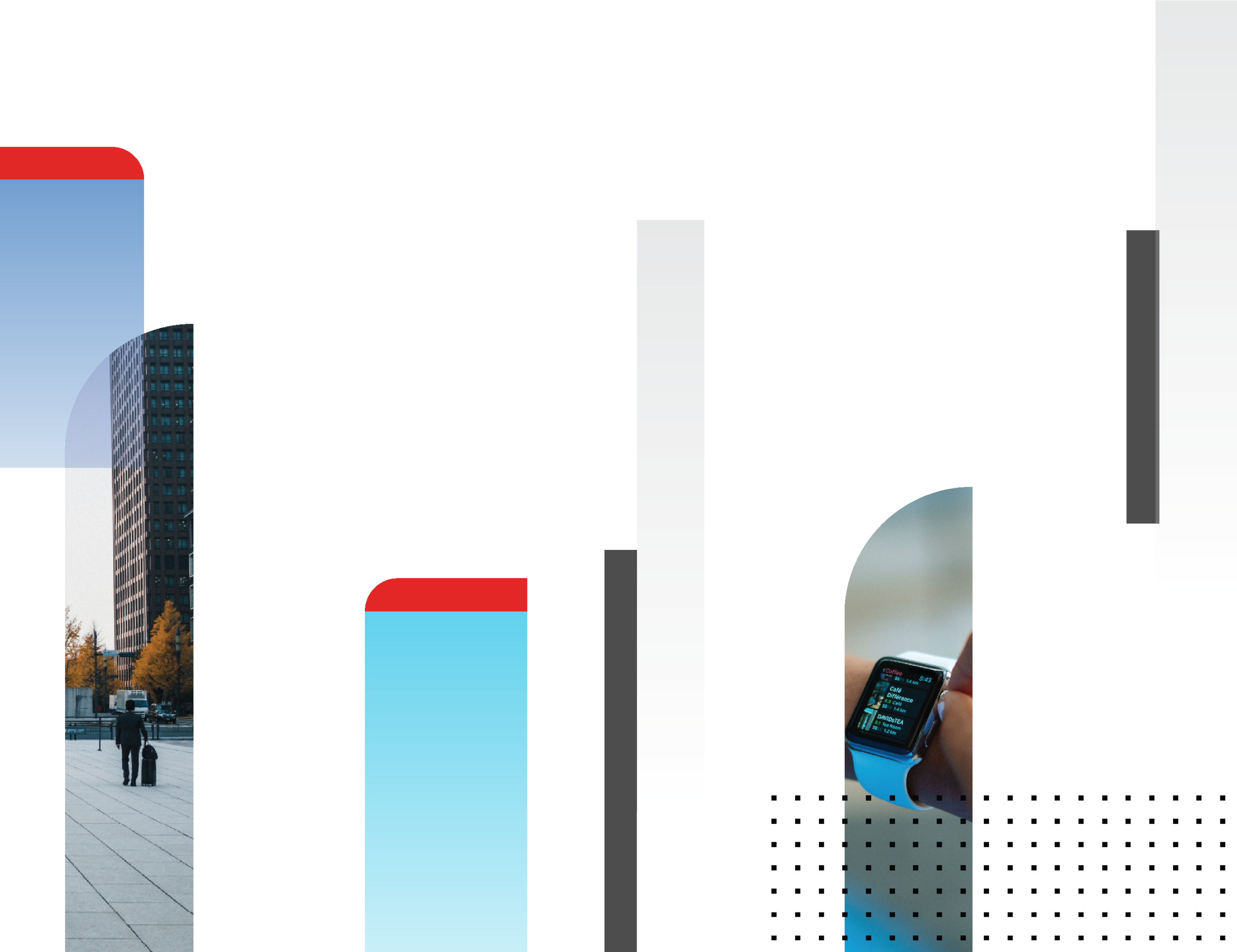
Nutanix AHV Installation and Migration Guide

FortiSIEM 6.1.1



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

10/04/2023
FortiSIEM 6.1.1 Nutanix AHV Installation and Migration Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
04/08/2019	Initial version of FortiSIEM Nutanix-AHV Installation Guide.
11/20/2019	Release of FortiSIEM Nutanix-AHV Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM Nutanix-AHV Installation Guide for 5.3.0.
03/17/2021	Release of FortiSIEM Nutanix-AHV Installation Guide for 6.1.x
03/19/2021	Added Migration section.
11/17/2021	Updated Register Collectors section for 6.1.1 Guide.
08/18/2022	Updated All-in-one Installation section.
10/20/2022	Updated Register Collectors instructions for 6.x guides.

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.
- Deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
  - All-in-one with Supervisor only, or
  - Cluster with Supervisor and Workers
- Storage type
  - Online – Local or NFS or Elasticsearch
  - Archive – NFS or HDFS
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	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 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	Minimum – 4GB	OS – 25GB

Node	vCPU	RAM	Local Disks
	Recommended – 8 (based on load)	Recommended – 8GB	OPT – 100GB

Note: compared to FortiSIEM 5.x, you need one more disk (OPT) which provides a cache for FortiSIEM.

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.

Before proceeding to FortiSIEM deployment, you must configure the external storage.

- *For NFS deployment, see FortiSIEM - NFS Storage Guide here.*
- *For Elasticsearch deployment, see FortiSIEM - Elasticsearch Storage Guide here.*

All-in-one Installation

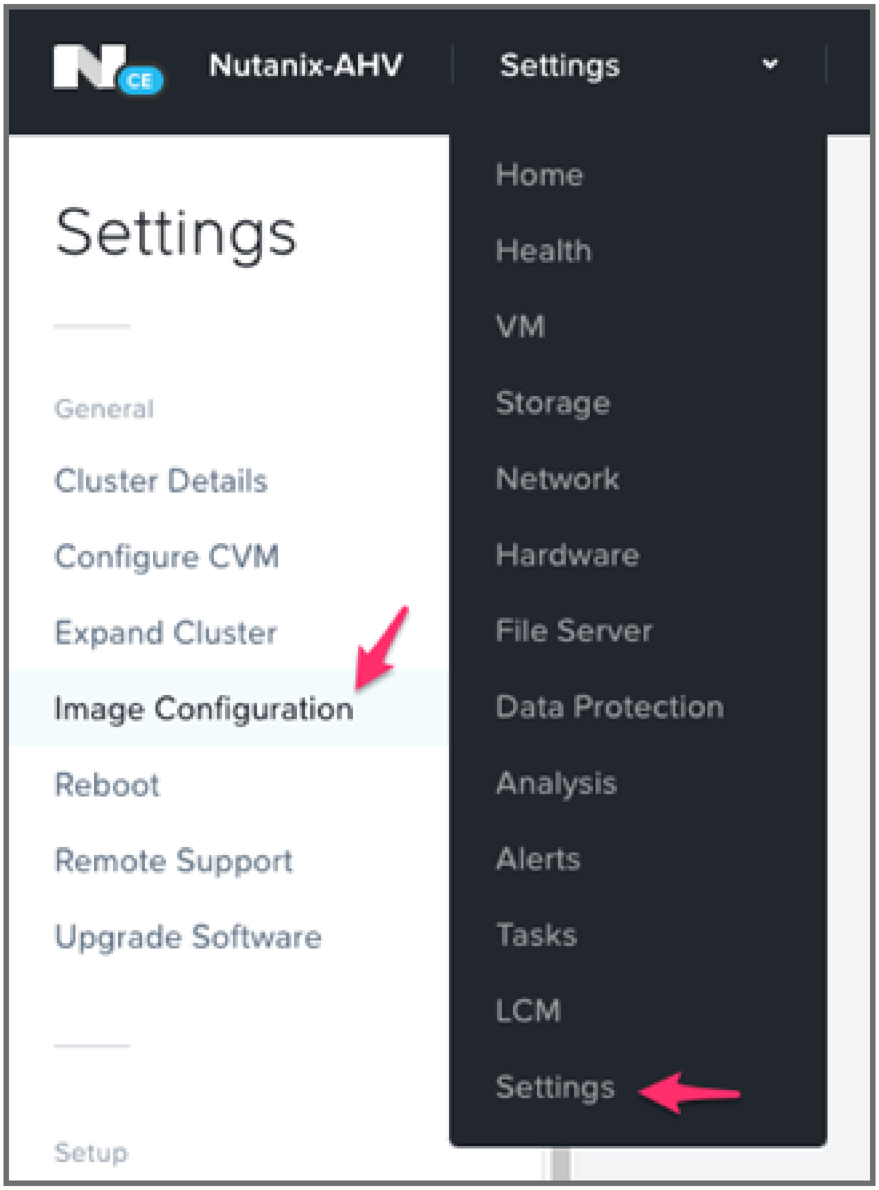
This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

- Import FortiSIEM into Nutanix-AHV Prism Console
- Configure FortiSIEM via GUI
- Upload the FortiSIEM License
- Choose an Event Database

Import FortiSIEM into Nutanix-AHV Prism Console

1. Go to the Fortinet Support website https://support.fortinet.com to download the KVM package `FSM_Full_All_KVM_6.1.1_build0118.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_6.1.1_build0118.zip`.
3. Unzip the `.zip` file to get the `FortiSIEM-6.1.1.0118.qcow2` file.
4. Login to the Nutanix-AHV Prism Console.

5. Click on the drop-down list and select **Settings > Image Configuration**.



6. Click **Upload Image** from the **Image Configuration** page.

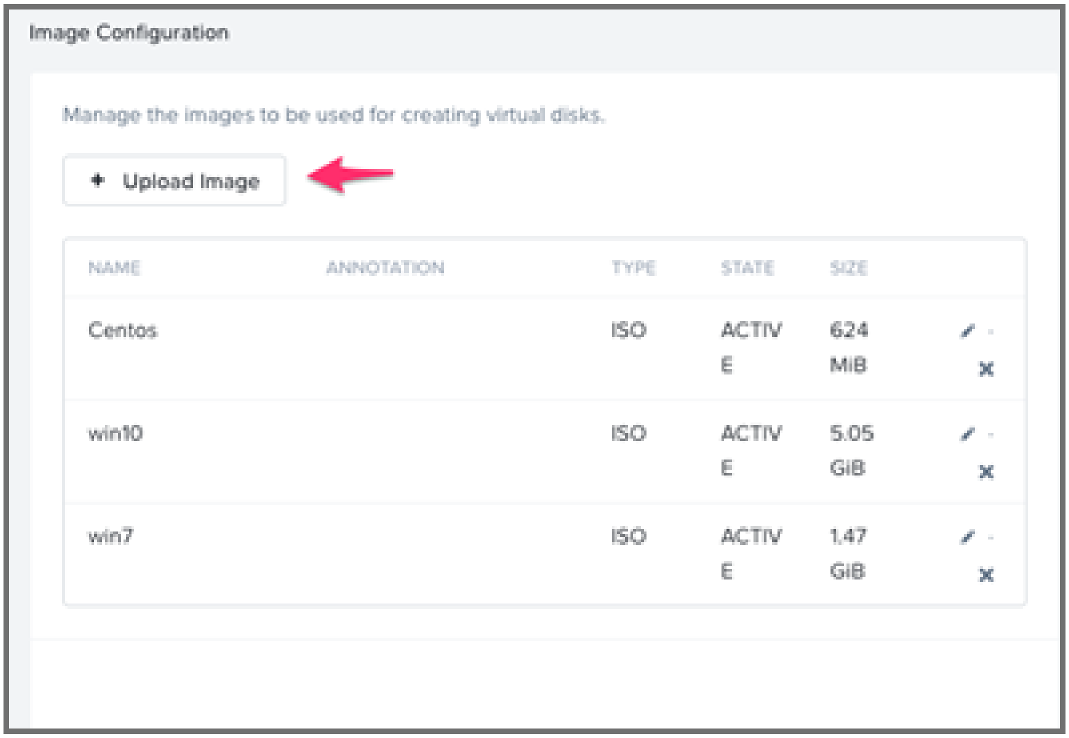


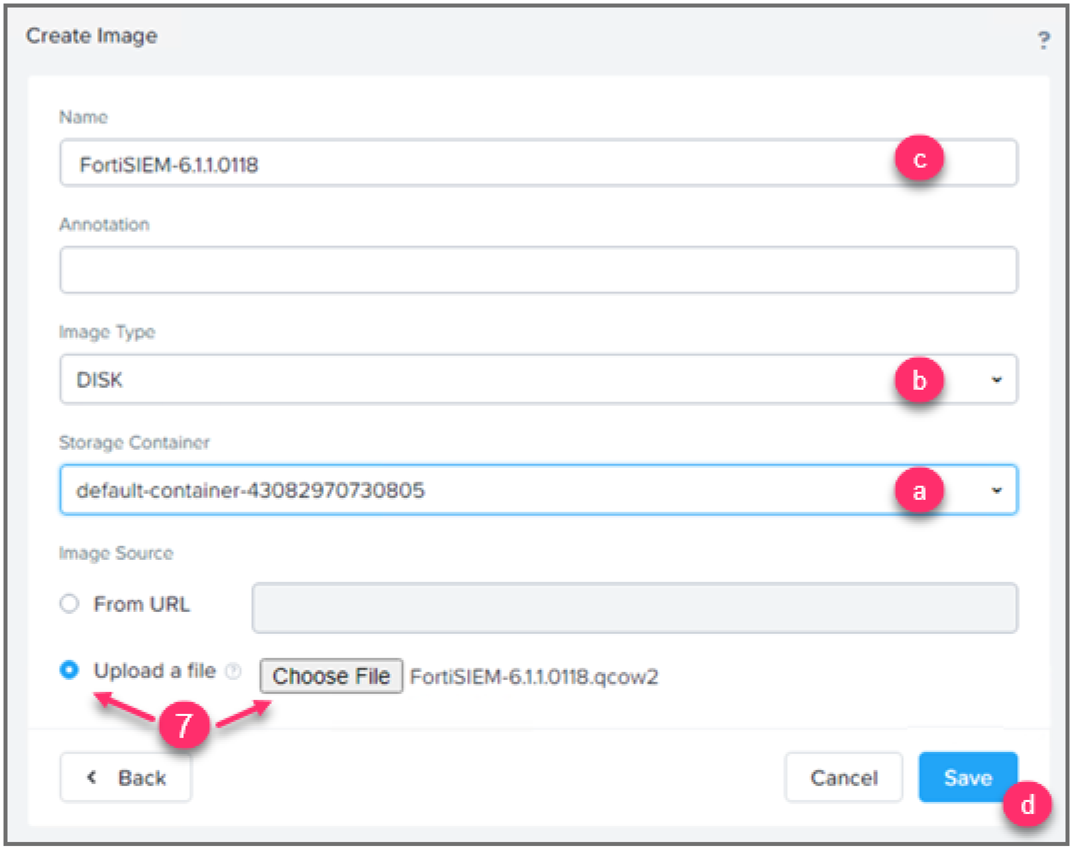
Image Configuration

Manage the images to be used for creating virtual disks.

NAME	ANNOTATION	TYPE	STATE	SIZE
Centos		ISO	ACTIVE	624 MiB
win10		ISO	ACTIVE	5.05 GiB
win7		ISO	ACTIVE	1.47 GiB

7. Select Upload a file, click on Choose File, and browse to the `FortiSIEM-6.1.1.0118.qcow2` file.
   a. From the **Storage Container** drop-down list, select a storage container.
   b. From the **Image Type** drop-down list, select **DISK**.
   c. In the **Name** field, provide the name of the image.
   d. Click **Save**.

e. Wait for the image upload to complete before proceeding to the next step.



Create Image ?

