

FortiSIEM - AWS Installation and Migration Guide

Version 6.1.0

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 6.1.0 AWS Installation and Migration Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Launch an Instance Using FortiSIEM 6.1.0 AMI	6
Configure FortiSIEM via GUI	10
Upload the FortiSIEM License	14
Choose an Event Database	14
Cluster Installation	15
Install Supervisor	15
Install Workers	16
Register Workers	17
Install Collectors	18
Register Collectors	18
Migrating from FortiSIEM 5.3.0, 5.3.1 or 5.3.2	22
Pre-Migration Checklist	22
Migrate All-in-one Installation	22
Download the Backup Script	23
Run the Backup Script and Shutdown System	23
Detach 5.3.0, 5.3.1 or 5.3.2 Root Disk	23
Attach the 6.1.0 Root Disk to the 5.3.0, 5.3.1 or 5.3.2 Instance	24
Boot Up the 5.3.0, 5.3.1 or 5.3.2 Instance and Migrate to 6.1.0	30
(Optional) Change Instance Type to the Latest Generation	33
Migrate Cluster Installation	34
Delete Workers	35
Migrate Supervisor	35
Install New Worker(s)	35
Register Workers	35
Set Up Collector-to-Worker Communication	35
Working with Pre-6.1.0 Collectors	35
Install 6.1.0 Collectors	35
Register 6.1.0 Collectors	36

Change Log

Date	Change Description
05/09/2019	Initial release of ForiSIEM - AWS Installation Guide
03/22/2019	Revision 2: updated instructions for Service Provider deployments.
11/11/2019	Revision 3: small change to installation instructions for FortiSIEM and FortiSIEM Report Server.
03/30/2020	Released document for 5.3.0.
08/15/2020	Revision 4: Updated deployment and installation for FortiSIEM 6.1 on AWS.
12/03/2020	Revision 6: Small addition to Pre-Installation Checklist.
12/07/2020	Revision 7: Small addition to Register Collectors.
02/04/2021	Revision 8: Updated Migration.
03/23/2021	Revision 9: Released for 6.2.0.
4/16/2021	Revision 10: Minor update to Run the Backup Script and Shutdown System section.
09/28/2021	Revision 11: Updated volume type information for 6.x guides.
11/19/2021	Revision 12: Updated Register Collectors section for 6.x guides.
08/18/2022	Revision 13: Updated All-in-one Installation section.
10/20/2022	Revision 14: Updated Register Collectors instructions for 6.x guides.

Fresh Installation

This section describes how to install FortiSIEM for the current release.

- [Pre-Installation Checklist](#)
- [All-in-one Installation](#)
- [Cluster 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 can respond to a 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
- Fortinet recommends that you do not choose AWS Spot instances for Supervisor and Worker nodes. Such instances can go down at any time with short notice, causing instability and performance issues.
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements and choose AWS instance type accordingly:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB

Node	vCPU	RAM	Local Disks
Workers	Minimum – 8	Minimum – 16GB	OS – 25GB
	Recommended - 16	Recommended – 24GB	OPT – 100GB
Collector	Minimum – 4	Minimum – 4GB	OS – 25GB
	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](#).

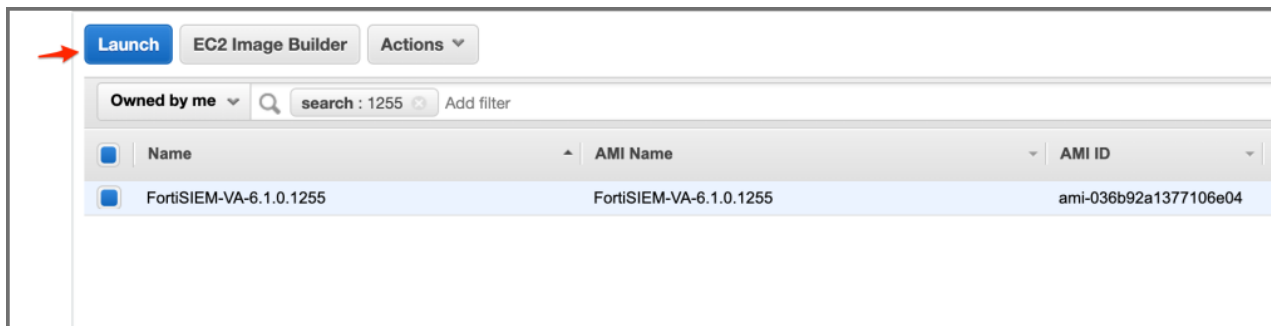
All-in-one Installation

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

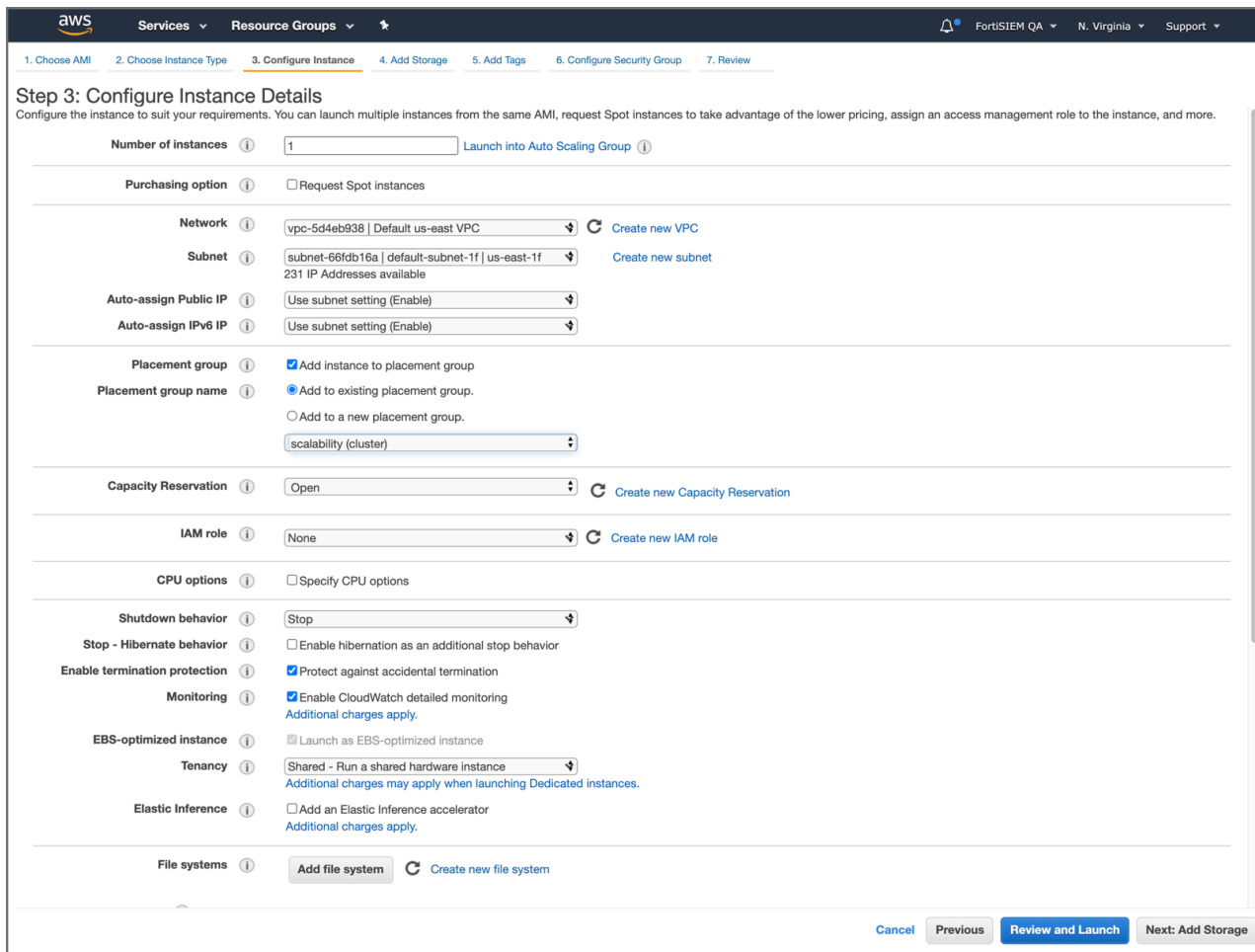
- [Launch an instance using FortiSIEM 6.1.0 AMI](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

Launch an Instance Using FortiSIEM 6.1.0 AMI

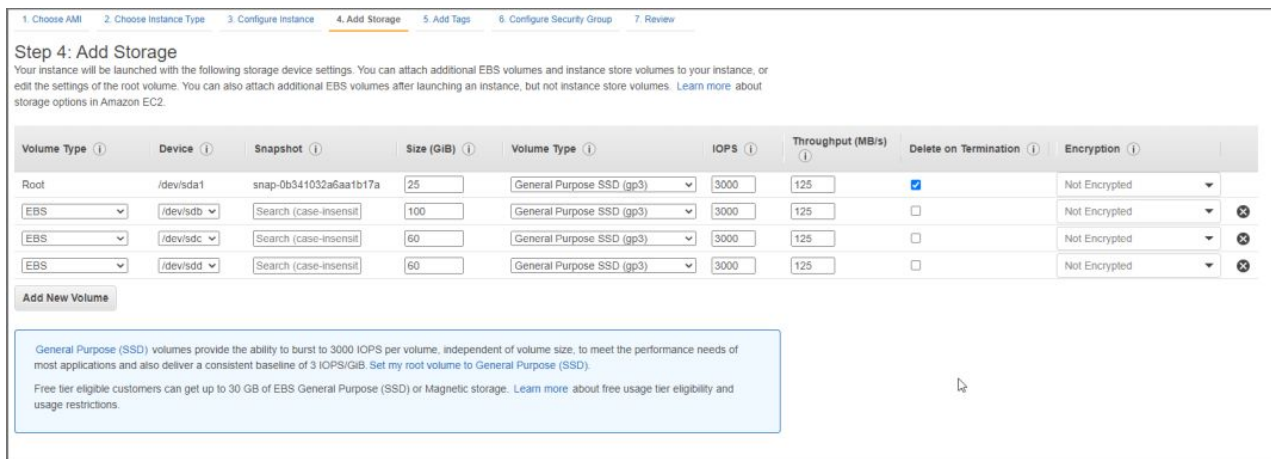
1. Navigate to the EC2 AMIs page and find FortiSIEM 6.1.0 AMI (or in AWS Marketplace after the GA release).
2. Launch FortiSIEM-6.1.0.0112.



3. Go to **Step 3: Configure Instance Details** in AWS Services. Configure instance details such as VPC, Subnet, IP, etc. Click **Next**.



4. In **Step 4: Add Storage**, add additional disks in the **Add Storage** page. These will be used for the additional partitions in the virtual appliance. An All In One deployment requires the [following additional partitions](#). Then click **Next**.



Note: If you plan to onboard greater than 500 devices, or 5000 eps, please consider increasing IOPS and Throughput for the disk used to mount /cmdb in FortiSIEM.

