KVM Installation Guide

FortiSIEM 6.7.2

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

FORTINET TRAINING 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

10/03/2023
FortiSIEM 6.7.2 KVM Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
09/05/2018	Initial version of FortiSIEM - KVM Installation Guide.
03/29/2019	Updated instructions for registering on a Supervisor node.
04/08/2019	Updated the names of the files imported to KVM.
11/05/2019	Changed the names of the volumes in the FortiSIEM distribution.
11/21/2019	Release of FortiSIEM - KVM Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM - KVM Installation Guide for 5.3.0.
08/15/2020	Release of FortiSIEM - KVM Installation and Migration Guide for 6.1.0.
12/07/2020	Small addition to Register Collectors.
02/04/2021	Migration update.
03/18/2021	Minor update to Pre-Migration for 6.1.1.
03/23/2021	Release of FortiSIEM - KVM Installation Guide for 6.2.0.
04/22/2021	Added Install Log section.
05/06/2021	Release of FortiSIEM - KVM Installation Guide for 6.2.1.
06/07/2021	Updated Elasticsearch screenshot for 6.2.x guides.
07/06/2021	Release of FortiSIEM - KVM Installation Guide for 6.3.0.
08/26/2021	Release of FortiSIEM - KVM Installation Guide for 6.3.1.
10/15/2021	Release of FortiSIEM - KVM Installation Guide for 6.3.2.
11/17/2021	Updated Register Collectors instructions for 6.x guides.
12/22/2021	Release of FortiSIEM - KVM Installation Guide for 6.3.3.
01/18/2022	Release of FortiSIEM - KVM Installation Guide for 6.4.0.
05/09/2022	Release of FortiSIEM - KVM Installation Guide for 6.5.0.
07/26/2022	Release of FortiSIEM - KVM Installation Guide for 6.6.0.
08/18/2022	Updated All-in-one Installation section.
09/12/2022	Release of FortiSIEM - KVM Installation Guide for 6.5.1.
09/14/2022	Release of FortiSIEM - KVM Installation Guide for 6.6.1.
09/19/2022	Release of FortiSIEM - KVM Installation Guide for 6.6.2.

Date	Change Description
10/20/2022	Updated Register Collectors instructions for 6.x guides.
01/03/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.0.
02/13/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.1.
02/24/2023	Pre-Installation Checklist, Choose an Event Database, Install Supervisor, Install Workers and Register Workers sections updated for 6.7.x Guides. Added Create ClickHouse Topology (Optional) and Final Check sections to 6.7.x Guides.
03/07/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.2.
03/28/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.3.
04/11/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.4.
05/22/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.5.
06/16/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.6.
07/13/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.7.
09/12/2023	Release of FortiSIEM - KVM Installation Guide for 6.7.8.

Fresh Installation

Pre-Installation Checklist

Before you begin, check the following:

- Ensure that your system can connect to the network. You will be asked to provide a DNS Server and a host that can be resolved by the DNS Server and responds to ping. The host can either be an internal host or a public domain host like google.com.
- Choose deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Determine whether FIPS should be enabled
- Choose install type:
  - All-in-one with FortiSIEM Manager
  - All-in-one with Supervisor only, or
  - Cluster with Supervisor and Workers
- Choose storage type for Supervisor, Worker, and/or Collector
  - Online storage - There are 4 choices
    - ClickHouse - Recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
    - EventDB on local disk
    - EventDB on NFS
    - Elasticsearch
  - Archive storage – There are 2 choices
    - EventDB on NFS
    - HDFS
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Manager	Minimum – 16 Recommended - 32	Minimum • 24GB Recommended • 32GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB	OS – 25GB OPT – 100GB CMDB – 60GB

Node	vCPU	RAM	Local Disks
		Recommended • without UEBA – 32GB • with UEBA - 64GB	SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended – 24GB	OS – 25GB OPT – 100GB
Collector	Minimum – 4 Recommended – 8 (based on load)	Minimum – 4GB Recommended – 8GB	OS – 25GB OPT – 100GB

- If your Online event database is external (e.g. EventDB on NFS or Elasticsearch), then you must configure external storage before proceeding to FortiSIEM deployment.
  - For NFS deployment, see here.
  - For Elasticsearch deployment, see here.
- If your Online event database is internal, that is, inside Supervisor or Worker nodes, then you need to determine the size of the disks based on your EPS and event retention needs.
  - For EventDB on local disk, see here.
  - For ClickHouse, see here.
- For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

All-in-one Installation

This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

- Import FortiSIEM into KVM
- Configure FortiSIEM
- Upload the FortiSIEM License
- Configure an Event Database
- Final Check

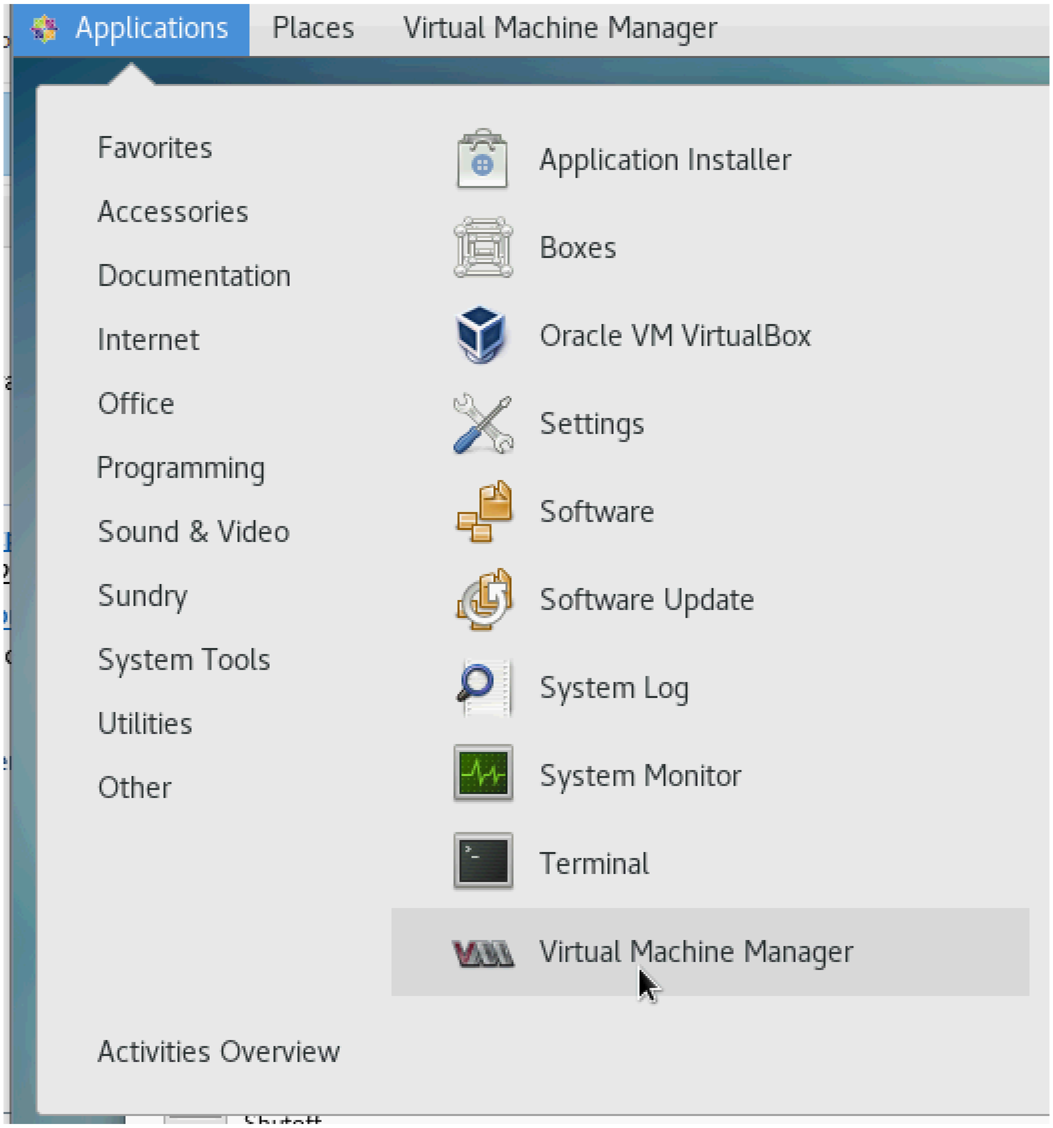
Import FortiSIEM into KVM

1. Go to the Fortinet Support website https://support.fortinet.com to download the KVM package `FSM_Full_All_KVM_6.7.2_build1727.zip`. See Downloading FortiSIEM Products for more information on downloading products from the support website.

2. Download the packages for Super/Worker and Collector to the location where you want to install the image. For example: `FSM_Full_All_KVM_6.7.2_build1727.zip`.
3. Unzip the `.zip` file to get the `FortiSIEM-6.7.2.1727.qcow2` file.
4. Copy the above unzipped `qcow2` file into the storage image location separately for the installation of super, worker, and collector. For example:

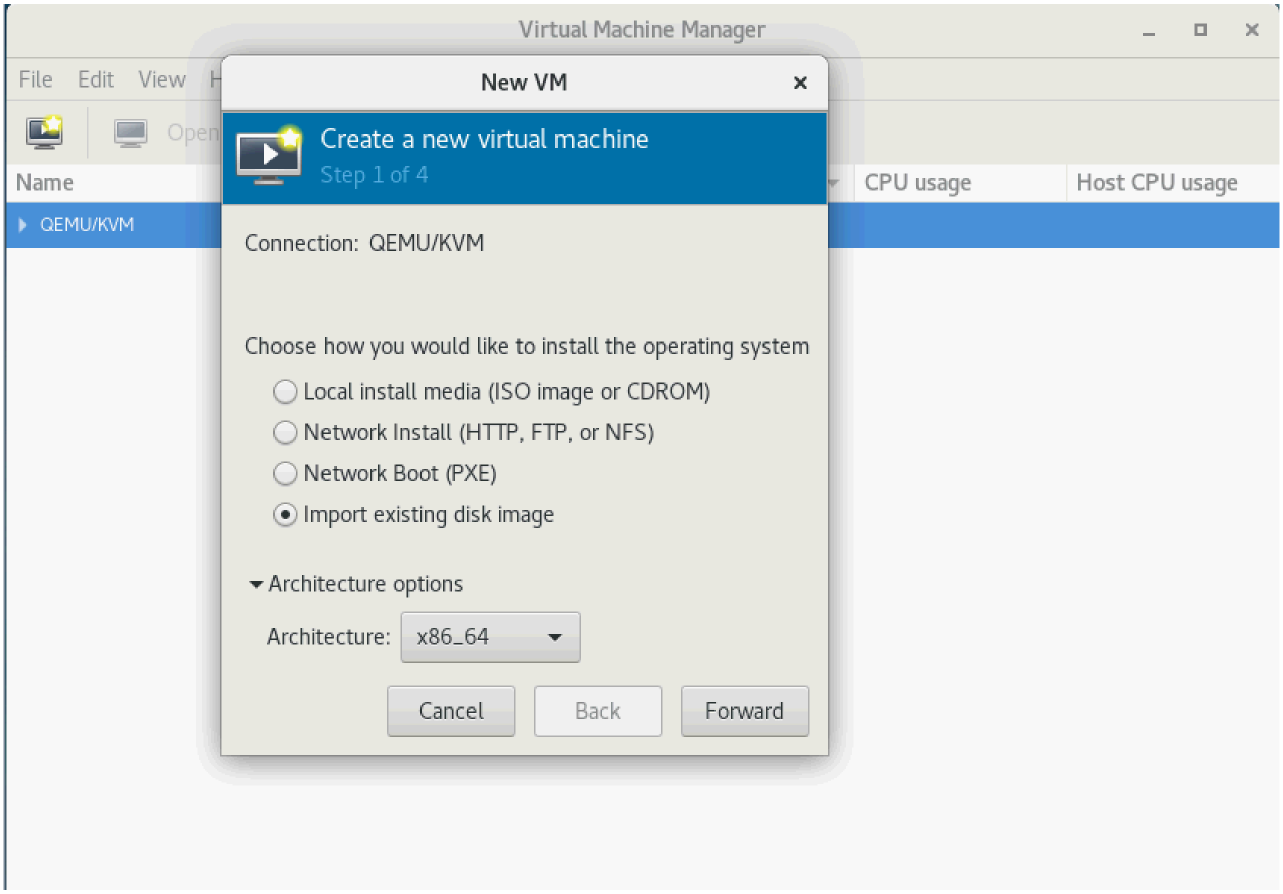
```
/var/lib/libvirt/images/super/FortiSIEM-6.7.2.1727.qcow2
/var/lib/libvirt/images/worker/FortiSIEM-6.7.2.1727.qcow2
/var/lib/libvirt/images/collector/FortiSIEM-6.7.2.1727.qcow2
```

5. Start the KVM Manager for the KVM server by clicking **Virtual Machine Manager**.



6. Click **Create a new virtual machine** from the **Virtual Machine Manager**.

7. Select **Import existing disk image** (Architecture defaults to x86_64).



Connection: QEMU/KVM

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)

○ Network Install (HTTP, FTP, or NFS)

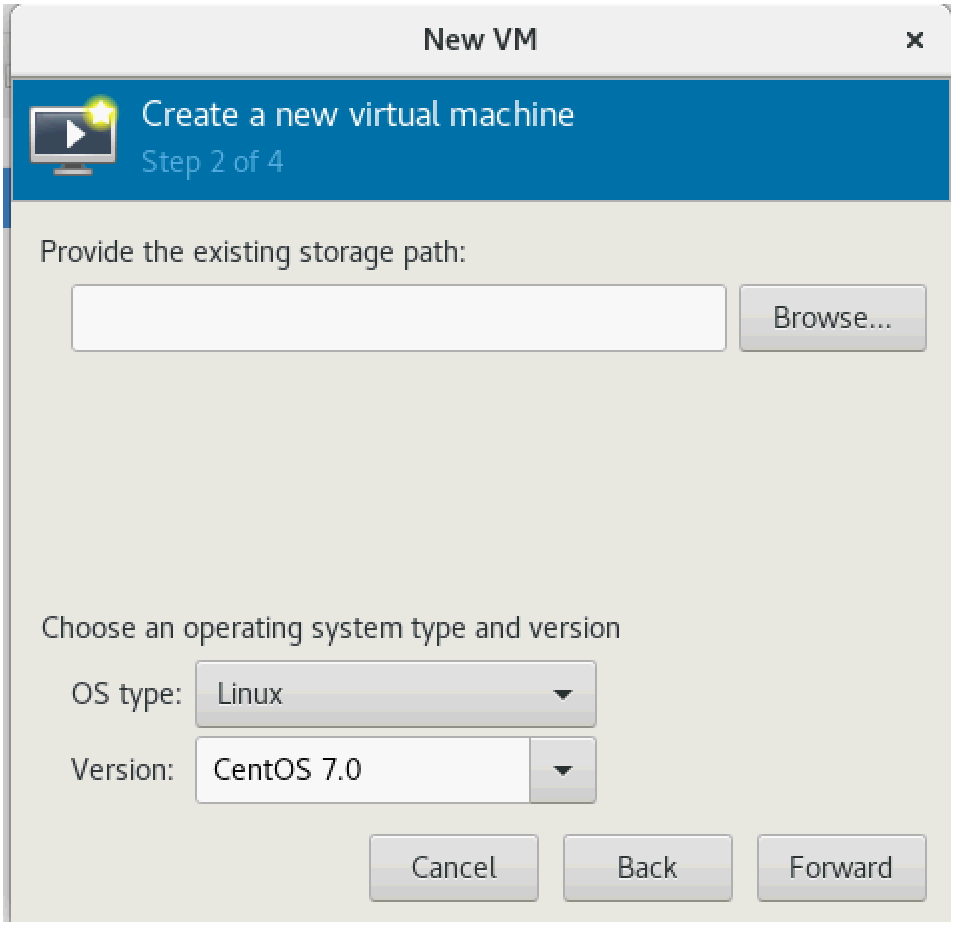
○ Network Boot (PXE)

● Import existing disk image

Architecture options

Architecture: x86_64

8. Click **Forward** from the above step, and select the OS type as **Linux** and Verision to **CentOS 7.0**, then click **Forward**.