Name: FortiSIEM-6.1.1.0118

Annotation:

Image Type: DISK

Storage Container: default-container-43082970730805

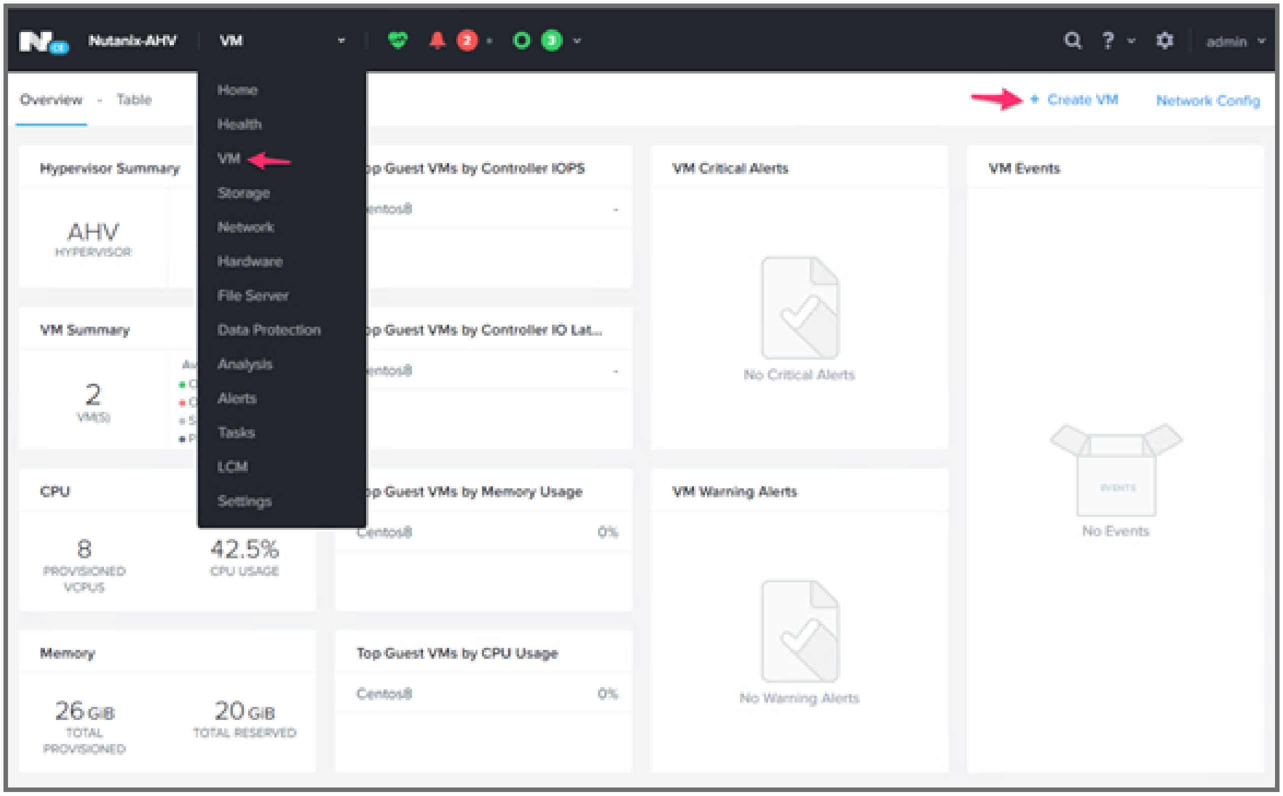
Image Source

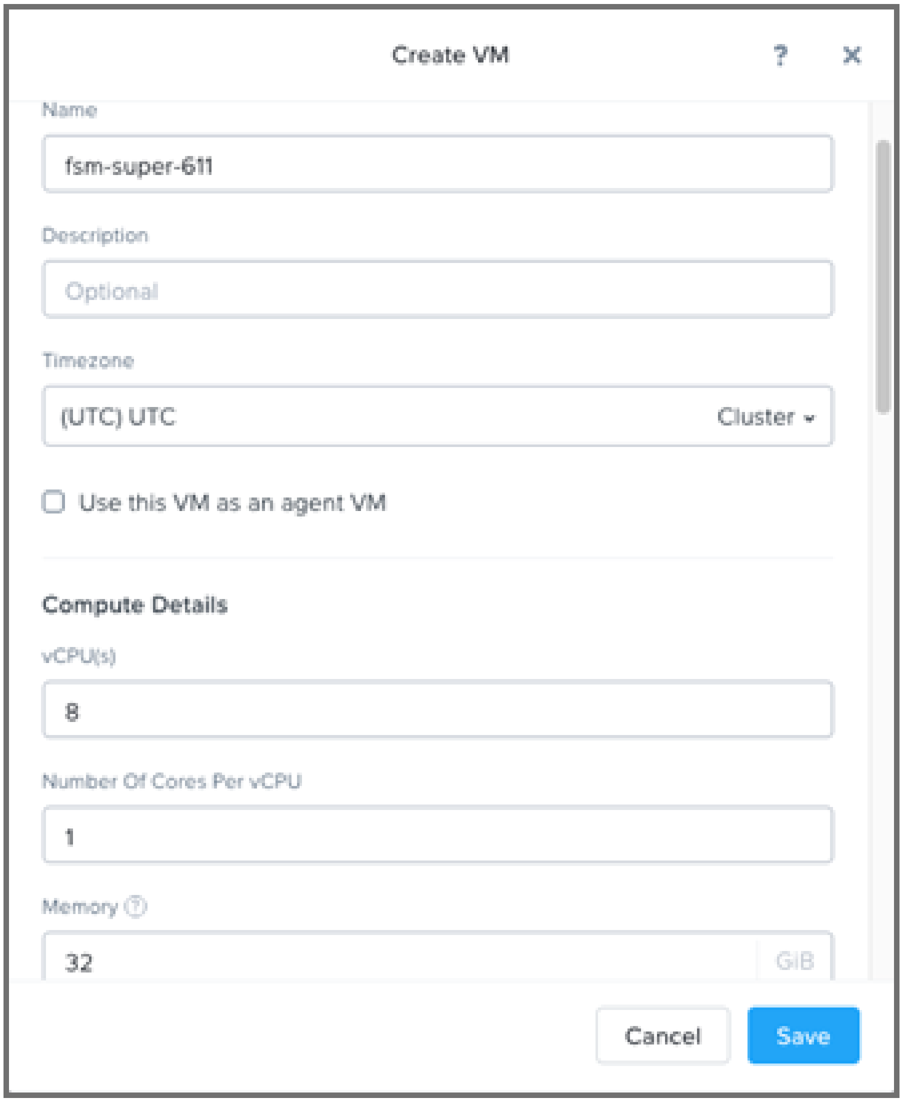
○ From URL

● Upload a file Choose File FortiSIEM-6.1.1.0118.qcow2

< Back Cancel Save

8. Navigate to **VM > Create VM**.





Create VM

Name

fsm-super-611

Description

Optional

Timezone

(UTC) UTC

Cluster

□ Use this VM as an agent VM

Compute Details

vCPU(s)

8

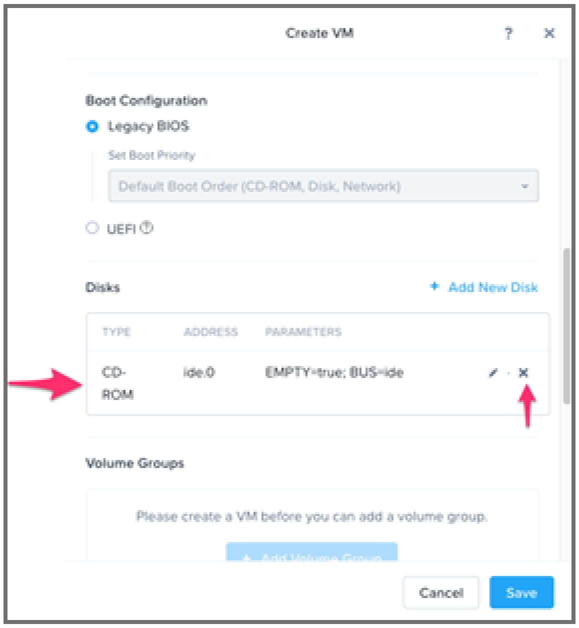
Number Of Cores Per vCPU

1

Memory

32 GiB

9. Scroll down in the Create VM window, continue to select Legacy BIOS, and at CD-ROM, click "X" to remove.



Boot Configuration

● Legacy BIOS

Set Boot Priority: Default Boot Order (CD-ROM, Disk, Network)

○ UEFI

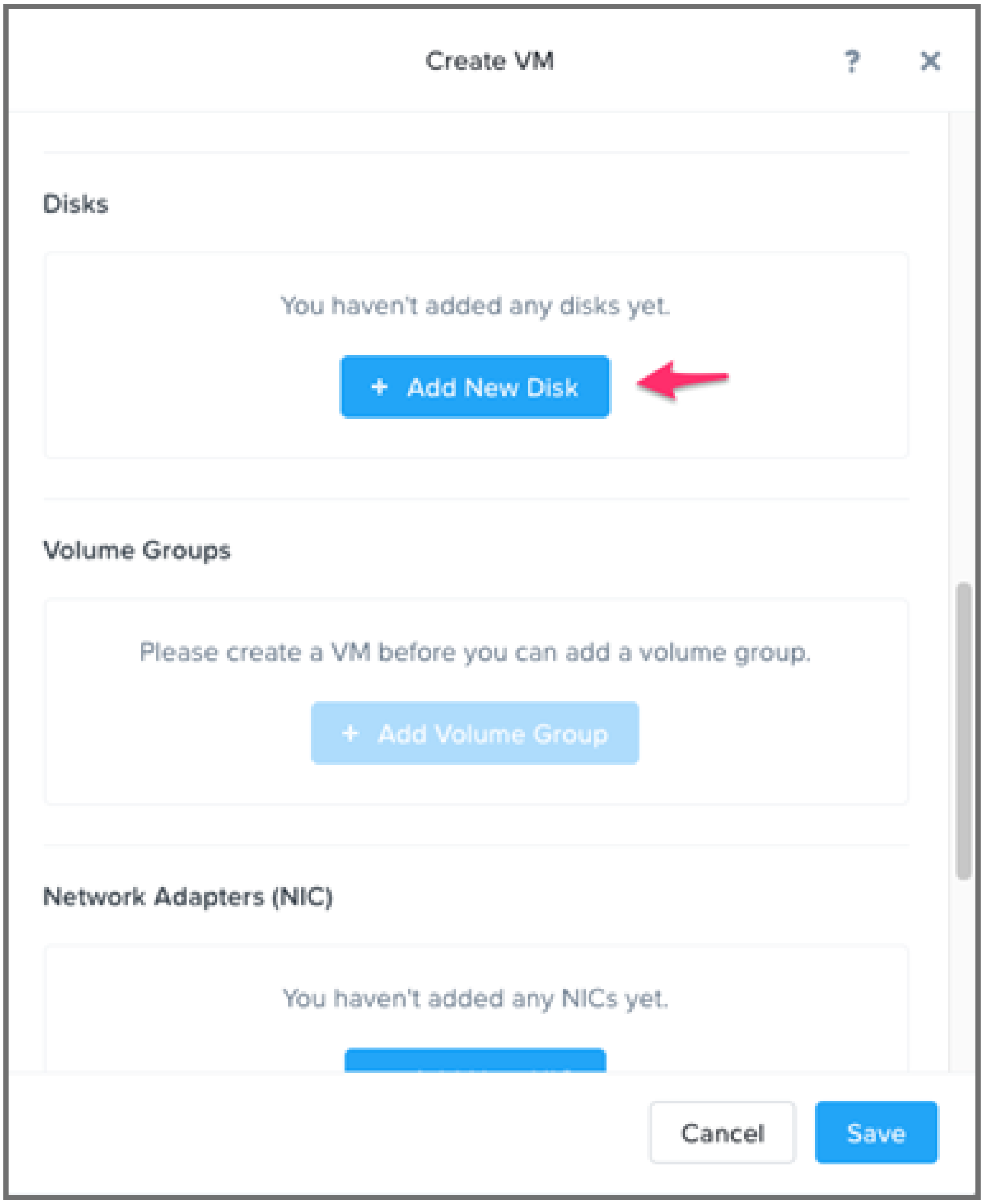
Disks

TYPE	ADDRESS	PARAMETERS
CD-ROM	ide.0	EMPTY=true; BUS=ide

Volume Groups

Please create a VM before you can add a volume group.

10. Click **Add New Disk**.



Create VM

Disks

You haven't added any disks yet.

Volume Groups

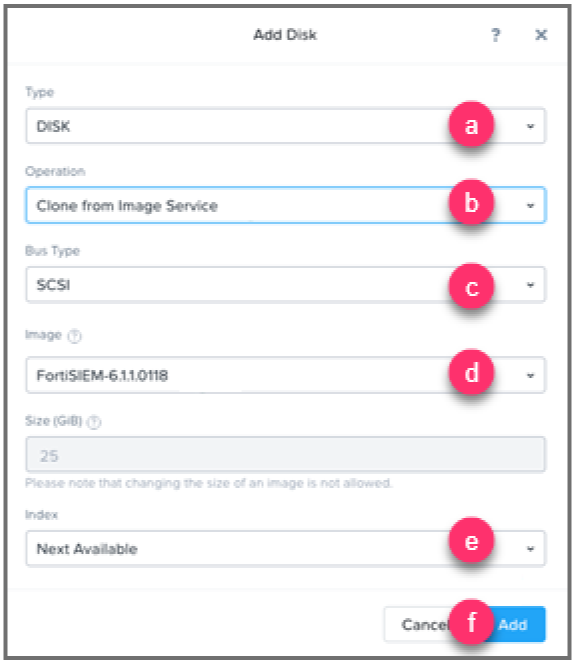
Please create a VM before you can add a volume group.

Network Adapters (NIC)

You haven't added any NICs yet.

11. In the **Add Disk** dialog, take the following steps:
    a. From the **Type** drop-down list, select **DISK**.
    b. From the **Operation** drop-down list, select **Clone from Image Service**.
    c. From the **Bus Type** drop-down list, select **SCSI**.
    d. From the **Image** drop-down list, select the FortiSIEM image you created earlier (`FortiSIEM-6.1.1.0118`).
    e. From the **Index** drop-down list, select **Next Available.**

f. Click **Add**.



Add Disk

Type: DISK

Operation: Clone from Image Service

Bus Type: SCSI

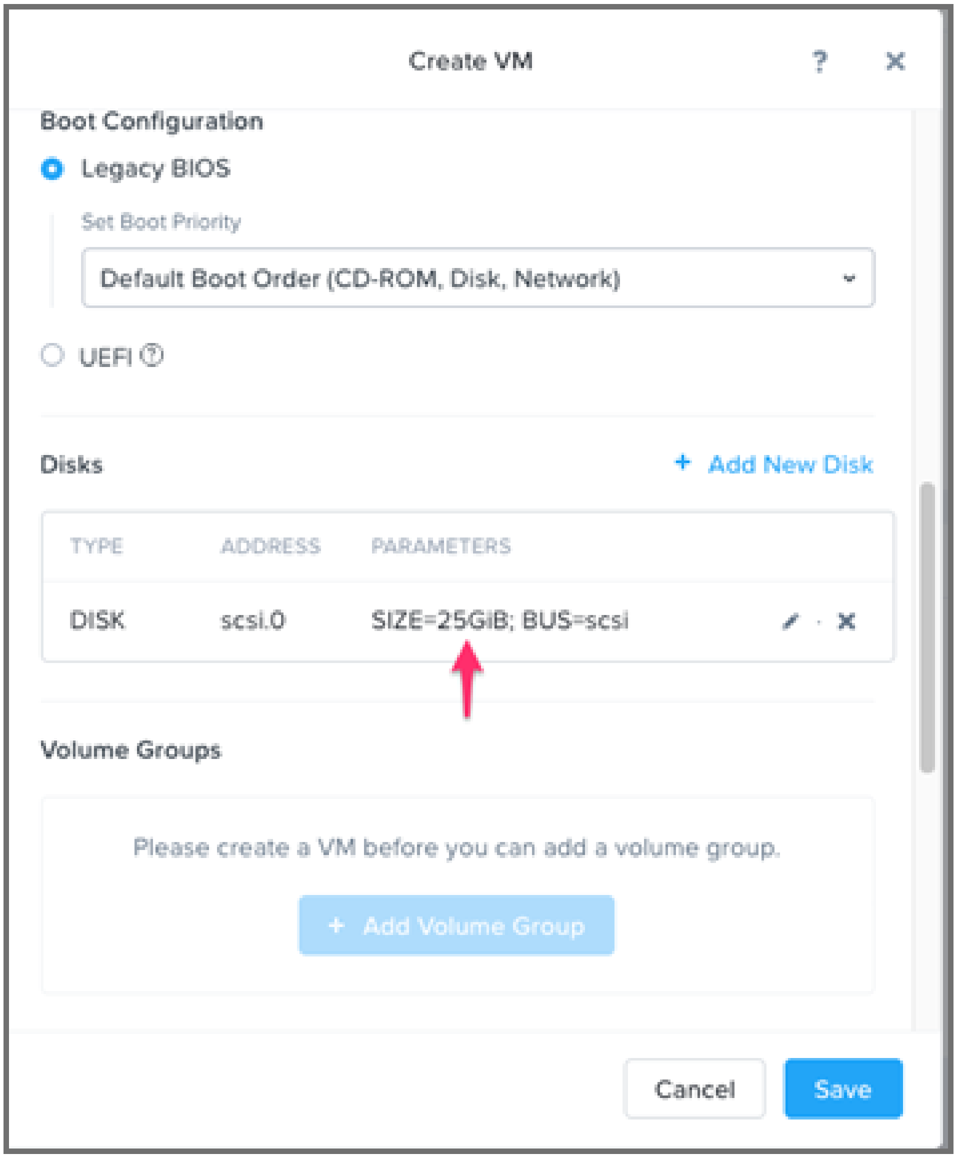
Image: FortiSIEM-6.1.1.0118

Size (GiB): 25

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

Index: Next Available

You will now see the OS disk 25GiB in the list of disks shown.