For instance, you can run the following command once FortiSIEM is initially deployed to determine which disk mounts the cmdb folder.

```
[admin@6 data-definition]$ lsblk | grep cmdb
└─sdc1 8:33 0 60G 0 part /cmdb
```

In this case /dev/sdc.

You can go into EBS volumes in AWS, and increase the IOPS to 5000, and Throughput to 400MB/s to be more in line with SSD performance.

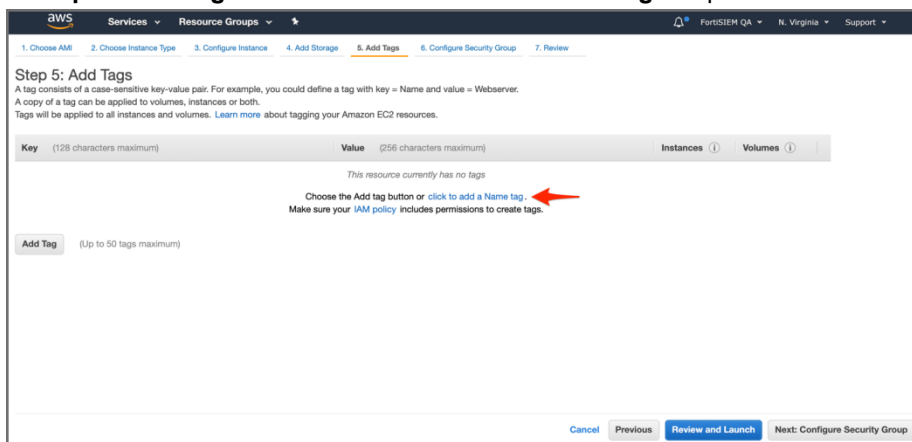
Use these partition values:

Volume Name	Size	Disk Name
EBS Volume 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.
EBS Volume 3	60GB	/cmdb
EBS Volume 4	60GB	/svn
EBS Volume 5	60GB+	/data (see the following note)

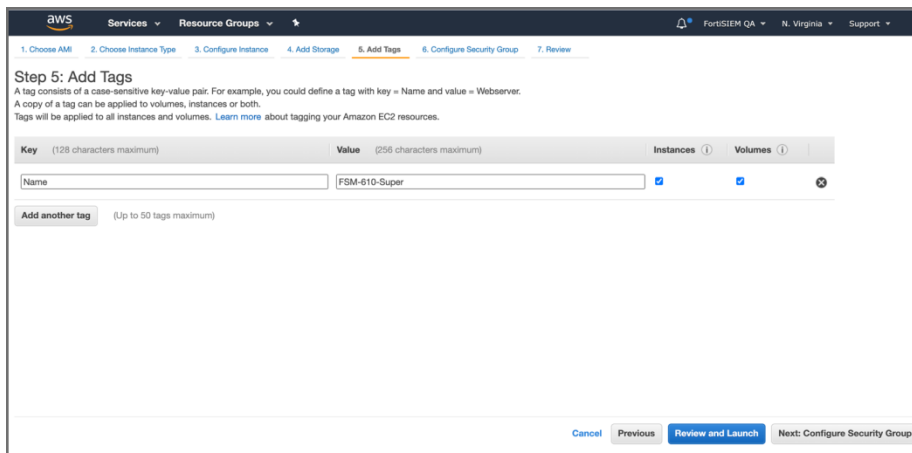
Note on EBS Volume 5:

- Add a 5th EBS Volume 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.
- Choose GP3 volume type for all volumes (GP3 is better than GP2 at a slightly lower cost). For the CMDB partition, you can choose to modify your volume type and IOPS based on your system workload if you see the consistently high IOPS requirement in your deployment.

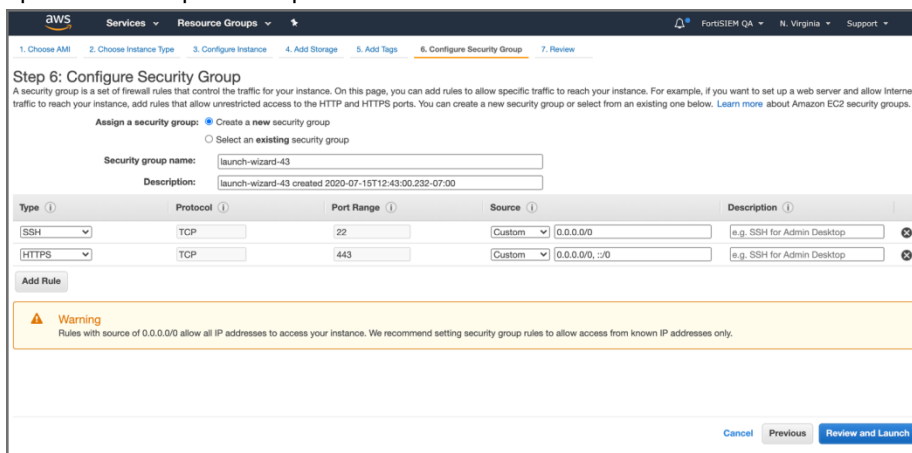
5. In **Step 5: Add Tags**: click **click to add a new Name Tag** and provide a name for the instance. Click **Next**.



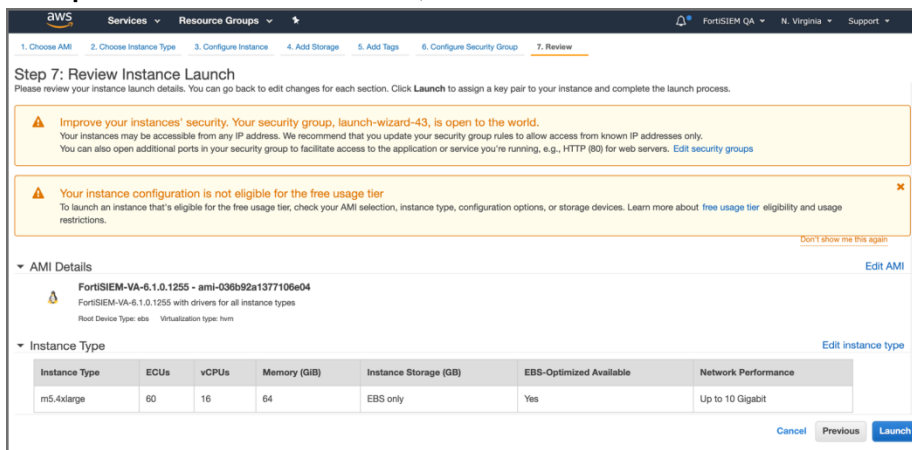
Add a new Name Tag.



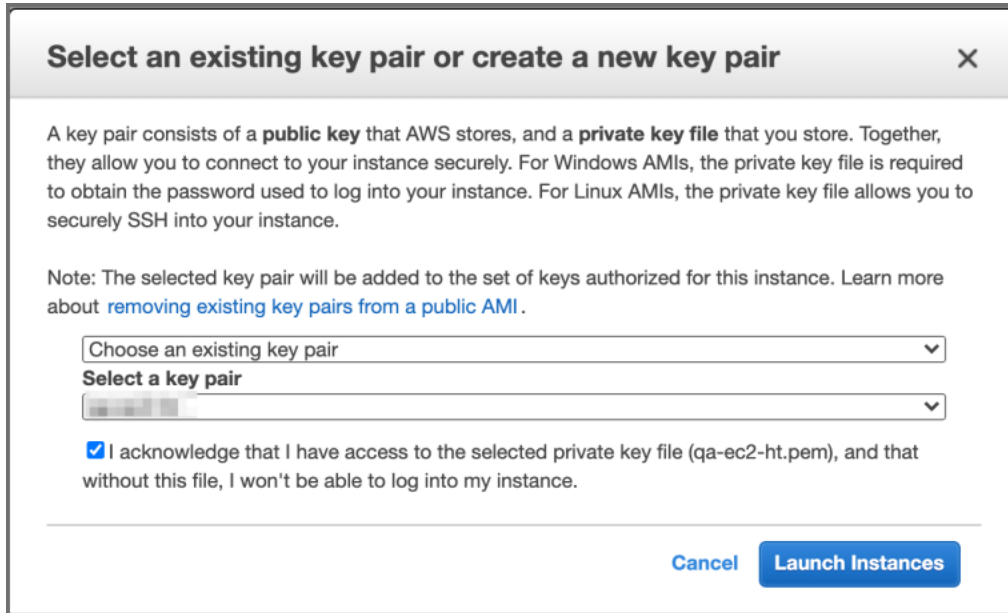
6. In **Step 6: Configure Security Group**, add the allowed inbound protocols for your instance. You will need ssh and https to begin with. Depending on whether this node will receive syslog or other inbound data, you may need to open additional protocols/ports. Click **Review and Launch**.



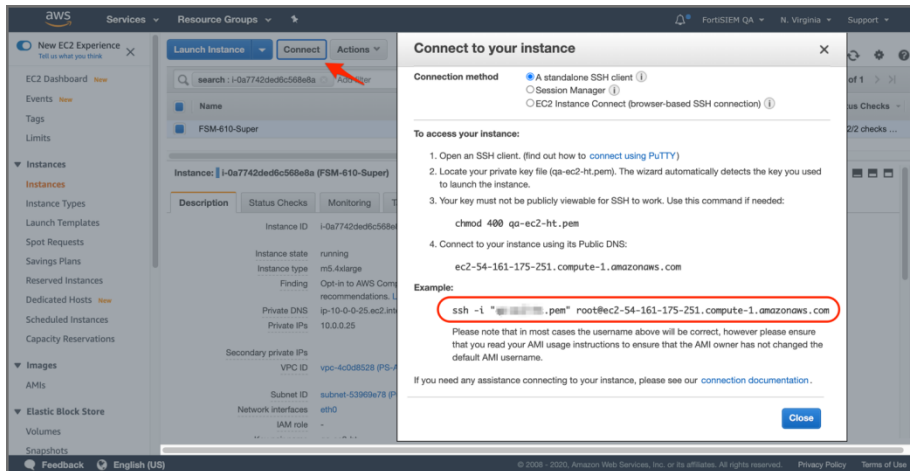
7. In **Step 7: Review Instance Launch**, click **Launch**.



- Select an existing key pair or create a new key pair, then click **Launch Instances**.



- Select the instance that you just created and click **Connect**.

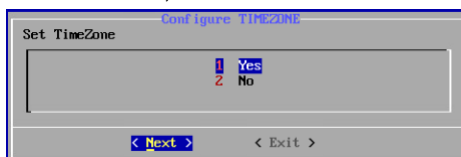


- Using the example above in the **Connect** popup, ssh to the instance you created. Replace `root` user with `ec2-user`. Once logged in, you can execute the `sudo su -` command to become root user

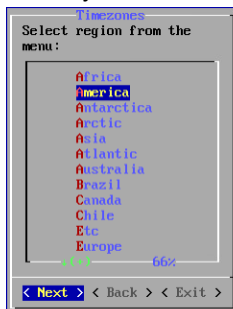
Configure FortiSIEM via GUI

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

- At the `root` command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`# configFSM.sh`
- In VM console, select **1 Set Timezone** and then press **Next**.



