KVM Administration Guide

FortiAnalyzer 7.2.0

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

September 9, 2023
FortiAnalyzer 7.2.0 KVM Administration Guide
05-720-0794619-20240126

TABLE OF CONTENTS

Change log

Date	Change description
2022-04-11	Initial release.
2022-09-07	Updated Minimum system requirements on page 7.
2022-11-18	Updated Minimum system requirements on page 7.
2023-02-01	Updated About FortiAnalyzer on KVM on page 5.
2023-02-02	Updated Minimum system requirements on page 7 for the FortiAnalyzer 7.2.2 release.
2024-01-09	Updated information about extending the LVM.
2024-01-26	Updated note about virtual hard disk sizing when configuring hardware settings.

About FortiAnalyzer on KVM

This document provides information about deploying a FortiAnalyzer virtual appliance in Linux KVM server environments.

This includes how to configure the virtual appliance's virtual hardware settings. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuring and operating the virtual appliance after successfully installing and starting it. For that information, see the *FortiAnalyzer Administration Guide*.

Licensing

Fortinet offers the FortiAnalyzer-VM with a limited, free trial license. Stackable licenses can be purchased, letting you expand your VM solution as your environment expands. You can purchase perpetual or subscription-based licenses. Perpetual licenses never expire.

For information on purchasing a FortiAnalyzer-VM license, contact your Fortinet-authorized reseller, or visit How To Buy.

When configuring your FortiAnalyzer-VM, ensure that you configure hardware settings acording to the minimum system requirements and consider future expansion. Contact your Fortinet-authorized reseller for more information.

License	GB/day of logs
Trial License	1
VM-GB1	+1
VM-GB5	+5
VM-GB25	+25
VM-GB100	+100
VM-GB500	+500
VM-GB2000	+2000

See Minimum system requirements on page 7.

See also the FortiAnalyzer product datasheet.

Trial license

With a FortiCare account, FortiAnalyzer-VM includes a free limited non-expiring trial license.

The free trial license includes support for 3 ADOMs and 1 GB/day of logs.

The free trial license does not include services or support.

You can activate the trial license when you connect to the GUI for the FortiAnalyzer-VM. Full-feature products and services are available for purchase with an add-on license. See Connecting to the GUI and enabling a trial license on page 14.

Add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Minimum system requirements
- Deployment package for Linux KVM on page 8
- Downloading a deployment package

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.

Deployment package for Linux KVM

FortiAnalyzer deployment packages are included with firmware images on the Customer Service & Support site. The following table list the available VM deployment package.

VM Platform	Deployment File
Linux KVM RedHat 7.1	`FAZ_VM64_KVM-vX-buildxxxx-FORTINET.out.kvm.zip`

The `.out.kvm.zip` file contains:

- `FAZ.qcow2`: TheFortiAnalyzer system hard disk in QCOW2 format.
  The log disk and virtual hardware settings have to be configured manually.

For more information FortiAnalyzer, see the FortiAnalyzer datasheet.

Downloading a deployment package

Firmware image FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention. Each firmware image is specific to the device model. For example, the `FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` image, found in the 5.6.0 directory, is specific to the 64-bit Microsoft Hyper-V Server virtualization environment.

You can download the *FortiAnalyzer Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the *FortiAnalyzer* > *Download* tab.

Download the `.out` file to upgrade your existing FortiAnalyzer installation.

To download deployment packages:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select *Download* > *Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiManager* from the *Select Product* dropdown list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on your management computer.

Deployment

Prior to deploying the FortiAnalyzer, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiAnalyzer presume that you are familiar with the management software and terminology of your VM platform.

You might also need to refer to the documentation provided with your VM server. The deployment information in this guide is provided as an example because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiAnalyzer appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiAnalyzer, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiAnalyzer GUI (see Enabling GUI access on page 13).

If the FortiAnalyzerdoes not have a valid Logical Volume Management (LVM) configuration, the LVM service will not start automatically upon boot-up when the disk already contains data. To manually enable the service, use the `execute lvm start` CLI command.

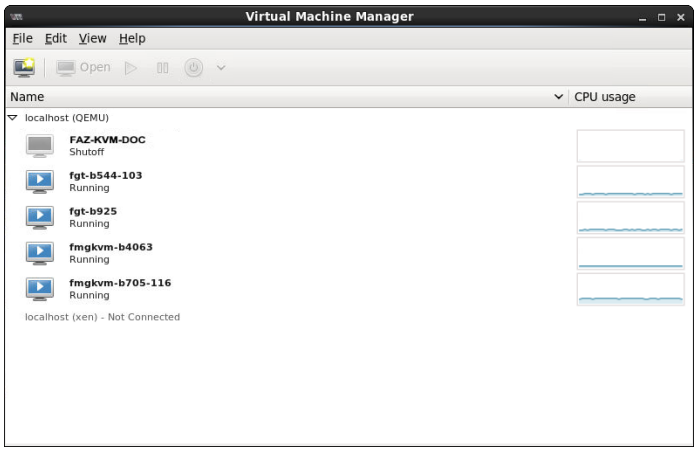
Deploying FortiAnalyzer on KVM

After you download the `FAZ_VM64_KVM-vX-buildxxxx-FORTINET.out.kvm.zip` file and extract the virtual hard drive image file, you can create the VM in your KVM environment.