Create VM

Boot Configuration

● Legacy BIOS

Set Boot Priority

Default Boot Order (CD-ROM, Disk, Network)

○ UEFI

Disks

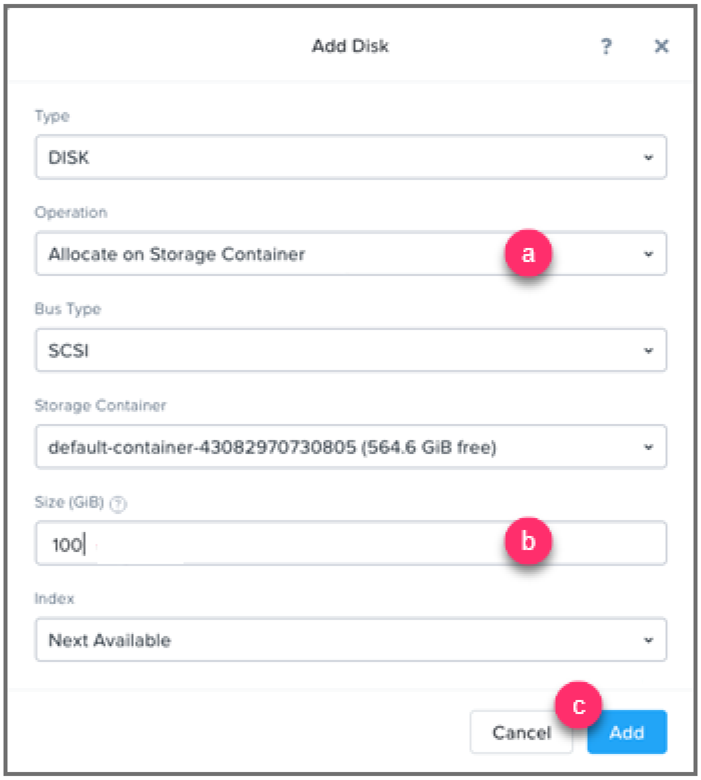
TYPE	ADDRESS	PARAMETERS
DISK	scsi.0	SIZE=25GiB; BUS=scsi

Volume Groups

Please create a VM before you can add a volume group.

12. For the Supervisor, you will need to add the 100GB /opt disk. Click **Add New Disk**, and take the following steps:
    a. From the **Operation** drop-down list, select **Allocate on Storage Container**.
    b. In the **Size (GiB)** field, enter "100".

c. Click **Add**.



Add Disk

Type: DISK

Operation: Allocate on Storage Container

Bus Type: SCSI

Storage Container: default-container-43082970730805 (564.6 GiB free)

Size (GiB): 100

Index: Next Available

13. Similar to the previous step, add an extra two disks by taking the following steps **twice**:
    a. Click **Add New Disk** for each new disk.
    b. In the **Size** field, enter "60".
    c. From the **Operation** drop-down list, select **Allocate on Storage Container**.
    d. Click **Add**.

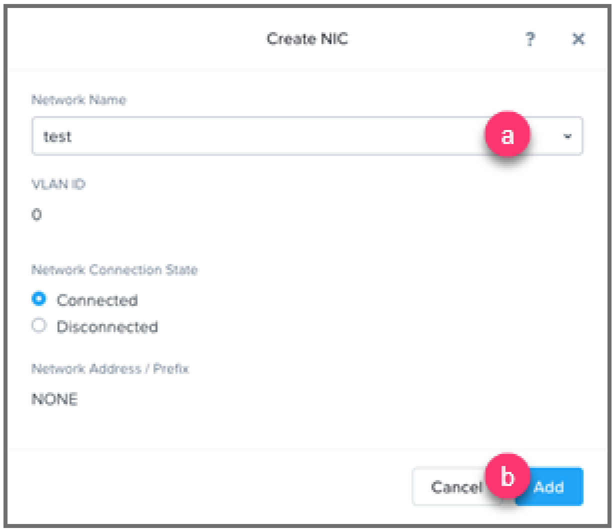
Disk	Size	Disk Name
Hard Disk 2	100GB	/opt For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.
Hard Disk 3	60GB	/cmdb
Hard Disk 4	60GB	/svn
Hard Disk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

Note on Hard Disk 5:

- Add a 5th disk if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.

- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the FortiSIEM Sizing Guide for additional information.
- NFS or Elasticsearch event DB storage is mandatory for multi-node cluster deployments.

14. Click on **Add New NIC**, and take the following steps:
    a. From the **Network Name** drop-down list, select the correct network.
    b. Click **Add**.
    c. Click **Save**.



Create NIC

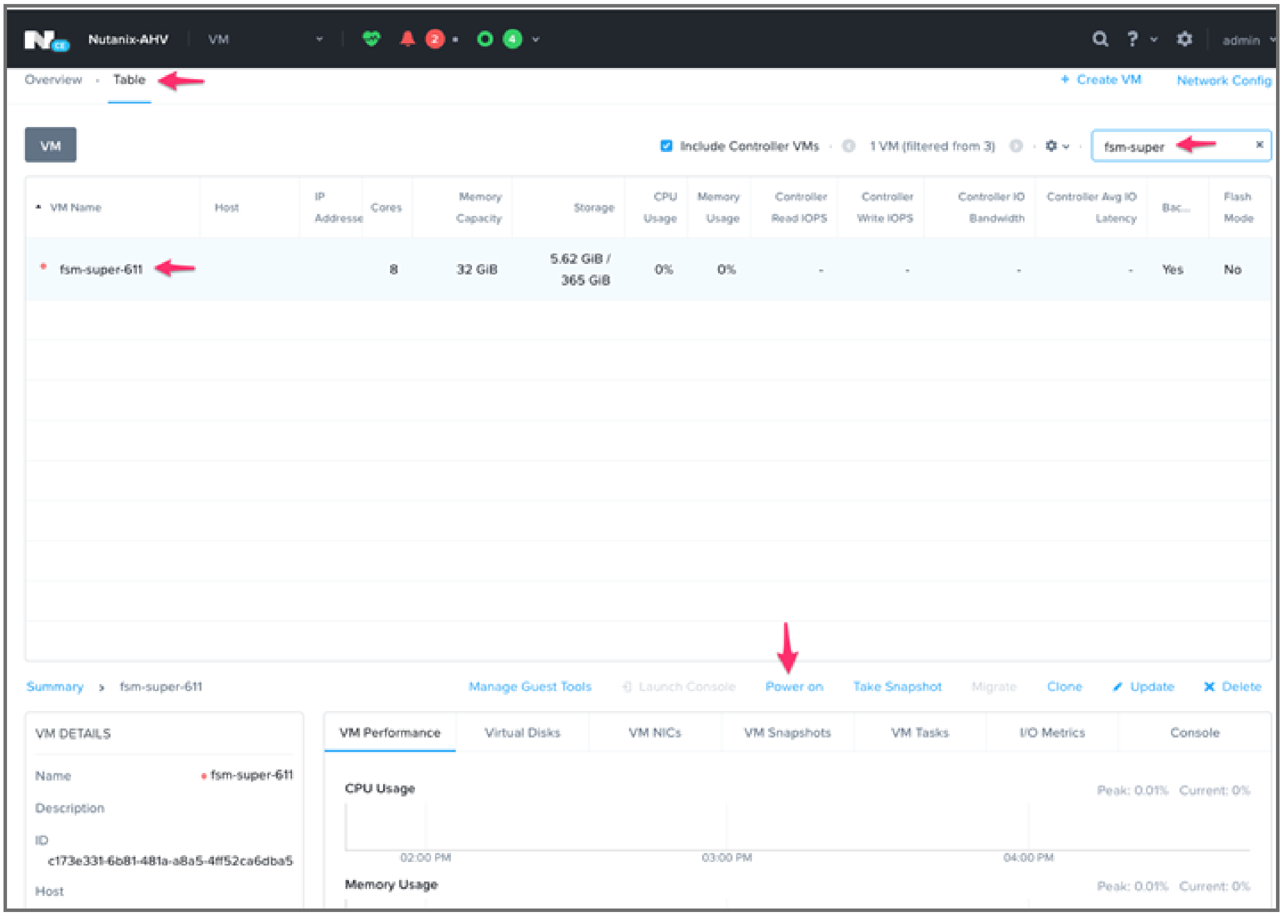
Network Name: test

VLAN ID: 0

Network Connection State
● Connected
○ Disconnected

Network Address / Prefix: NONE

15. Navigate to **VM > Table** to find your newly created fsm-super-6## VM, then click **Power On**.



VM Name	Host	IP Addresse	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth	Controller Avg IO Latency	Bac...	Flash Mode
fsm-super-611			8	32 GiB	5.62 GiB / 365 GiB	0%	0%	-	-	-	-	Yes	No

VM DETAILS

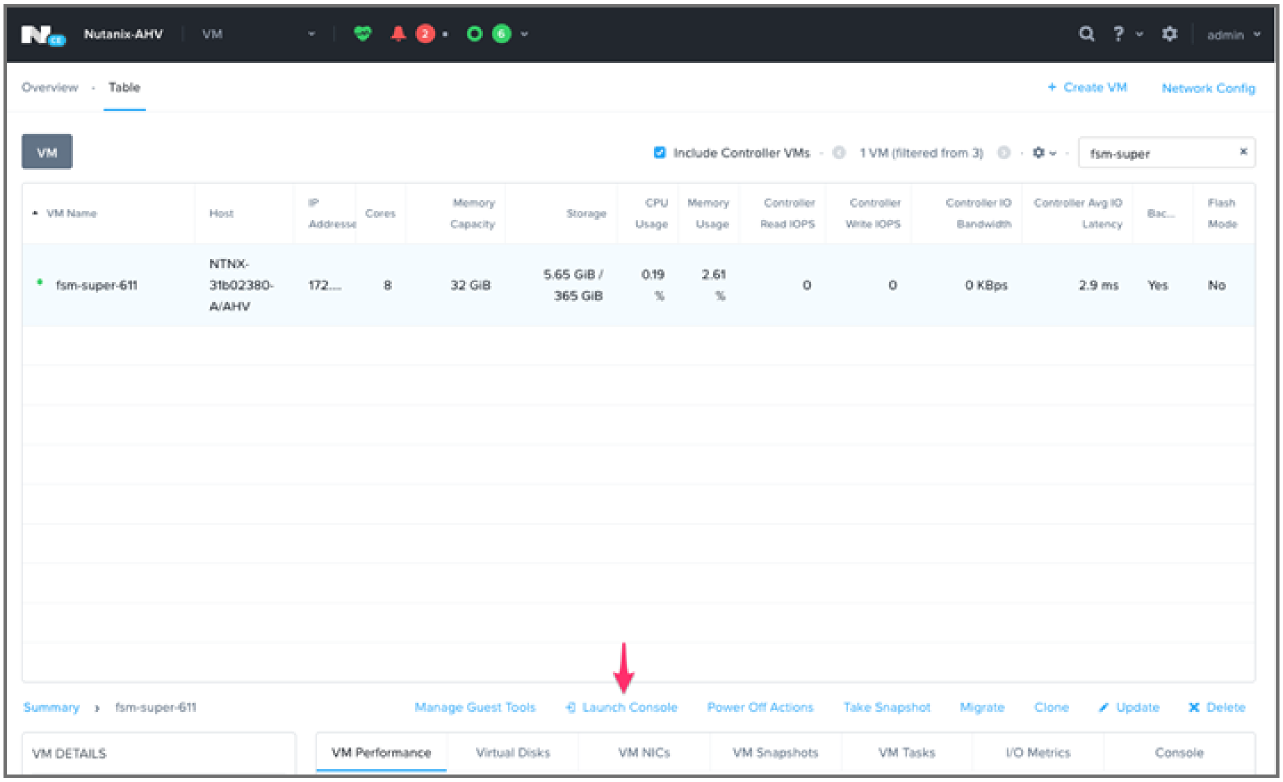
Name fsm-super-611

Description

ID c173e331-6b81-481a-a8a5-4ff52ca6dba5

Host

16. Click on **Launch Console** to open the console.



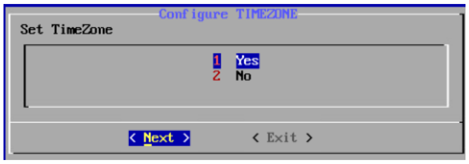
VM Name	Host	IP Addresse	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth	Controller Avg IO Latency	Bac...	Flash Mode
fsm-super-611	NTNX-31b02380-A/AHV	172....	8	32 GiB	5.65 GiB / 365 GiB	0.19 %	2.61 %	0	0	0 KBps	2.9 ms	Yes	No

17. After the VM has booted up to the login prompt, log in with the default login credentials:
    User: `root`
    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 via GUI

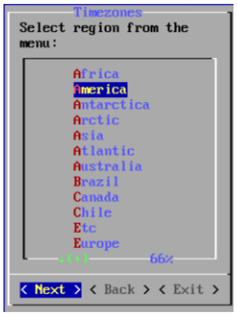
Follow these steps to configure FortiSIEM by using a simple GUI.

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.**



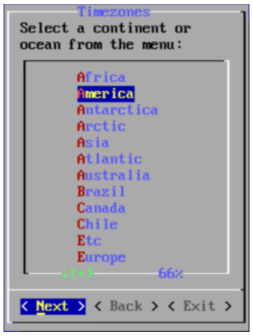
```
Configure TIMEZONE
Set TimeZone
        1  Yes
        2  No
   < Next >        < Exit >
```

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



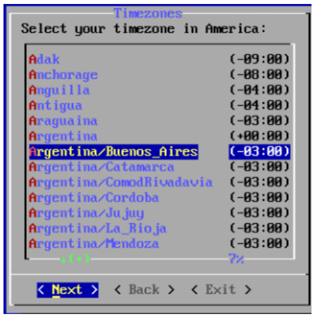
```
Timezones
Select region from the
menu:

      Africa
      America
      Antarctica
      Arctic
      Asia
      Atlantic
      Australia
      Brazil
      Canada
      Chile
      Etc
      Europe
   v(+)        66%

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

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



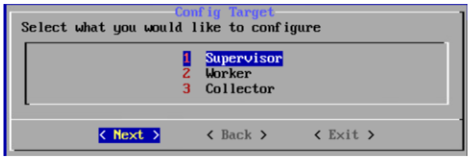
```
Timezones
Select a continent or
ocean from the menu:

      Africa
      America
      Antarctica
      Arctic
      Asia
      Atlantic
      Australia
      Brazil
      Canada
      Chile
      Etc
      Europe
   v(+)        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)
      v(+)                   7%

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

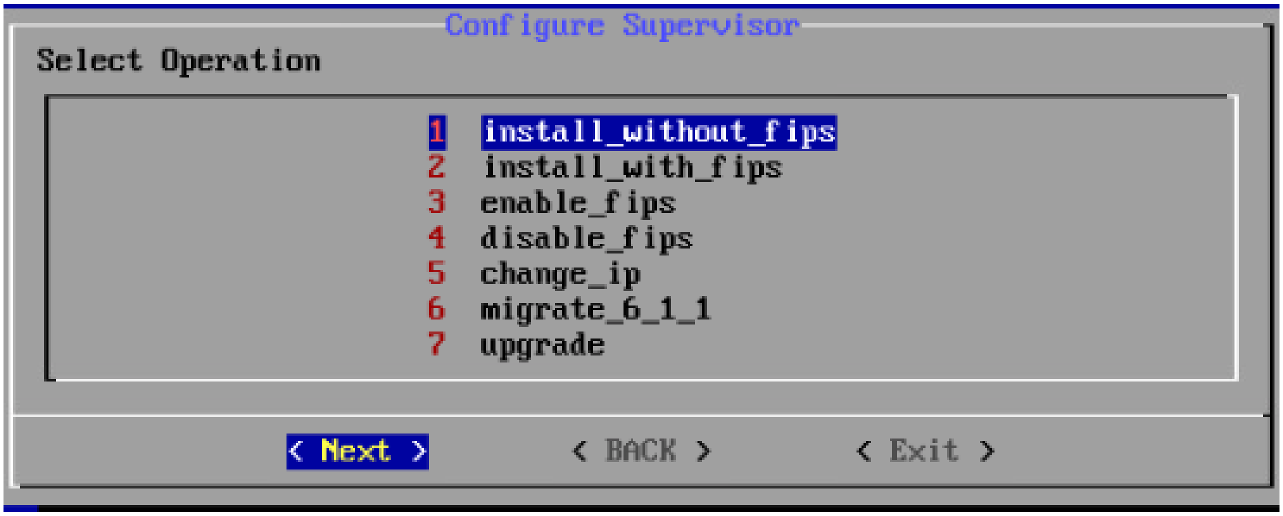
7. Select **1 Supervisor**. Press **Next.**