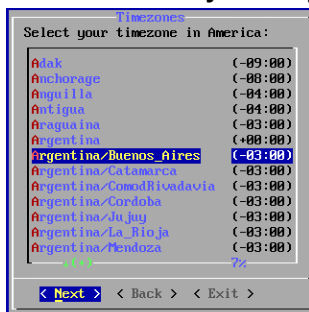
3. Select your **Location**, and press **Next**.



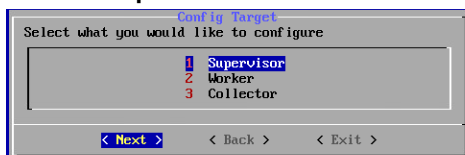
4. Select your **Continent**, and press **Next**.



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

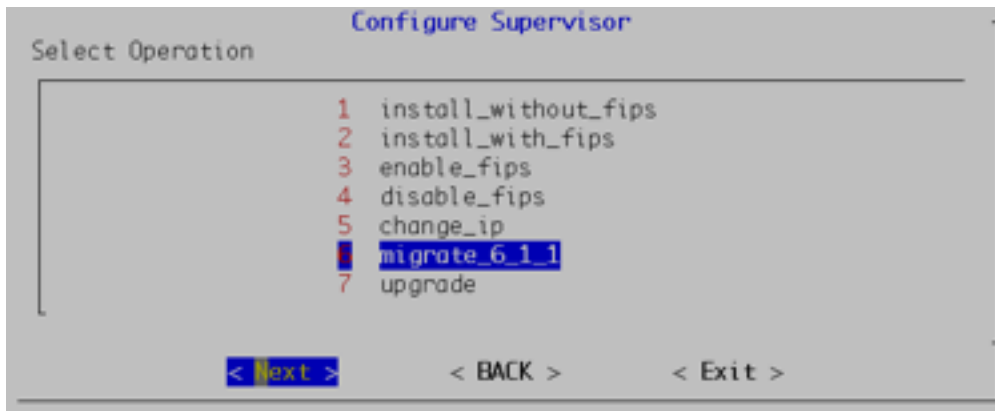


6. Select **1 Supervisor**. Press **Next**.



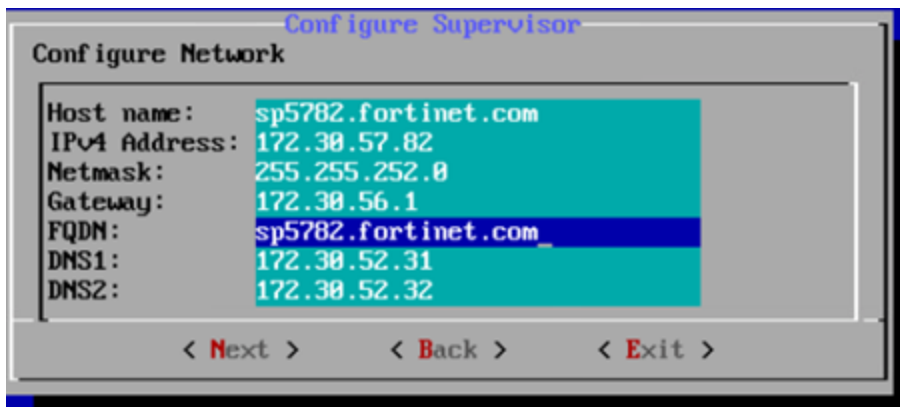
Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

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



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

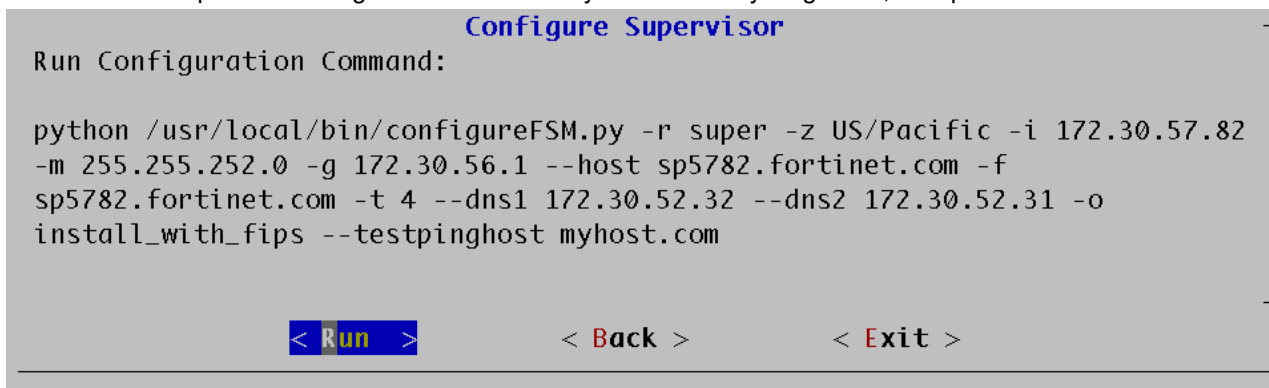
Option	Description
Host Name	The Supervisor's host name
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS servers



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**.



10. 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**.



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 server 1 and DNS server 2.
-o	Installation option (install_without_fips , install_with_fips , enable_fips , disable_fips , change_ip , or migrate_6_1_0)
-z	Time zone. Possible values are US/Pacific ,

Option	Description
	Asia/Shanghai, Europe/London, or Africa/Tunis
<code>--testinghost</code>	The host used to test connectivity

- 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](#).

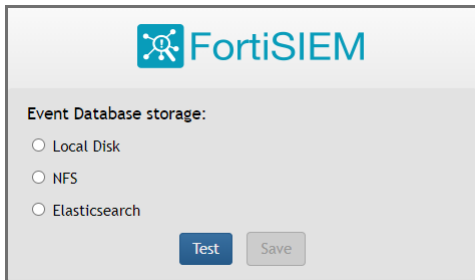
You will now be asked to input a license.

- Open a Web browser and log in to the FortiSIEM UI.
- The License Upload dialog box will open.

- Click **Browse** and upload the license file. Make sure that the **Hardware ID** shown in the License Upload page matches the license.
- 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.
- 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.
- 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](#).



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/phenix/bin/phstatus.py
System uptime: 21:12:02 up 1:11, 1 user, load average: 0.16, 0.20, 0.36
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16.0% user, 6.2% sys, 2.1% iowait, 0.0% irq, 0.0% steal, 0.0% idle, 0.0% nic, 0.2% softirq, 0.1% softirq, 0.0% bsd, 0.0% oost
Mem: 65782100k total, 10366036k used, 55336064k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465020k cached

