



Deploying FortiTester-VM on OCI

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



Deploying FortiTester-VM on OCI

TABLE OF CONTENTS

About FortiTester-VM on OCI	4
Overview	4
Instance Type Support	4
Deploying FortiTester-VM instances	5
Obtaining the Deployment Image	5
Creating the VCN and public subnets	5
Creating a FortiTester-VM instance	6
Attaching storage to the FortiTester-VM	8
Attaching traffic VNICs to FortiTester-VM	9
Accessing the FortiTester-VM	11
Creating and running test case	12

About FortiTester-VM on OCI

Overview

Welcome, and thank you for selecting Fortinet products for your testing environment.

FortiTester™ appliances offer enterprises and service providers a cost-effective solution for performance testing and validating their network security infrastructure and services, providing a comprehensive range of application test cases to evaluate equipment and right-size infrastructure. All test functionality is included in one simple device-based license.

FortiTester provides powerful yet easy-to-use test cases that simulate many applications and a case history browser for simple analysis. It enables you to establish performance standards and run audits to validate they continue to be met. The virtual appliance version provides an ideal tester for NFV and SDN environments.

Instance Type Support

From FortiTester 3.7.1, FortiTester for OCI can be deployed as "Virtual Machine," and supported instances are the "Standard" types. To ensure high performance and use, it's recommended to deploy FortiTester on the machine types with VM.Standard2.4. Also, you can deploy FortiTester on machine types with VM.Standard2.16, VM.Standard2.24, and VM.Standard2.4. See [Oracle Cloud Infrastructure Documentation](#) for details.

Deploying FortiTester-VM instances

The following topics introduces how to deploy FortiTester-VM on OCI.

Obtaining the Deployment Image

1. Go to the Fortinet support site (<https://support.fortinet.com>) and log in.
2. Navigate to **Download > Firmware Images**.
3. Under **Select Product**, select **FortiTester**, then select the firmware version directory.
4. Download the image file **FTS_VM_OCI_BYOL-vxxx-buildxxxx-FORTINET.out.oci.zip**, where vxxx is the major version number, and buildxxxx is the build number.

Creating the VCN and public subnets

To deploy the FortiTester-VM instance in a new virtual cloud network, follow steps below:

1. On the OCI Console, click **Create a virtual cloud network**.
2. For the **NAME** field, enter a VCN name, for example, fts_mgmt_vcn.
3. 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. You can also select **CREATE VIRTUAL CLOUD NETWORK ONLY** to create each resource separately accordingly. Here, we take **CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES** as an example.
4. Click **Create Virtual Cloud Network**.
5. Click **Close** from the pop-up window.
6. Click **Create Subnet** from the **Virtual Cloud Network Details** page for the management subnet.
 - For the **NAME** field, enter a subnet name, for example, fts_mgmt; for **SUBNET ACCESS**, select **PUBLIC SUBNET**. For other options, follow the default ones.
 - For **SECURITY LIST**, you can select **Default Security List for fts_mgmt**.
 - a. Edit the default security list
Go to **Resources > Security Lists**, click **Default Security List for fts_mgmt**. Click **Add Ingress Rules** to add a rule to allow TCP port 443.
 - b. Create a new security list
Go to **Resources > Security Lists > Create Security List**.
7. Click **Create Subnet**.
8. Click **Create Subnet** from the **Virtual Cloud Network Details** page for the traffic subnet.
 - For the **NAME** field, enter a subnet name, for example, fts_traffic; for **SUBNET ACCESS**, select **PRIVATE SUBNET**. For other options, follow the default ones.
 - For **SECURITY LIST**, you can select **Default Security List for fts_traffic**.
 - a. Edit the default security list
Go to **Resources > Security Lists**, click **Default Security List for traffic**. Click **Add Ingress**

Rules to add a rule to allow all traffic.

- b. Create a new security list

Go to **Resources > Security Lists > Create Security List**.

9. Click **Create Subnet**.

Creating a FortiTester-VM instance

To create a FortiTester-VM instance by importing an image file, follow steps below:

1. Obtain the deployment image file image.out.oci.zip, and unzip the file (ftsos.oci).
2. On the OCI Console, create a storage bucket.
 - Click **Store data**.
 - Configure the bucket as below.

