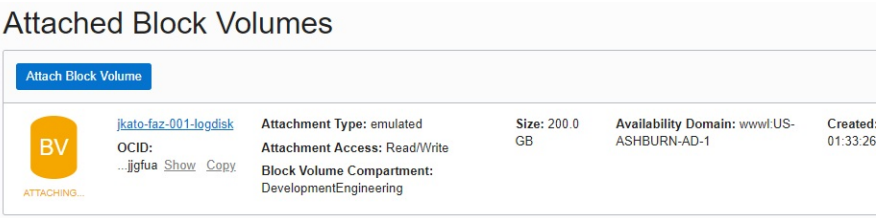
2. Once provisioned, return to the FortiAnalyzer instance. Click *Attach Block Volume*.



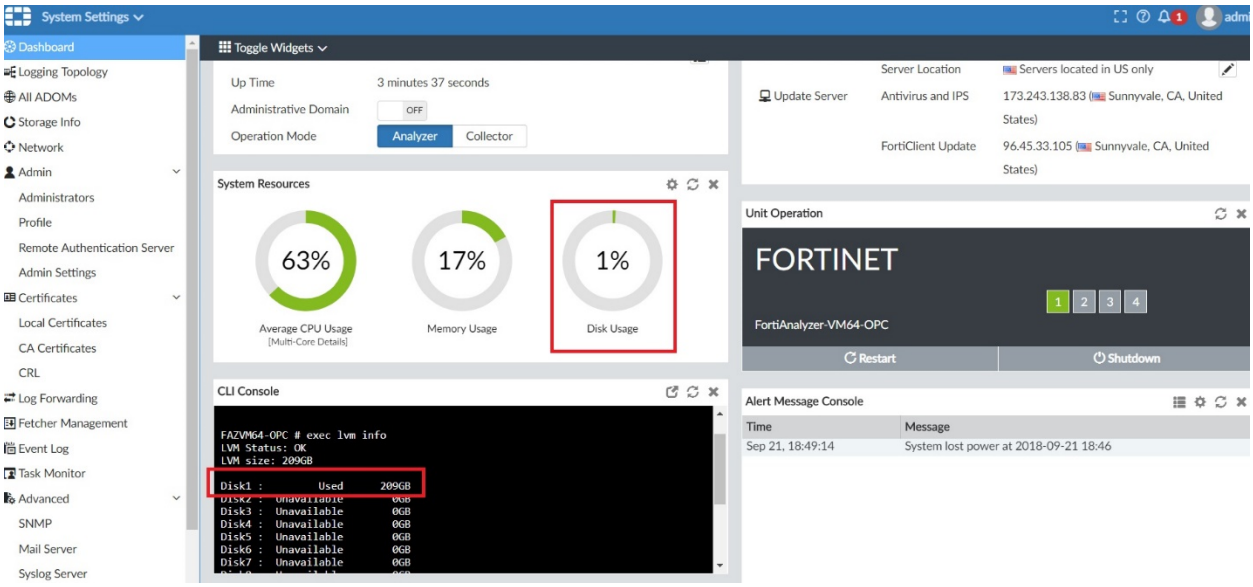
3. Under *Choose how you want to attach your block volume*, select either *EMULATED* or *PARAVIRTUALIZED*. Under *ACCESS*, select *READ/WRITE*.



4. Click *Attach*.



5. After attaching the block volume, ensure you reboot (stop and start) the FortiAnalyzer instance. Otherwise, the added disk is not recognized.
6. After the instance has rebooted, log into the FortiAnalyzer-VM management GUI. It may take some time before you are able to connect. You will see that the disk was successfully added. You can check it by running the CLI command `exec lvm info`. The added 200 GB is shown as Used.



If the status is Unused, enter `exec lvm start` in the CLI to start LVM disk management. Enter `y` to continue. The system reboots.

After rebooting and logging into FortiAnalyzer, the disk should appear as Used. To add additional disks, use `exec lvm extend <disk>` as shown in steps 4 to 6 here. Check the disk space was added on the Dashboard.

Change log

Date	Change description
2021-04-22	Initial release.
2021-08-17	Updated Connecting to the FortiAnalyzer-VM on page 14.
2022-09-23	Updated Instance type support on page 4.

www.fortinet.com