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

                 1  Supervisor
                 2  Worker
                 3  Collector

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

Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

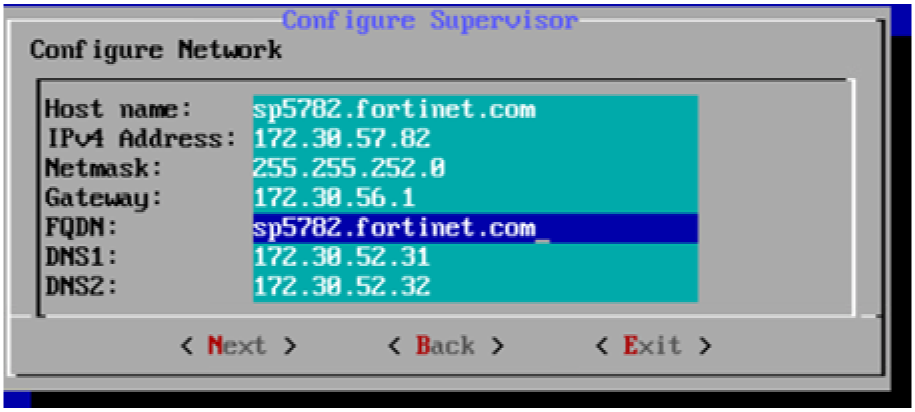
8. If you want to enable FIPS, then choose **2.** Otherwise, choose **1.** You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.



```
Configure Supervisor
Select Operation

  1  install_without_fips
  2  install_with_fips
  3  enable_fips
  4  disable_fips
  5  change_ip
  6  migrate_6_1_1
  7  upgrade
```

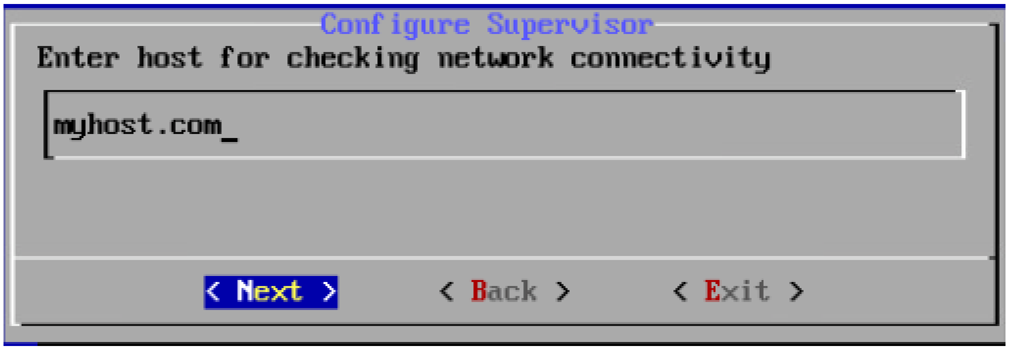
9. Configure the network by entering the following fields. Press **Next**.

Option	Description
Host Name	The Supervisor's host name
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS servers



```
Configure Supervisor
Configure Network

Host name:     sp5782.fortinet.com
IPv4 Address:  172.30.57.82
Netmask:       255.255.252.0
Gateway:       172.30.56.1
FQDN:          sp5782.fortinet.com_
DNS1:          172.30.52.31
DNS2:          172.30.52.32
```

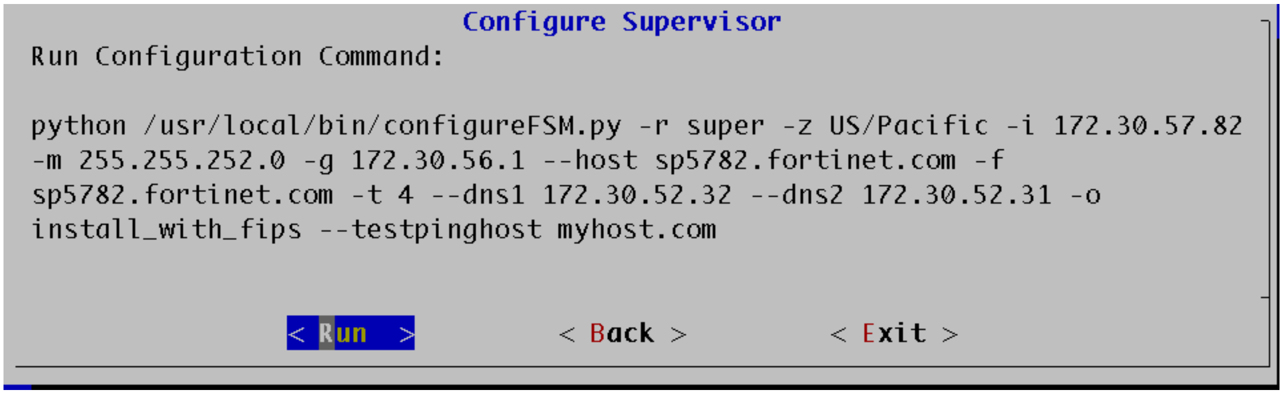
10. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.



Enter host for checking network connectivity

```
myhost.com_
```

11. 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 US/Pacific -i 172.30.57.82
-m 255.255.252.0 -g 172.30.56.1 --host sp5782.fortinet.com -f
sp5782.fortinet.com -t 4 --dns1 172.30.52.32 --dns2 172.30.52.31 -o
install_with_fips --testpinghost myhost.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
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either **4** (for **ipv4**) or **6** (for **v6**) **Note:** the **6** value is not currently supported.
--dns1, --dns2	Addresses of the DNS servers
-o	Installation option (**install_without_fips**, **install_with_fips**, **enable_fips**, **disable_fips**, **migrate_6_1_0**, or **change_ip**)
-z	Time zone. Possible values are **US/Pacific**, **Asia/Shanghai**, **Europe/London**, or

Option	Description
	Africa/Tunis
--testpinghost	The URL used to test connectivity

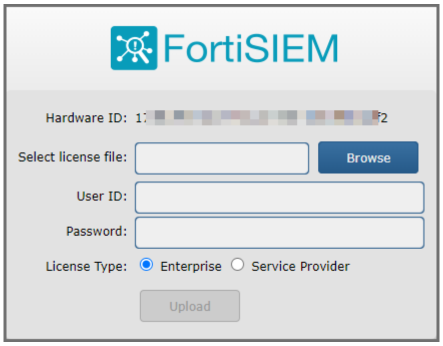
12. It will take some time for this process to finish. When it is done, proceed to Upload the FortiSIEM License. If the VM fails, you can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` to try and identify the problem.

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.
2. The License Upload dialog box will open.



FortiSIEM

Hardware ID: [redacted]

Select license file: Browse

User ID:

Password:

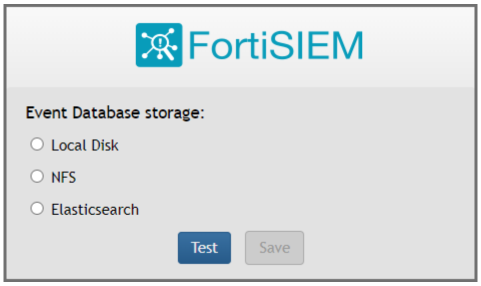
License Type: ● Enterprise ○ Service Provider

Upload

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.
6. Proceed to Choose an Event Database.

Choose an Event Database

For a fresh installation, you will be taken to the Event Database Storage page. You will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options. For more details, see Configuring Storage.



Event Database storage:

○ Local Disk

○ NFS

○ Elasticsearch

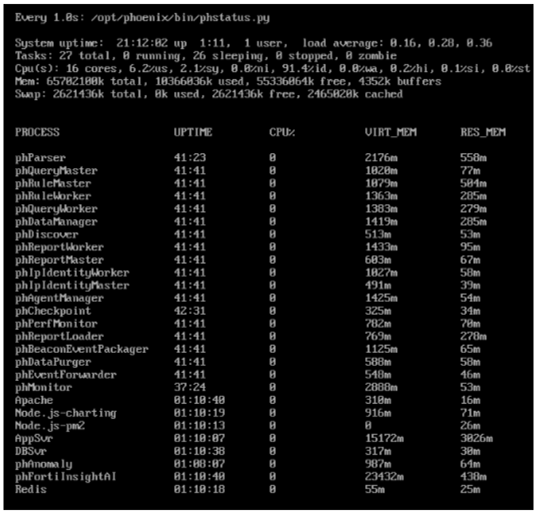
After the License has been uploaded, and the Event Database Storage setup is configured, FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

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
```

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           270m
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         430m
Redis                     01:10:18       0              55m            25m
```

Cluster Installation

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

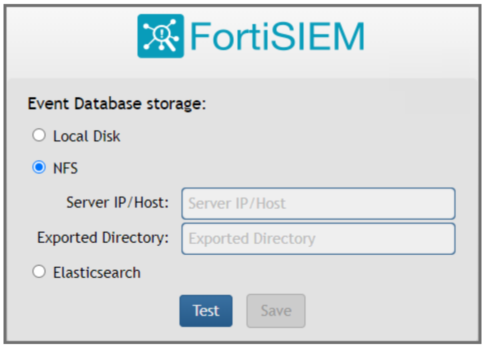
- Install Supervisor
- Install Workers
- Register Workers
- Install Collectors
- Register Collectors

Install Supervisor

Follow the steps in All-in-one Install with two differences:

- Setting up hardware - you do not need an event database.
- Setting up an Event database - Configure the cluster for either NFS or Elasticsearch.

NFS



FortiSIEM

Event Database storage:

○ Local Disk

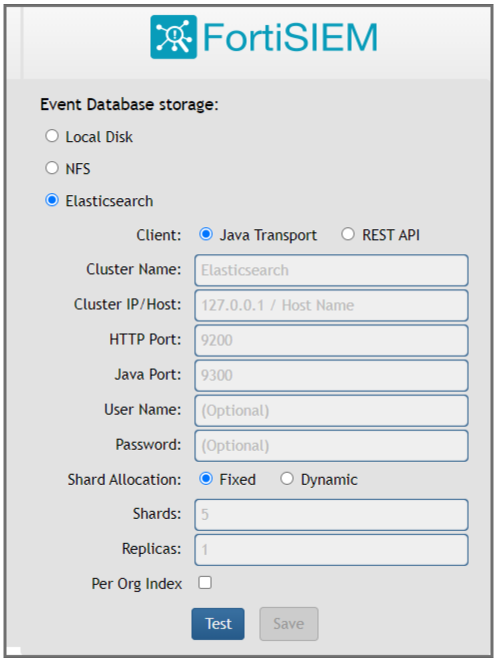
● NFS

Server IP/Host: Server IP/Host

Exported Directory: Exported Directory

○ Elasticsearch

Elasticsearch



FortiSIEM

Event Database storage:

○ Local Disk

○ NFS

● Elasticsearch

Client: ● Java Transport ○ REST API

Cluster Name: Elasticsearch

Cluster IP/Host: 127.0.0.1 / Host Name

HTTP Port: 9200

Java Port: 9300

User Name: (Optional)

Password: (Optional)

Shard Allocation: ● Fixed ○ Dynamic

Shards: 5

Replicas: 1

Per Org Index □

You must choose external storage listed in Choose an Event Database.

Install Workers

Once the Supervisor is installed, follow the same steps in All-in-one Install to install a Worker except you need to only choose OS and OPT disks. The recommended CPU and memory settings for Worker node, and required hard disk settings are:

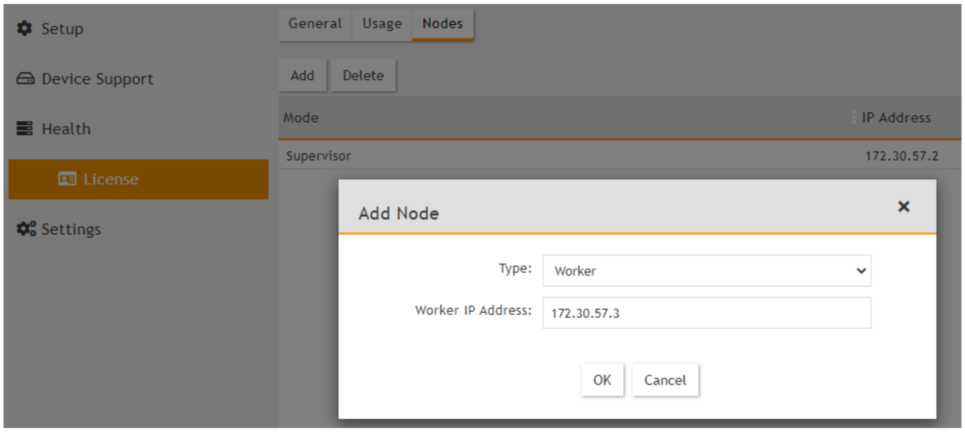
- CPU = 8
- Memory = 24 GB
- Two hard disks:
  - OS – 25GB

- 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.

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 drop-down list and enter the Worker's IP address. Click **Add**.

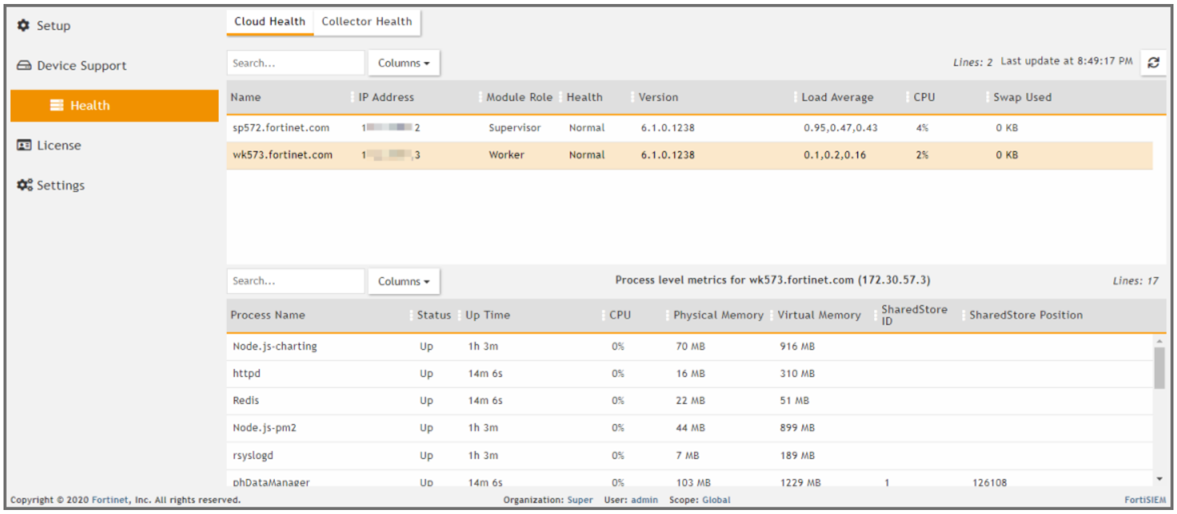


Mode	IP Address
Supervisor	172.30.57.2

Type: Worker

Worker IP Address: 172.30.57.3

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	1[redacted]2	Supervisor	Normal	6.1.0.1238	0.95,0.47,0.43	4%	0 KB
wk573.fortinet.com	1[redacted]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

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. The recommended CPU and memory settings for Collector node, and required hard disk settings 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.

