Nutanix Administration Guide

FortiAnalyzer 7.2

January 29, 2024
FortiAnalyzer 7.2 Nutanix Administration Guide
05-700-704277-20200409

TABLE OF CONTENTS

About FortiAnalyzer for Nutanix

Fortinet FortiAnalyzer securely aggregates log data from physical and virtual Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customized reports, you can filter and review records, including traffic, event, virus, attack, web content, and email data, mining the data to determine your security stance and assure regulatory compliance.

Highlights of FortiAnalyzer for Nutanix include the following:

- Predefined and customized charts help monitor, maintain, and identify attack patterns, acceptable use policies, and demonstrate policy compliance
- Scalable architecture allows the device to run in collector or analyzer modes for optimized log processing
- Advanced features such as event correlation, forensic analysis, and vulnerability assessment provide essential tools for in-depth protection of complex networks

FortiAnalyzer is one of several versatile Fortinet network security management products that provide diverse deployment types, growth flexibility, advanced customization through APIs, and simple licensing, all through central management and configuration.

Instance type support

You can deploy FortiAnalyzer for Nutanix as VM instances. Supported machine types may change without notice.

Region support

FortiAnalyzer-VM is available for purchase in all the regions/datacenters the Nutanix global marketplace covers. Available regions are:

- Hong Kong
- Asia Pacific SE 1 (Singapore)
- US East 1 (Virginia)
- Asia Pacific NE 1 (Tokyo)
- US West 1 (Silicon Valley)
- EU Central 1 (Frankfurt)
- Middle East 1 (Dubai)
- Asia Pacific SE 2 (Sydney)
- Asia Pacific SE 3 (Kuala Lumpur)
- Asia Pacific SOU 1 (Mumbai)
- Asia Pacific SE 5 (Jakarta)
- North China 1
- North China 2
- China North 3 (Zhangjiakou)

- China North 5 (Huhehaote)
- East China 1
- East China 2
- South China 1

Models

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

You can deploy FortiAnalyzer-VM using different CPU and RAM sizes and launch it on various private and public cloud platforms.

Registering and downloading licenses

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 Fortinet 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. 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.
3. 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.

Minimum system requirements

FortiAnalyzer-VM has a minimum requirement of 4 CPU, 8 GB of RAM, and 500 GB of disk storage. For v7.2.2 and later, the minimum requirement for RAM is increased to 16 GB.

The following table lists the minimum system requirements for your VM hardware, based on your VM's analytic sustained rate.

Analytic sustained rate (logs/sec)	VM hardware requirements		
	RAM (GB)	CPU cores	IOPS
3000	16	4	300
4000	16	4	400
5000	16	4	500
6000	16	8	600
7000	16	8	700
8000	16	8	800
9000	16	8	900
10000	16	8	1000
20000	32	16	2000
30000	32	16	3000
40000	64	32	4000
50000	64	32	5000

You can calculate the collector sustained rate by multiplying the analytic sustained rate by 1.5.

This table does not take into account other hardware specifications, such as bus speed, CPU model, or storage type.

Deploying FortiAnalyzer on Nutanix

This section describes how to deploy FortiAnalyzer on Nutanix. It includes the following steps:

1. Obtaining the deployment image on page 7
2. Uploading the FortiAnalyzer deployment image to Nutanix on page 7
3. Creating the FortiAnalyzer deployment image on page 8
4. Connecting to the FortiAnalyzer-VM on page 10
5. Configuring the second NIC on page 11

Obtaining the deployment image

You can find the FortiAnalyzer-VM deployment packages on the Customer Service & Support site.

To obtain the deployment image:

1. Log in to the Customer Service & Support site.
2. From the *Download* dropdown list, select *VM Images* to access the available VM deployment packages.
3. From the *Select Product* dropdown list, select *Other*.
4. Click *to download other firmware images, please click here.* You are redirected to the download page for Firmware Images.
5. In the *Select Product* list, select *FortiAnalyzer*.
6. Click the *Download* tab, and navigate to the latest build.
7. Download the following deployment package file by clicking the *HTTPS* link in the corresponding row: *FAZ_KVM-v6-buildxxxx-FORTINET.out.kvm.zip*
8. Extract the package file, which contains the file *image.out.qcow2*.