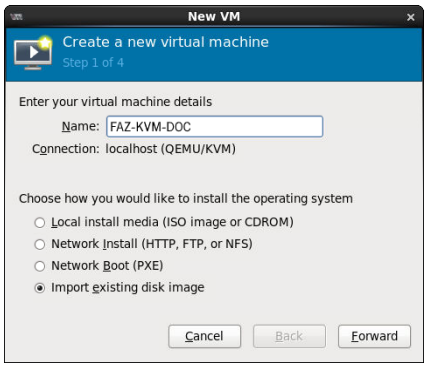
Creating the virtual machine

To create the virtual machine:

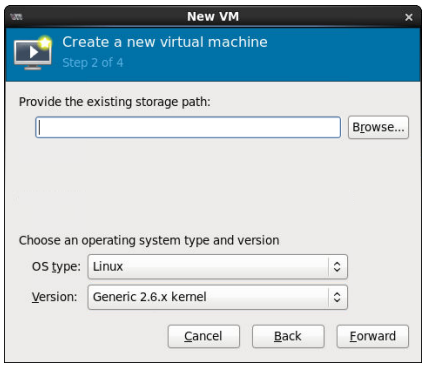
1. Launch Virtual Machine Manager (virt-manager) on you KVM host server. The *Virtual Machine Manager* homepage opens.



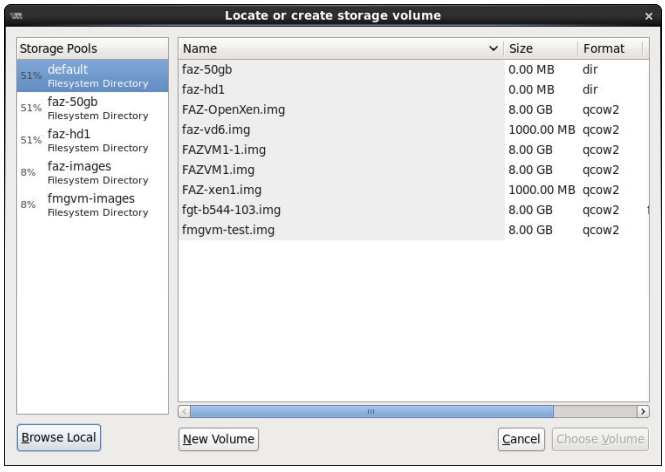
2. On the toolbar, click *Create a new virtual machine*.



3. Configure the VM:
   a. Enter the VM name, such as *FAZ-KVM-DOC*.
   b. Ensure that *Connection* is *localhost*, select *Import existing disk image*, then click *Forward* to continue.

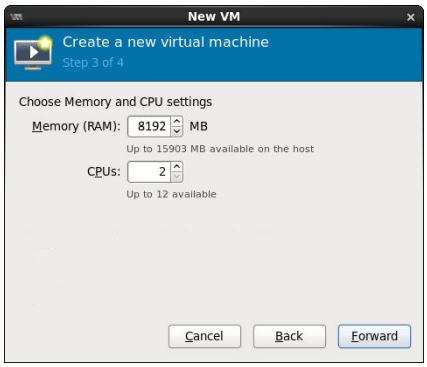


   c. From the *OS type* dropdown list, select *Linux*.
   d. From the *Version* dropdown list, select *Generic 2.6.x kernel*. You may have to first select *Show all OS options*.
   e. Click *Browse* to locate the storage volume.



   f. If you copied the *faz.qcow2* file to `/var/lib/libvirt/images` it shows on the right. If you saved it elsewhere on the server, click *Browse Local* to find it.

g. Once the file has been located, click *Choose Volume*, then click *Forward*.



h. Specify the amount of memory and the number of CPUs to allocate to this VM, then select *Forward*. To determine your required memory, see Minimum system requirements on page 7.

i. Expand the *Advanced options* section. By default, a new VM includes one network adapter. Select a network adapter on the host computer.
Optionally, set a specific MAC address for the virtual network interface.

j. Set *Virt Type* to *virtio* and set *Architecture* to *qcow2*.

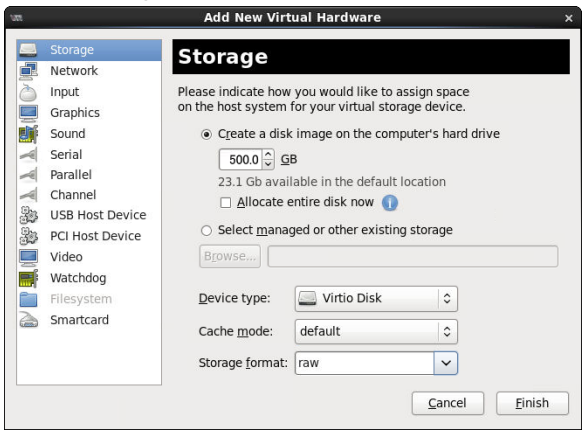
4. Click *Finish* to create the VM.

