FortiSIEM - KVM Installation Guide

Version 5.2.8

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

02/04/2020
FortiSIEM 5.2.8 KVM Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
09/05/2018	Initial version of FortiSIEM - KVM Installation Guide.
03/29/2019	Revision 1: updated instructions for registering on a Supervisor node.
04/08/2019	Revision 2: updated the names of the files imported to KVM.
11/05/2019	Revision 3: changed the names of the volumes in the FortiSIEM distribution.
11/21/2019	Release of FortiSIEM - KVM Installation Guide for 5.2.6.
02/04/2020	Release of FortiSIEM - KVM Installation Guide for 5.2.8.

Installing FortiSIEM in Linux KVM

This document provides instructions to install FortiSIEM on Linux KVM.

Pre-installation check-list

Step A: Determine your FortiSIEM hardware needs and deployment type

Before you begin, check the following:

1. Number of Workers needed, if any.
2. Number of Collectors needed, if any.
3. Hardware specification of Supervisor, Worker and Collectors (CPU, RAM, Local Storage)

If Elasticsearch is chosen as the Event Database, the Supervisor needs an additional 8 GB RAM - in this case, the minimum requirement of the Supervisor is 32 GB RAM.

4. Event Database Storage – Local or Remote (For Remote - NFS or Elasticsearch)
   Note: Remote option is required if you are deploying Workers. If you are going to add Workers in the future, then it is recommended to choose a Remote database option to avoid data migration.
5. Deployment type – Enterprise or Service Provider

Step B: Deploy Remote Storage

If required, install and configure NFS or Elasticsearch before beginning the installation below:

- *For NFS deployment, see here.*
- *For Elasticsearch deployment, see here.*

Installing FortiSIEM Virtual Appliance in KVM

The basic process for installing FortiSIEM Supervisor, Worker, or Collector node in KVM is the same as installing these nodes under VMware ESX. Since Worker nodes are only used in deployments that use NFS storage, you should first configure your Supervisor node to use NFS storage, and then configure your Worker node using the Supervisor NFS mount point as the mount point for the Worker. Collector nodes are only used in Service Provider deployments, and must be registered with a running Supervisor node.

Follow the steps below to install FortiSIEM Virtual Appliance in KVM:

Step 1: Setup a Network Bridge for Installing FortiSIEM in KVM

If FortiSIEM is the first guest on KVM, then a bridge network may be required to enable network connectivity. For details see the Red Hat documentation on KVM Bridge Configuration.

Step 2: Import the Supervisor, Worker or Collector into KVM

1. Go to the Fortinet Support website https://support.fortinet.com to download the KVM package. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Download and unzip the packages for Super/Worker and Collector to the location where you want to install the image.
   When you open the zip file `FSM_Full_Super-Worker_KVM_5.2.8_build1626.zip`, there will be three files for Supervisor/Worker:
   - `system.qcow2`
   - `cmdb.qcow2`
   - `svn.qcow2`

   and one file in the Collector zip file `FSM_Full_Collector_KVM_5.2.8_build1626.zip`:
   - `system.qcow2`
3. Start the KVM Virtual Machine Manager.
4. Select and right-click on a host to open the **Host Options** menu, and select **New**.
5. In the **New VM** dialog, enter a **Name** for your FortiSIEM node.
6. Select **Import existing disk image**, and click **Forward**.
7. **Browse** to the location and select `system.qcow2` for Supervisor/Worker or `system.qcow2` for the Collector.
8. Choose the **OS Type** and **Version** you want to use with this installation, and click **Forward**.
9. Allocate **Memory** and **CPUs** to the FortiSIEM node, and click **Forward**.
10. Select the checkbox for **Customize configuration before install**.
11. Confirm the installation configuration of your node, and click **Finish**.

Step 3: Configure the Supervisor Hardware Settings in KVM

1. In KVM Virtual Machine Manager, select the FortiSIEM Supervisor, and click **Open**.
2. Click the **Information** icon to view the Supervisor hardware settings.
3. Select the **Virtual Network Interface**.

4. For **Source Device**, select an available bridge network.
   See Setup a Network Bridge for Installing FortiSIEM in KVM for more information.
5. For **Device Model**, select **Virtio** and click **Apply**.
6. In the Supervisor **Hardware** settings, select **Virtual Disk**.
7. In the **Virtual Disk** dialog, open the **Advanced options**. For **Disk bus**, select **Virtio** and for **Storage format** select **qcow2**.
8. Click **Add Hardware**, and select **Storage**.
9. Select the **Select managed or other existing storage** option, and browse to select `cmdb.qcow2`.
10. Select the **Device type** as **Virtio Disk**, **Cache mode** as 'default' and **Storage format** as `qcow2`.
11. Add the disk `svn.qcow2` as above.
12. If the storage type is **Local**, add one more disk for EventDB using the option **Create a disk image on the computer's hardware** with **Device type** as **Virtio Disk**, **Cache mode** as **default** and **Storage format** as **qcow2**.