Uploading the FortiAnalyzer deployment image to Nutanix

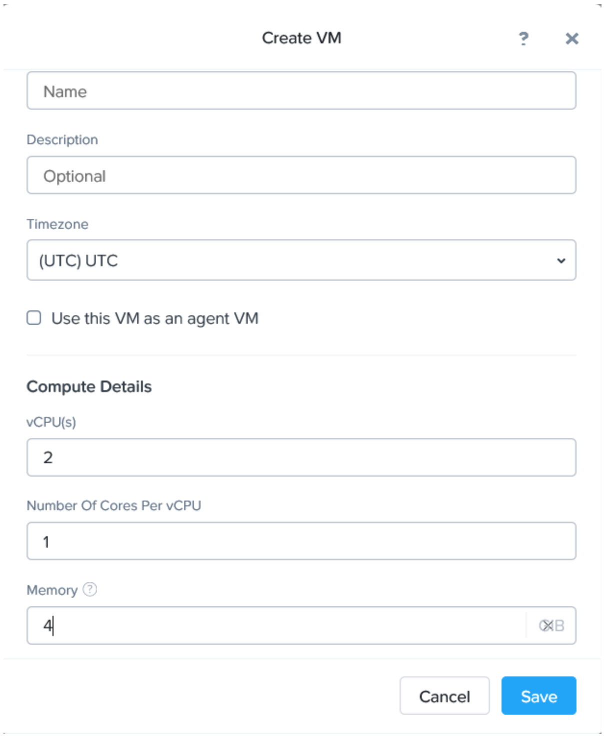
To upload the FortiAnalyzer deployment image to Nutanix:

1. Launch the Prism Element web console.
2. Go to *Settings* > *Image Configuration*.
3. Upload the FortiAnalyzer image by clicking *Upload Image*.
4. In the *Name* field, enter *FortiAnalyzer*.
5. In the *Image Type* dropdown list, ensure *Disk* is selected.
6. In the *Image Source* window, click *Upload a file*.
7. Select the `image.out.qcow2` image file downloaded in Obtaining the deployment image on page 7.
8. Click *Save*.
9. Wait a few minutes and you will find the newly created VM image in the list. Confirm that its state is active.

Creating the FortiAnalyzer deployment image

To create the FortiAnalyzer deployment image:

1. In the Prism Element web console, go to *VM > Create VM*.
2. For *General Configuration* and *Compute Details*, enter the following configuration information:
   - a. In the *NAME* field, enter a name for your VM, for example, FortiAnalyzer-VM.
   - b. In the *VCPU(S)* field, enter 2.
   - c. In the *MEMORY* field, enter 4.



Create VM

Name

Description

Optional

Timezone

(UTC) UTC

□ Use this VM as an agent VM

Compute Details

vCPU(s)