PROCESS                UPTIME      CPU%      UIRT_MEM    RES_MEM
phParser                41:23       0          2176m       550m
phQueryMaster           41:41       0          1020m       77m
phReporter              41:41       0          1079m       594m
phRuleKeeper            41:41       0          1363m       295m
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          689m        67m
phIdentityWorker        41:41       0          1027m       50m
phIdentityMaster        41:41       0          491m        39m
phAgentManager          41:41       0          1425m       54m
phCheckpoint            42:31       0          325m        34m
phPerfMonitor           41:41       0          702m        70m
phReportLoader          41:41       0          769m       270m
phBeaconEventPackager   41:41       0          1125m       65m
phDataPurger            41:41       0          500m        50m
phEventForwarder        41:41       0          240m        46m
phMonitor               37:24       0          2000m       53m
apache                  01:10:40    0          310m        16m
node_js-charting        01:10:19    0          916m        71m
node_js-pm2              01:10:13    0          26m         26m
appSvc                   01:10:07    0          15172m      3826m
DBSvc                    01:10:30    0          317m        30m
phnomaly                01:00:07    0          907m        64m
phFortiInsightAI        01:10:40    0          23432m     430m
redis                   01:10:10    0          55m         25m
```

Cluster Installation

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

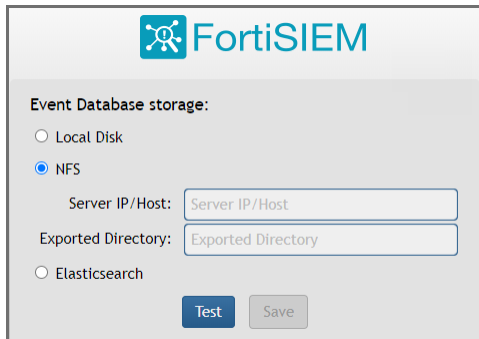
- Install Supervisor
- Install Workers
- Register Workers
- Install Collectors
- Register Collectors

Install Supervisor

Follow the steps in [All-in-one Install](#) with two differences:

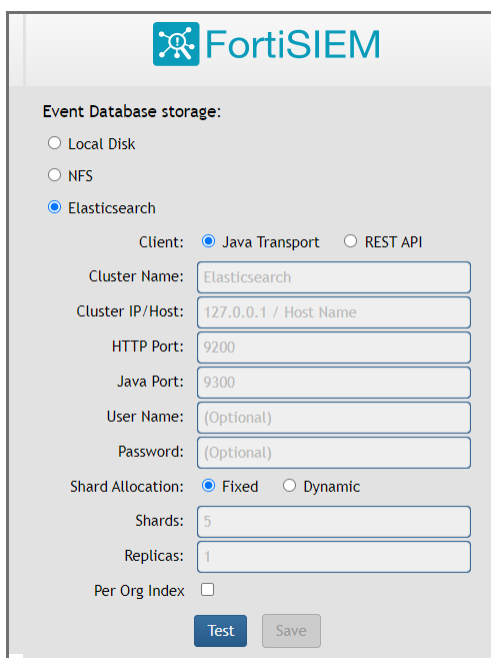
- Setting up hardware - you do not need to add an EBS Volume 5 for Event database.
- Setting up an Event database - Configure the cluster for either NFS or Elasticsearch.

NFS



The screenshot shows the FortiSIEM Event Database storage configuration interface. The 'Event Database storage:' section has three radio button options: 'Local Disk', 'NFS' (which is selected), and 'Elasticsearch'. Below the 'NFS' option, there are two input fields: 'Server IP/Host:' and 'Exported Directory:'. At the bottom of the form, there are two buttons: 'Test' and 'Save'.

Elasticsearch



The screenshot shows the FortiSIEM Event Database storage configuration interface for Elasticsearch. The 'Event Database storage:' section has three radio button options: 'Local Disk', 'NFS', and 'Elasticsearch' (which is selected). Below the 'Elasticsearch' option, there is a 'Client:' section with two radio button options: 'Java Transport' (selected) and 'REST API'. Below this, there are several input fields: 'Cluster Name:' (with 'Elasticsearch' entered), 'Cluster IP/Host:' (with '127.0.0.1 / Host Name' entered), 'HTTP Port:' (with '9200' entered), 'Java Port:' (with '9300' entered), 'User Name:' (with '(Optional)' entered), and 'Password:' (with '(Optional)' entered). Below these fields, there is a 'Shard Allocation:' section with two radio button options: 'Fixed' (selected) and 'Dynamic'. Below this, there are two input fields: 'Shards:' (with '5' entered) and 'Replicas:' (with '1' entered). At the bottom, there is a 'Per Org Index' checkbox which is unchecked. At the bottom of the form, there are two buttons: 'Test' and 'Save'.

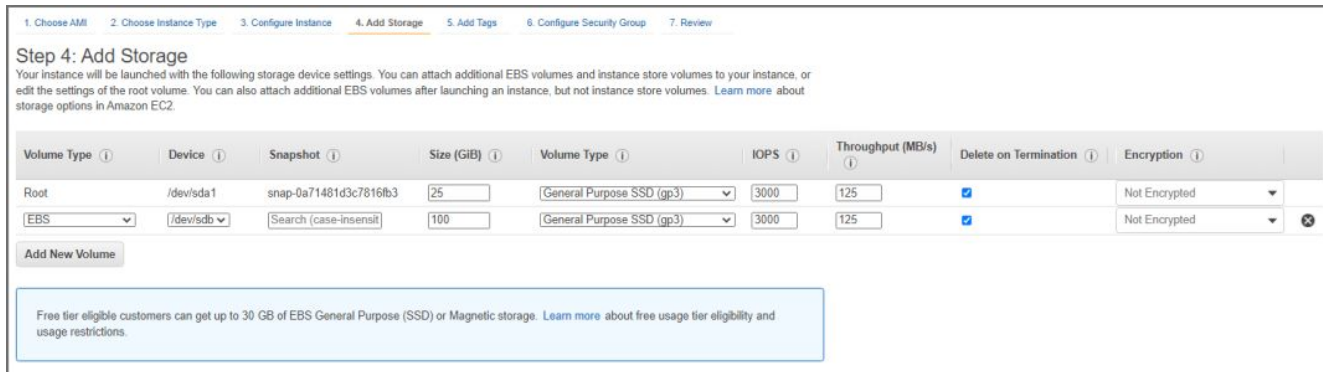
You must choose external storage listed in [Choose an Event Database](#).

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

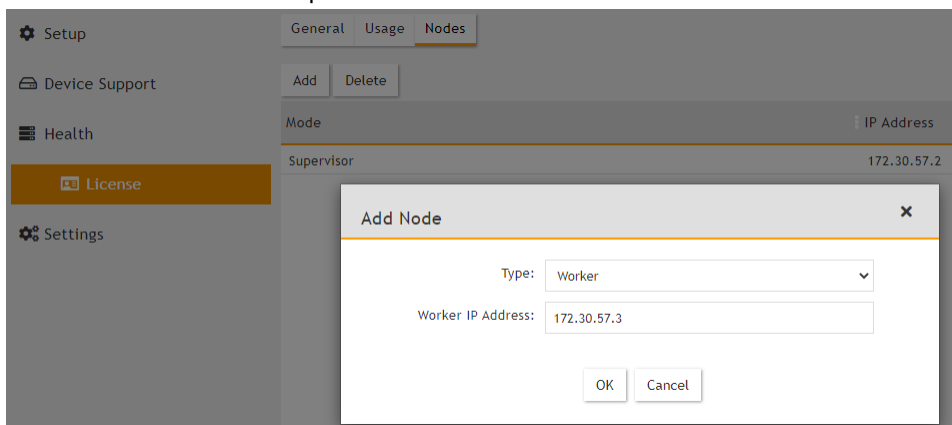
- **OPT – 100GB**
 For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.



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**.



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

system.

The screenshot displays the FortiSIEM Cloud Health interface. It features a sidebar with navigation options: Setup, Device Support, Health (selected), License, and Settings. The main content area is divided into two sections. The top section, titled 'Collector Health', shows a table with columns for Name, IP Address, Module Role, Health, Version, Load Average, CPU, and Swap Used. Two nodes are listed: 'sp572.fortinet.com' (Supervisor, Normal, 6.1.0.1238) and 'wk573.fortinet.com' (Worker, Normal, 6.1.0.1238). The bottom section, titled 'Process level metrics for wk573.fortinet.com (172.30.57.3)', shows a table with columns for Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. Processes listed include Node.js-charting, httpd, Redis, Node.js-pm2, rsyslogd, and dhDataManager. At the bottom, there is a footer with copyright information and user details: 'Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM'.

Install Collectors

Once Supervisor and Workers are installed, follow the same steps in [All-in-one Install](#) to install a Collector except in [Edit FortiSIEM Hardware Settings](#), 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.

The screenshot shows the AWS Management Console 'Step 4: Add Storage' configuration page. It includes a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (active), 5. Add Tags, 6. Configure Security Group, 7. Review. Below the progress bar, there is a description: 'Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.' The main configuration area contains a table with columns: Volume Type, Device, Snapshot, Size (GiB), Volume Type, IOPS, Throughput (MB/s), Delete on Termination, and Encryption. Two volumes are configured: 'Root' (25 GiB, General Purpose SSD (gp3), 3000 IOPS, 125 MB/s) and an 'EBS' volume (100 GiB, General Purpose SSD (gp3), 3000 IOPS, 125 MB/s). A button 'Add New Volume' is visible. A blue information box at the bottom states: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.'

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.

The screenshot shows the 'Collector Health' page in FortiSIEM. It displays a table with the following data:

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	1.1.1.1	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

Below the main table, there is a detailed view of processes:

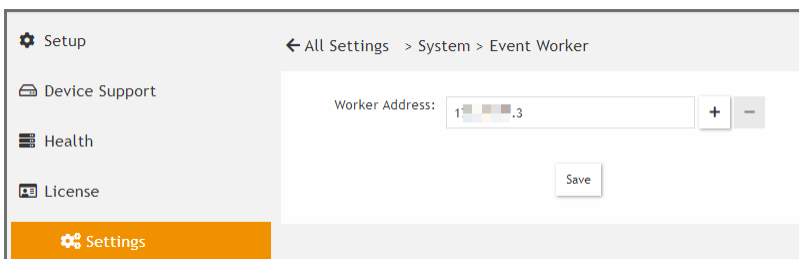
Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Service Provider Deployments

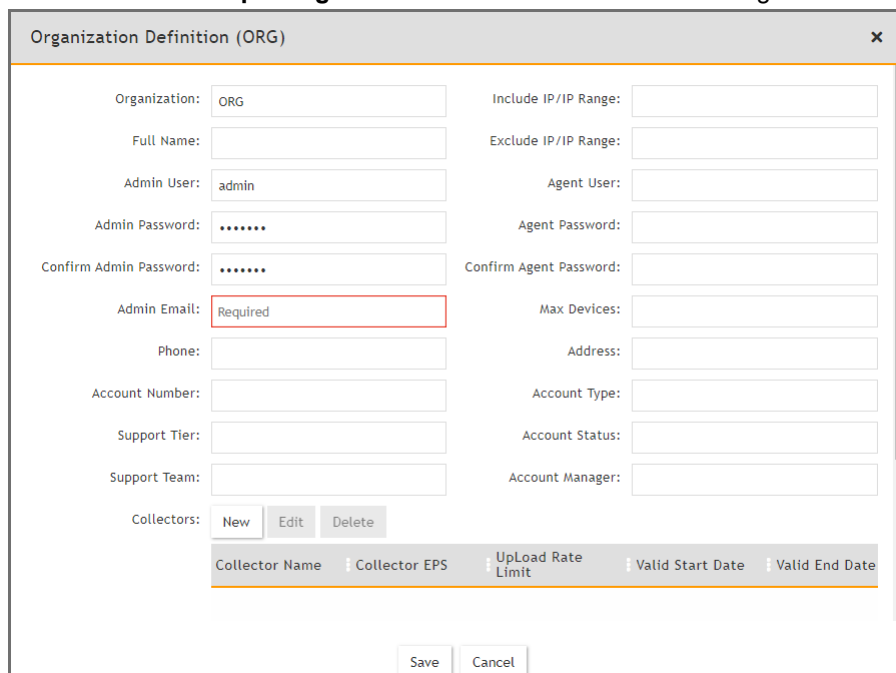
For Service Provider deployments, follow these steps.

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**.



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



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.

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=11.172.38.57.2 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.

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	1.172.38.57.2	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

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 5.3.0, 5.3.1 or 5.3.2

WARNING: FortiSIEM 5.3.3 and 5.4.0 cannot be upgraded to FortiSIEM 6.1.0. You must upgrade to FortiSIEM 6.1.1.

This section describes how to migrate from FortiSIEM 5.3.0, 5.3.1 or 5.3.2 to FortiSIEM 6.1.0. FortiSIEM performs migration in-place. The migration process backs up some important information from the original 5.3.0, 5.3.1 or 5.3.2 root disk, and then changes the root disk to boot up from a new 6.1.0 root disk. There is no need to copy disks. The instance identity remains the same.

- [Pre-Migration Checklist](#)
- [Migrate All-in-one Installation](#)
- [Migrate Cluster](#)

Pre-Migration Checklist

To perform the migration, the following prerequisites must be met:

- Delete the Worker from the Super GUI.
- Stop/Shutdown the Worker.
- Note the `/svn` partition by running the `df -h` command. the partition is used to mount `/svn/53x-settings`. You will need this information for a later step.
- Create a `/svn/53x-settings` directory and symlink it to `/images`. In AWS, you need only a small amount of space to backup 5.3.0, 5.3.1 or 5.3.2 system settings, so use the `/svn` partition (that is, a partition other than `root`) instead of a new disk. See the following example:

```
[root@fsm-531-to-610-migrate ~]# cat /opt/phoenix/bin/VERSION
Version: 5.3.1.1668
DSVersion: 5.3.1.1668
CommitHash:725c388e6
Built on: 1590816258
Local time: Fri May 29 22:24:18 PDT 2020
[root@fsm-531-to-610-migrate ~]#
[root@fsm-531-to-610-migrate ~]# mkdir /svn/53x-settings
[root@fsm-531-to-610-migrate ~]# ln -sf /svn/53x-settings /images
[root@fsm-531-to-610-migrate ~]# █
```

Migrate All-in-one Installation

- [Download the Backup Script](#)
- [Run the Backup Script and Shutdown](#)

- Detach 5.3.0, 5.3.1 or 5.3.2 Root Disk
- Attach the 6.1.0 Root Disk to the 5.3.0, 5.3.1 or 5.3.2 Instance
- Boot Up the 5.3.0, 5.3.1 or 5.3.2 Instance and Migrate to 6.1.0
- (Optional) Change Instance Type to the Latest Generation

Download the Backup Script

Download FortiSIEM AWS backup script to start migration. Follow these steps:

1. # Download the file `FSM_Backup_5.3_Files_6.1.0_0112.zip` from the [support site](#) and copy it to the 5.3.x AWS instance that you are planning to migrate to 6.1.0 (for example, `/svn/53x-settings`).
2. Unzip the `.zip` file, for example:
`unzip FSM_Backup_5.3_Files_6.1.0_0112.zip`

Run the Backup Script and Shutdown System

Follow these steps to run the backup script and shut down the system:

1. Go to the directory where you downloaded the backup script, for example:
`cd /svn/53x-settings/FSM_Backup_5.3_Files_6.1.0_0112`
2. Run the backup script with the `sh backup` command to backup 5.3.0, 5.3.1 or 5.3.2 settings that will be migrated later into the new 6.1.0 OS. For example:
`sh backup`
3. Run the `shutdown` command to shut down the FortiSIEM instance, for example:
`shutdown -h now`

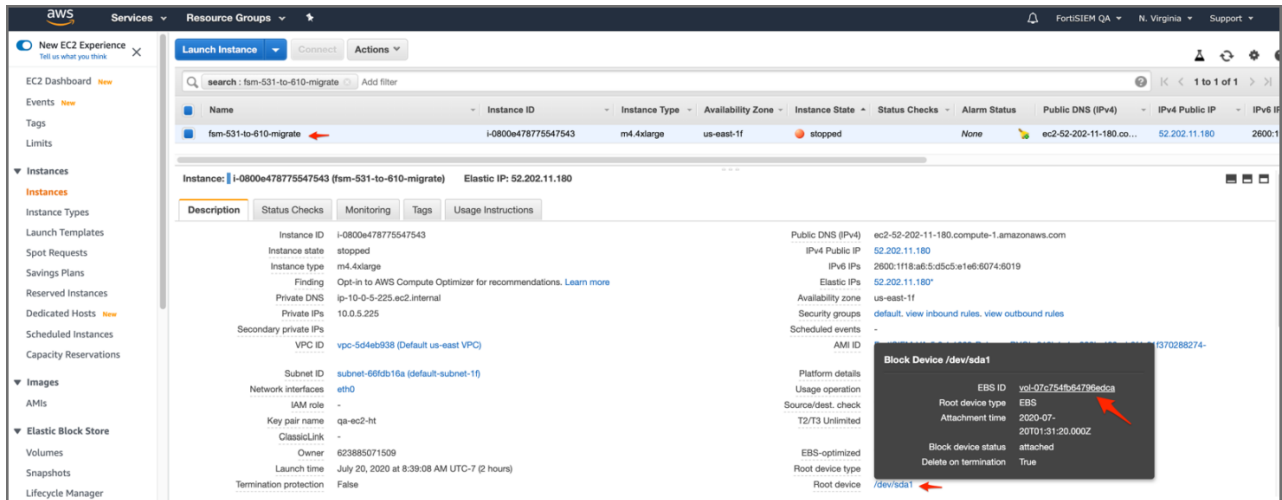
```
[root@fsm-531-to-610-migrate aws-backup]# shutdown -h now
Broadcast message from ec2-user@fsm-531-to-610-migrate
(/dev/pts/0) at 16:05 ...