Step 4: Configure the Supervisor, Worker, or Collector from the VM Console

1. In the KVM Virtual Machine Manager, select the Supervisor node.
2. Right-click to open the **Virtual Appliance Options** menu, and select **Power > Power On**.
3. In the **Virtual Appliance Options** menu, select **Open Console**
   Network Failure Message: When the console starts up for the first time you may see a `Network eth0 Failed` message, but this is expected behavior.
4. In VM console, select **Set Timezone** and press **Enter**.
5. Select your **Location** and press **Enter**.
6. Select your **Country** and press **Enter**.
7. Select your **Timezone** and press **Enter**.
8. Review your Timezone information, select **1**, and press **Enter**.
9. When the **Configuration** screen reloads, select **Login**, and press **Enter**.
10. Enter the default login credentials:
    - Login: `root`
    - Password: `ProspectHills`
11. Run the `vami_config_net` script to configure the network:

    ```
    /opt/vmware/share/vami/vami_config_net
    ```

12. Based on your network type, enter one of the options below:
    - **1** for **IPv6 Network Only**
      - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
    - **2** for **IPv4 Network Only**
      - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
    - **3** for **Both Networks**
      i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
      ii. Follow Step 13 below to turn off the proxy server and continue with step c.

iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).

13. Enter **n**.
Note: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the KVM host.
14. Enter **y** to accept the network configuration settings.
15. Enter the **Host name,** and press **Enter**.
16. For Supervisor and Worker: You will be prompted to choose Supervisor [s] or Worker [w].
Choose accordingly:
    a. For Supervisor, the system will initialize the PostGreSQL database which will take around 40 minutes and then reboot the system. A few minutes after reboot, the system GUI will be ready to upload license and configure the Event Database Storage option.
    b. For a Worker node, the system will reboot quickly and a few minutes after reboot, it will be ready to be added as a Worker from the Supervisor GUI.
17. For Collector, the system will reboot and after a few minutes it will be ready.

Step 5: Upload the FortiSIEM License on Supervisor

You will now be asked to input a license.

1. Click **Browse** and upload the license file.
Make sure that the 'Hardware ID' shown in the **License Upload** page matches the license.
2. For **User ID** and **Password**, choose any 'Full Admin' credentials.
For the first time, install by choosing user as 'admin' and password as 'admin*1'
3. Choose **License type** as 'Enterprise' or 'Service Provider'.
This option is available only on first install. Once the database is configured, this option will not be available.

Step 6: Choose FortiSIEM Event Database Storage

For fresh installation, you will be taken to the Event Database Storage page. Based on Step B: Deploy Remote Storage, you will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options.

For more details, see here.

Step 7: (Optional) Install Workers and Add to Supervisor Node

1. Follow Step 4 to configure a Worker.
2. Add the Worker node to the Supervisor by visiting **ADMIN** > **License** > **Nodes** > **Add**.
3. See **ADMIN** > **Health** > **Cloud Health** to ensure that the Workers are up, healthy and properly added to the system.

Step 8: (Optional) Install Collectors

Collectors can be installed as Virtual Appliances or Hardware appliances (FSM-500F). Follow the steps from Step 1 to 9 in this section, but exclude Step 3.

Step 9: (Optional) Register Collectors to Supervisor Node

For Enterprise deployments, follow these steps:

1. Login to Supervisor with 'Admin' privileges.
2. Go to **ADMIN** > **Setup** > **Collectors** and add a Collector by entering:
   a. **Name** – Collector Name
   b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set 'Unlimited'.
3. SSH to the Collector and run following script to register Collectors:
   `phProvisionCollector --add <user> <password> <Super IP or Host> <Organization> <CollectorName>`
   a. Set **User** and **Password** use the admin User Name and password for the Supervisor
   b. Set **IP Address** as 'Supervisor IP'.
   c. Set **Organization** as 'Super'.
   d. Set **CollectorName** from Step 2a.
   The Collector will reboot during the Registration
4. Go to **ADMIN** > **Health** > **Collector Health** and see the status.

Installing FortiSIEM Report Server on KVM

Follow the steps below to install the FortiSIEM Report Server on KVM:

Step 1: Import the Report Server Image into KVM

1. Go to the Fortinet Support website https://support.fortinet.com to download the KVM package. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Download and unzip the packages for Report Server to the location where you want to install the image.
   There are two files in the `FSM_Full_ReportServer_KVM_5.2.8_build1626.zip` file:
   - `system.qcow2`
   - `cmdb.qcow2`
3. Start the KVM Virtual Machine Manager.
4. Select and right-click on a host to open the **Host Options** menu, and select **New**.
5. In the **New VM** dialog, enter a **Name** for your FortiSIEM node.
6. Select **Import existing disk image**, and click **Forward**.
7. **Browse** to the location of `system.qcow2` and select it.
8. Choose the **OS Type** and **Version** you want to use with this installation, and click **Forward**.
9. Allocate the **Memory** and **CPUs** to the FortiSIEM node, and click **Forward**.
10. Select the checkbox for **Customize configuration before install**.
11. Confirm the installation configuration of your node, and click **Finish**.