Create Bucket [help](#) [cancel](#)

BUCKET NAME
bucket-20191105-1535

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)		

[+ Additional Tag](#)

[Create Bucket](#) [Cancel](#)

- Click the created bucket, and update the deployment image file ftsos.oci by clicking **Upload Objects**.
- Once the file is uploaded, click **Pre-Authenticated Requests**.
For **NAME**, you can use the default one or specify a name.
For **PRE-AUTHENTICATED REQUEST TARGET**, select **OBJECT**.
For OBJECT NAME, enter the object name you have created.
For ACCESS TYPE, use the default type.
Click **Create Pre-Authenticated Request**.
- Note down the URL below.

Pre-Authenticated Request Details [close](#)

NAME READ-ONLY
par-bucket-20191105-1503

PRE-AUTHENTICATED REQUEST URL READ-ONLY
https://objectstorage.us-ashburn-1.oraclecloud.com/p/qxF3pLfiG8zqBjM3r8QgdoaYkOAr5E_UdIR_-cm-bA/n/fortinetoraclecloud1/b/bucket-20191105-1535/o/

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

[Close](#)

3. Import the image.
 - Go to **Compute > Custom Images**. Click **Import Image**.
 - For the **OBJECT STORAGE URL** field, enter the URL link you have noted in last step; for **IMAGE TYPE**, select OCI.
 - Click **Import Image**.
 - Wait until the IMPORTING... status changes to AVAILABLE.
4. Create the FortiTester-VM instance.
 - For the newly imported image, click **Create Instance**.
 - Enter a name to identify the instance;
for **Availability Domain**, select the desired domain;
for **Instance Type**, select Virtual Machine;
for **Instance Shape**, select Standard2 instance families such as VM.Standard2.4, VM.Standard2.8, VM.Standard2.16, and VM.Standard2.24.
for **Virtual cloud network**, select the VCN to launch the instance.
for **Subnet** field, select a subnet on the Internet-facing side of the network.
 - Click **Create**.
 - Wait until the PROVISIONING... status changes to RUNNING. You can also check the FortiTester's public IP address in this screen once it becomes available.

Attaching storage to the FortiTester-VM

1. Go to **Block Storage > Block Volumes > Create Block Volume**.
2. Enter a unique name for the block volume, select an AVAILABILITY DOMAIN, and specify the size to around 50 GB.
3. Click **Create Block Volume**. This provisions the volume.
4. Once provisioned, return to the FortiTester-VM instance. Click **Attach Block Volume**.

Attach Block Volume [help](#) [cancel](#)

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 enables attachment to a single instance only and 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

fortinetoradcloud1 (root) ^

BLOCK VOLUME

Select a Block Volume or a Boot Volume ^

Attach

Attaching traffic VNICs to FortiTester-VM

1. Go to **Compute > Instances**, click the instance you have created.
2. Go to **Resources > Attached VNICs**.
3. Click **Create VNIC** to create for example, vnic_attach_traffic_port1.

Create VNIC [cancel](#)

VNIC Information

If the Virtual Cloud Network, or Subnet is in a different Compartment than the VNIC, enable Compartment selection for those resources: [Click here](#).

NAME (Optional)

VNIC_attach_traffic_port1

VIRTUAL CLOUD NETWORK

Fortitester-VCN

SUBNET ⓘ

fts_traffic

☐ Use Network Security Groups To Control Traffic (Optional) ⓘ

☒ 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)

10.0.1.11

☐ Assign public IP address

HOSTNAME (Optional)

First select "Subnet" above

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

FULLY QUALIFIED DOMAIN NAME (Read-only)

First select "Subnet" above

4. Click **Create VNIC**.

5. Continue creating vnic_attach_traffic_port2.

Create VNIC

[cancel](#)

VNIC Information

If the Virtual Cloud Network, or Subnet is in a different Compartment than the VNIC, enable Compartment selection for those resources: [Click here.](#)

NAME (Optional)

vnic_attach_traffic_port2

VIRTUAL CLOUD NETWORK

FortiTester-VCN

SUBNET (Optional)

fts_traffic

☐ Use Network Security Groups To Control Traffic (Optional) ⓘ

☒ 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)