The system is going down for halt NOW!
[root@fsm-531-to-610-migrate aws-backup]# Connection to ec2-52-202-11-180.compute-1.amazonaws.com closed by remote host.
Connection to ec2-52-202-11-180.compute-1.amazonaws.com closed.
$
```

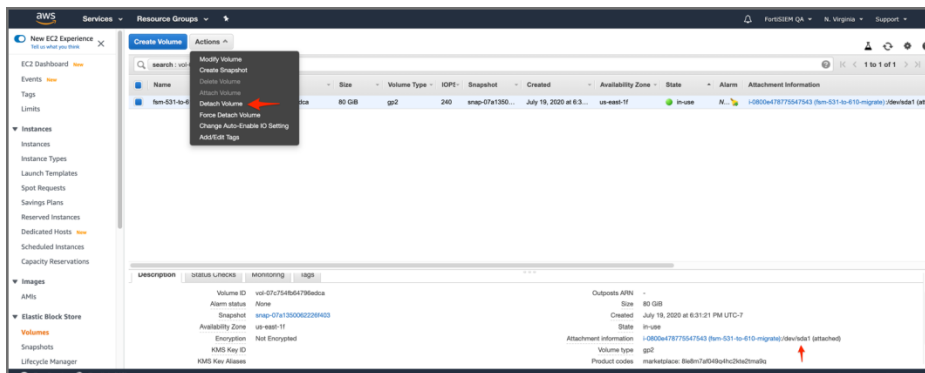
Detach 5.3.0, 5.3.1 or 5.3.2 Root Disk

Follow these steps to detach the 5.3.0, 5.3.1 or 5.3.2 root disk from the AWS console.

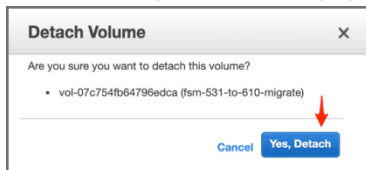
1. Log in to the AWS Console, select EC2 service, and select your FortiSIEM 5.3.0, 5.3.1 or 5.3.2 instance.



2. Click the /dev/sda1 volume and navigate to the volume by clicking the volume EBS ID.
3. Click Action > Detach Volume.



4. Confirm the operation in the popup by clicking Yes, Detach.



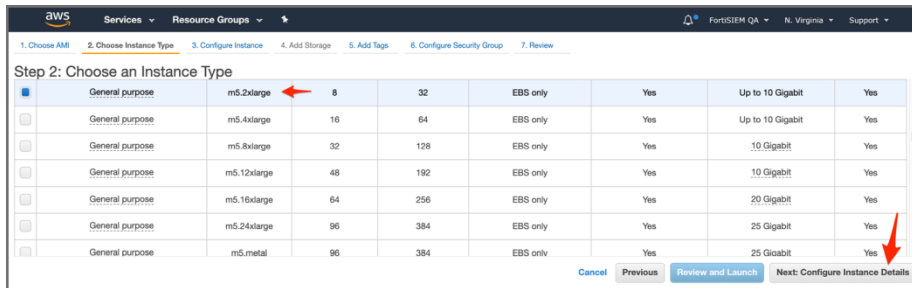
Attach the 6.1.0 Root Disk to the 5.3.0, 5.3.1 or 5.3.2 Instance

Follow these steps to attach the 6.1.0 root disk to the 5.3.0, 5.3.1 or 5.3.2 instance which you obtained from a fresh 6.1.0 instance.

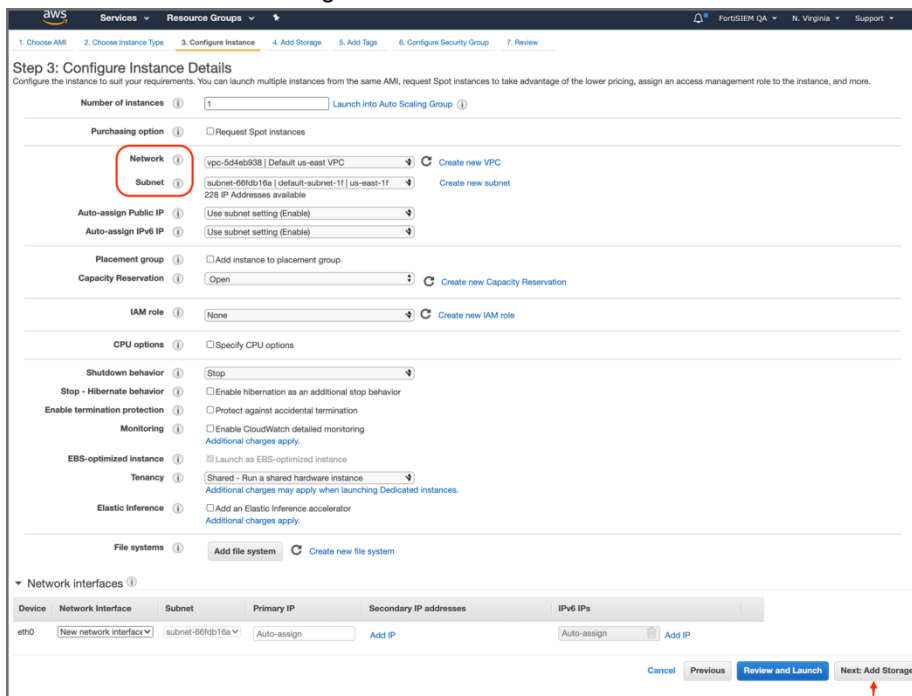
1. Navigate to the EC2 AMIs page and find FortiSIEM 6.1.0 AMI (or in AWS Marketplace after GA).
2. Launch FortiSIEM-6.1.0.0112.



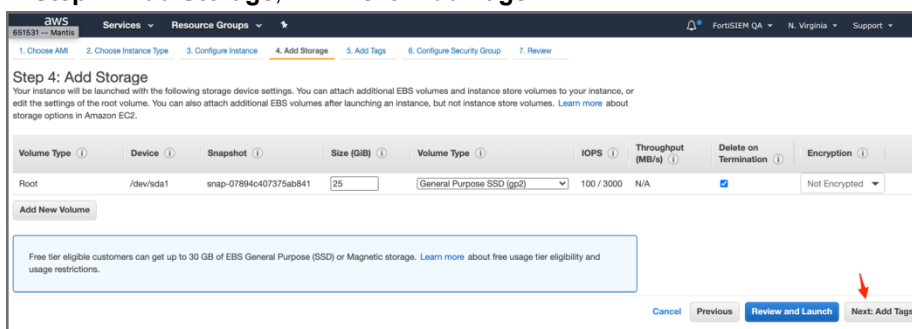
3. In **Step 2: Choose an Instance Type**, select the **m5.2xlarge** instance type (it does not matter if you pick another instance type). The purpose of this is only to get a root volume. Click **Next: Configure Instance Details**.



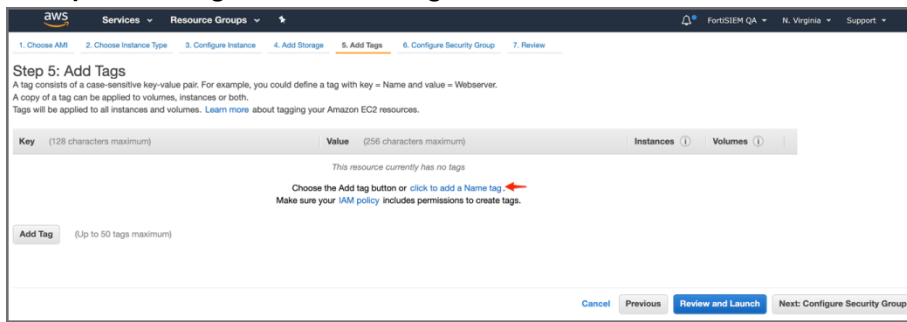
4. In **Step 3: Configure Instance Details** choose the same VPC and subnet where you deployed your 5.3.0, 5.3.1 or 5.3.2 instance. The remaining details can be default values.



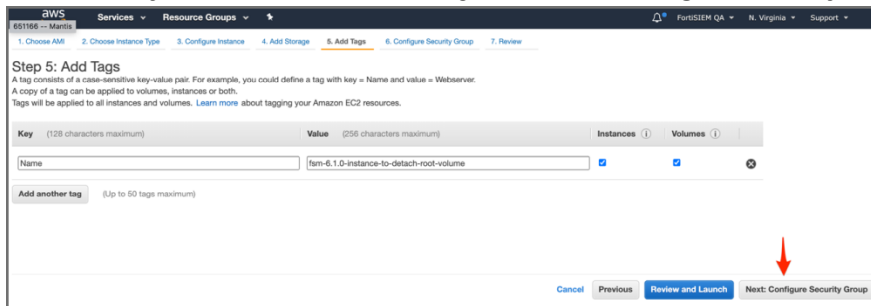
5. In **Step 4: Add Storage**, click **Next: Add Tags**.



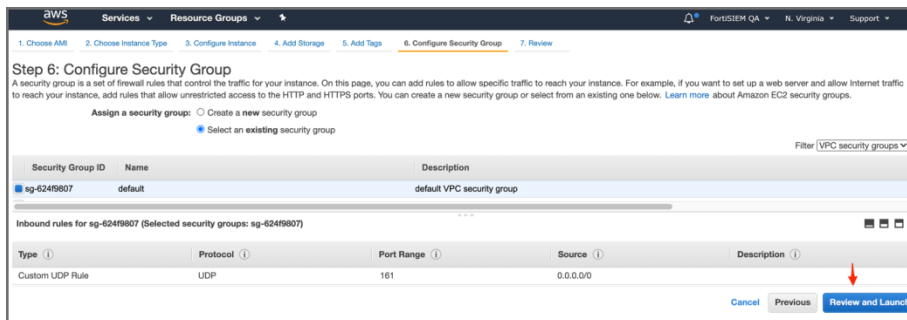
6. In Step 5: Add Tags click the **Add Tag** button.



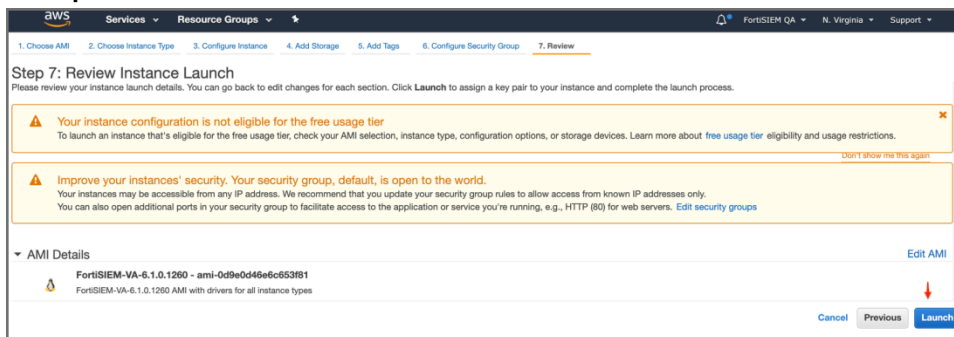
7. Provide a Key name and Value for the tag. Click Next: Configure Security Group.



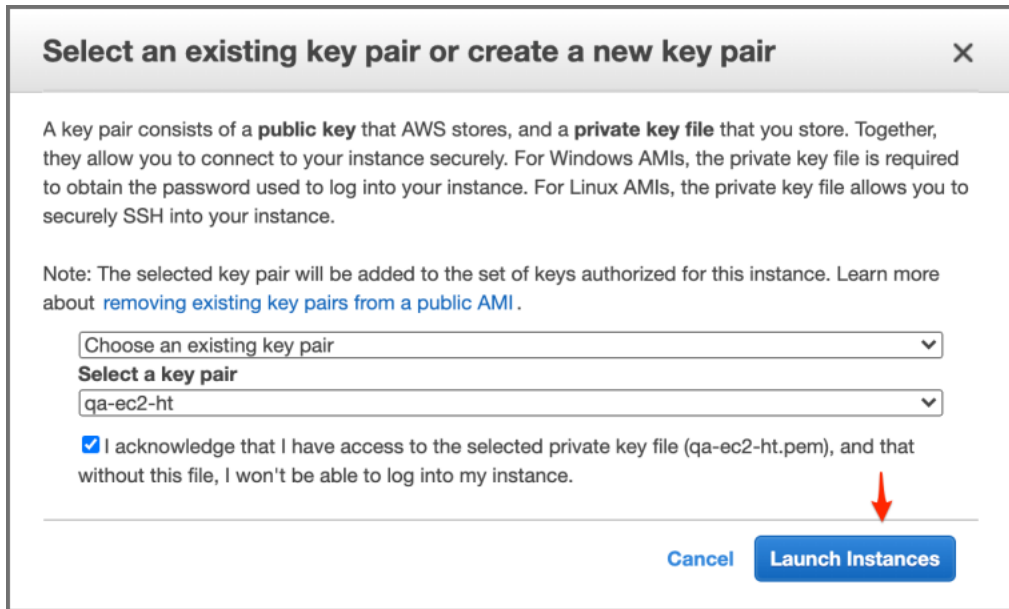
8. In Step 6: Configure Security Group, select any security group because FortSIEM will not be logging into this instance. Click **Review and Launch**.



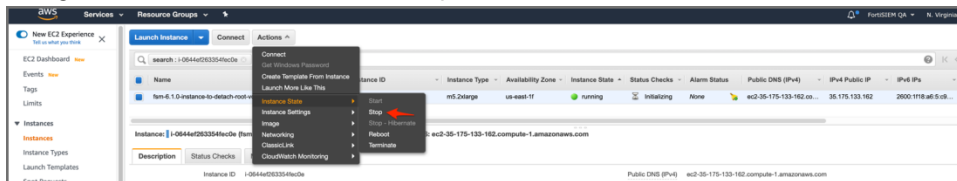
9. In Step 7: Review Instance Launch. Click Launch.



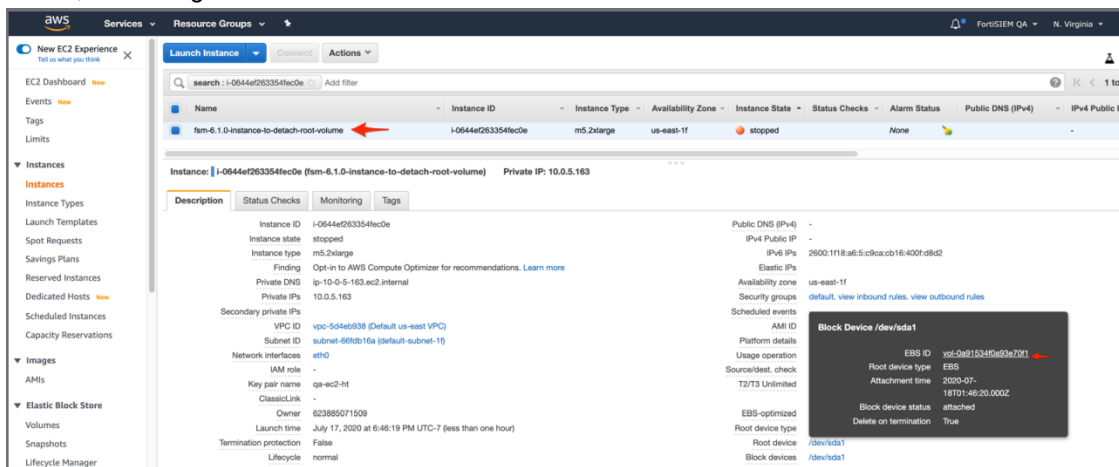
10. Select an existing key pair or create a new key pair. Click **Launch Instances**.



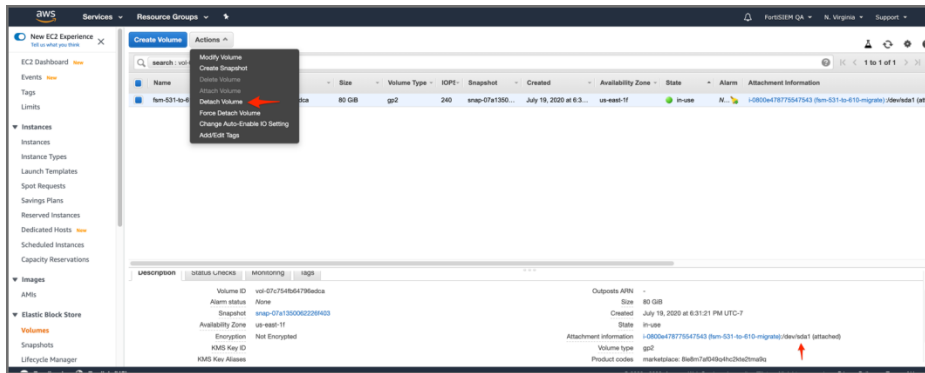
11. Navigate to **Instances**. Select, then stop the instance.



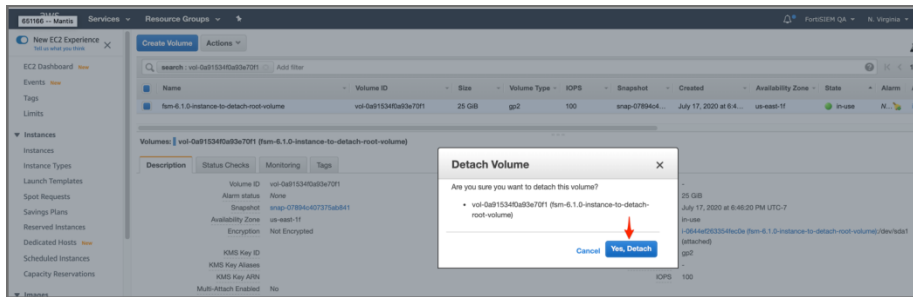
12. Select, then navigate to the root volume.



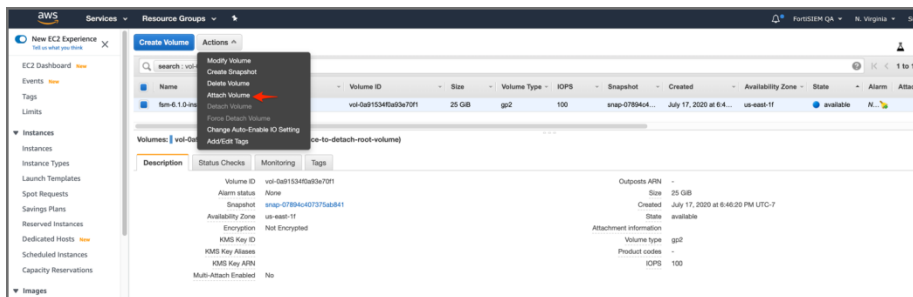
13. Click **Actions > Detach Volume**.