Step 2: Configure the Report Server Hardware Settings in KVM

1. In KVM Virtual Machine Manager, select the FortiSIEM Supervisor, and click **Open**.
2. Click the **Information** icon to view the Supervisor hardware settings.
3. Select the **Virtual Network Interface**.
4. For **Source Device**, select an available bridge network.
   See Setup a Network Bridge for Installing FortiSIEM in KVM for more information.
5. For **Device Model**, select **Virtio** and click **Apply**.
6. In the Report Server **Hardware** settings, select **Virtual Disk**.
7. In the **Virtual Disk** dialog, open the **Advanced options**, and for **Disk bus**, select **Virtio** and for storage format select 'qcow2'.
8. Click **Add Hardware**, and select **Storage**.
9. Select the **Select managed or other existing storage** option, and browse to `cmdb.qcow2`.
10. Select the **Device type** as 'Virtio Disk', **Cache mode** as 'default' and **Storage format** as 'qcow2'.
11. If the storage type is 'Local', add one more disk for EventDB using the option **Create a disk image on the computer's hardware** with **Device type** as 'Virtio Disk', **Cache mode** as 'default' and **Storage format** as 'qcow2'. Use the command `fdisk -l` to get the disk name.

Step 3: Configure the Report Server from the VM Console

1. In the KVM Virtual Machine Manager, select the Report Server node.
2. Right-click to open the **Virtual Appliance Options** menu, and select **Power > Power On**.
3. In the **Virtual Appliance Options** menu, select **Open Console**
   Network Failure Message: When the console starts up for the first time you may see a `Network eth0 Failed` message, but this is expected behavior.
4. In VM console, select **Set Timezone** and press **Enter**.
5. Select your **Location** and press **Enter**.
6. Select your **Country** and press **Enter**.
7. Select your **Timezone** and press **Enter**.
8. Review your Timezone information, select **1**, and press **Enter**.
9. When the **Configuration** screen reloads, select **Login**, and press **Enter**.
10. Enter the default login credentials:
    - Login: `root`
    - Password: `ProspectHills`
11. Run the `vami_config_net` script to configure the network.

    ```
    /opt/vmware/share/vami/vami_config_net
    ```

12. Based on your network type, enter one of the options below:
    - **1** for **IPv6 Network Only**
      - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
    - **2** for **IPv4 Network Only**
      - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
    - **3** for **Both Networks**
      i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
      ii. Follow Step 13 below to turn off the proxy server and continue with step c.
      iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).
13. Enter **n**. **Note**: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the KVM host.
14. Press **y** to accept the network configuration settings.
15. Enter the **Host name**, and then press **Enter**.
16. Enter the mount point for your data. Set one of the following:
    - 'Local' (`/dev/<disk_name>`).
      Use the `disk_name` from Step 2 - 11.
    - 'NFS' storage mount point
      Note: Do not use the same mount point as EventDB on Supervisor. This should be a different mount point/storage path.

    After you set the mount point, the Report Server will automatically reboot, and in 10 to 15 minutes the Report Server will be successfully configured.

Step 4: Register FortiSIEM Report Server to Supervisor

1. Log in to your Supervisor node.
2. Open the 'License Management' page on:
   - Flash GUI: Go to **Admin** > **License Management**. Under 'Report Server Information', click **Add**.
   - HTML5 GUI: Go to **ADMIN** > **License** > **Nodes** tab. Click **Add** and select '**Report Server**' from the **Type** drop-down.
3. Enter the **Report Server IP Address**, **Database Username** and **Database Password** of the Report Server you want to use to administer.
   Use the same credentials to set up the Visual Analytics Server for reading data from the Report Server.
4. Click **Run in Background** if you want Report Server registration to run in the background for larger installations. When CMDB size is below 1 GB, registration takes approximately three minutes to complete.
5. When the registration is complete, click **OK** in the confirmation dialog.
6. Make sure the Report Server is up and running by navigating to:
   - Flash GUI: **Admin** > **Cloud Health**
   - HTML5 GUI: **ADMIN** > **Health** > **Cloud Health**

Step 5: Sync Reports from FortiSIEM Supervisor to Report Server

1. Log in to your Supervisor node.
2. Select **Synced Reports** from:
   - Flash GUI: **RESOURCE > Reports** > **Synced Reports**
   - HTML5 GUI: **RESOURCES** > **Reports** > **Synced Reports**
3. Select a Report.
   Currently, only reports that contain a 'Group By' condition can be synced. Both system and user-created reports can be synched as long as it contains a 'Group By' condition.
4. Select **Sync**.
   When the sync process initiates, the Supervisor node dynamically creates a table within the Report Server reportdb database. When the sync is established, it will run every five minutes, and the last five minutes of data in the synced report will be pushed to the corresponding table. This lets you run Visual Analytics on event data stored in the Report Server reportdb database.