New VM

Create a new virtual machine

Step 2 of 4

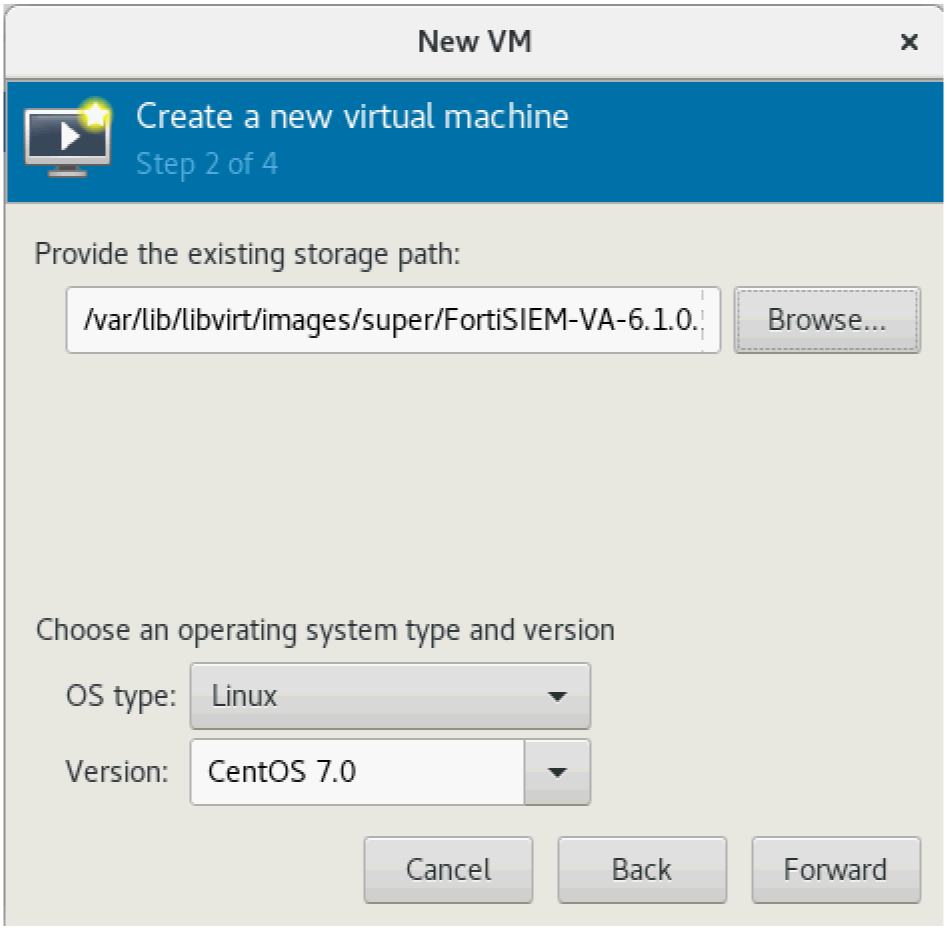
Provide the existing storage path:

Choose an operating system type and version

OS type: Linux

Version: CentOS 7.0

9. Click **Browse...** from the **New VM** dialog box to find the location for the file (for example, `FortiSIEM-6.7.2.1727.qcow2`). Or, you can directly copy the path and the `qcow2` file name under **Provide the existing storage path**. Click **Forward**.



New VM

Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

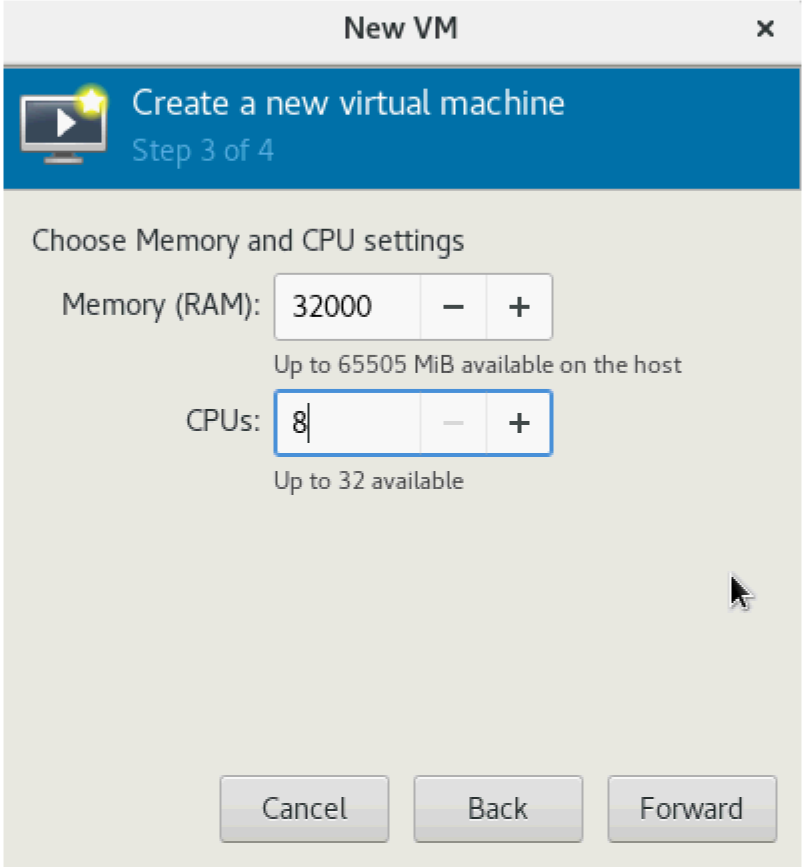
/var/lib/libvirt/images/super/FortiSIEM-VA-6.1.0.

Choose an operating system type and version

OS type: Linux

Version: CentOS 7.0

10. In the New VM dialog box, change **Memory** from **1024** to **32000 (32 GB)**. Change the **CPUs** from **1** to **8**. Click **Forward**.



Choose Memory and CPU settings

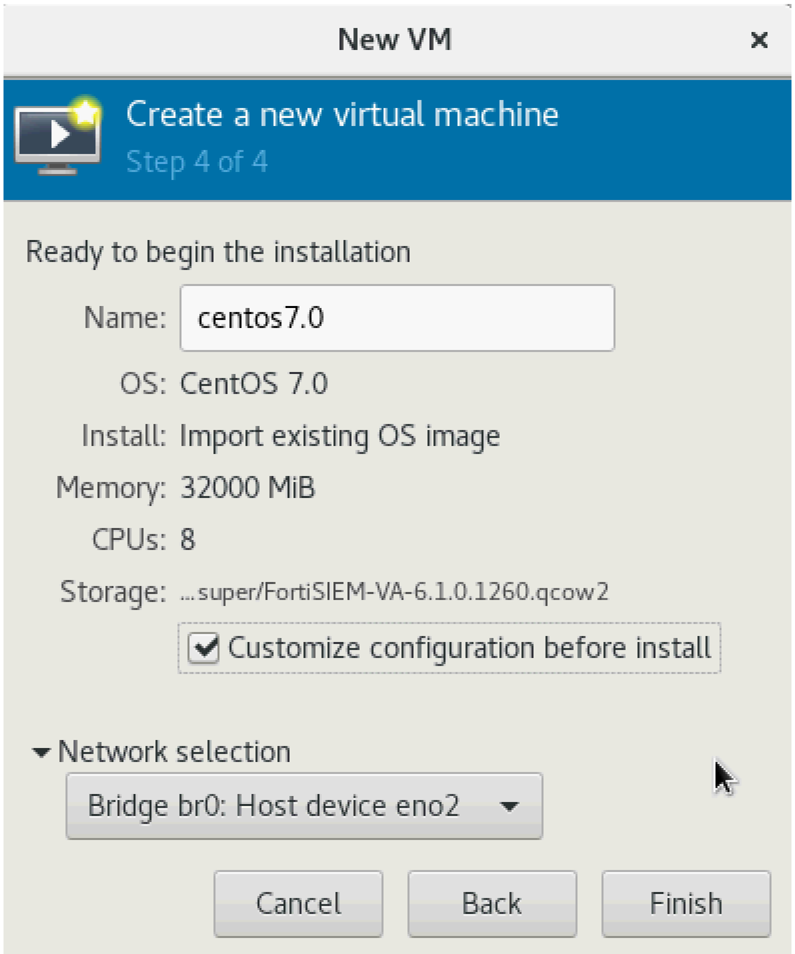
Memory (RAM): 32000

Up to 65505 MiB available on the host

CPUs: 8

Up to 32 available

11. Before clicking **Finish**, make sure to check that the **Network selection** is a **Bridge**, and **Customize configuration before install** is selected. Then, click **Finish**.



Ready to begin the installation

Name: centos7.0

OS: CentOS 7.0

Install: Import existing OS image

Memory: 32000 MiB

CPUs: 8

Storage: ...super/FortiSIEM-VA-6.1.0.1260.qcow2

☑ Customize configuration before install

Network selection

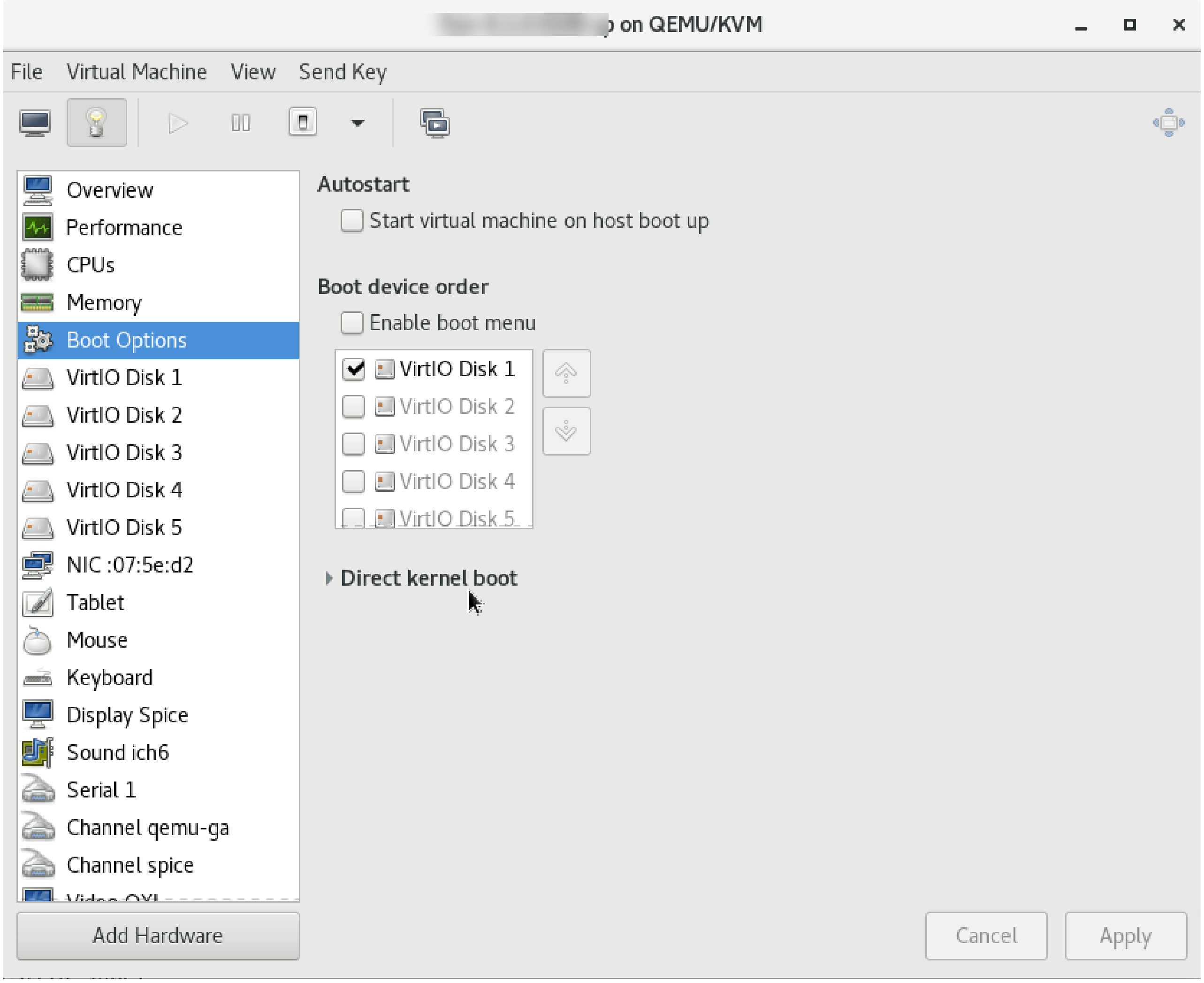
Bridge br0: Host device eno2

12. Start to make the configuration. This is the place where you change the name from the default name centos 7.0 in the Overview.

> ⚠ In every step in this configuration, you must click **Apply** to save your changes.