2

Number Of Cores Per vCPU

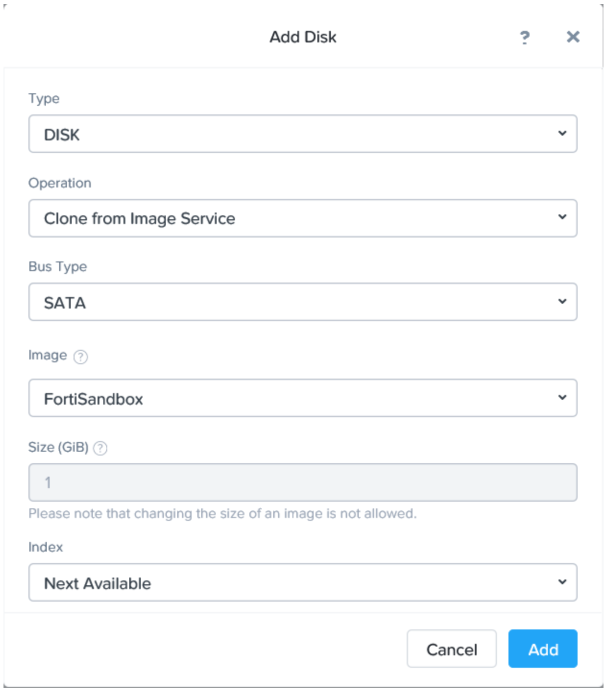
1

Memory

4

3. By default, a *CD-ROM* is listed under *Disks*. Delete the CD-ROM.
   You must create a boot disk and a data disk for the VM.
4. Create the boot disk:
   - a. Click *Add New Disk*.
   - b. The boot disk will be cloned from the VM image that you uploaded. Under *OPERATION*, select *Clone from Image Service*.
   - c. Under *BUS TYPE*, select *SATA*.
   - d. Under *IMAGE*, select the FortiAnalyzer disk image.

e. Click *Add*. The boot disk has been added.



Add Disk

Type: DISK

Operation: Clone from Image Service

Bus Type: SATA

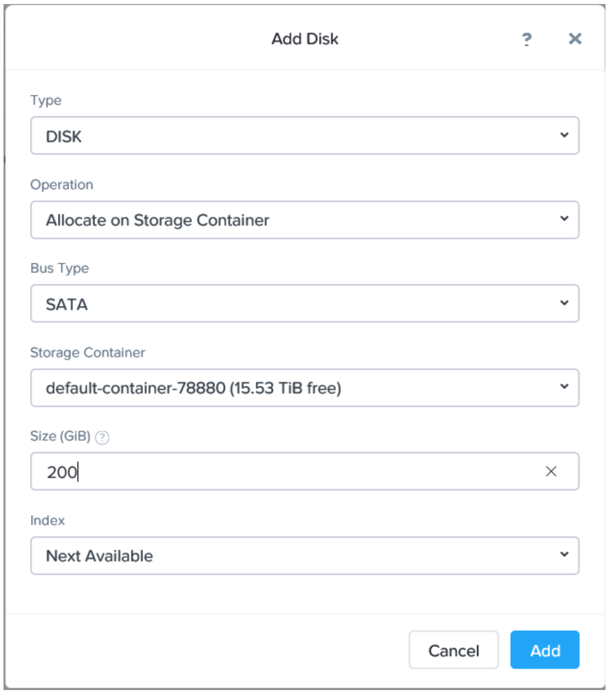
Image: FortiSandbox

Size (GiB): 1

Please note that changing the size of an image is not allowed.

Index: Next Available

5. Create the data disk by first Clicking *Add New Disk*.
   a. Under *OPERATION*, select *Allocate on Storage Container*.
   b. Under *BUS TYPE*, select *SATA*.
   c. Under *SIZE (GB)*, enter 200.
   d. Click *Add*. The data disk has been added.



Add Disk

Type: DISK

Operation: Allocate on Storage Container

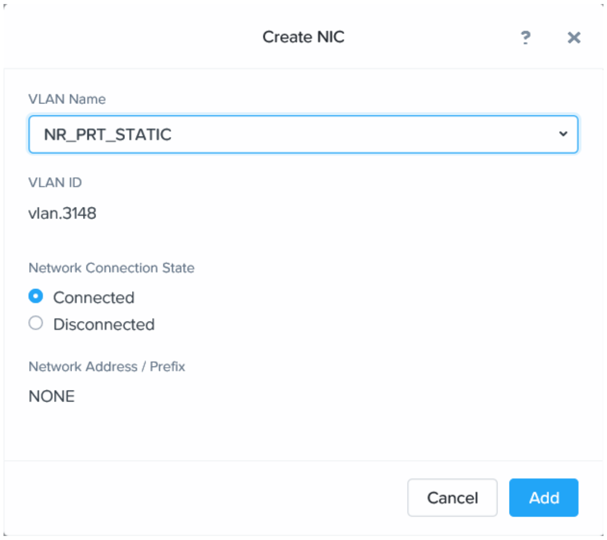
Bus Type: SATA

Storage Container: default-container-78880 (15.53 TiB free)

Size (GiB): 200

Index: Next Available

6. Add a network interface for the VM.
   a. Under *Network Adapters (NIC)*, click *Add New NIC*.
   b. Under *VLAN NAME*, select *NR_PRT_STATIC*.