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- Enterprise Deployments
- Service Provider Deployments

Enterprise Deployments

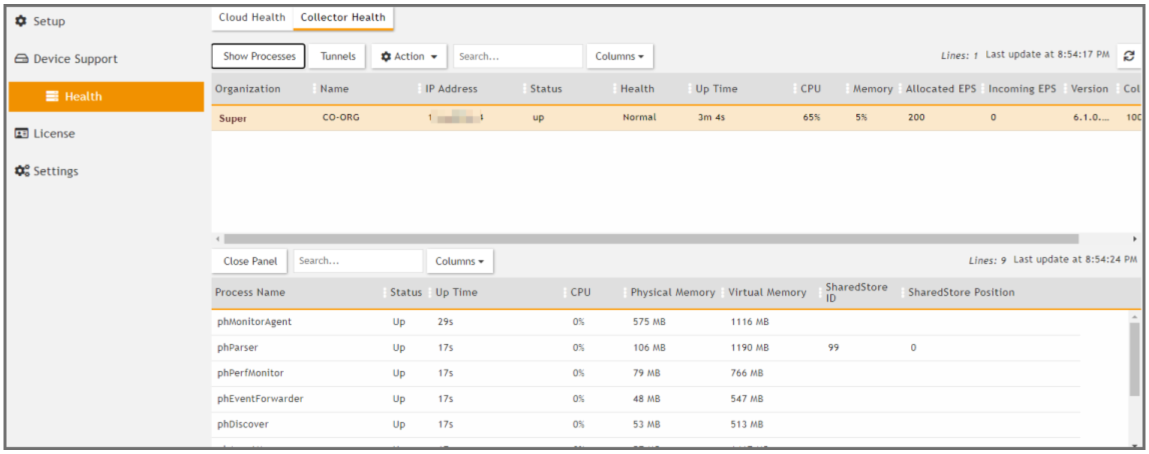
For Enterprise deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
   a. Enter the IP of the Worker node. 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 **OK**.
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	1[redacted]	up	Normal	3m 4s	65%	5%	200	0	6.1.0....	10

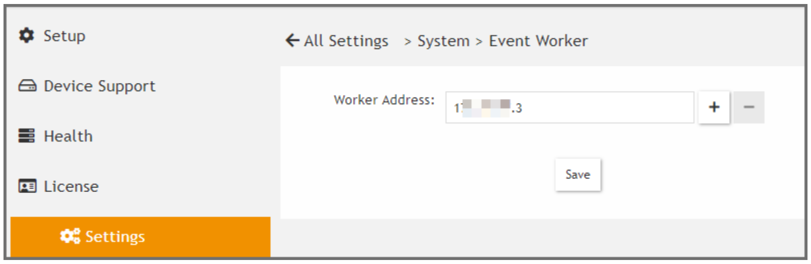
Lines: 9 Last update at 8:54:24 PM

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

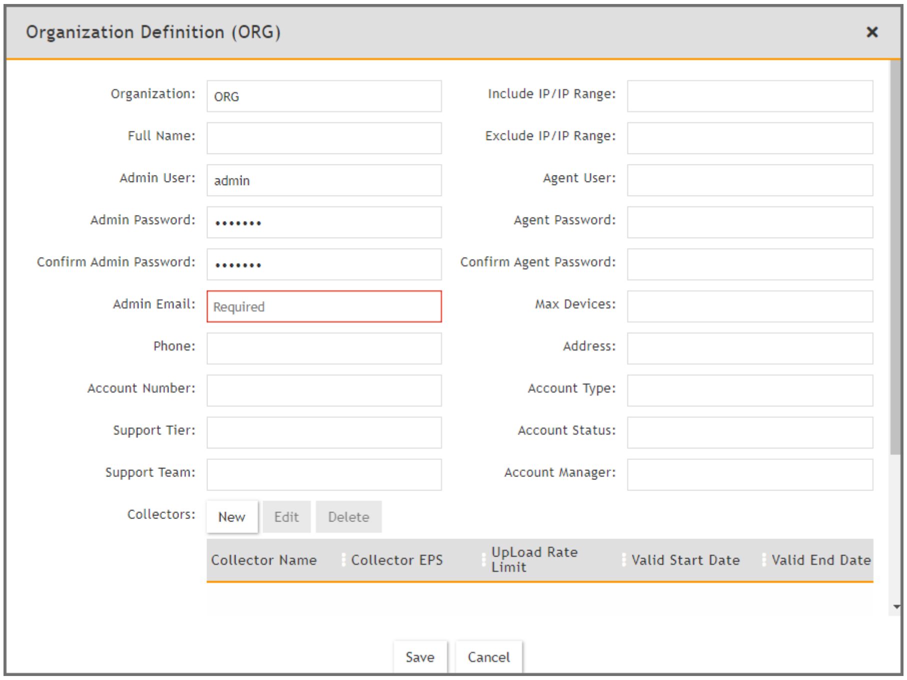
For Service Provider deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
   a. Enter the IP of the Worker node. 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 **OK**.



Worker Address: 1[redacted].3

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



Organization Definition (ORG) ×

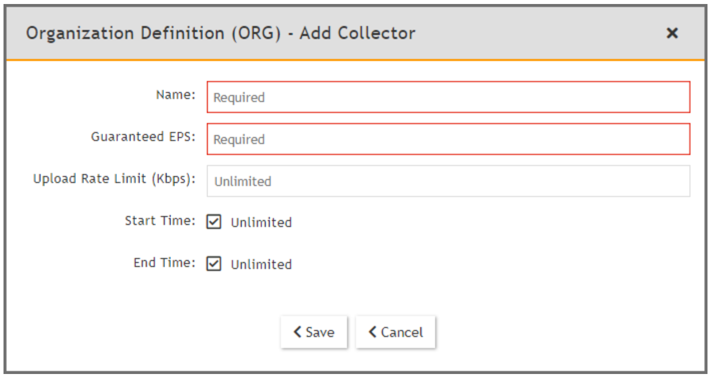
Organization:	ORG	Include IP/IP Range:	
Full Name:		Exclude IP/IP Range:	
Admin User:	admin	Agent User:	
Admin Password:	•••••••	Agent Password:	
Confirm Admin Password:	•••••••	Confirm Agent Password:	
Admin Email:	Required	Max Devices:	
Phone:		Address:	
Account Number:		Account Type:	
Support Tier: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

Collectors: New Edit Delete

Collector Name	Collector EPS	UpLoad Rate Limit	Valid Start Date	Valid End Date

Save Cancel

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

< Save < Cancel

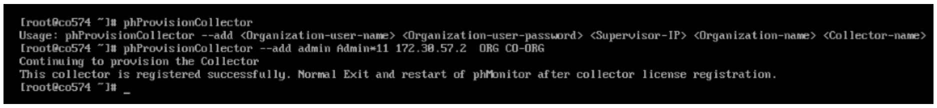
7. SSH to the Collector and run following script to register Collectors:

```
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.

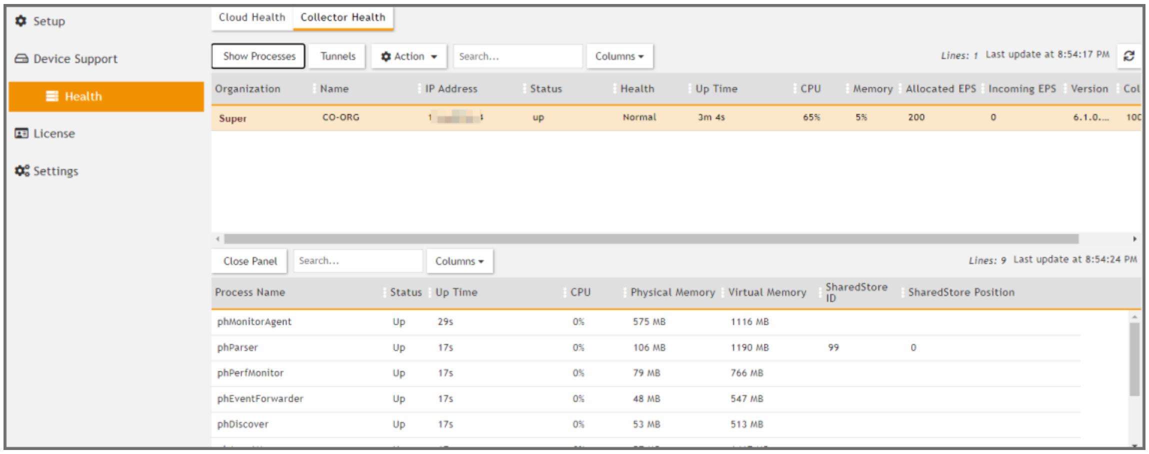
d. Set `CollectorName` from Step 6.



```
[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	[redacted]	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		

Migrating from FortiSIEM 5.3.x or 5.4.0

Migration limitations: If migrating from 5.3.3 or 5.4.0 to 6.1.1, please be aware that the following features will not be available after migration.

- Pre-compute feature
- Elastic Cloud support

If any of these features are critical to your organization, then please wait for a later version where these features are available after migration.

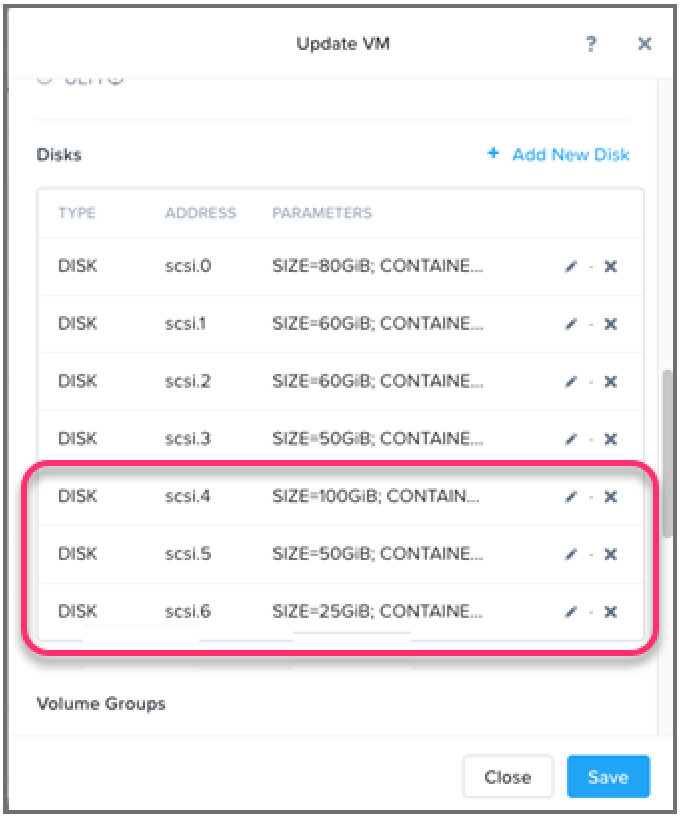
This section describes how upgrade from FortiSIEM 5.3.x or 5.4.0 to FortiSIEM 6.1.1. FortiSIEM performs migration in-place, via a bootloader. There is no need to create a new image or copy disks. The bootloader shell contains the new version of FortiSIEM.

- Pre-Migration checklist
- Migrate All-in-one Installation
- Migrate Cluster

Pre-Migration Checklist

To perform the migration, the following prerequisites must be met

1. 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.
2. Make sure you are running FortiSIEM 5.3.x or 5.4.0.
3. Take a SnapShot of the running FortiSIEM instance.
4. Delete the Worker from Super GUI.
5. Stop/Shutdown the Worker.
6. Make sure the `root` directory (`/`) has at least 1 GB of available space before proceeding.
7. Shut down the Supervisor VM.
   WARNING: Your supervisor license will become invalid after migration because the system UUID will change when you boot up a new OS disk. You will need to get the new UUID after migration and talk to Forticare to reset your license.
8. Right-click the 5.3.x or 5.4.0 FortiSIEM Supervisor VM in the Nutanix AHV Prism Console, click **Update**, and scroll down to the Disks section.
9. Add three extra hard disks and apply the changes:
   - `Hd5/100G - scsi.4`
   - `Hd6/50G/ - scsi.5`
   - `Hd7/25G - scsi.6`

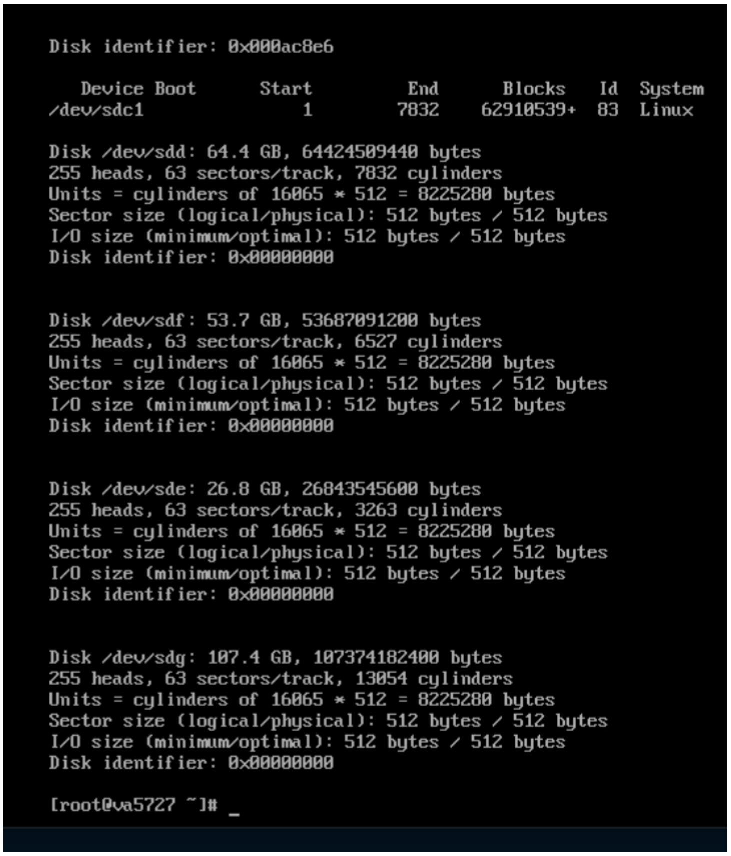


TYPE	ADDRESS	PARAMETERS
DISK	scsi.0	SIZE=80GiB; CONTAINE...
DISK	scsi.1	SIZE=60GiB; CONTAINE...
DISK	scsi.2	SIZE=60GiB; CONTAINE...
DISK	scsi.3	SIZE=50GiB; CONTAINE...
DISK	scsi.4	SIZE=100GiB; CONTAIN...
DISK	scsi.5	SIZE=50GiB; CONTAINE...
DISK	scsi.6	SIZE=25GiB; CONTAINE...

10. Log in to the console as user `root`, with password `ProspectHills`.
11. In the console, run `fisk -l`, for example:

```
# fisk -l
```

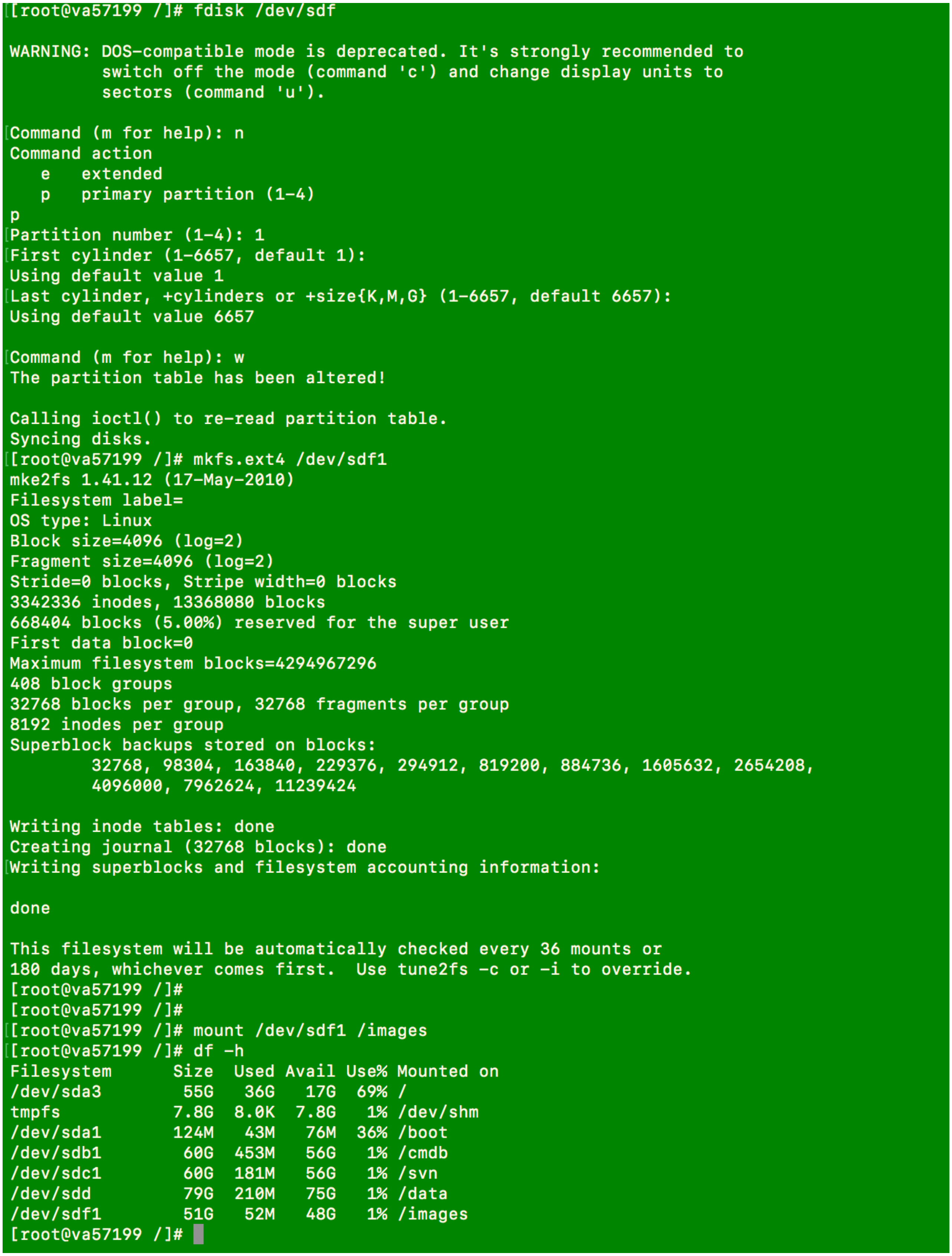
12. Note the list of the partition tables, the disk names, and their approximate sizes. You will need this information for a later step.



```
Disk identifier: 0x000ac8e6

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1        7832    62910539+  83  Linux

Disk /dev/sdd: 64.4 GB, 64424509440 bytes
255 heads, 63 sectors/track, 7832 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000


Disk /dev/sdf: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000


Disk /dev/sde: 26.8 GB, 26843545600 bytes
255 heads, 63 sectors/track, 3263 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000


Disk /dev/sdg: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

[root@va5727 ~]# _
```