13. Click **VirtIO Disk 1** (the default disk) and check that the **Source** path is correct. Click **Apply**.

14. Click **Boot Options** and make sure that **VirtIO Disk 1** is checked. Click **Apply**.



[redacted] on QEMU/KVM

Autostart

☐ Start virtual machine on host boot up

Boot device order

☐ Enable boot menu

☑ VirtIO Disk 1
☐ VirtIO Disk 2
☐ VirtIO Disk 3
☐ VirtIO Disk 4
☐ VirtIO Disk 5

▸ **Direct kernel boot**

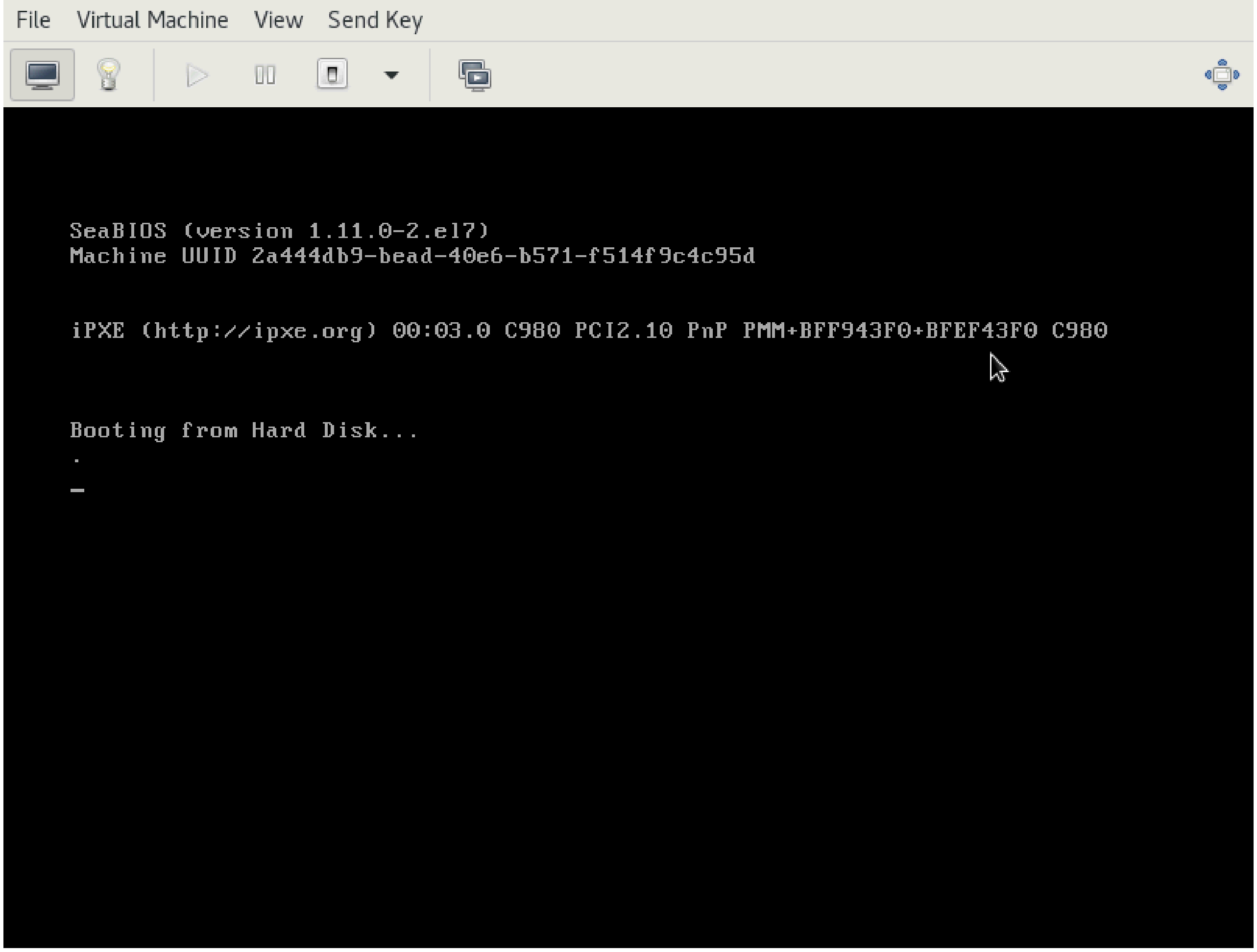
15. Add an extra three disks by clicking **Add Hardware**. Assign to them the disk image size to 100GB, 60GB, and 60GB respectively with the same Bus type of **VirtIO**. Click **Finish** to save the result.

Disk	Size	Disk Name
Hard Disk 2	100GB	/opt For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.
Hard Disk 3	60GB	/cmdb
Hard Disk 4	60GB	/svn
Hard Disk 5	60GB+	/data (see the following note)

Note on Hard Disk 5:

- Add the 5th disk only if using EventDB on local storage or ClickHouse. In all other cases, this disk is not required. ClickHouse is recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
- For EventDB on local disk, choose a disk based on your EPS and event retention policy. See EventDB Sizing Guide for guidance. 60GB is the minimum.
- For ClickHouse, choose disks based on the number of Tiers and disks on each Tier. These depend on your EPS and event retention policy. See ClickHouse Sizing Guide for guidance. For example, you can choose 1 large disk for Hot Tier. Or you can choose 2 Tiers - Hot Tier comprised of one or more SSD disks and Warm Tier comprised of one or more magnetic hard disks.

16. Click **Begin Installation** at the top of the dialog box to start the installation process.



```
SeaBIOS (version 1.11.0-2.el7)
Machine UUID 2a444db9-bead-40e6-b571-f514f9c4c95d


iPXE (http://ipxe.org) 00:03.0 C980 PCI2.10 PnP PMM+BFF943F0+BFEF43F0 C980


Booting from Hard Disk...
.
_
```

17. At the end of booting, log in with the default login credentials: User: `root` and Password: `ProspectHills`.
18. You will be required to change the password. Remember this password for future use.

    At this point, you can continue configuring FortiSIEM by using the GUI.

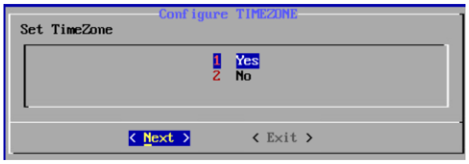
Configure FortiSIEM

Follow these steps to configure FortiSIEM by using a simple GUI.

1. Log in as user `root` with the password you set in Step 18 above.
2. At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:

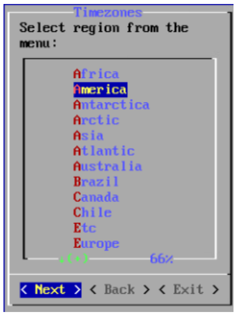
   ```
   # configFSM.sh
   ```

3. In VM console, select **1 Set Timezone** and then press **Next**.

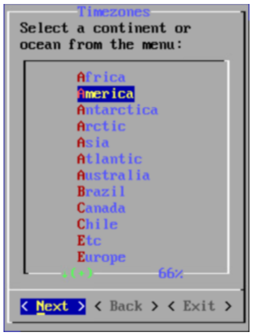
   ```
   Configure TIMEZONE
   Set TimeZone
   1  Yes
   2  No
   < Next >        < Exit >
   ```

4. Select your **Region**, and press **Next**.

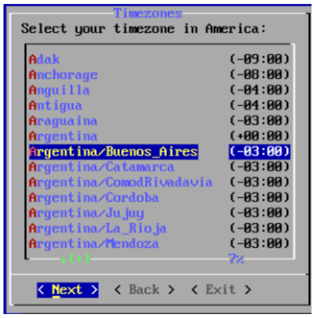
   ```
   Timezones
   Select region from the
   menu:
   Africa
   America
   Antarctica
   Arctic
   Asia
   Atlantic
   Australia
   Brazil
   Canada
   Chile
   Etc
   Europe
   ↓(+)          66%
   < Next > < Back > < Exit >
   ```

5. Select your **Country**, and press **Next**.

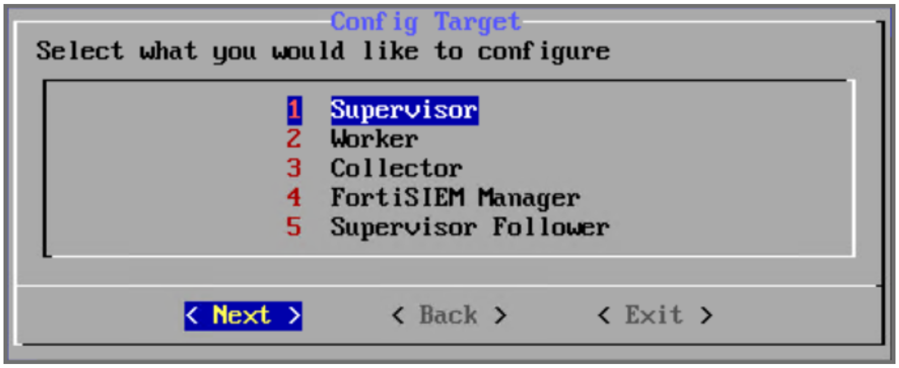
   ```
   Timezones
   Select a continent or
   ocean from the menu:
   Africa
   America
   Antarctica
   Arctic
   Asia
   Atlantic
   Australia
   Brazil
   Canada
   Chile
   Etc
   Europe
   ↓(+)          66%
   < Next > < Back > < Exit >
   ```

6. Select the **Country** and **City** for your timezone, and press **Next**.

   ```
   Timezones
   Select your timezone in America:
   Adak                          (-09:00)
   Anchorage                     (-08:00)
   Anguilla                      (-04:00)
   Antigua                       (-04:00)
   Araguaina                     (-03:00)
   Argentina                     (+00:00)
   Argentina/Buenos_Aires        (-03:00)
   Argentina/Catamarca           (-03:00)
   Argentina/ComodRivadavia      (-03:00)
   Argentina/Cordoba             (-03:00)
   Argentina/Jujuy               (-03:00)
   Argentina/La_Rioja            (-03:00)
   Argentina/Mendoza             (-03:00)
   ↓(+)                          7%
   < Next >  < Back >  < Exit >
   ```

7. If installing a Supervisor, select **1 Supervisor**, and press **Next**.
   If installing a Worker, select **2 Worker**, and press **Next**.
   If installing a Collector, select **3 Collector**, and press **Next**.
   If Installing FortiSIEM Manager, select **4 FortiSIEM Manager**, and press **Next**.
   If Installing FortiSIEM Supervisor Follower, select **5 Supervisor Follower** and press **Next**.
   Note: The appliance type cannot be changed once it is deployed, so ensure you have selected the correct option.

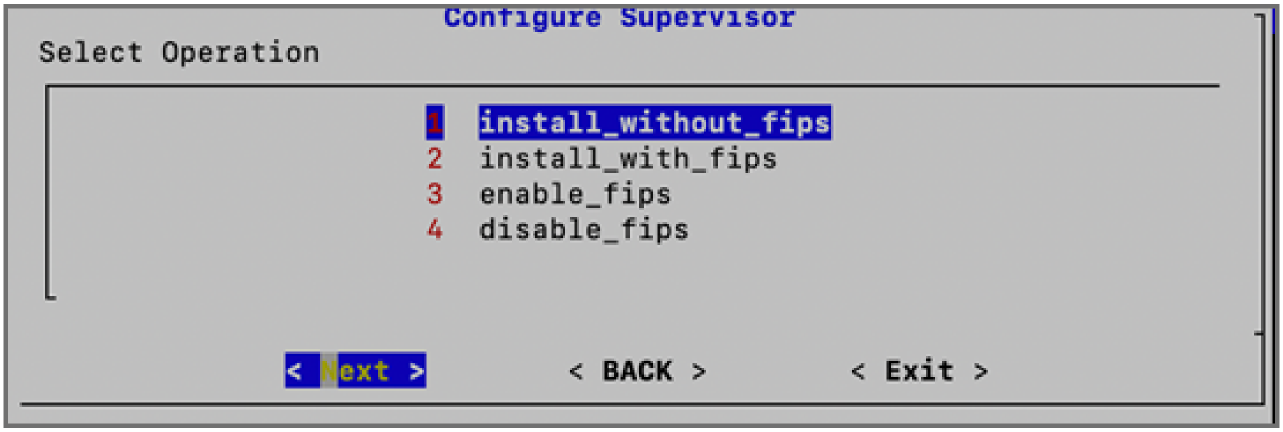


```
Config Target
Select what you would like to configure

1 Supervisor
2 Worker
3 Collector
4 FortiSIEM Manager
5 Supervisor Follower

< Next >      < Back >      < Exit >
```

Regardless of whether you select **FortiSIEM Manager**,**Supervisor**, **Supervisor Follower**, **Worker**, or **Collector**, you will see the same series of screens with only the header changed to reflect your target installation, unless noted otherwise.

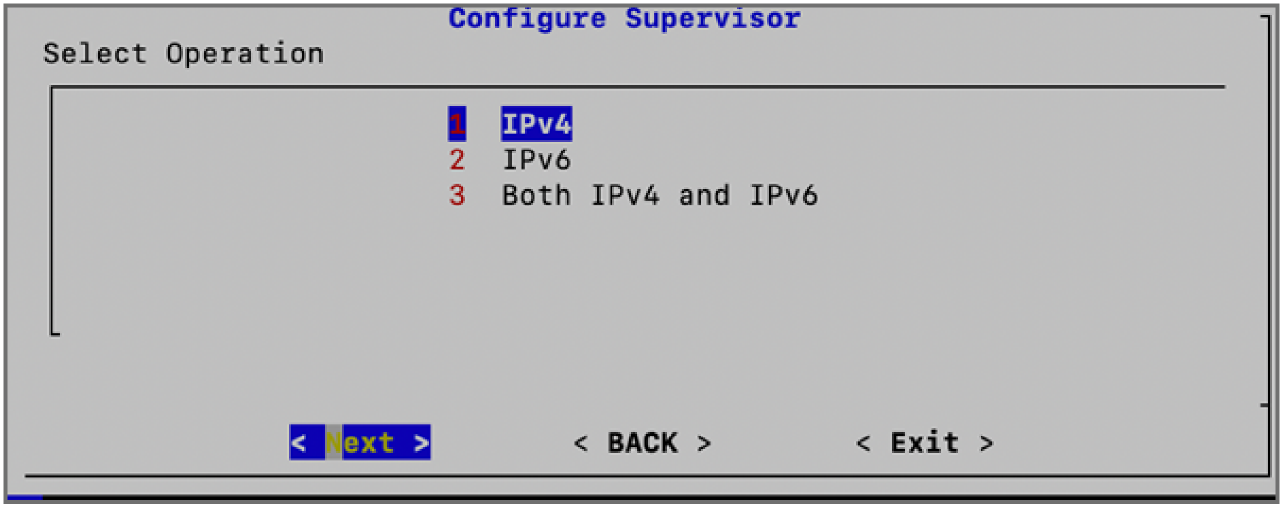
A dedicated ClickHouse Keeper uses a Worker, so first install a Worker and then in later steps configure the Worker as a ClickHouse Keeper.