Configuring hardware settings

Before powering on your FortiAnalyzer-VM, you must configure virtual disks and at least four network interfaces.

To configure settings on the server:

1. In the Virtual Machine Manager, locate the VM name, then click *Open* on the toolbar.
2. In the Virtual Machine window, select *Show virtual hardware details*.
3. Click *Add Hardware* to open the *Add Hardware* window
4. Select *Storage*.



5. Select *Create a disk image on the computer's harddrive*, and set the size.

If you know your environment will expand in the future, or if you will be using ADOMs, add hard disks larger than 500 GB. This allows your environment to expand as required while not taking up more space than is needed. See Licensing on page 5 for more information.

The FortiAnalyzer-VM allows you to add twelve virtual log disks to a deployed instance. When adding additional hard disks, use the following CLI command to extend the LVM logical volume:

```
execute lvm extend
```

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.

6. Enter the following information:

Device Type	Virtio disk
Cache mode	writethrough
Storage format	raw

7. Select *Network* to add more network interfaces. The *Device Model* must be *Virtio*.

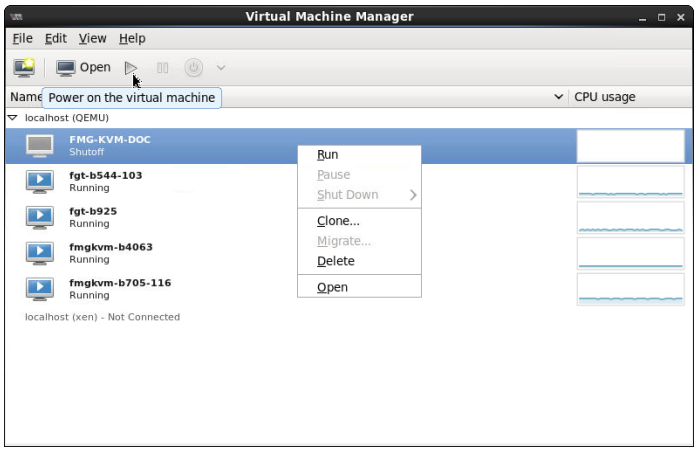
A new VM includes one network adapter by default. You can add more through the *Add Hardware* window. FortiAnalyzer-VM supports up to four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

8. Click *Finish*.

Starting the VM

You can now proceed to power on your FortiAnalyzer-VM.

1. Do one of the following:
   a. Right-click the FortiAnalyzer-VM and select *Run*.
   b. Select the FortiAnalyzer-VM from the list of VMs, then click *Power on the virtual machine* from the toolbar.



After the VM starts, proceed with the initial configuration. See Configuring initial settings on page 13.

Configuring initial settings

Before you can connect to the FortiAnalyzer-VM, you must configure basic network settings via the CLI console. Once configured, you can connect to the FortiAnalyzer GUI.

Enabling GUI access

To enable GUI access to the FortiAnalyzer, you must configure the IP address and network mask of the appropriate port on the FortiAnalyzer. The following instructions use port 1.

You can determine the appropriate by matching the network adapter's MAC address and the `HWaddr` that the CLI command `diagnose fmnetwork interface list` provides.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiAnalyzer and access the console window. You might need to press *Enter* to see the login prompt.
2. At the FortiAnalyzer login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

```
config system interface
   edit port1
      set ip <IP address> <netmask>
end
```

The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor VM settings.

4. To configure the default gateway, enter the following commands:

```
config system route
   edit 1
      set device port1
      set gateway <gateway_ipv4_address>
end
```

The Customer Service & Support portal does not currently support IPv6 for FortiAnalyzer license validation. You must specify an IPv4 address in the support portal and the port management interface.

Connecting to the GUI and enabling a trial license

Once you have configured a port's IP address and network mask, you can connect to the GUI by using a web browser.

To connect to the GUI and enable a trial license:

1. Launch a web browser, and enter the IP address you configured for the port management interface.
2. At the login page, select *Free Trial*, and click *Login with FortiCloud* to start the process of activating your free trial license.
   If you do not have a FortiCloud account, click *Register with FortiCloud* to create one.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Upgrading to an add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also the FortiAnalyzer VM Trial License Guide on the Document Library.

Configuring your FortiAnalyzer

Once the FortiAnalyzer license has been validated, you can configure your device.

If the amount of memory or number of CPUs is too small for the VM, or if the allocated hard drive space is less than the licensed VM storage volume, warning messages show in the GUI in the *System Resources* widget on the dashboard and in the *Notification* list.

www.fortinet.com