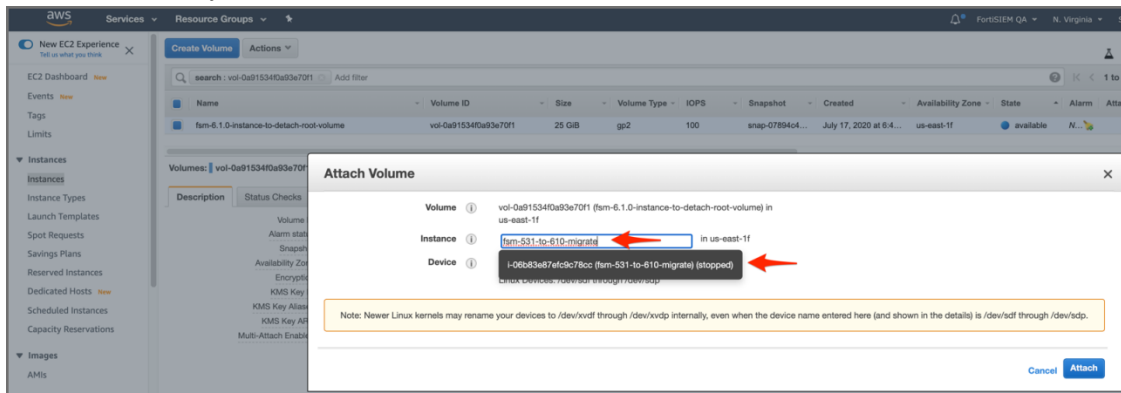
14. Click **Yes, Detach** in the popup window. Wait for the instance state to be Available.



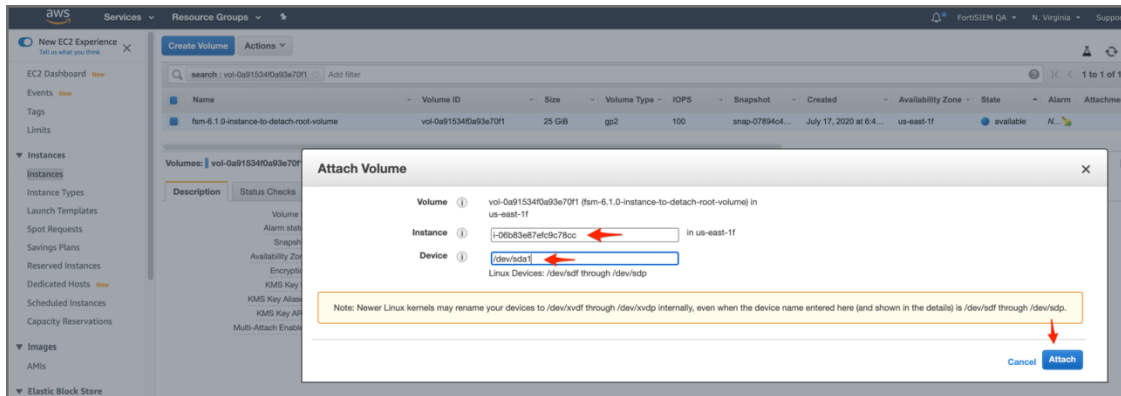
15. Click **Actions > Attach Volume**.



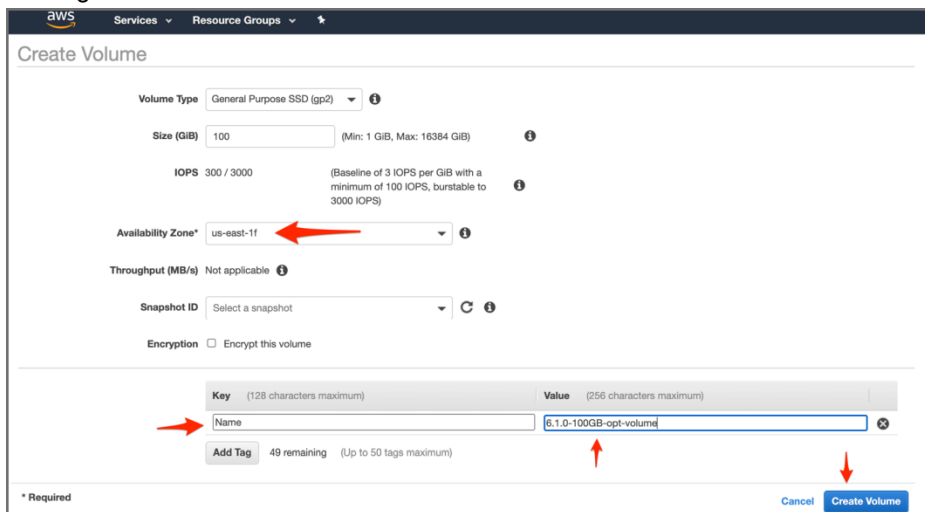
16. Enter the name of your 5.3.0, 5.3.1 or 5.3.2 instance in the **Instance** search box and select it.



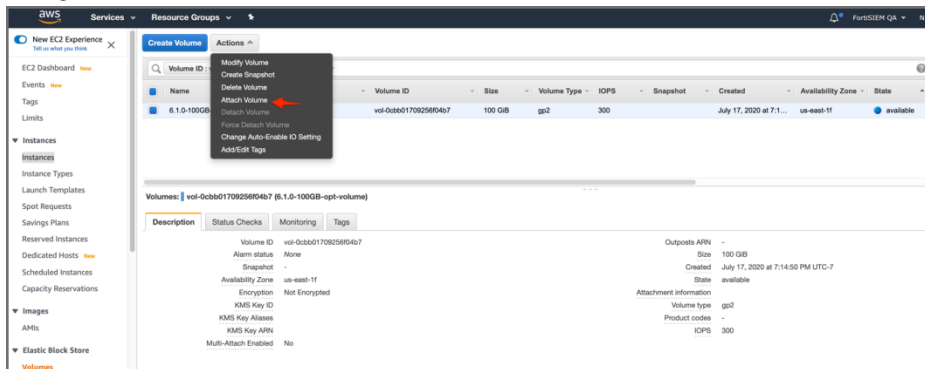
17. Enter the **Device** as `/dev/sda1` and click **Attach**.



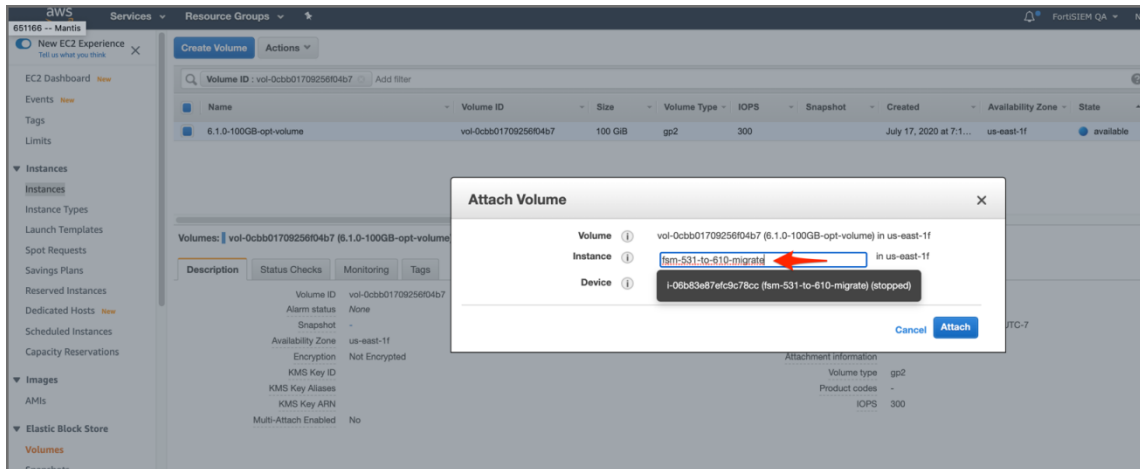
18. Create a new 100GB volume for `/opt` in the same availability zone where your 5.3.0, 5.3.1 or 5.3.2 instance is running. Click **Create Volume**.



19. Navigate to **Volumes**, then click **Actions > Attach Volume**.



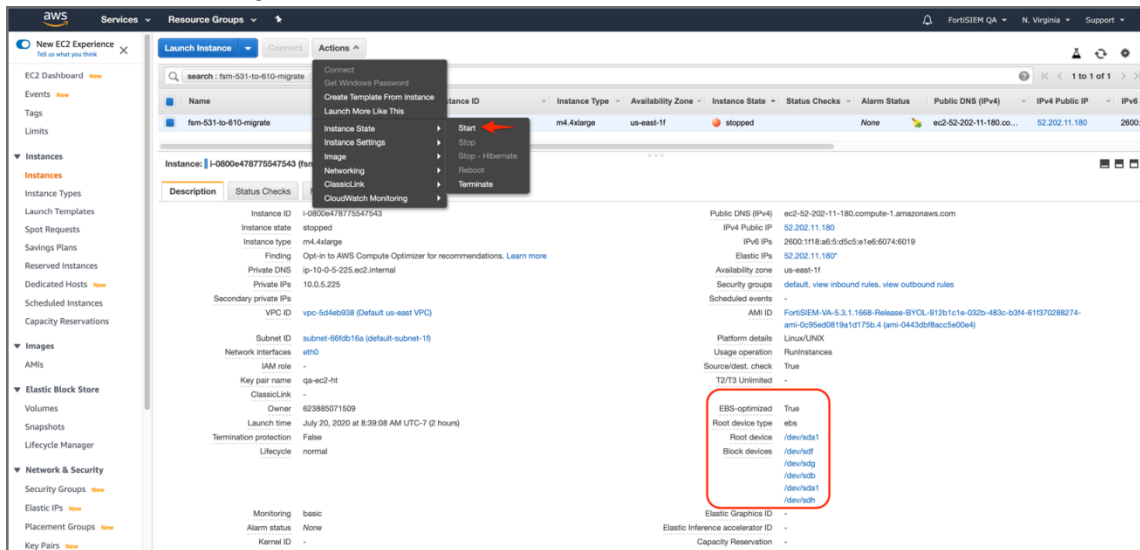
20. Navigate to **Instances** page and select the 5.3.0, 5.3.1 or 5.3.2 instance that you want to migrate to 6.1.0.



Boot Up the 5.3.0, 5.3.1 or 5.3.2 Instance and Migrate to 6.1.0

Follow these steps to complete the migration process:

1. Start the instance using **Actions > Instance State > Start**.

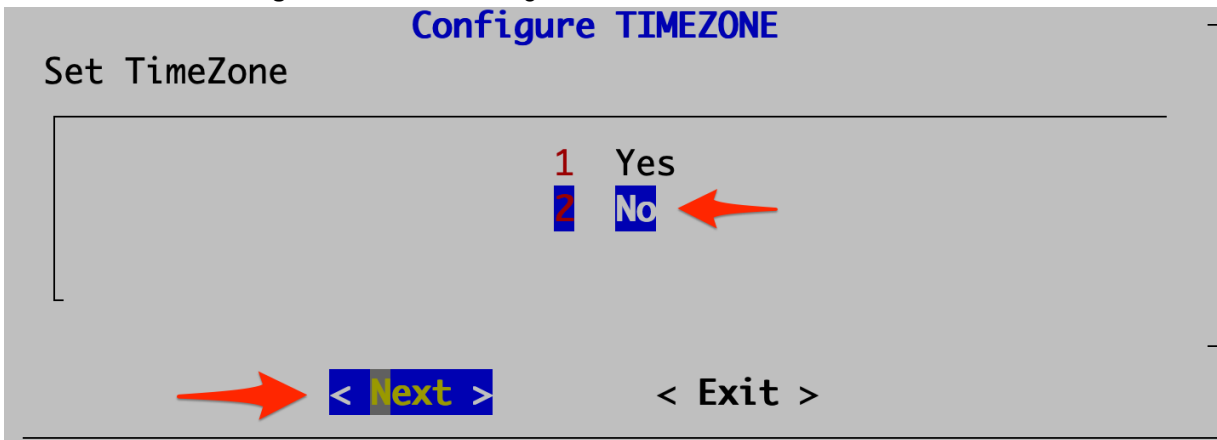


2. Use the `/svn` partition noted earlier and mount it to `/mnt`. This contains the backup of the 5.3.0, 5.3.1 or 5.3.2 system settings that will be used during migration. Copy the 5.3.0, 5.3.1 or 5.3.2 settings that were previously backed up and unmount `/mnt`. For example:

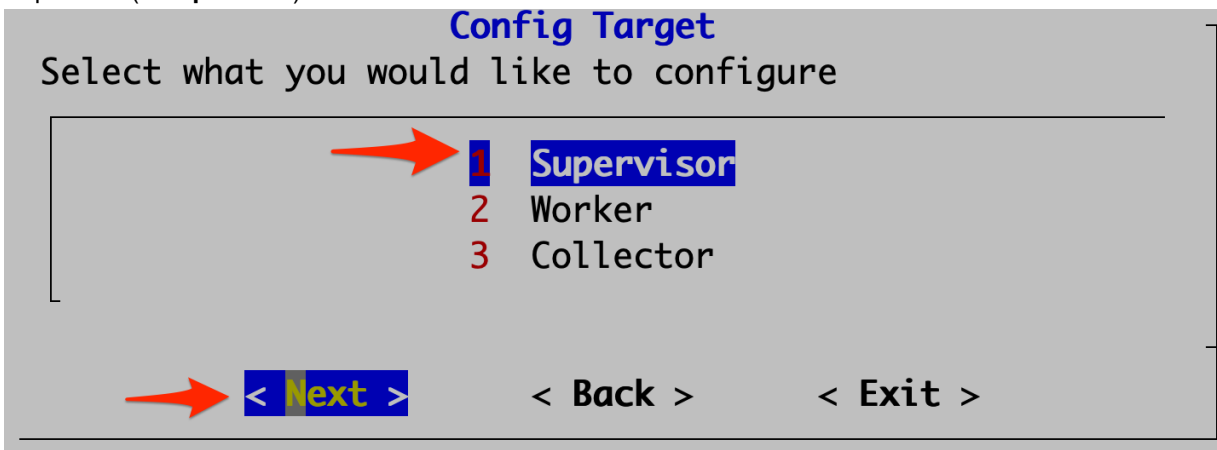
```
# mount /dev/xvdx1 /mnt
# mkdir /restore-53x-settings
# cd /restore-53x-settings
# rsync -av /mnt/53x-settings/.
# ln -sf /restore-53x-settings/images
# umount /mnt
```

3. Run the command `configFSM.sh` script to open the configuration GUI:

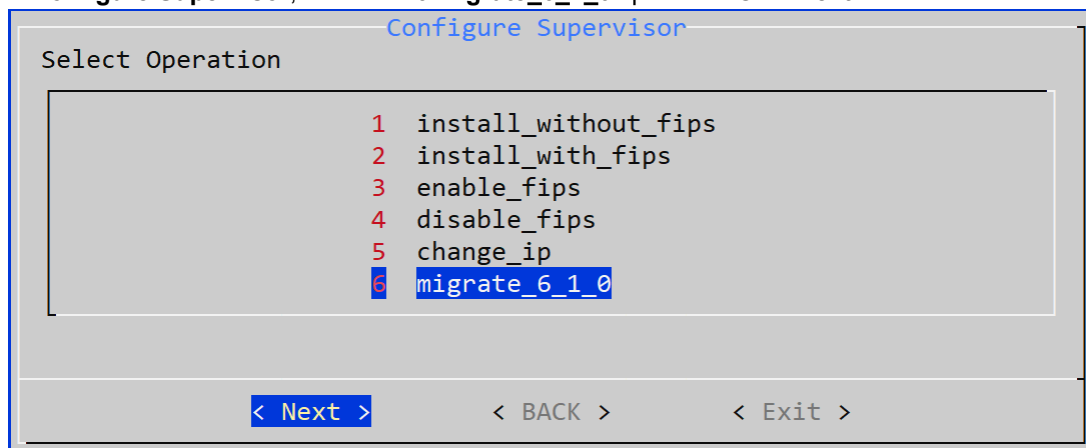
a. Select **2 No** in the **Configure TIMEZONE** dialog. Click **Next**.



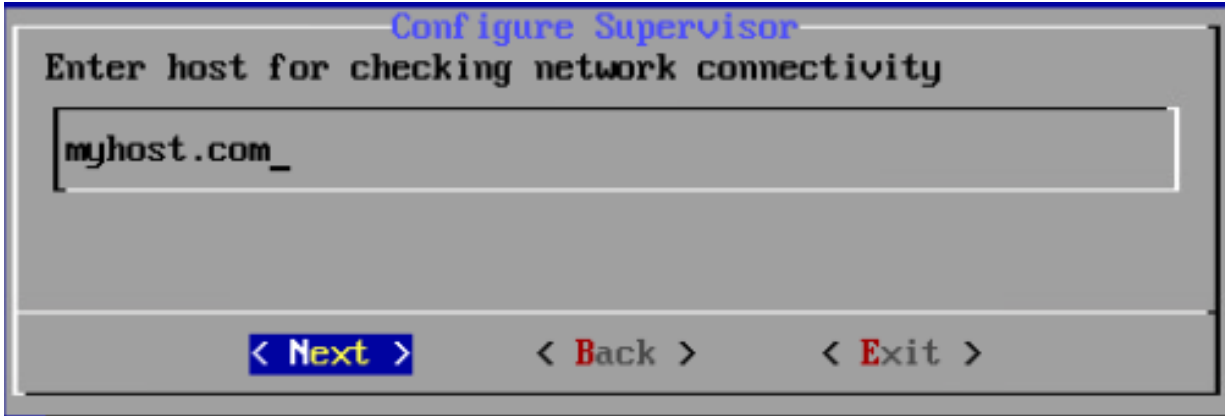
b. In **Config Target**, select your node type: Supervisor, Worker, or Collector. This step is usually performed on Supervisor (**1 Supervisor**). Click **Next**.



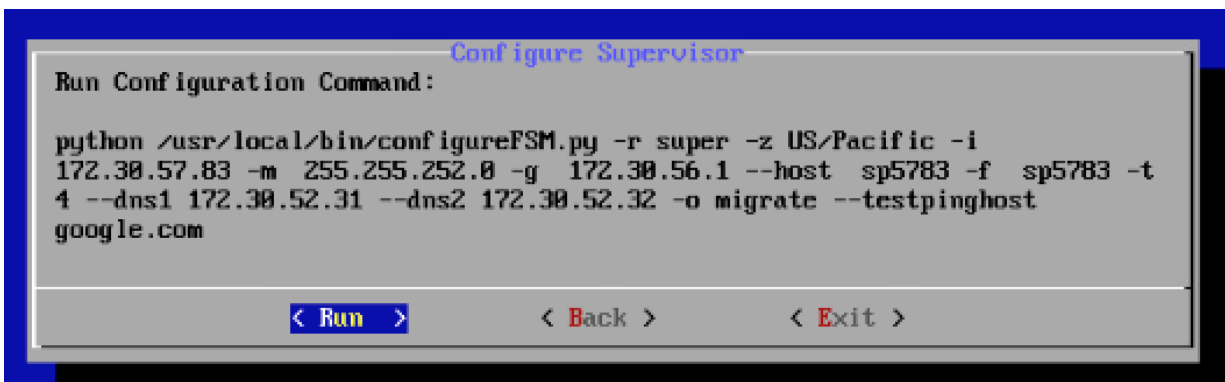
c. In **Configure Supervisor**, select the **6 migrate_6_1_0** operation. Click **Next**.



d. 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. Click **Next**.



- e. Click **Run** on the confirmation page once you make sure all the values are correct. The options are described in the table [here](#).



- f. Wait for the operations to complete and the system to reboot.



- g. Wait for about 2 minutes before logging in to the system. Wait another 5-10 minutes for all of the processes to start up. Execute the `phstatus` command to see the status of FortiSIEM processes.