8. If you want to enable FIPS, then choose **2**. Otherwise, choose **1**. You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.
   Note: After Installation, a 5th option to change your network configuration (**5 change_network_config**) is available. This allows you to change your network settings and/or host name.



```
Configure Supervisor
Select Operation

1 install_without_fips
2 install_with_fips
3 enable_fips
4 disable_fips

< Next >      < BACK >      < Exit >
```

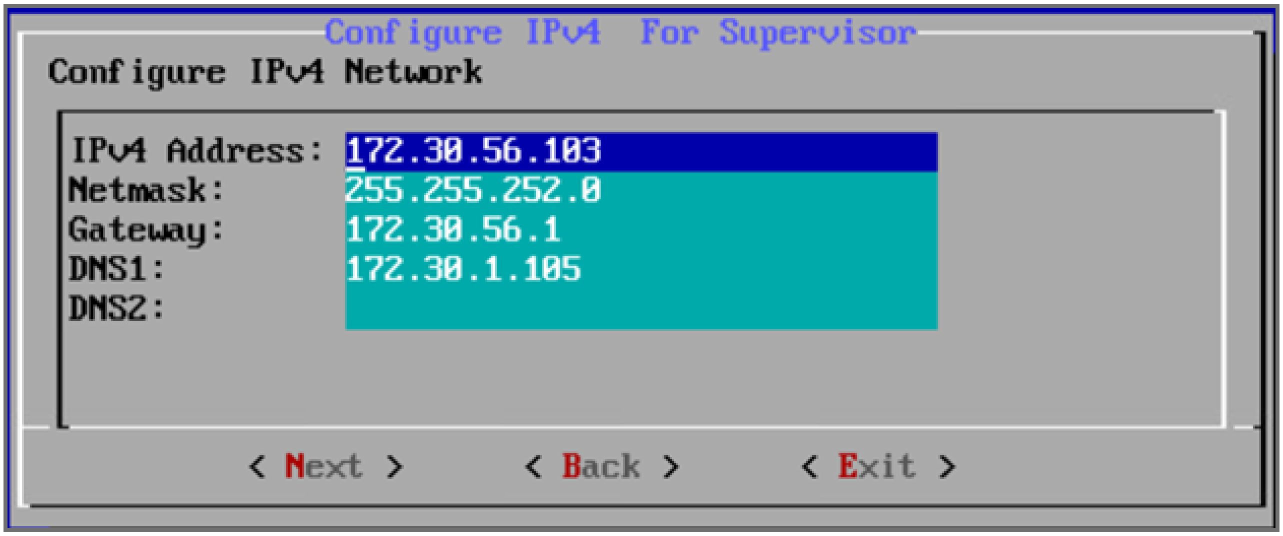
9. Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, choose **2** for IPv6-only, or choose **3** for both IPv4 and IPv6.



10. If you choose **1** (IPv4) or choose **3** (Both IPv4 and IPv6), and press **Next**, then you will move to step 11. If you choose **2** (IPv6), and press **Next**, then skip to step 12.

11. Configure the network by entering the following fields. Press **Next**.

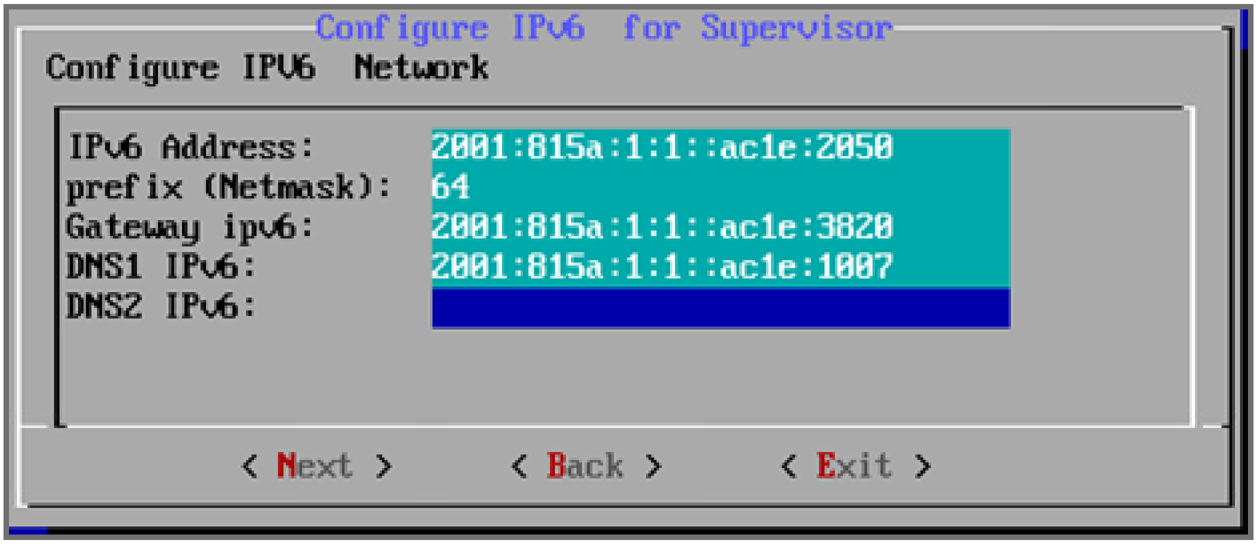
Option	Description
IPv4 Address	The Manager/Supervisor/Worker/Collector's IPv4 address
NetMask	The Manager/Supervisor/Worker/Collector's subnet
Gateway	Network gateway address
DNS1, DNS2	Addresses of the DNS servers



```
IPv4 Address: 172.30.56.103
Netmask:      255.255.252.0
Gateway:      172.30.56.1
DNS1:         172.30.1.105
DNS2:
```

12. If you chose **1** in step 9, then you will need to skip to step 13. If you chose **2** or **3** in step 9, then you will configure the IPv6 network by entering the following fields, then press **Next**.

Option	Description
IPv6 Address	The Manager/Supervisor/Worker/Collector's IPv6 address
prefix (Netmask)	The Manager/Supervisor/Worker/Collector's IPv6 prefix
Gateway ipv6	IPv6 Network gateway address
DNS1 IPv6, DNS2 IPv6	Addresses of the IPv6 DNS server 1 and DNS server2



Configure IPv6 for Supervisor

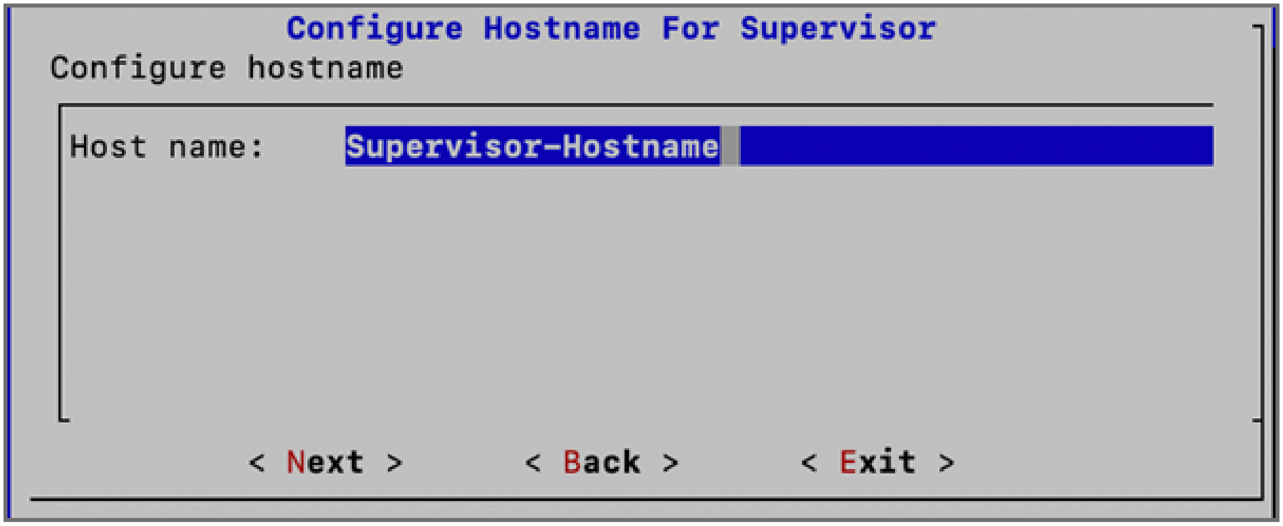
Configure IPV6 Network

```
IPv6 Address:        2001:815a:1:1::ac1e:2050
prefix (Netmask):    64
Gateway ipv6:        2001:815a:1:1::ac1e:3820
DNS1 IPv6:           2001:815a:1:1::ac1e:1007
DNS2 IPv6:
```

Note: If you chose option **3** in step 9 for both IPv4 and IPv6, then even if you configure 2 DNS servers for IPv4 and IPv6, the system will only use the first DNS server from IPv4 and the first DNS server from the IPv6 configuration.

Note: In many dual stack networks, IPv4 DNS server(s) can resolve names to both IPv4 and IPv6. In such environments, if you do not have an IPv6 DNS server, then you can use public IPv6 DNS servers or use IPv4-mapped IPv6 address.

13. Configure Hostname for FortiSIEM Manager/Supervisor/Worker/Collector. Press **Next**.



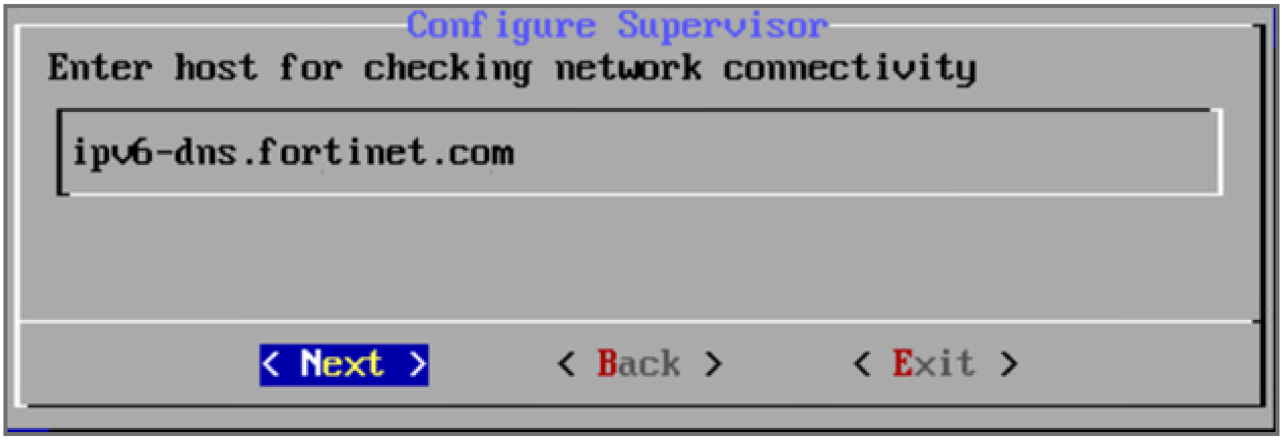
Configure Hostname For Supervisor

Configure hostname

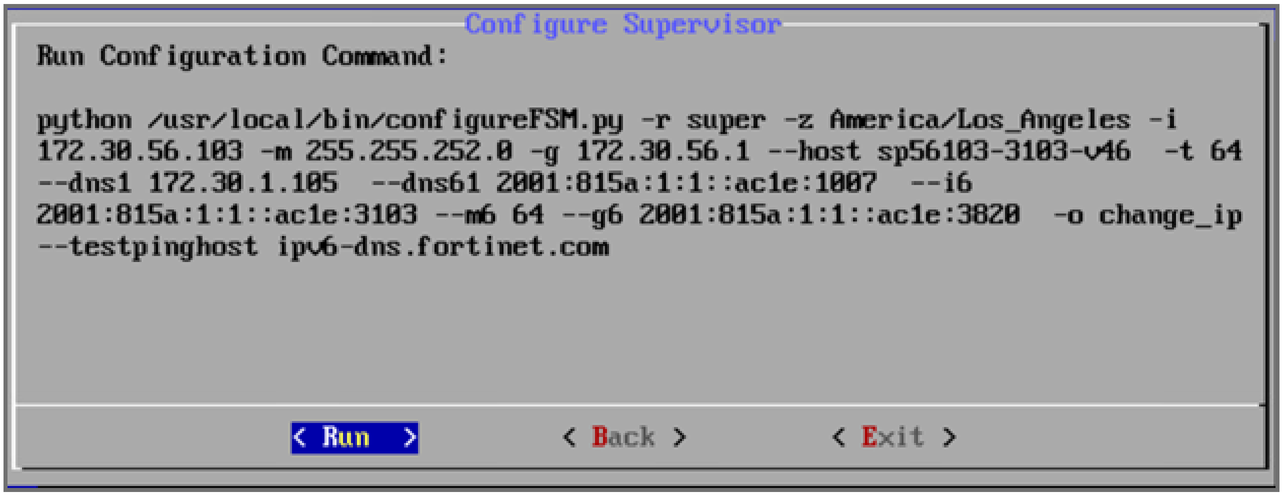
```
Host name:     Supervisor-Hostname
```

Note: FQDN is no longer needed.

14. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.
    Note: By default, “google.com” is shown for the connectivity test, but if configuring IPv6, you must enter an accessible internally approved IPv6 DNS server, for example: “ipv6-dns.fortinet.com"
    Note: When configuring both IPv4 and IPv6, only testing connectivity for the IPv6 DNS is required because the IPV6 takes higher precedence. So update the host field with an approved IPv6 DNS server.



15. The final configuration confirmation is displayed. Verify that the parameters are correct. If they are not, then press **Back** to return to previous dialog boxes to correct any errors. If everything is OK, then press **Run**.



Run Configuration Command:

```
python /usr/local/bin/configureFSM.py -r super -z America/Los_Angeles -i
172.30.56.103 -m 255.255.252.0 -g 172.30.56.1 --host sp56103-3103-v46  -t 64
--dns1 172.30.1.105  --dns61 2001:815a:1:1::ac1e:1007  --i6
2001:815a:1:1::ac1e:3103 --m6 64 --g6 2001:815a:1:1::ac1e:3820  -o change_ip
--testpinghost ipv6-dns.fortinet.com
```

The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
--host	Host name

Option	Description
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either **4** (for **ipv4**) or **6** (for **v6**) or **64** (for both ipv4 and ipv6).
--dns1, --dns2	Addresses of the DNS servers
--i6	IPv6-formatted address
--m6	IPv6 prefix
--g6	IPv6 gateway
-o	Installation option (**install_without_fips**, **install_with_fips**, **enable_fips**, **disable_fips**, **change_network_config***) *Option only available after installation.
-z	Time zone. Possible values are **US/Pacific**, **Asia/Shanghai**, **Europe/London**, or **Africa/Tunis**
--testpinghost	The URL used to test connectivity

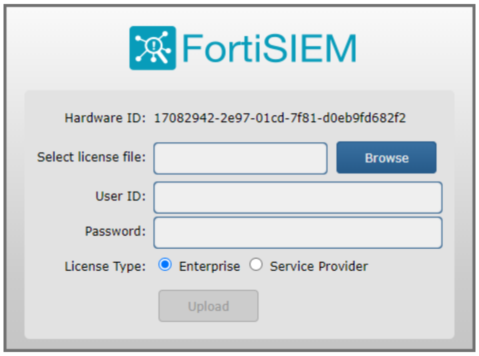
16. It will take some time for this process to finish. When it is done, proceed to Upload the FortiSIEM License. If the VM fails, you can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` to try and identify the problem.

Upload the FortiSIEM License

Before proceeding, make sure that you have obtained valid FortiSIEM license from Forticare. For more information, see the Licensing Guide.

You will now be asked to input a license.