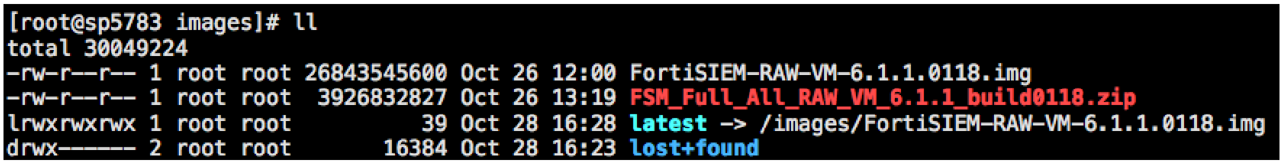
13. Mount the ~50GB disk to the `/images` directory. In the console, enter these commands and options:
    a. Enter `# fdisk /dev/<your_50GB_disk>` Press Return.
    b. Enter `n` to add a new partition. Press Return.
    c. Enter `p` to choose primary partition. Press Return.
    d. Enter `1` to choose partition number. Press Return.
    e. Press Return to accept the default.
    f. Press Return to accept the default.
    g. Enter `w` to write the table to disk and exit. Press Return.
    h. Enter the `mkfs.ext4 /dev/sdf1` command (where `sdf1` is the 50GB disk) to make a file system.
    i. Enter the `mkdir -p /images` command to create an `images` directory.
    j. Enter `mount /dev/sdf1 /images` to mount the 50GB disk to the `/images` directory.
       Or using the UUID if the disk name changed, for example

       ```
       blkid /dev/sdf1 /dev/sdf1: UUID="d4a5b82f-6e73-456b-ab08-d6e6d845d1aa" TYPE="ext4"
       mount -U d4a5b82f-6e73-456b-ab08-d6e6d845d1aa /images
       ```
14. Enter the `df -h` command to get the file system disk space usage.
    The following screen shot illustrates Steps 13 and 14.



```
[root@va57199 /]# fdisk /dev/sdf

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-6657, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-6657, default 6657):
Using default value 6657

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
[root@va57199 /]# mkfs.ext4 /dev/sdf1
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
3342336 inodes, 13368080 blocks
668404 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
408 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information:

done

This filesystem will be automatically checked every 36 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
[root@va57199 /]#
[root@va57199 /]#
[root@va57199 /]# mount /dev/sdf1 /images
[root@va57199 /]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        55G   36G   17G  69% /
tmpfs           7.8G  8.0K  7.8G   1% /dev/shm
/dev/sda1       124M   43M   76M  36% /boot
/dev/sdb1        60G  453M   56G   1% /cmdb
/dev/sdc1        60G  181M   56G   1% /svn
/dev/sdd         79G  210M   75G   1% /data
/dev/sdf1        51G   52M   48G   1% /images
[root@va57199 /]# 
```

15. Download the 6.1.1 FortiSIEM image file, `6.1.1/HW/FSM_Full_All_RAW_VM_6.1.1_build0118.zip`, from the support site and copy it to the `/images` directory.
16. Use unzip to extract the file.
    `# unzip FSM_Full_All_RAW_VM_6.1.1_build0118.zip`
    Note: The image size is about 5.5GB after extracting.
17. Create a soft link to the image folder, for example:
    `# ln -sf /images/FortiSIEM-RAW-VM-6.1.1.0118.img /images/latest`
18. Enter the `ll` command to ensure `latest` link is defined, for example:
    `# ll`



```
[root@sp5783 images]# ll
total 30049224
-rw-r--r-- 1 root root 26843545600 Oct 26 12:00 FortiSIEM-RAW-VM-6.1.1.0118.img
-rw-r--r-- 1 root root  3926832827 Oct 26 13:19 FSM_Full_All_RAW_VM_6.1.1_build0118.zip
lrwxrwxrwx 1 root root          39 Oct 28 16:28 latest -> /images/FortiSIEM-RAW-VM-6.1.1.0118.img
drwx------ 2 root root       16384 Oct 28 16:23 lost+found
```

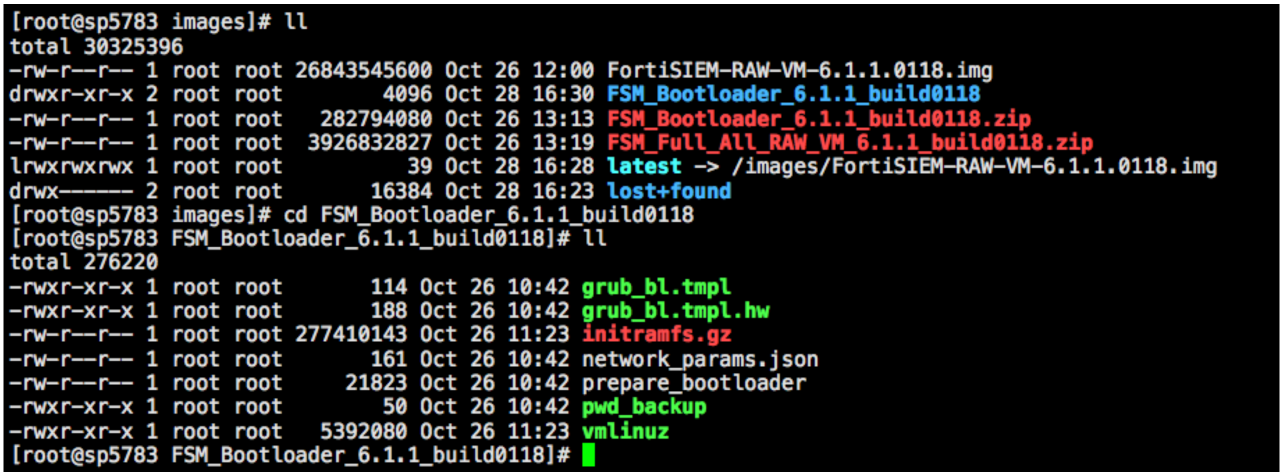
Migrate All-in-one Installation

- Download the Bootloader
- Prepare the Bootloader
- Load the FortiSIEM 6.1.1 Image
- Prepare the FortiSIEM VM for 6.1.1
- Migrate to FortiSIEM 6.1.1

Download the Bootloader

Install and configure the FortiSIEM bootloader to start migration. Follow these steps:

1. Download the bootloader `FSM_Bootloader_6.1.1_Build0118.zip` from the support site and copy it to the `/images` directory.
2. Unzip the `.zip` file, for example:
   `# unzip FSM_Bootloader_6.1.1_Build0118.zip`

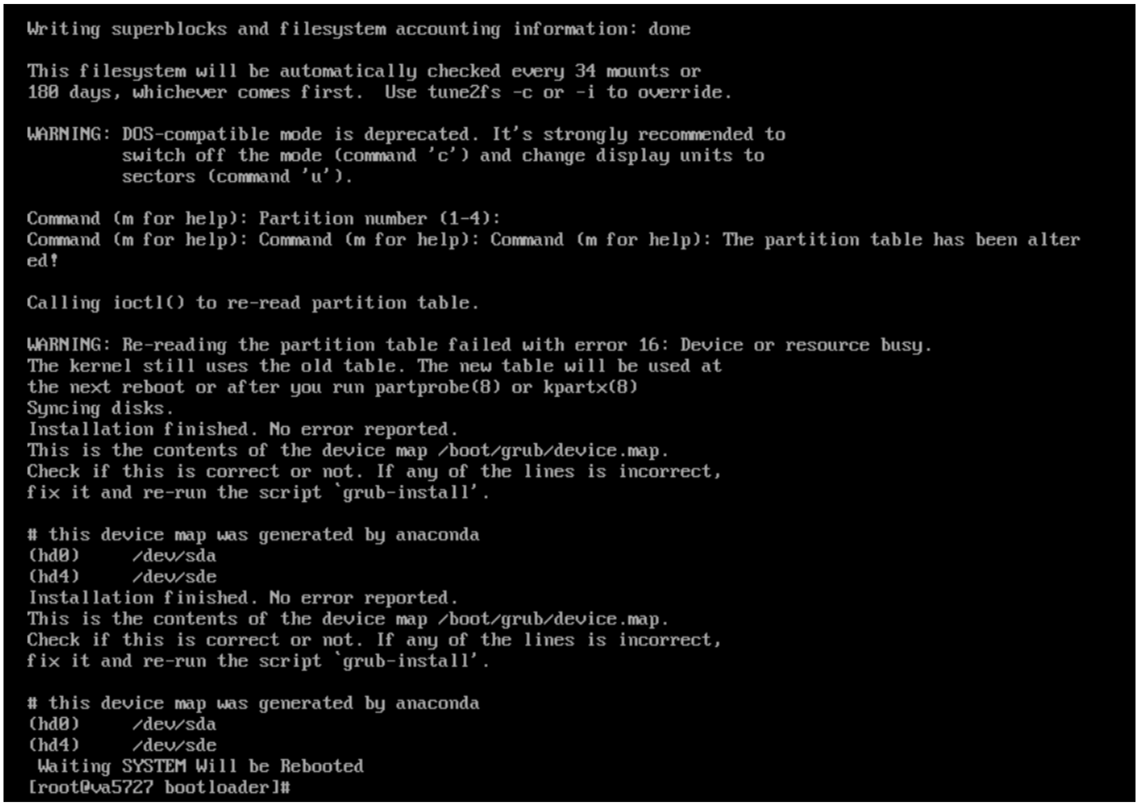


```
[root@sp5783 images]# ll
total 30325396
-rw-r--r-- 1 root root 26843545600 Oct 26 12:00 FortiSIEM-RAW-VM-6.1.1.0118.img
drwxr-xr-x 2 root root        4096 Oct 28 16:30 FSM_Bootloader_6.1.1_build0118
-rw-r--r-- 1 root root   282794080 Oct 26 13:13 FSM_Bootloader_6.1.1_build0118.zip
-rw-r--r-- 1 root root  3926832827 Oct 26 13:19 FSM_Full_All_RAW_VM_6.1.1_build0118.zip
lrwxrwxrwx 1 root root          39 Oct 28 16:28 latest -> /images/FortiSIEM-RAW-VM-6.1.1.0118.img
drwx------ 2 root root       16384 Oct 28 16:23 lost+found
[root@sp5783 images]# cd FSM_Bootloader_6.1.1_build0118
[root@sp5783 FSM_Bootloader_6.1.1_build0118]# ll
total 276220
-rwxr-xr-x 1 root root       114 Oct 26 10:42 grub_bl.tmpl
-rwxr-xr-x 1 root root       188 Oct 26 10:42 grub_bl.tmpl.hw
-rw-r--r-- 1 root root 277410143 Oct 26 11:23 initramfs.gz
-rw-r--r-- 1 root root       161 Oct 26 10:42 network_params.json
-rw-r--r-- 1 root root     21823 Oct 26 10:42 prepare_bootloader
-rwxr-xr-x 1 root root        50 Oct 26 10:42 pwd_backup
-rwxr-xr-x 1 root root   5392080 Oct 26 11:23 vmlinuz
[root@sp5783 FSM_Bootloader_6.1.1_build0118]#
```

Prepare the Bootloader

Follow these steps to run the `prepare_bootloader` script:

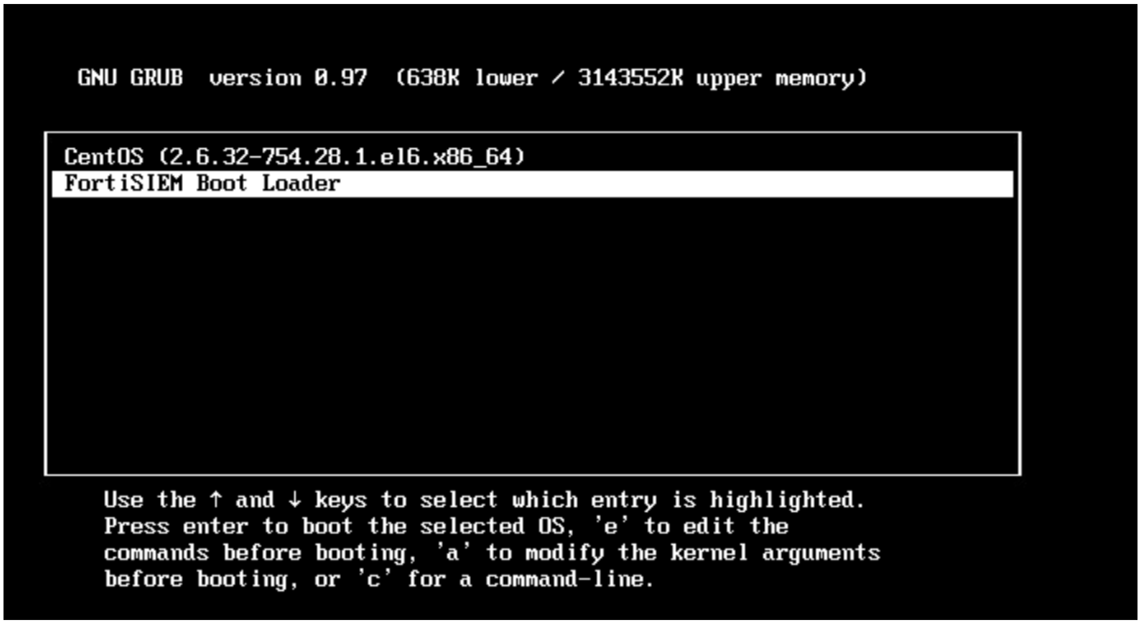
1. Go to the `bootloader` directory, for example:
   `# cd /images/FSM_Bootloader_6.1.1_build0118`
2. Run the `prepare_bootloader` script to install and configure the bootloader. This script installs, configures, and reboots the system. The script may take a few minutes to complete.
   `# sh prepare_bootloader`
3. The script will open the FortiSIEM bootloader shell.



```
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 34 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): Partition number (1-4):
Command (m for help): Command (m for help): Command (m for help): The partition table has been alter
ed!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script `grub-install'.

# this device map was generated by anaconda
(hd0)     /dev/sda
(hd4)     /dev/sde
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script `grub-install'.

# this device map was generated by anaconda
(hd0)     /dev/sda
(hd4)     /dev/sde
 Waiting SYSTEM Will be Rebooted
[root@va5727 bootloader]#
```

   Note: you might have to reboot the system manually if auto-reboot does not work.
4. Go to the console view in your Nutanix-AHV Prism Console.