10.0.1.41

☐ Assign public IP address

HOSTNAME (Optional)

First select "Subnet" above

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

FULLY QUALIFIED DOMAIN NAME (Read-only)

First select "Subnet" above

6. Go to **Compute > Instances, click the instance created.****7. On **Instance Details** page, click **Reboot** to reboot the created instance.**

Accessing the FortiTester-VM

1. In the FortiTester-VM instance, find the public IP address.
2. Enter the public IP address of the FortiTester-VM instance in your browser.
3. Log in with the default username admin, and no password is required. For the first login, the system will prompt to set a password.

Creating and running test case

Create and run a test case to verify the IP address configurations are correct.

1. Go to **Cases > Performance Testing > HTTP > CPS**.
2. Click **Add** to display the **Select case options** dialog box.
3. Configure the network settings.
4. Click **OK** to continue.
5. Configure the test case options.
6. Click **Start** to run the test case.

If all configurations are correct, you can see the case running page.

CLIENT				SERVER			
Layer7 (App Process)				Layer7 (App Process)			
	Second	Total		Second	Total		Second
Http_Attempted	0	2,421,890	Http_Attempted	0	0	Http_Attempted	0
Http_Successful	0	2,421,888	Http_Successful	0	0	Http_Successful	0
Http_Unsuccessful	0	2	Http_Unsuccessful	0	0	Http_Unsuccessful	0
Http_Reply2xx	0	2,421,888	Http_Reply2xx	0	0	Http_Reply2xx	0
Http_Reply3xx	0	0	Http_Reply3xx	0	0	Http_Reply3xx	0
Http_Reply4xx	0	0	Http_Reply4xx	0	0	Http_Reply4xx	0
Http_Reply5xx	0	0	Http_Reply5xx	0	0	Http_Reply5xx	0
Http_Request_Timeout	0	2	Http_Request_Timeout	0	0	Http_Request_Timeout	0
Http_Latency (ms)	0	0	Http_Latency (ms)	0	0	Http_Latency (ms)	0
Http_Url_Response_Time (ms)	0	0	Http_Url_Response_Time (ms)	0	0	Http_Url_Response_Time (ms)	0
Layer4 (Sessions)				Layer4 (Sessions)			
	Second	Total		Second	Total		Second
TCPv4_Attempted	0	258	TCPv4_Attempted	0	0	TCPv4_Attempted	0
TCPv4_Active_Established	0	258	TCPv4_Active_Established	0	0	TCPv4_Active_Established	0
TCPv4_Passive_Established	0	0	TCPv4_Passive_Established	0	257	TCPv4_Passive_Established	0
TCPv4_Concurrency	0	0	TCPv4_Concurrency	0	256	TCPv4_Concurrency	0
TCPv4_3WayFin_Done	0	0	TCPv4_3WayFin_Done	0	1	TCPv4_3WayFin_Done	0
TCPv4_Active_Reset	0	258	TCPv4_Active_Reset	0	0	TCPv4_Active_Reset	0
TCPv4_Passive_Reset	0	0	TCPv4_Passive_Reset	0	0	TCPv4_Passive_Reset	0
TCPv4_TCP_Timeout	0	0	TCPv4_TCP_Timeout	0	0	TCPv4_TCP_Timeout	0
Layer3 (Packet Sent and Received)				Layer3 (Packet Sent and Received)			
	Second	Total		Second	Total		Second
Tx	0	44,797,222	Tx	0	87,465,766	Rx	0
Rx	0	85,689,204	Rx	0	32,614,176	Unicast_Tx	0
Unicast_Tx	0	44,797,222	Unicast_Tx	0	87,465,766	Unicast_Rx	0
Unicast_Rx	0	85,689,204	Unicast_Rx	0	32,614,176	Multicast_Tx	0
Multicast_Tx	0	0	Multicast_Tx	0	0	Multicast_Rx	0
Multicast_Rx	0	0	Multicast_Rx	0	0	Broadcast_Tx	0
Broadcast_Tx	0	0	Broadcast_Tx	0	0		



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.