1. Open a Web browser and log in to the FortiSIEM UI. Use link https://<*supervisor-ip*> to login. Please note that if you are logging into FortiSIEM with an IPv6 address, you should input https://[*IPv6 address*] on the browser tab.
2. The License Upload dialog box will open.



Hardware ID: 17082942-2e97-01cd-7f81-d0eb9fd682f2

Select license file:

User ID:

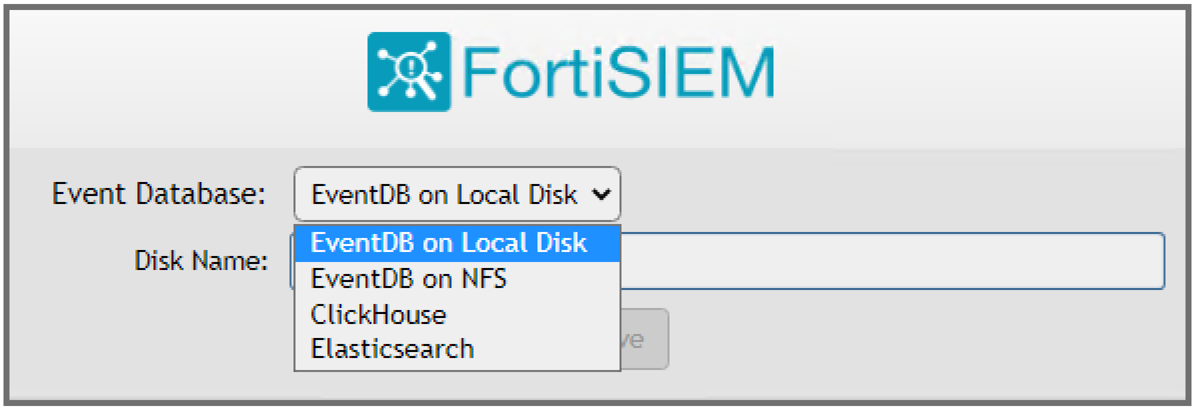
Password:

License Type: ● Enterprise ○ Service Provider

3. Click **Browse** and upload the license file.
   Make sure that the **Hardware ID** shown in the License Upload page matches the license.
4. For **User ID** and **Password**, choose any **Full Admin** credentials.
   For the first time installation, enter `admin` as the user and `admin*1` as the password. You will then be asked to create a new password for GUI access.
5. Choose **License type** as **Enterprise** or **Service Provider**.
   This option is available only for a first time installation. Once the database is configured, this option will not be available.
   For FortiSIEM Manager, **License Type** is not an available option, and will not appear. At this point, FortiSIEM Manager installation is complete. You will not be taken the Event Database Storage page, so you can skip **Configure an Event Database**.
   Note: The FortiSIEM Manager license allows a certain number of instances that can be registered to FortiSIEM Manager.
6. Proceed to Configure an Event Database.

Configure an Event Database

Choose the event database.



If the Event Database is one of the following options, additional disk configuration is required.

- **ClickHouse**: See Case 2 in Creating ClickHouse Online Storage.
  Recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
- **EventDB on Local Disk**: See Case 2 in Creating EventDB Online Storage.

Final Check

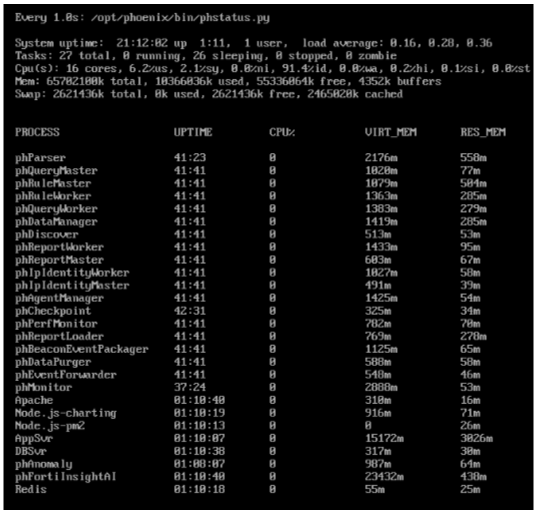
FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

You can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` if you encounter any issues during FortiSIEM installation.

After installation completes, ensure that the `phMonitor` is up and running, for example:

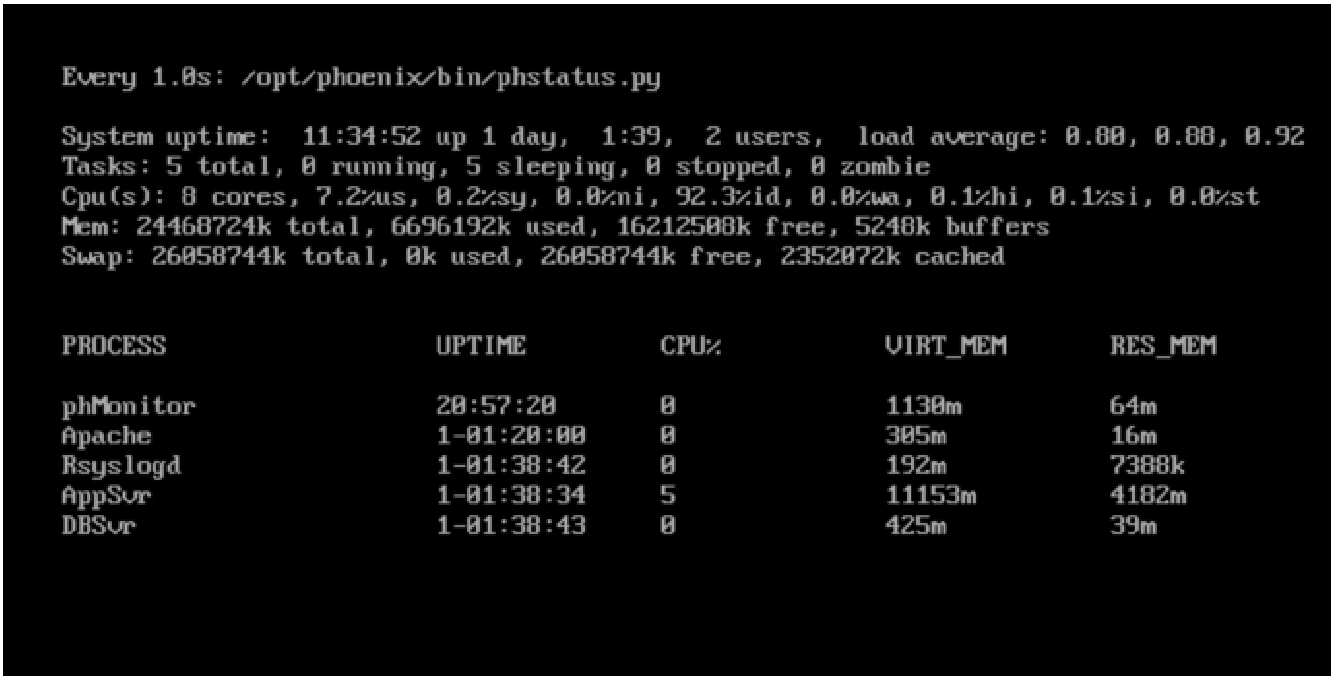
```
# phstatus
```

For the Supervisor, Supervisor Follower, Worker and Collector, the response should be similar to the following.



```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  21:12:02 up  1:11,  1 user,  load average: 0.16, 0.28, 0.36
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16 cores, 6.2%us, 2.1%sy, 0.0%ni, 91.4%id, 0.0%wa, 0.2%hi, 0.1%si, 0.0%st
Mem: 65702100k total, 10366036k used, 55336064k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465020k cached


PROCESS                  UPTIME         CPU%           VIRT_MEM       RES_MEM

phParser                 41:23          0              2176m          558m
phQueryMaster            41:41          0              1020m          77m
phRuleMaster             41:41          0              1079m          504m
phRuleWorker             41:41          0              1363m          285m
phQueryWorker            41:41          0              1383m          279m
phDataManager            41:41          0              1419m          285m
phDiscover               41:41          0              513m           53m
phReportWorker           41:41          0              1433m          95m
phReportMaster           41:41          0              603m           67m
phIpIdentityWorker       41:41          0              1027m          58m
phIpIdentityMaster       41:41          0              491m           39m
phAgentManager           41:41          0              1425m          54m
phCheckpoint             42:31          0              325m           34m
phPerfMonitor            41:41          0              782m           70m
phReportLoader           41:41          0              769m           278m
phBeaconEventPackager    41:41          0              1125m          65m
phDataPurger             41:41          0              588m           58m
phEventForwarder         41:41          0              548m           46m
phMonitor                37:24          0              2888m          53m
Apache                   01:10:40       0              310m           16m
Node.js-charting         01:10:19       0              916m           71m
Node.js-pm2              01:10:13       0              0              26m
AppSvr                   01:10:07       0              15172m         3026m
DBSvr                    01:10:38       0              317m           30m
phAnomaly                01:08:07       0              987m           64m
phFortiInsightAI         01:10:40       0              23432m         438m
Redis                    01:10:18       0              55m            25m
```

For FortiSIEM Manager, the response should look similar to the following.



```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  11:34:52 up 1 day,  1:39,  2 users,  load average: 0.80, 0.88, 0.92
Tasks: 5 total, 0 running, 5 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 7.2%us, 0.2%sy, 0.0%ni, 92.3%id, 0.0%wa, 0.1%hi, 0.1%si, 0.0%st
Mem: 24468724k total, 6696192k used, 16212508k free, 5248k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2352072k cached


PROCESS                  UPTIME         CPU%           VIRT_MEM       RES_MEM

phMonitor                20:57:20       0              1130m          64m
Apache                   1-01:20:00     0              305m           16m
Rsyslogd                 1-01:38:42     0              192m           7388k
AppSvr                   1-01:38:34     5              11153m         4182m
DBSvr                    1-01:38:43     0              425m           39m
```

Cluster Installation

For larger installations, you can choose Worker nodes, Collector nodes, and external storage (NFS, ClickHouse, or Elasticsearch).

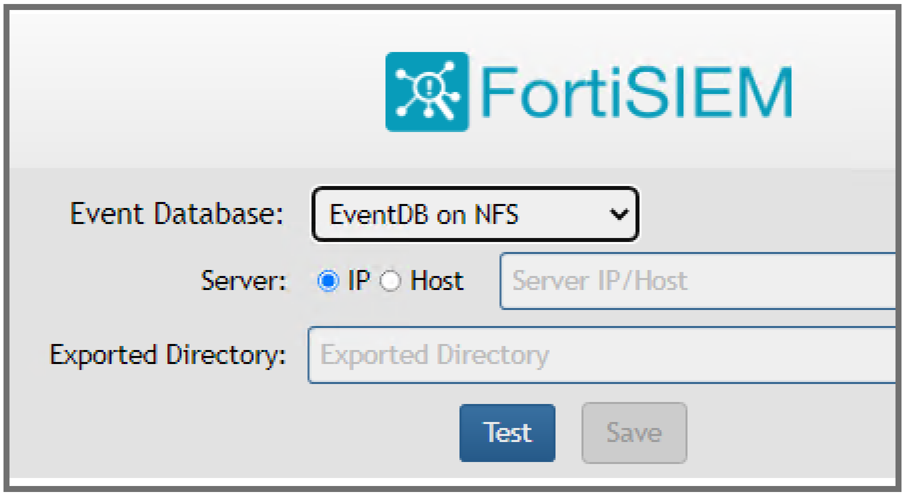
- Install Supervisor
- Install Workers
- Register Workers

- Create ClickHouse Topology (Optional)
- Install Collectors
- Register Collectors
- Install Manager
- Register Instances to Manager

Install Supervisor

Follow the steps in All-in-one Installation, except with the following differences.

1. Event Database choices are **EventDB on NFS**, **ClickHouse**, or **Elasticsearch**.
2. If you choose **EventDB on NFS**
   a. Disk 5 is not required (From Import FortiSIEM into KVM Step 15).
   b. You need to configure NFS after license upload.