5. In the FortiSIEM bootloader shell, choose **FortiSIEM Boot Loader**. Press Return.

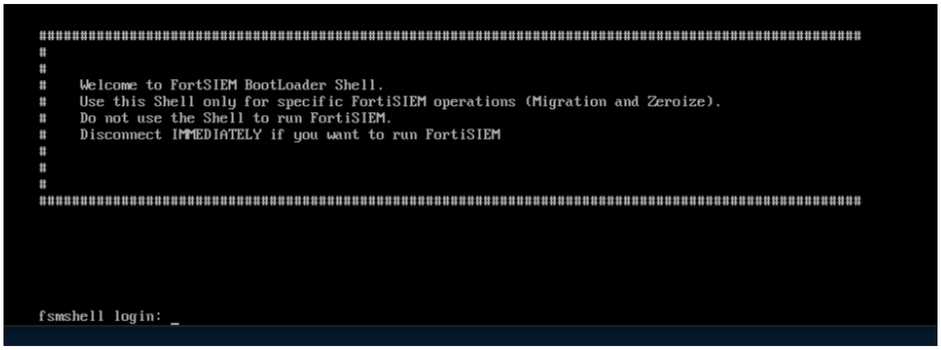


```
    GNU GRUB  version 0.97  (638K lower / 3143552K upper memory)

 CentOS (2.6.32-754.28.1.el6.x86_64)
 FortiSIEM Boot Loader

      Use the ↑ and ↓ keys to select which entry is highlighted.
      Press enter to boot the selected OS, 'e' to edit the
      commands before booting, 'a' to modify the kernel arguments
      before booting, or 'c' for a command-line.
```

Load the FortiSIEM 6.1.1 Image

Follow these steps to load the FortiSIEM image:

1. Log in to the bootloader shell as user `root` with password `ProspectHills`.



```
####################################################################################################
#
#
#    Welcome to FortSIEM BootLoader Shell.
#    Use this Shell only for specific FortiSIEM operations (Migration and Zeroize).
#    Do not use the Shell to run FortiSIEM.
#    Disconnect IMMEDIATELY if you want to run FortiSIEM
#
#
#
####################################################################################################



fsmshell login: _
```

2. Create and mount the `/images` directory:

   a. Create a `/images` directory if it is not already present, for example:
      ```
      # mkdir -p /images
      ```

   b. Mount the `sdf1` (the 50GB disk) to the `/images` directory, for example:
      ```
      # mount /dev/sdf1 /images
      ```
      Use `# fdisk -l` to find the image drive, which should be the 50GB disk.

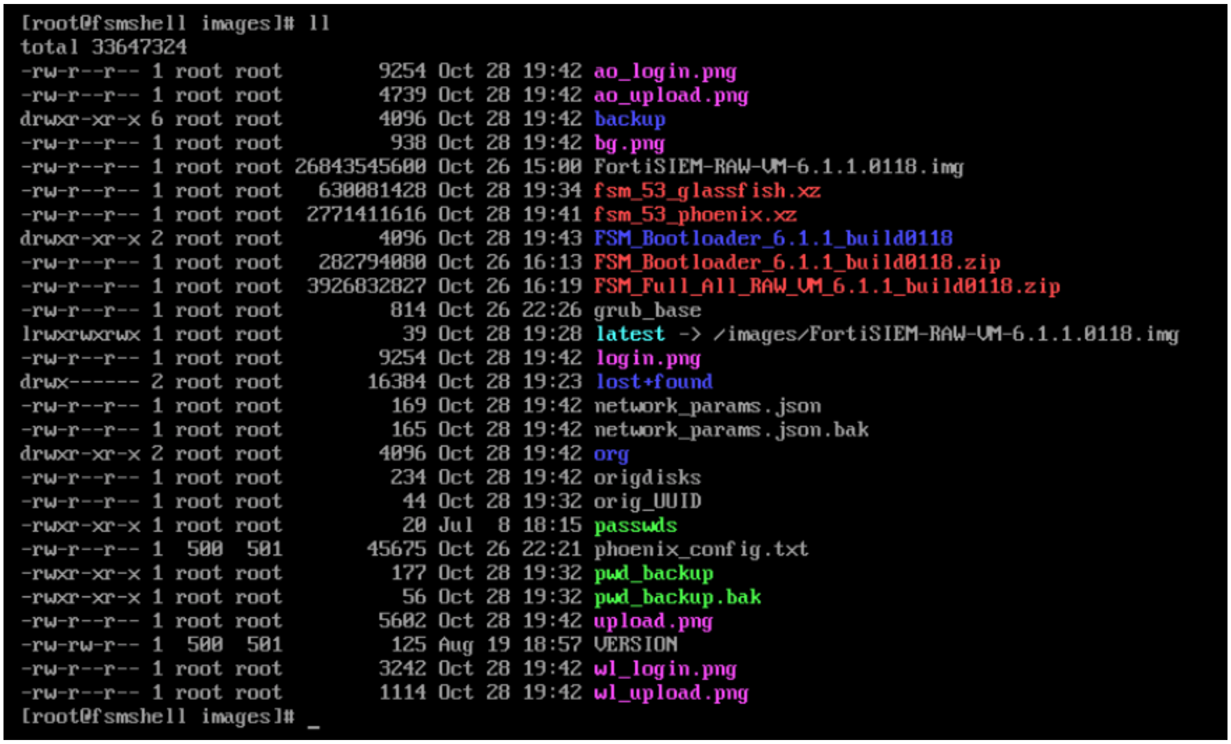
      Or using the UUID if the disk name changed, for example:

      ```
      # blkid /dev/sdf1 /dev/sdf1: UUID="d4a5b82f-6e73-456b-ab08-d6e6d845d1aa"
      TYPE="ext4"
      ```

      ```
      # mount -U d4a5b82f-6e73-456b-ab08-d6e6d845d1aa /images
      ```

   c. Change to the `/images` directory, for example:
      ```
      # cd /images
      ```

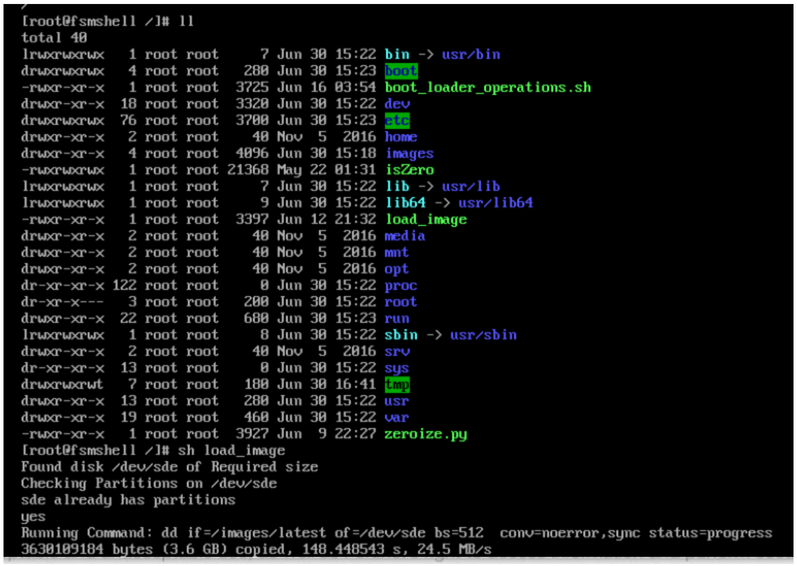
d. Run the `ll` command to check disk usage.
   `# ll`
   These steps are illustrated in the following screen shot.



```
[root@fsmshell images]# ll
total 33647324
-rw-r--r-- 1 root root        9254 Oct 28 19:42 ao_login.png
-rw-r--r-- 1 root root        4739 Oct 28 19:42 ao_upload.png
drwxr-xr-x 6 root root        4096 Oct 28 19:42 backup
-rw-r--r-- 1 root root         938 Oct 28 19:42 bg.png
-rw-r--r-- 1 root root 26843545600 Oct 26 15:00 FortiSIEM-RAW-VM-6.1.1.0118.img
-rw-r--r-- 1 root root   630081428 Oct 28 19:34 fsm_53_glassfish.xz
-rw-r--r-- 1 root root  2771411616 Oct 28 19:41 fsm_53_phoenix.xz
drwxr-xr-x 2 root root        4096 Oct 28 19:43 FSM_Bootloader_6.1.1_build0118
-rw-r--r-- 1 root root   282794080 Oct 26 16:13 FSM_Bootloader_6.1.1_build0118.zip
-rw-r--r-- 1 root root  3926832827 Oct 26 16:19 FSM_Full_All_RAW_VM_6.1.1_build0118.zip
-rw-r--r-- 1 root root         814 Oct 26 22:26 grub_base
lrwxrwxrwx 1 root root          39 Oct 28 19:28 latest -> /images/FortiSIEM-RAW-VM-6.1.1.0118.img
-rw-r--r-- 1 root root        9254 Oct 28 19:42 login.png
drwx------ 2 root root       16384 Oct 28 19:23 lost+found
-rw-r--r-- 1 root root         169 Oct 28 19:42 network_params.json
-rw-r--r-- 1 root root         165 Oct 28 19:42 network_params.json.bak
drwxr-xr-x 2 root root        4096 Oct 28 19:42 org
-rw-r--r-- 1 root root         234 Oct 28 19:42 origdisks
-rw-r--r-- 1 root root          44 Oct 28 19:32 orig_UUID
-rwxr-xr-x 1 root root          20 Jul  8 18:15 passwds
-rw-r--r-- 1  500  501       45675 Oct 26 22:21 phoenix_config.txt
-rwxr-xr-x 1 root root         177 Oct 28 19:32 pwd_backup
-rwxr-xr-x 1 root root          56 Oct 28 19:32 pwd_backup.bak
-rw-r--r-- 1 root root        5602 Oct 28 19:42 upload.png
-rw-rw-r-- 1  500  501         125 Aug 19 18:57 VERSION
-rw-r--r-- 1 root root        3242 Oct 28 19:42 wl_login.png
-rw-r--r-- 1 root root        1114 Oct 28 19:42 wl_upload.png
[root@fsmshell images]# _
```

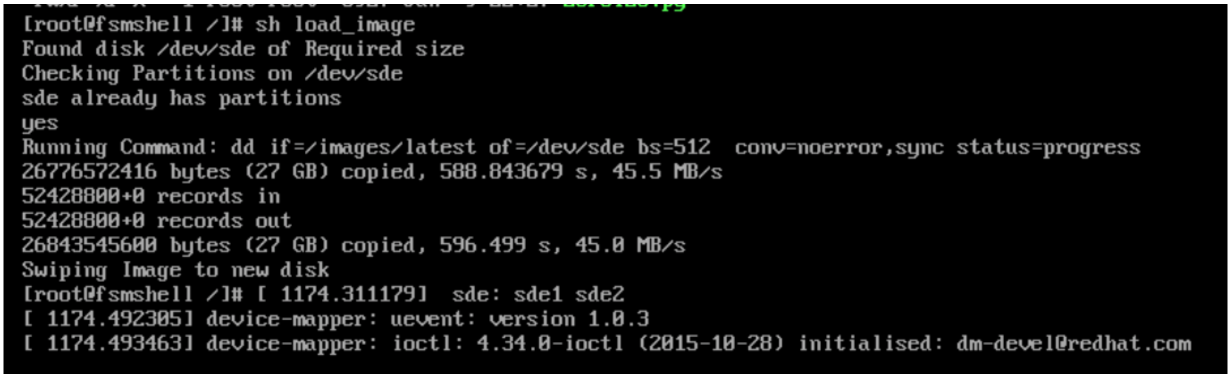
3. Run the `load_image` script to swipe the old image with the new image, for example:

   a. Change to the `root` directory and check the contents, for example:
      `# cd /`
      `# ll`



```
[root@fsmshell /]# ll
total 40
lrwxrwxrwx   1 root root     7 Jun 30 15:22 bin -> usr/bin
drwxrwxrwx   4 root root   280 Jun 30 15:23 boot
-rwxr-xr-x   1 root root  3725 Jun 16 03:54 boot_loader_operations.sh
drwxr-xr-x  18 root root  3320 Jun 30 15:22 dev
drwxrwxrwx  76 root root  3700 Jun 30 15:23 etc
drwxr-xr-x   2 root root    40 Nov  5  2016 home
drwxr-xr-x   4 root root  4096 Jun 30 15:18 images
-rwxrwxrwx   1 root root 21368 May 22 01:31 isZero
lrwxrwxrwx   1 root root     7 Jun 30 15:22 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Jun 30 15:22 lib64 -> usr/lib64
-rwxr-xr-x   1 root root  3397 Jun 12 21:32 load_image
drwxr-xr-x   2 root root    40 Nov  5  2016 media
drwxr-xr-x   2 root root    40 Nov  5  2016 mnt
drwxr-xr-x   2 root root    40 Nov  5  2016 opt
dr-xr-xr-x 122 root root     0 Jun 30 15:22 proc
dr-xr-x---   3 root root   200 Jun 30 15:22 root
drwxr-xr-x  22 root root   680 Jun 30 15:23 run
lrwxrwxrwx   1 root root     8 Jun 30 15:22 sbin -> usr/sbin
drwxr-xr-x   2 root root    40 Nov  5  2016 srv
dr-xr-xr-x  13 root root     0 Jun 30 15:22 sys
drwxrwxrwt   7 root root   180 Jun 30 16:41 tmp
drwxr-xr-x  13 root root   280 Jun 30 15:22 usr
drwxr-xr-x  19 root root   460 Jun 30 15:22 var
-rwxr-xr-x   1 root root  3927 Jun  9 22:27 zeroize.py
[root@fsmshell /]# sh load_image
Found disk /dev/sde of Required size
Checking Partitions on /dev/sde
sde already has partitions
yes
Running Command: dd if=/images/latest of=/dev/sde bs=512  conv=noerror,sync status=progress
3630109184 bytes (3.6 GB) copied, 148.448543 s, 24.5 MB/s
```

   b. Run the `load_image` script, for example:
      `# sh load_image`



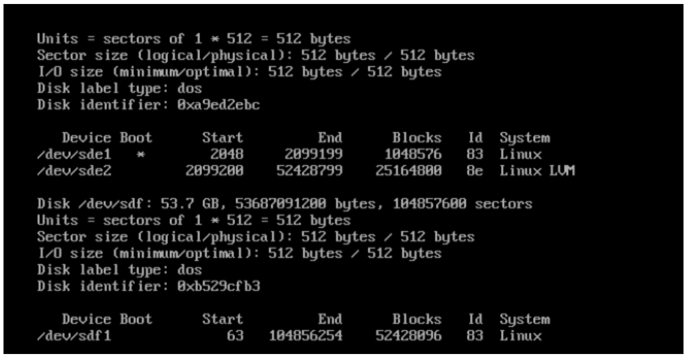
```
[root@fsmshell /]# sh load_image
Found disk /dev/sde of Required size
Checking Partitions on /dev/sde
sde already has partitions
yes
Running Command: dd if=/images/latest of=/dev/sde bs=512  conv=noerror,sync status=progress
26776572416 bytes (27 GB) copied, 588.843679 s, 45.5 MB/s
52428800+0 records in
52428800+0 records out
26843545600 bytes (27 GB) copied, 596.499 s, 45.0 MB/s
Swiping Image to new disk
[root@fsmshell /]# [ 1174.311179]  sde: sde1 sde2
[ 1174.492305] device-mapper: uevent: version 1.0.3
[ 1174.493463] device-mapper: ioctl: 4.34.0-ioctl (2015-10-28) initialised: dm-devel@redhat.com
```

When the script completes, press Return.

c. Press Return again to end the `load_image` script.

d. Run the `fdisk -l` command to check that the disks have been configured, for example:

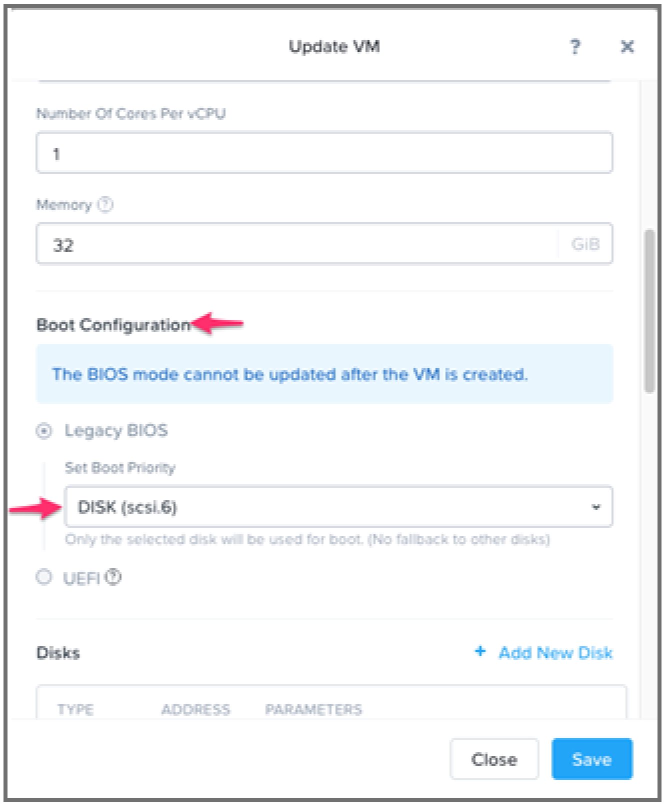
```
# fdisk -l
```



```
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xa9ed2ebc

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1   *        2048     2099199     1048576   83  Linux
/dev/sde2         2099200    52428799    25164800   8e  Linux LVM

Disk /dev/sdf: 53.7 GB, 53687091200 bytes, 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xb529cfb3

   Device Boot      Start         End      Blocks   Id  System
/dev/sdf1              63   104856254    52428096   83  Linux
```

4. In the Nutanix-AHV Prism Console, power off the VM after `load_image` completes.
5. **Important:** At this stage, you must change the boot disk as follows:
   - **a.** Identify the 25GB disk which is the boot disk. In our example, it is identified by scsi.6 (Note that it is not in any particular order).
   - **b.** Select the 25GB boot disk under **Boot Configuration > Legacy BIOS > Set Boot Priority**. In this case, it is **DISK (scsi.6)**.

c. Click **Save** to save the result.