VLAN Name

NR_PRT_STATIC

VLAN ID

vlan.3148

Network Connection State

● Connected

○ Disconnected

Network Address / Prefix

NONE

   c. Click *Add*.
7. Click *Save*.
   The system displays a *Successfully submitted Create operation* message when the VM has been created successfully with no error.

The FortiAnalyzer-VM requires at least two virtual hard disks. Before powering on the FortiAnalyzer-VM, you must add at least one more virtual hard disk (ideally above 500 GB).

The VM should therefore be configured with the following disks:

- The default hard drive that contains the OS and **should not** be modified.
- One or more additional disks, for example *Disk1* and Disk2, used by LVM for logs, reports, swap, and other storage requirements.

The default virtual hard disk storage size should not be modified to increase capacity, only increasing *Disk1* or adding extra disks will extend LVM disk on the FortiAnalyzer-VM.

Connecting to the FortiAnalyzer-VM

To connect to the FortiAnalyzer-VM:

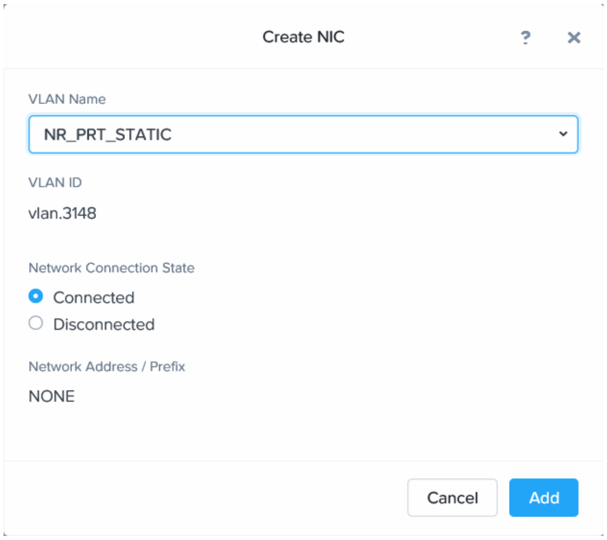
1. In the Prism Element web console, go to *VM*.
2. Click the newly created FortiAnalyzer-VM. By default, the FortiAnalyzer-VM is shut down after initial creation.
3. Click *Power On* to power on the VM.
4. Click the *Launch Console* tab to ensure that the VM boots up successfully. Once booting is completes, the console prompts for login credentials. Log in to FortiAnalyzer, using the username *admin* and no password.
5. Configure the interface port1 IP address by using the CLI command `config system interface` with the IP address set in Registering and Downloading Your License.
6. Access FortiAnalyzer in your browser.
7. Log in to FortiAnalyzer-VM with the username `admin` and no password.

8. After logging in successfully, upload your license (.lic) file to activate the FortiAnalyzer-VM. FortiAnalyzer-VM automatically restarts. After it restarts, wait about 30 minutes, until the license is fully registered at Fortinet, and then log in again.
9. Go to *System Settings* > *Network* > *All Interfaces* to check the network interface setting. The assigned IP address displays and is configurable.

Configuring the second NIC

To configure the second NIC:

1. In the Prism Element web console, go to *VM*.
2. Select the FortiAnalyzer-VM instance.
3. Click *Update*.
4. Under *Network Adapters (NIC)*, click *Add New NIC*.
5. From the *VLAN NAME* dropdown list, select *NR_PRT_STATIC*.



Create NIC

VLAN Name

NR_PRT_STATIC

VLAN ID

vlan.3148

Network Connection State

● Connected

○ Disconnected

Network Address / Prefix

NONE

6. Click *Add*.
7. Click *Save*.
8. In your browser, log in to the FortiAnalyzer-VM.
9. Go to *System Settings* > *Network* > *All Interfaces*. The second NIC has been added, with no need to reboot FortiAnalyzer.
10. Edit port2, and enter the IP address and netmask.
11. Configure the other elements as needed, then click *OK*.

Change log

Date	Change description
2022-04-11	Initial release.
2023-02-08	Added Minimum system requirements on page 6.
2024-01-29	Updated Creating the FortiAnalyzer deployment image on page 8.

www.fortinet.com