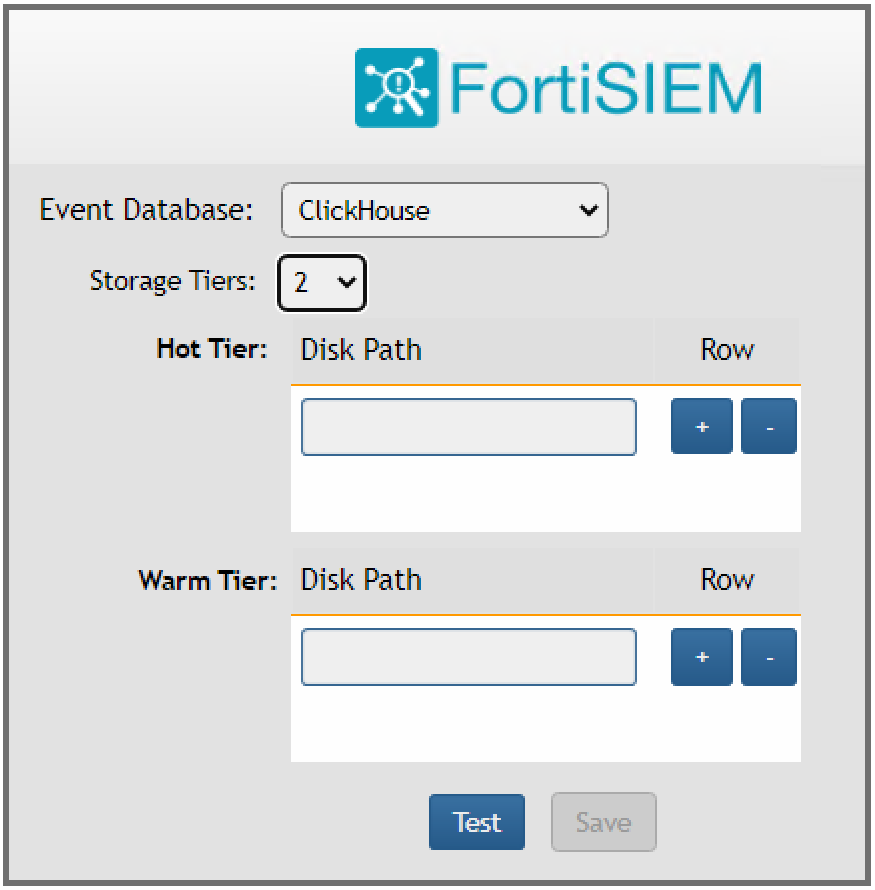


Event Database: EventDB on NFS

Server: ● IP ○ Host Server IP/Host

Exported Directory: Exported Directory

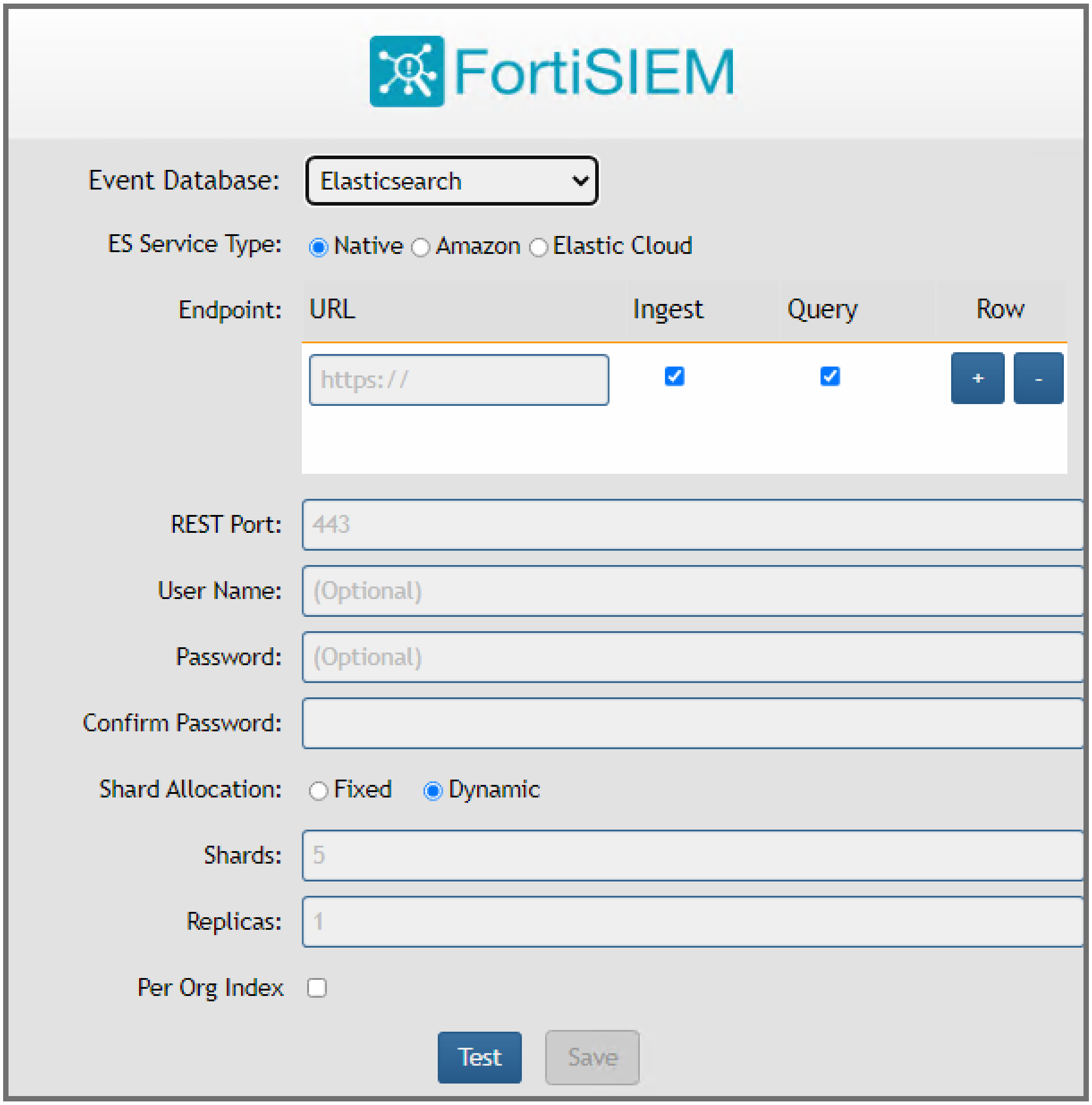
3. If you choose **ClickHouse**
   a. You need to create disks during Import FortiSIEM into KVM Step 15 based on the role of the Supervisor node in the ClickHouse cluster. See the ClickHouse Sizing Guide for details.
   b. You need to configure disks after license upload.



Event Database: ClickHouse

Storage Tiers: 2

4. If you choose **Elasticsearch**, define Elasticsearch endpoints after license upload. See the Elasticsearch Sizing Guide for details.



Event Database:	Elasticsearch
ES Service Type:	● Native ○ Amazon ○ Elastic Cloud
Endpoint:	URL: https:// ☑ Ingest ☑ Query
REST Port:	443
User Name:	(Optional)
Password:	(Optional)
Confirm Password:	
Shard Allocation:	○ Fixed ● Dynamic
Shards:	5
Replicas:	1
Per Org Index	□

Install Workers

Once the Supervisor is installed, take the same steps in All-in-one Installation to install a Worker with the following differences.

1. Choose appropriate CPU and memory for the Worker nodes based on Sizing guide.
2. Two hard disks for Operating Systems and FortiSIEM Application:
   - OS – 25GB
   - OPT – 100GB

     For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

3. If you are running ClickHouse, then create additional data disks based on the role of the Worker in ClickHouse topology. If it is a Keeper node, then a smaller disk is needed. If it is a data node, then a bigger disk is needed based on your EPS and retention policy. See ClickHouse Sizing Guide for details.

Sizing Guide References:

- ClickHouse Sizing Guide
- EventDB Sizing Guide
- Elasticsearch Sizing Guide

Register Workers

Once the Worker is up and running, add the Worker to the Supervisor node.

1. Go to **ADMIN > License > Nodes**.
2. Select Worker from the **Mode** drop-down list and enter the following information:
   a. In the **Host Name** field, enter the Worker's host name.
   b. In the **IP Address** field, enter the Worker's IP address.
   c. If you are running ClickHouse, then select the number for Storage Tiers from the **Storage Tiers** drop-down list, and input disk paths for disks in each Tier in the **Disk Path** fields.

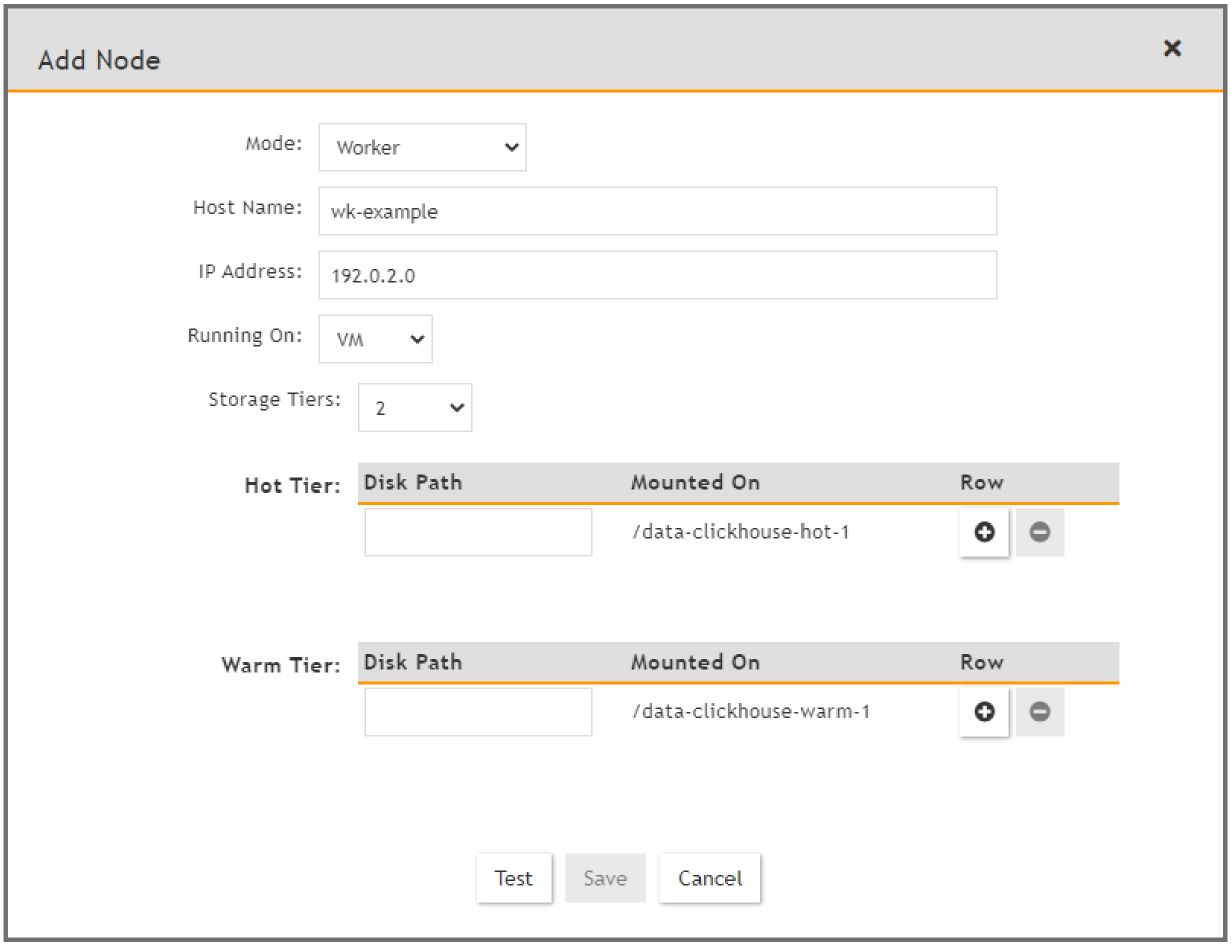
      For **Disk Path**, use one of the following CLI commands to find the disk names.

      ```
      fdisk -l
      ```

      or

      ```
      lsblk
      ```

      When using `lsblk` to find the disk name, please note that the path will be `/dev/<disk>`. As an example KVM, the 3rd disk (hot) will be `/dev/vdc` and the 4th disk (warm) will be `/dev/vdc`.
   d. Click **Test**.



Mode: Worker

Host Name: wk-example

IP Address: 192.0.2.0

Running On: VM

Storage Tiers: 2

Hot Tier:

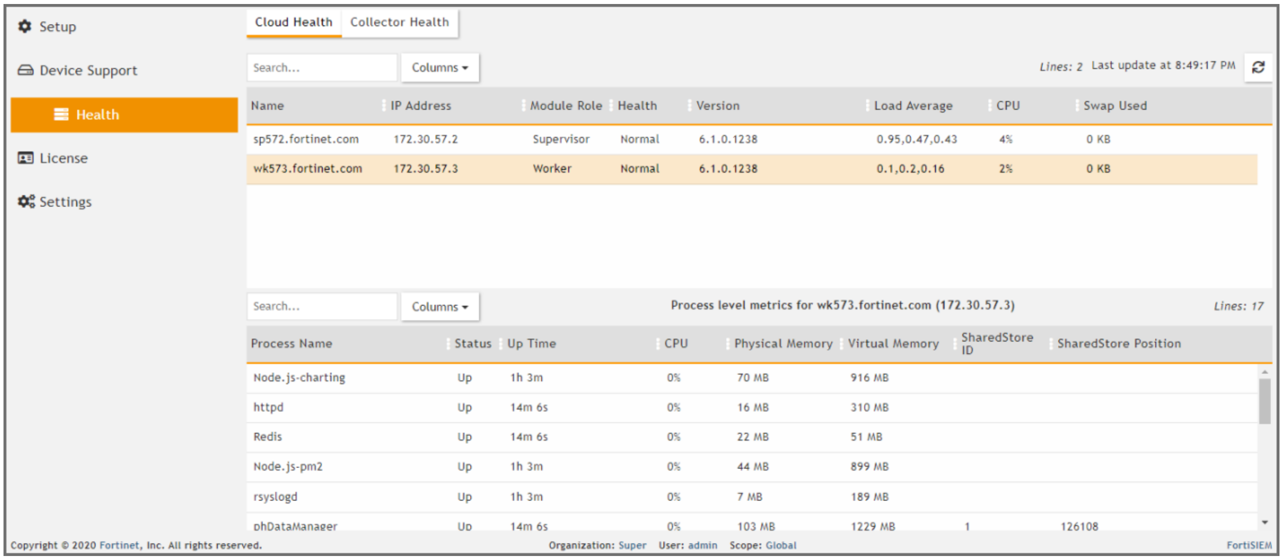
Disk Path	Mounted On	Row
	/data-clickhouse-hot-1	⊕ ⊖

Warm Tier:

Disk Path	Mounted On	Row
	/data-clickhouse-warm-1	⊕ ⊖

e. If the test succeeds, then click **Save**.

3. See **ADMIN > Health > Cloud Health** to ensure that the Workers are up, healthy, and properly added to the system.



Lines: 2 Last update at 8:49:17 PM

Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used
sp572.fortinet.com	172.30.57.2	Supervisor	Normal	6.1.0.1238	0.95,0.47,0.43	4%	0 KB
wk573.fortinet.com	172.30.57.3	Worker	Normal	6.1.0.1238	0.1,0.2,0.16	2%	0 KB

Process level metrics for wk573.fortinet.com (172.30.57.3)

Lines: 17

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
Node.js-charting	Up	1h 3m	0%	70 MB	916 MB		
httpd	Up	14m 6s	0%	16 MB	310 MB		
Redis	Up	14m 6s	0%	22 MB	51 MB		
Node.js-pm2	Up	1h 3m	0%	44 MB	899 MB		
rsyslogd	Up	1h 3m	0%	7 MB	189 MB		
phDataManager	Up	14m 6s	0%	103 MB	1229 MB	1	126108

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM

Create ClickHouse Topology (Optional)

If you are running ClickHouse, you need to configure ClickHouse topology by specifying which nodes belong to ClickHouse Keeper and Data Clusters. Follow the steps in Configuring ClickHouse Topology.

Install Collectors

Once Supervisor and Workers are installed, follow the same steps in All-in-one Install to install a Collector except you need to only choose OS and OPT disks.