Number Of Cores Per vCPU: 1

Memory: 32 GiB

Boot Configuration

The BIOS mode cannot be updated after the VM is created.

● Legacy BIOS

Set Boot Priority: DISK (scsi.6)

Only the selected disk will be used for boot. (No fallback to other disks)

○ UEFI

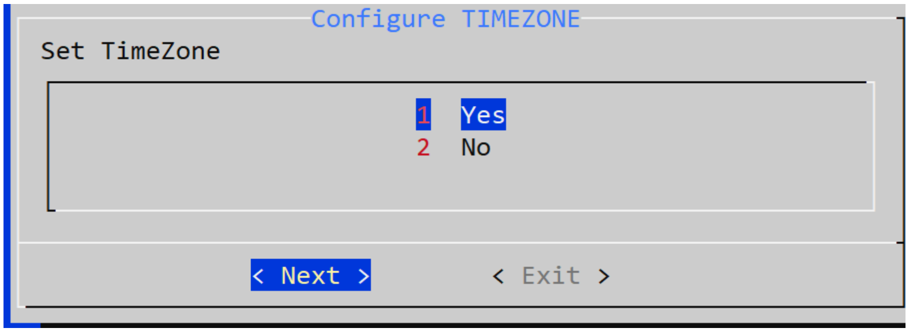
6. Power on the image and move to the next step for the migration.

Migrate to FortiSIEM 6.1.1

Follow these steps to complete the migration process:

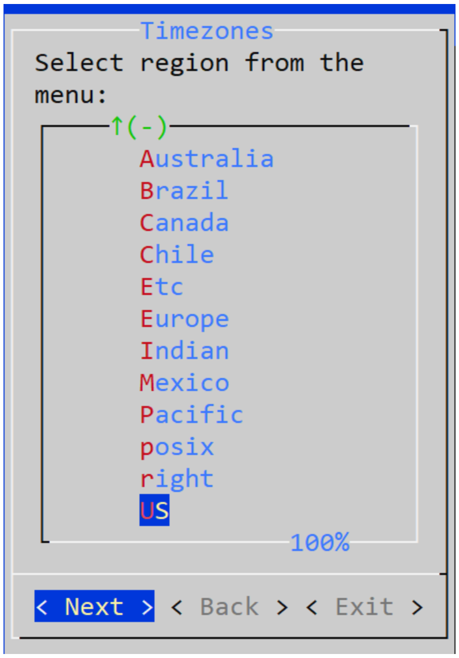
1. Log in to the bootloader shell as user `root` with password `ProspectHills`. You will immediately be asked to change your password.
2. Create and mount the `/images` directory:
   a. Change directory to `root`, for example:
      ```
      # cd /
      ```
   b. Create the `/images` directory, for example:
      ```
      # mkdir -p /images
      ```
   c. Mount the `sdf1` (the 50GB disk) to `/images`, for example:
      ```
      # mount /dev/sdf1 /images
      ```
      Or using the UUID if the disk name changed, for example:
      ```
      # mount -U d4a5b82f-6e73-456b-ab08-d6e6d845d1aa /images
      ```
3. Run the `configFSM.sh` command to configure the migration via a GUI, for example:
   ```
   # configFSM.sh
   ```

4. In the first screen of the GUI select **1 Yes** to set a timezone. Press **Next**.



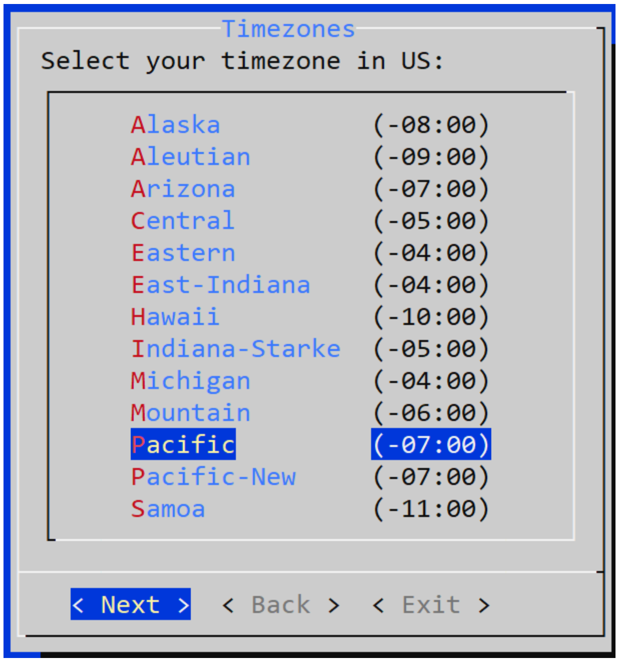
```
                    Configure TIMEZONE
 Set TimeZone

                     1   Yes
                     2   No

          < Next >          < Exit >
```

5. Select a region for the timezone. In this example, **US** is selected. Press **Next**.



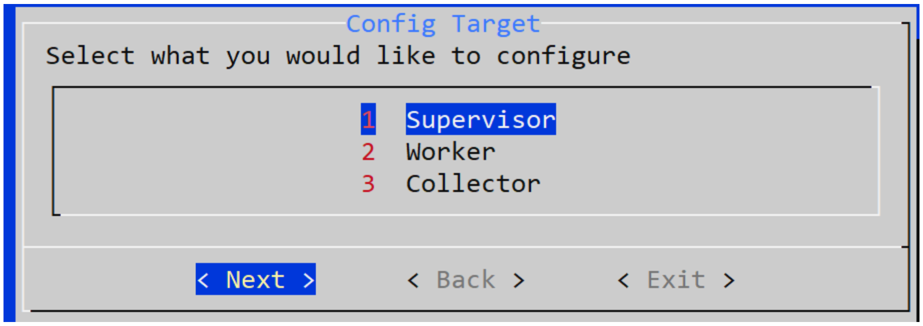
```
        Timezones
 Select region from the
 menu:
     ↑(-)
          Australia
          Brazil
          Canada
          Chile
          Etc
          Europe
          Indian
          Mexico
          Pacific
          posix
          right
          US
                 100%

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

6. Select a timezone in the selected region. In this example, **Pacific** is selected. Press **Next**.



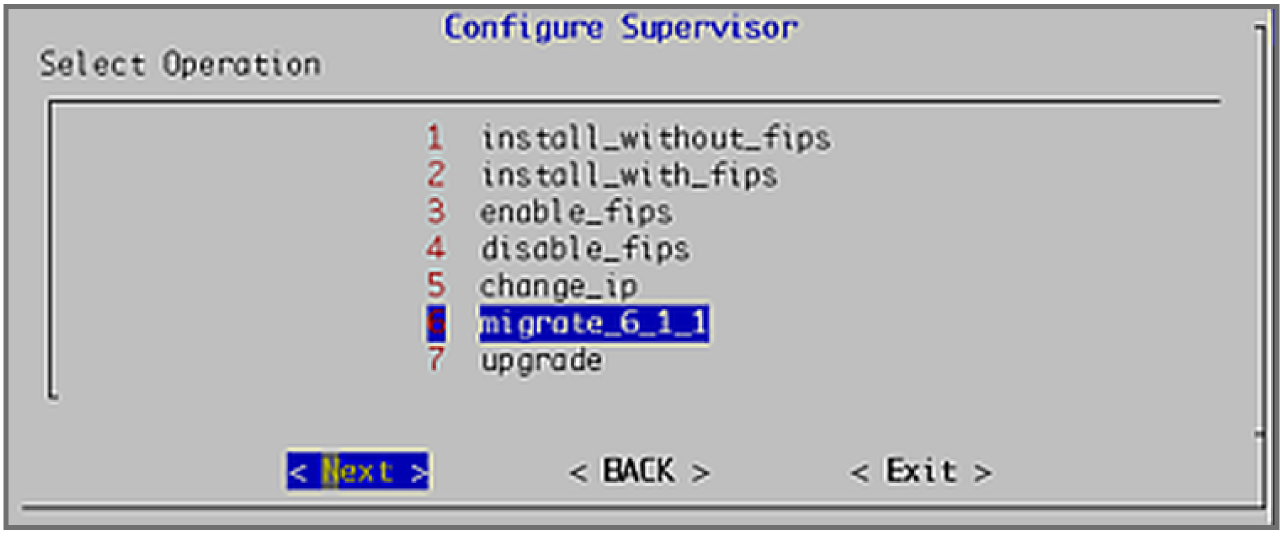
```
Timezones
Select your timezone in US:

    Alaska          (-08:00)
    Aleutian        (-09:00)
    Arizona         (-07:00)
    Central         (-05:00)
    Eastern         (-04:00)
    East-Indiana    (-04:00)
    Hawaii          (-10:00)
    Indiana-Starke  (-05:00)
    Michigan        (-04:00)
    Mountain        (-06:00)
    Pacific         (-07:00)
    Pacific-New     (-07:00)
    Samoa           (-11:00)

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

7. Select a target to configure. In this example, the **Supervisor** is selected. Press **Next**.



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

    1  Supervisor
    2  Worker
    3  Collector

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

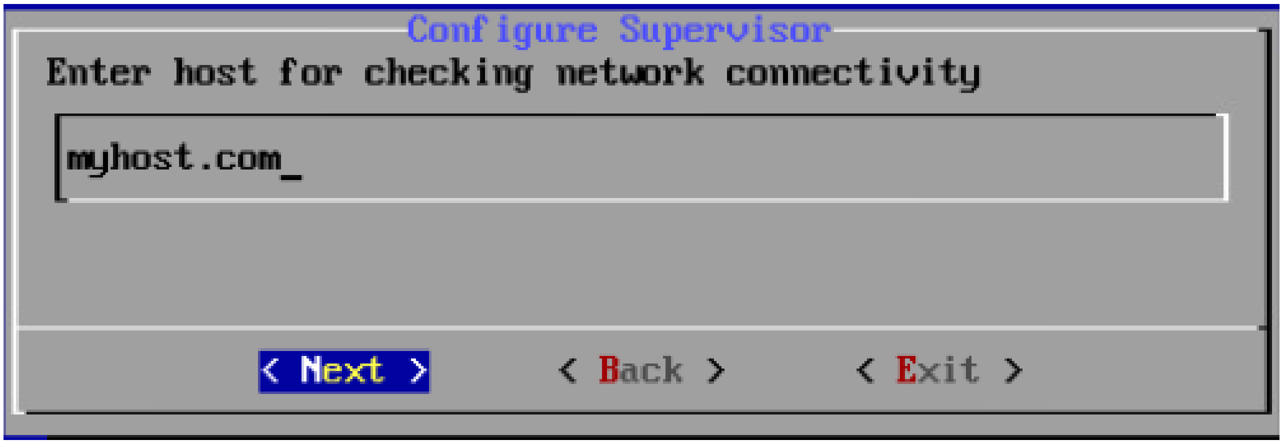
8. Select the **6 migrate_6_1_1** Operation option. Press **Next**.



```
Configure Supervisor
Select Operation

    1  install_without_fips
    2  install_with_fips
    3  enable_fips
    4  disable_fips
    5  change_ip
    6  migrate_6_1_1
    7  upgrade

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

9. 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**.

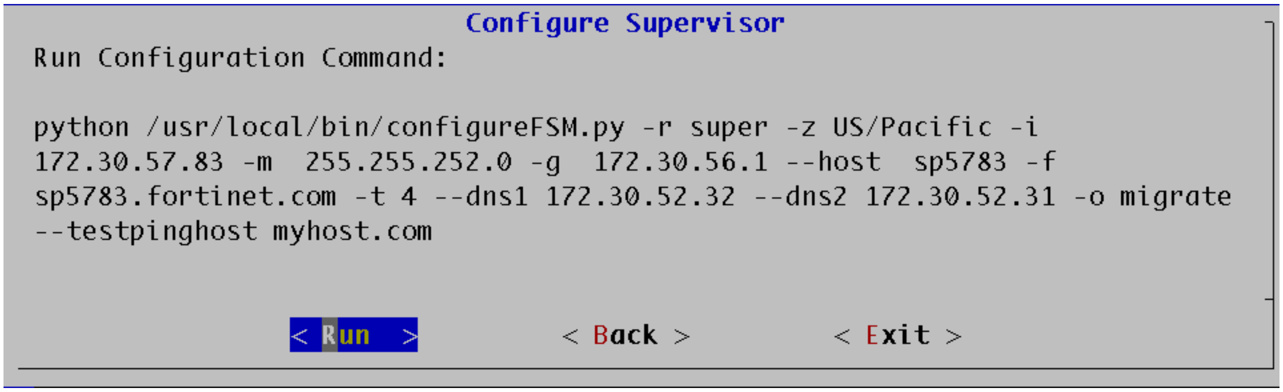


Configure Supervisor

Enter host for checking network connectivity

myhost.com_

10. Press the **Run** command to complete migration, for example:



Configure Supervisor

Run Configuration Command:

```
python /usr/local/bin/configureFSM.py -r super -z US/Pacific -i
172.30.57.83 -m  255.255.252.0 -g  172.30.56.1 --host  sp5783 -f
sp5783.fortinet.com -t 4 --dns1 172.30.52.32 --dns2 172.30.52.31 -o migrate
--testpinghost myhost.com
```

The options for the `configureFSM.py` script are described in the table here.

11. The script will take some minutes to run. When it is finished, migration is complete.
12. To ensure `phMonitor` is running, execute the `phstatus` command, for example:

```
# phstatus
```

13. 13.On Nutanix AHV, the system UUID has changed because you booted from a different OS disk than prior one you were running in 5.3.x or 5.4.0. You can obtain this UUID using the `phgetUUID` command. You will need to work with Forticare support to reset your license to use this new UUID. When you have the updated license, navigate to the GUI and upload this license. Until this is done, the backend processes will not run and migration is not complete.

Migrate Cluster Installation

This section provides instructions on how to migrate Supervisor, Workers, and Collectors separately in a cluster environment,

- Delete Workers
- Migrate Supervisor
- Install New Worker(s)
- Register Workers
- Set Up Collector-to-Worker Communication
- Working with Pre-6.1.0 Collectors

- Install 6.1.1 Collectors
- Register 6.1.1 Collectors

Delete Workers

1. Login to the Supervisor.
2. Go to **Admin > License > Nodes** and delete the Workers one-by-one.
3. Go to the **Admin > Cloud Health** page and make sure that the Workers are not present.
   Note that the Collectors will buffer events while the Workers are down.
4. Shutdown the Workers.
   SSH to the Workers one-by-one and shutdown the Workers.

Migrate Supervisor

Follow the steps in Migrate All-in-one Installation to migrate the supervisor node. **Note:** FortiSIEM 6.1.1 does not support Worker or Collector migration.

Install New Worker(s)

Follow the steps in Cluster Installation > Install Workers to install new Workers. You can either keep the same IP address or change the address.

Register Workers

Follow the steps in Cluster Installation > Register Workers to register the newly created 6.1.1 Workers to the 6.1.1 Supervisor. The 6.1.1 FortiSIEM Cluster is now ready.

Set Up Collector-to-Worker Communication

1. Go to **Admin > Systems > Settings**.
2. Add the Workers to the Event Worker or Query Worker as appropriate.
3. Click **Save**.

Working with Pre-6.1.0 Collectors

Pre-6.1.0 Collectors and agents will work with 6.1.1 Supervisor and Workers. You can install 6.1.1 collectors at your convenience.

Install 6.1.1 Collectors

FortiSIEM does not support Collector migration to 6.1.1. You can install new 6.1.1 Collectors and register them to 6.1.1 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. Follow these steps:

1. Copy the http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector.
2. Disconnect the pre-6.1.1 Collector.
3. Install the 6.1.1 Collector with the old IP address by the following the steps in Cluster Installation > Install Collectors.
4. Copy the saved http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector to the 6.1.1 Collector.
   This step is needed for Agents to work seamlessly with 6.1.1 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.1 migration, this password is lost.

Register 6.1.1 Collectors

Follow the steps in Cluster Installation > Register Collectors, with the following difference: in the `phProvisionCollector` command, use the `--update` option instead of `--add`. Other than this, use the exactly the same parameters that were used to register the pre-`6.1.1` Collector. Specifically, use this form of the

`phProvisionCollector` command to register a `6.1.1` Collector and keep the old associations:

```
# /opt/phoenix/bin/phProvisionCollector --update <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.

Re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.

www.fortinet.com