- Collector in Regular IT Environments
- Collector with Reduced Disk in OT Environments

Collector in Regular IT Environments

The recommended settings for Collector node are:

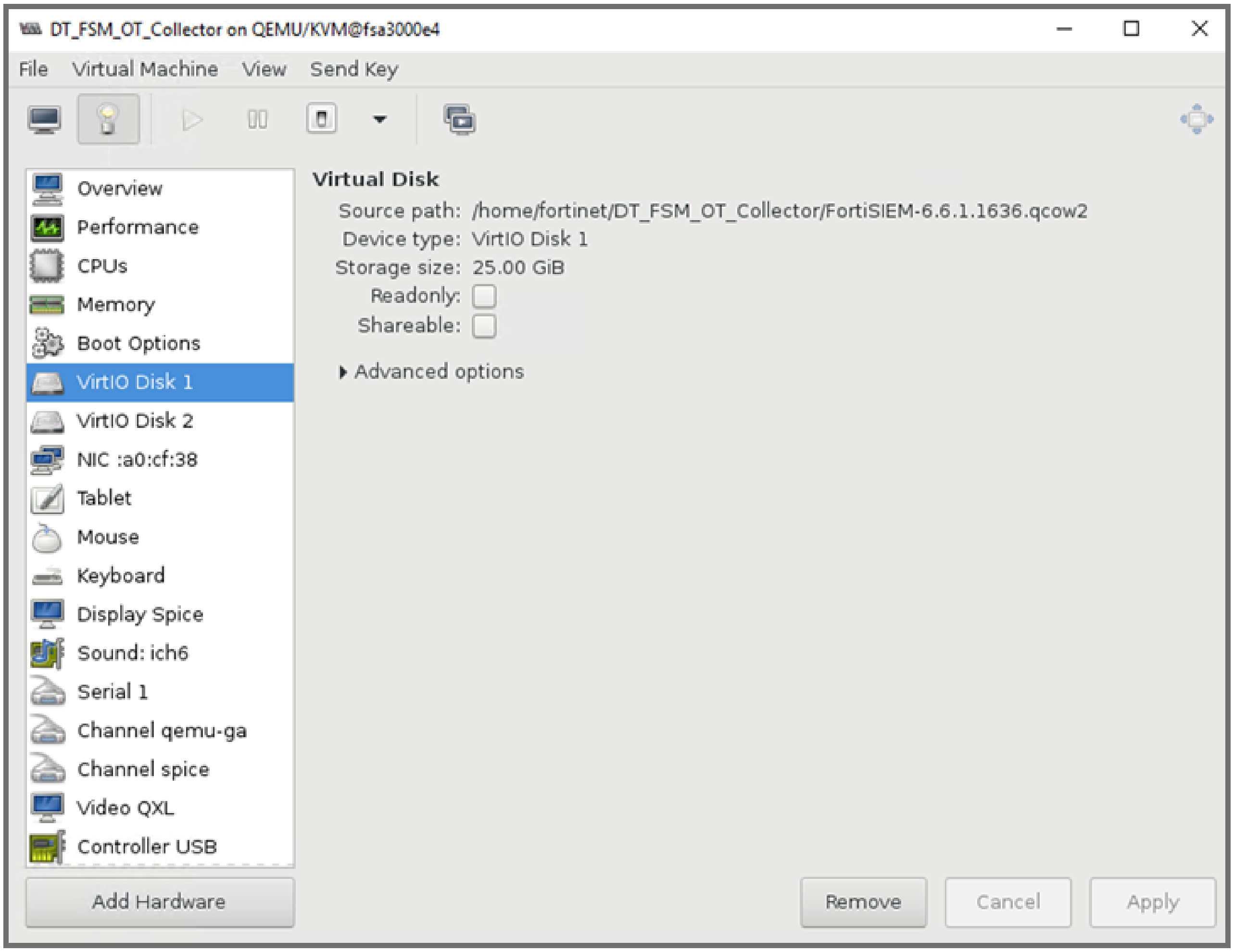
- CPU = 4
- Memory = 8GB
- Two hard disks:
  - OS – 25GB
  - OPT – 100GB
    For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Collector with Reduced Disk in OT Environments

FortiSIEM installations require the disk for OPT+SWAP to have exactly 100 GB. This is valid for all three node options (Supervisor, Worker and Collectors).

Certain environments such as Operational Technology (OT) may find it difficult to dedicate 125 GB to a log collector. The steps here explain how to bypass the requirement for Collector install. Be aware that reducing the size of the disk also reduces the size of the available cache when there is a connection interruption between Collector and Workers/Supervisor, and may result in loss of logs.

1. Follow the installation guide but instead of adding a 100 GB disk for OPT, add a disk of whatever size you require.
2. In this example, we will assume the OPT disk is 35 GB, so in total, the Collector VM will have 70 GB (25 for OS + 35 for OPT).



Virtual Disk

Source path: /home/fortinet/DT_FSM_OT_Collector/FortiSIEM-6.6.1.1636.qcow2

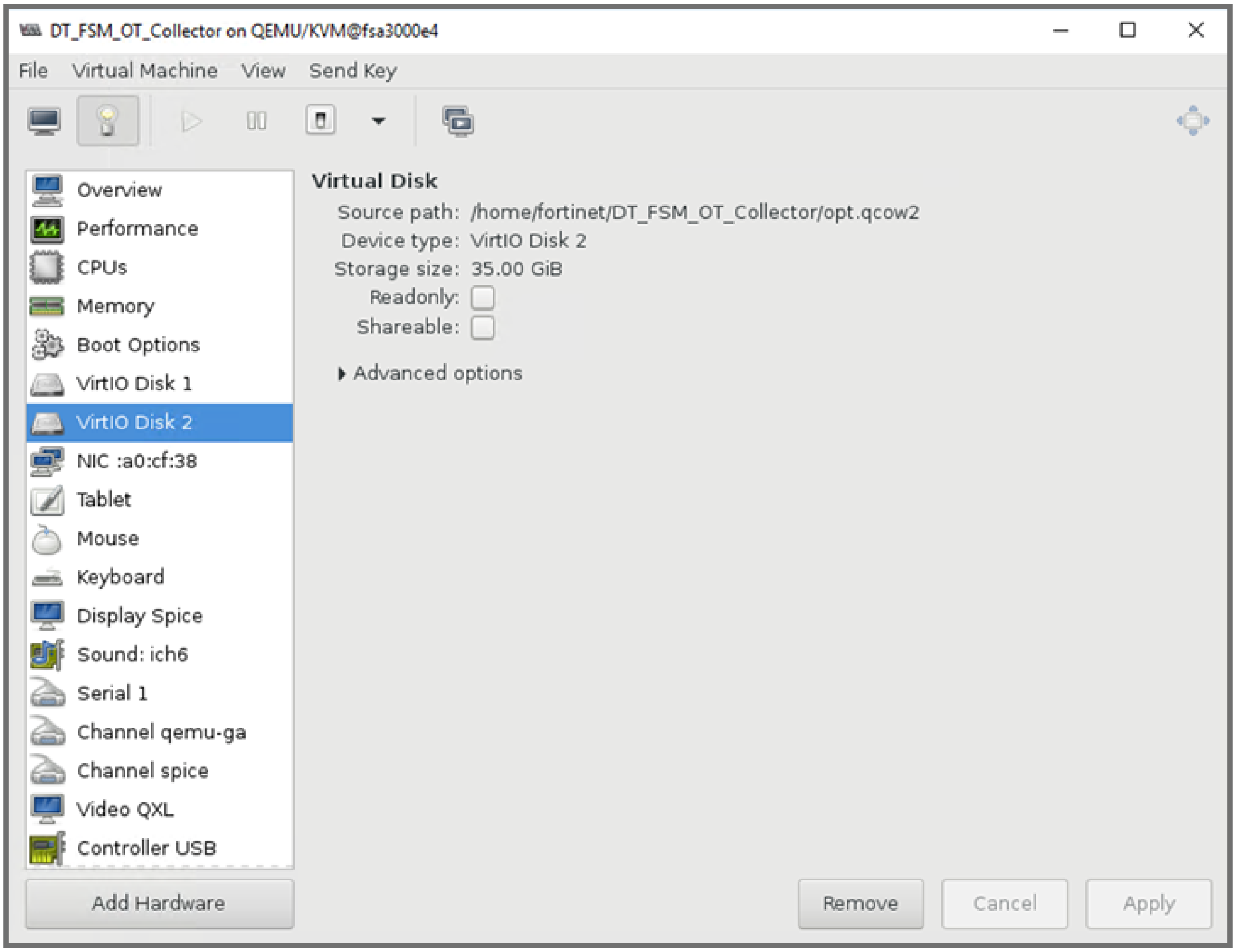
Device type: VirtIO Disk 1

Storage size: 25.00 GiB

Readonly: □

Shareable: □

▸ Advanced options



Virtual Disk

Source path: /home/fortinet/DT_FSM_OT_Collector/opt.qcow2
Device type: VirtIO Disk 2
Storage size: 35.00 GiB
Readonly: □
Shareable: □

Advanced options

3. After you boot the VM and change the password, you will be editing the following files.
   - /usr/local/syslib/config/disksConfig.json
   - /usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml

   Note: You must make changes to these files **before** running the configureFSM.sh installer.
4. The `disksConfig.json` file contains a map of installation types and node types. It defines the required sizes of disks so that the installer can validate them. Since we are changing the KVM Collector opt disk requirement to 35 GB in this example, we must reflect that size in this file. Using a text editor, modify the "opt" line in the `disksConfig.json` file, shown in blue to your requirement.

```
"FSIEMKVM": {
  "SUPER": {
    "number": "3",
    "opt": "100",
    "svn": "60",
    "cmdb": "60"
  },
  "FSMMANAGER": {
    "number": "2",
    "opt": "100",
    "cmdb": "60"
  },
  "WORKER": {
        "number": "1",
        "opt": "100"
      },
      "COLLECTOR": {
        "number": "1",
        "opt": "35"
      }
    },
```

5. Save the `disksConfig.json` file.
6. Load the `/usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml` file via a text editor. You can choose to adjust only the (step a) OPT disk or (step b) adjust the swap disk and OPT disk. To change only the OPT disk, proceed with step a, then skip to step 7. To adjust the swap disk and reduce the OPT disk, skip step a and proceed with step b.
   a. **ADJUST OPT DISK ONLY**

      Navigate to line 54 in the /usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml file and change the line.

      Original line (The original line assumes the drive is 100 GB)

      ```
      parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
      100G && sleep 5
      ```

      Change this line to reflect the size of your OPT disk (in this example 35 GB), marked in blue.

      ```
      parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
      35G && sleep 5
      ```

      Skip step b and c, and proceed to step 7.
   b. **ADJUST SWAP DISK and REDUCE OPT DISK**

      Reduce the Swap Disk by changing the following original line (The original line assumes swap disk to be 25GB).

      ```
      parted -a optimal --script "{{ item.disk }}" mklabel gpt mkpart primary linux-swap 1G
      25G && sleep 5
      ```

      Change to (in this example 10G), marked in blue:

      ```
      parted -a optimal --script "{{ item.disk }}" mklabel gpt mkpart primary linux-swap 1G
      10G && sleep 5
      ```
   c. Reduce /OPT disk: by changing the following line (The original line assumes the drive is 100 GB).

      ```
      parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
      100G && sleep 5
      ```

      Change to reflect the size of your OPT disk (in this example 35 GB), marked in blue.

      ```
      parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 11G
      35G && sleep 5
      ```
7. Save the `disks.yml` file.
8. Run configFSM.sh to install the collector. When it reboots, you can provision it using the `phProvisionCollector` command. Your partition output should appear similar to the following.

   ```
   Partition Output of deployment:
   sdb           8:16   0   35G  0 disk
   ├─sdb1        8:17   0  8.4G  0 part [SWAP]
   └─sdb2        8:18   0 22.4G  0 part /opt
   ```

```
# df -h
Filesystem            Size  Used Avail Use% Mounted on
devtmpfs               12G     0   12G   0% /dev
tmpfs                  12G     0   12G   0% /dev/shm
tmpfs                  12G   17M   12G   1% /run
tmpfs                  12G     0   12G   0% /sys/fs/cgroup
/dev/mapper/rl-root    22G  8.1G   14G  38% /
/dev/sdb2              23G  4.3G   19G  19% /opt
/dev/sda1            1014M  661M  354M  66% /boot
tmpfs                 2.4G     0  2.4G   0% /run/user/500
tmpfs                 2.4G     0  2.4G   0% /run/user/0
```

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- Enterprise Deployments
- Service Provider Deployments

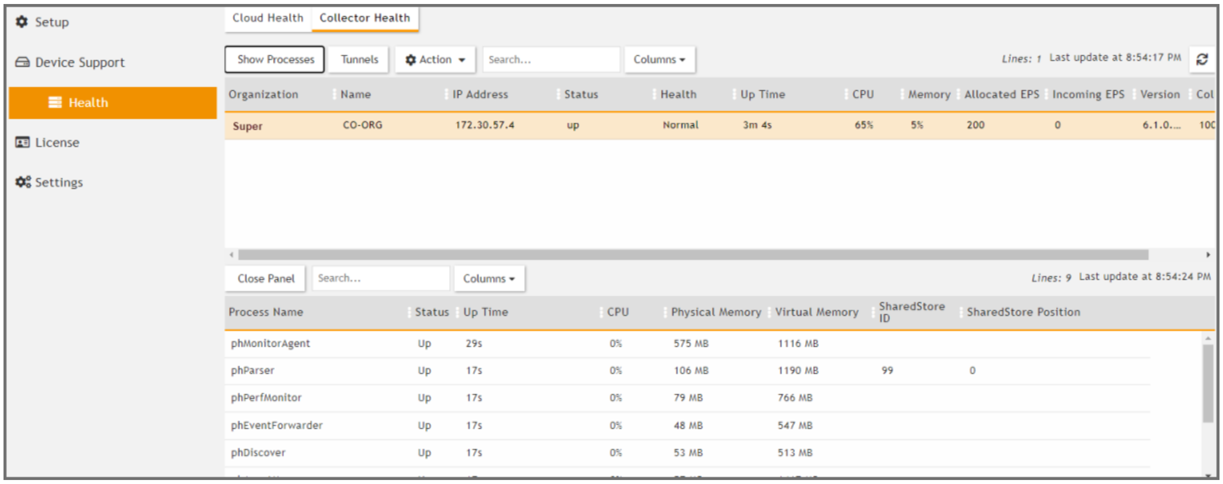
Enterprise Deployments

For Enterprise deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
   a. Enter the IP of the Worker node in the **Event Upload Workers** column. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
   Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
   b. Click **Save**.
   c. In the **Supervisors** column, enter the IP of the Supervisor node and click **Save**.
3. 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 to **Unlimited**.
4. SSH to the Collector and run following script to register Collectors:
   `phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization> <CollectorName>`

   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.
   a. Set `user` and `password` using the admin user name and password for the Supervisor.
   b. Set `Super IP or Host` as the Supervisor's IP address.
   c. Set `Organization`. For Enterprise deployments, the default name is Super.
   d. Set `CollectorName` from Step 2a.
   The Collector will reboot during the Registration.

5. Go to **ADMIN > Health > Collector Health** for the status.



Lines: 1 Last update at 8:54:17 PM

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	172.30.57.4	up	Normal	3m 4s	65%	5%	200	0	6.1.0....	10C

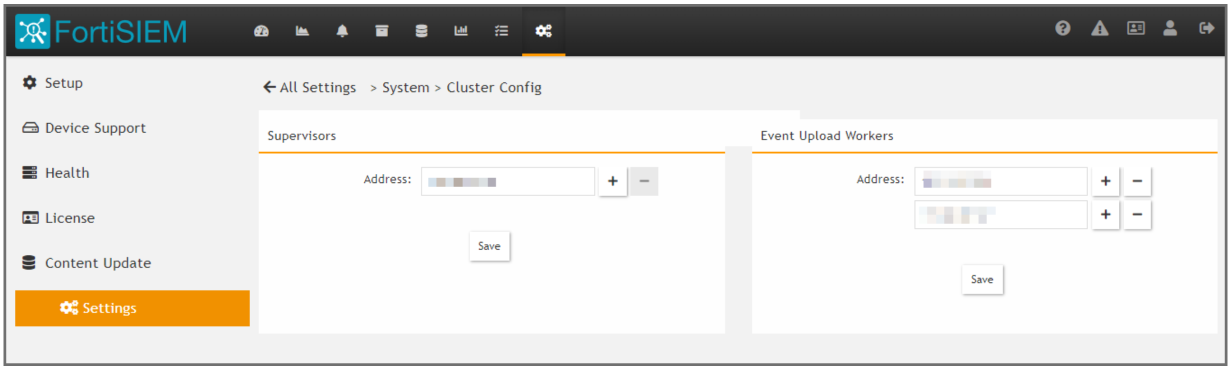
Lines: 9 Last update at 8:54:24 PM

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Service Provider Deployments

For Service Provider deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
   a. Enter the IP of the Worker node in the **Event Upload Workers** column. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
   Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
   b. Click **Save**.
   c. In the **Supervisors** column, enter the IP of the Supervisor node and click **Save**.



Supervisors

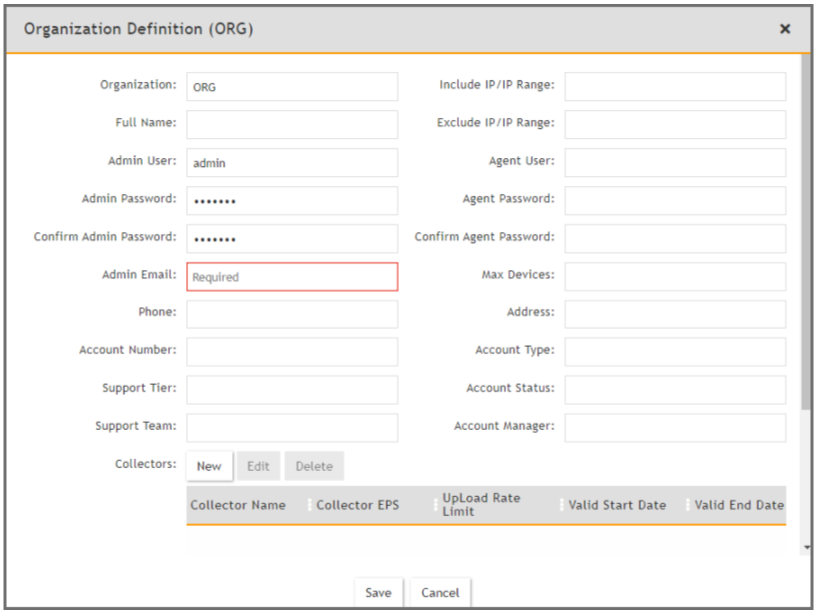
Address: [redacted]

Event Upload Workers

Address: [redacted]

[redacted]

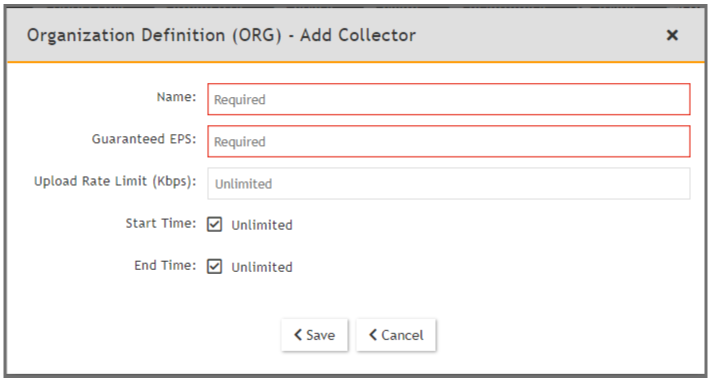
3. Go to **ADMIN > Setup > Organizations** and click **New** to add an Organization.



Organization Definition (ORG)

Organization:	ORG	Include IP/IP Range:	
Full Name:		Exclude IP/IP Range:	
Admin User:	admin	Agent User:	
Admin Password:	•••••••	Agent Password:	
Confirm Admin Password:	•••••••	Confirm Agent Password:	
Admin Email:	Required	Max Devices:	
Phone:		Address:	
Account Number:		Account Type:	
Support Tier:		Account Status:	
Support Team:		Account Manager:	

4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
5. Under **Collectors**, click **New.**
6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.
   The last two values could be set as **Unlimited. Guaranteed EPS** is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.



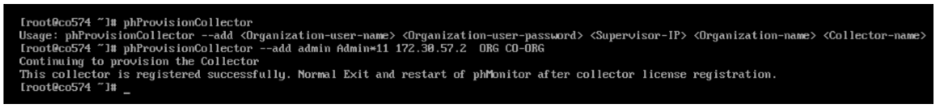
Organization Definition (ORG) - Add Collector

Name:	Required
Guaranteed EPS:	Required
Upload Rate Limit (Kbps):	Unlimited
Start Time:	☑ Unlimited
End Time:	☑ Unlimited

7. SSH to the Collector and run following script to register Collectors:
   `phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization> <CollectorName>`

   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

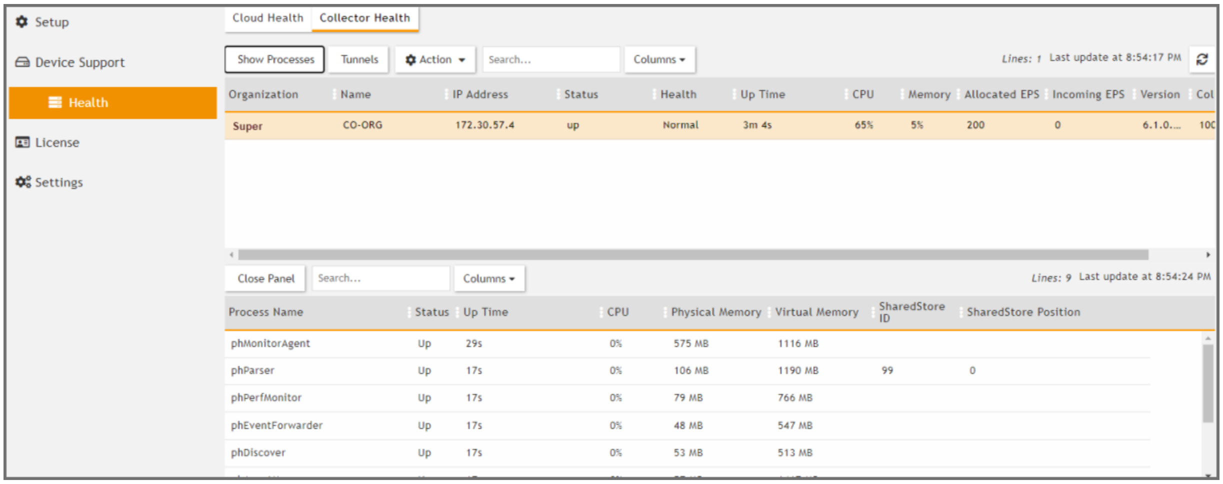
   a. Set `user` and `password` using the admin user name and password for the Organization that the Collector is going to be registered to.
   b. Set `Super IP or Host` as the Supervisor's IP address.
   c. Set `Organization` as the name of an organization created on the Supervisor.
   d. Set `CollectorName` from Step 6.



```
[root@co574 ~]# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
[root@co574 ~]# phProvisionCollector --add admin Admin*11 172.30.57.2  ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
[root@co574 ~]# _
```

The Collector will reboot during the Registration.

8. Go to **ADMIN > Health > Collector Health** and check the status.



Lines: 1 Last update at 8:54:17 PM

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	172.30.57.4	up	Normal	3m 4s	65%	5%	200	0	6.1.0....	10C

Lines: 9 Last update at 8:54:24 PM

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Install Manager

Starting with release 6.5.0, you can install FortiSIEM Manager to monitor and manage multiple FortiSIEM instances. An instance includes a Supervisor and optionally, Workers and Collectors. The FortiSIEM Manager needs to be installed on a separate Virtual Machine and requires a separate license. FortiSIEM Supervisors must be on 6.5.0 or later versions.

Follow the steps in All-in-one Install to install Manager. After any Supervisor, Workers, and Collectors are installed, you add the Supervisor instance to Manager, then Register the instance to Manager. See Register Instances to Manager.

Register Instances to Manager

To register your Supervisor instance with Manager, you will need to do two things in the following order.

- First, add the instance to Manager
- Then register the instance itself to Manager

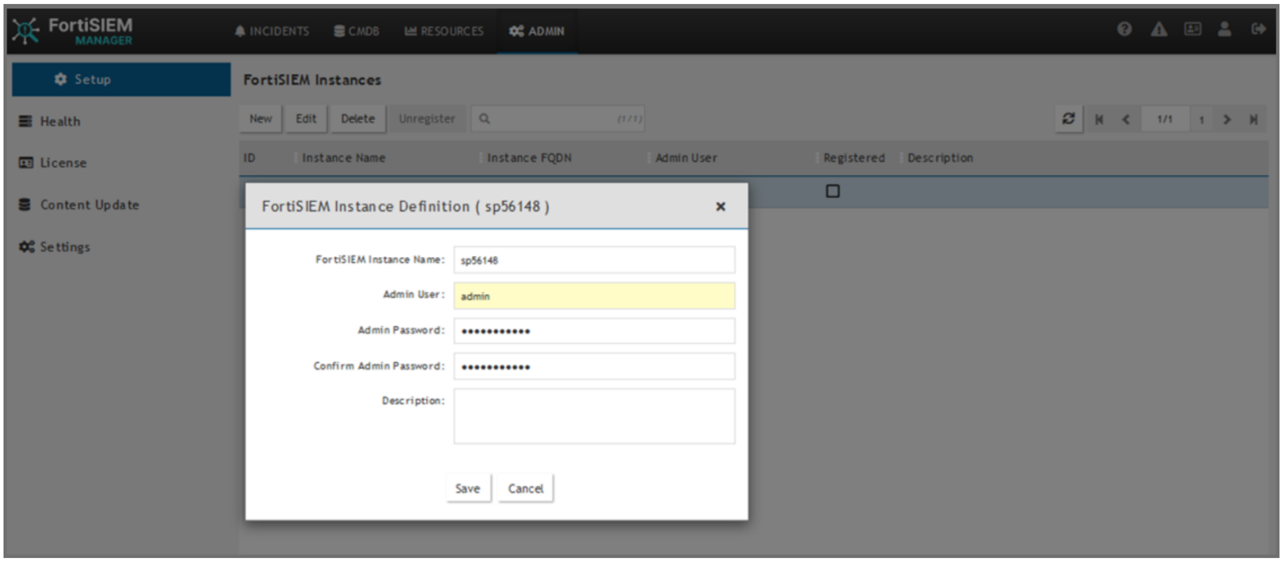
Note that Communication between FortiSIEM Manager and instances is via REST APIs over HTTP(S).

Adding Instance to Manager

You can add an instance to Manager by taking the following steps.
Note: Make sure to record the FortiSIEM Instance Name, Admin User and Admin Password, as this is needed when you register your instance.

1. Login to FortiSIEM Manager.
2. Navigate to **ADMIN > Setup**.
3. Click **New**.
4. In the **FortiSIEM Instance** field, enter the name of the Supervisor instance you wish to add.
5. In the **Admin User** field, enter the Account name you wish to use to access Manager.
6. In the **Admin Password** field, enter the Password that will be associated with the Admin User account.
7. In the **Confirm Admin Password** field, re-enter the Password.

8. (Optional) In the **Description** field, enter any information you wish to provide about the instance.
9. Click **Save**.



FortiSIEM Instance Definition (sp56148)

FortiSIEM Instance Name: sp56148

Admin User: admin

Admin Password: •••••••••••

Confirm Admin Password: •••••••••••

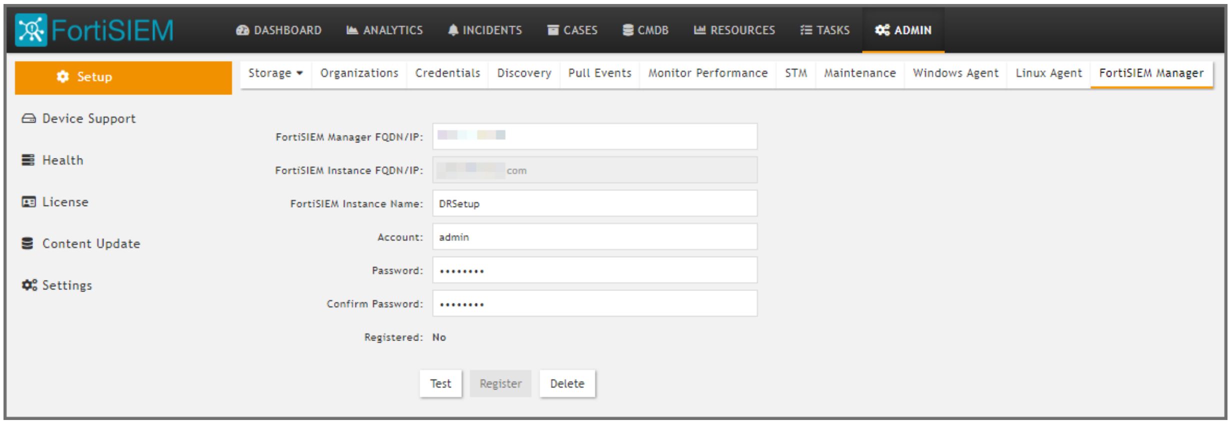
Description:

10. Repeat steps 1-9 to add any additional instances to Manager.
Now, follow the instructions in Register the Instance Itself to Manager for each instance.

Register the Instance Itself to Manager

To register your instance with Manager, take the following steps.

1. From your FortiSIEM Supervisor/Instance, navigate to **ADMIN > Setup > FortiSIEM Manager**, and take the following steps.
   a. In the **FortiSIEM Manager FQDN/IP** field, enter the FortiSIEM Manager Fully Qualified Domain Name (FQDN) or IP address.
   b. If the Supervisor is under a Supervisor Cluster environment, in the **FortiSIEM super cluster FQDN/IP** field, enter the Supervisor Cluster Fully Qualified Domain Name (FQDN) or IP address.
   c. In the **FortiSIEM Instance Name** field, enter the instance name used when adding the instance to Manager.
   d. In the **Account** field, enter the Admin User name used when adding the instance to Manager.
   e. In the **Password** field, enter your password to be associated with the Admin User name.
   f. In the **Confirm Password** field, re-enter your password.
   g. Click **Test** to verify the configuration.
   h. Click **Register**.
   A dialog box displaying "Registered successfully" should appear if everything is valid.



FortiSIEM Manager FQDN/IP: [redacted]

FortiSIEM Instance FQDN/IP: [redacted]com

FortiSIEM Instance Name: DRSetup

Account: admin

Password: ••••••••

Confirm Password: ••••••••

Registered: No

i. Login to Manager, and navigate to any one of the following pages to verify registration.

- **ADMIN > Setup** and check that the box is marked in the **Registered** column for your instance.
- **ADMIN > Health**, look for your instance under FortiSIEM Instances.
- **ADMIN > License**, look for your instance under FortiSIEM Instances.

Install Log

The install ansible log file is located here: `/usr/local/fresh-install/logs/ansible.log`.

Errors can be found at the end of the file.

FORTINET®

www.fortinet.com