```
$ ssh ec2-user@ec2-52-202-11-180.compute-1.amazonaws.com
Last login: Mon Jul 20 14:54:35 2020 from 69.181.213.37
[ec2-user@fsm-531-to-610-migrate ~]$ sudo su -
Last login: Mon Jul 20 14:54:39 EDT 2020 on pts/0
[root@fsm-531-to-610-migrate ~]# phstatus.py
System uptime: 14:55:11 up 2 min, 1 user, load average: 1.55, 0.84, 0.33
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16 cores, 0.2%us, 0.1%sy, 0.0%ni, 99.6%id, 0.0%wa, 0.1%hi, 0.0%si, 0.0%st
Mem: 65675424k total, 9388188k used, 56287236k free, 9184k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2493084k cached
```

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	00:55	0	2161m	585m
phQueryMaster	00:55	0	954m	74m
phRuleMaster	00:55	0	638m	56m
phRuleWorker	00:55	0	1357m	281m
phQueryWorker	00:55	0	1377m	277m
phDataManager	00:55	0	1196m	60m
phDiscover	00:55	0	516m	67m
phReportWorker	00:55	0	1420m	90m
phReportMaster	00:55	0	558m	58m
phIpIdentityWorker	00:55	0	1030m	57m
phIpIdentityMaster	00:55	0	492m	50m
phAgentManager	00:55	0	1452m	53m
phCheckpoint	00:55	0	325m	33m
phPerfMonitor	00:55	0	809m	82m
phReportLoader	00:55	0	763m	277m
phBeaconEventPackager	00:55	0	1129m	64m
phDataPurger	00:55	0	583m	60m
phEventForwarder	00:55	0	549m	45m
phMonitor	00:58	0	1455m	612m
Apache	02:33	0	311m	15m
Node.js-charting	02:26	0	913m	84m
Node.js-pm2	02:26	0	0	7164
AppSvr	02:24	0	15111m	2852m
DBSvr	02:33	0	317m	30m
phAnomaly	00:56	0	1495m	67m
phFortiInsightAI	02:33	0	23425m	296m
Redis	02:26	0	53m	22m

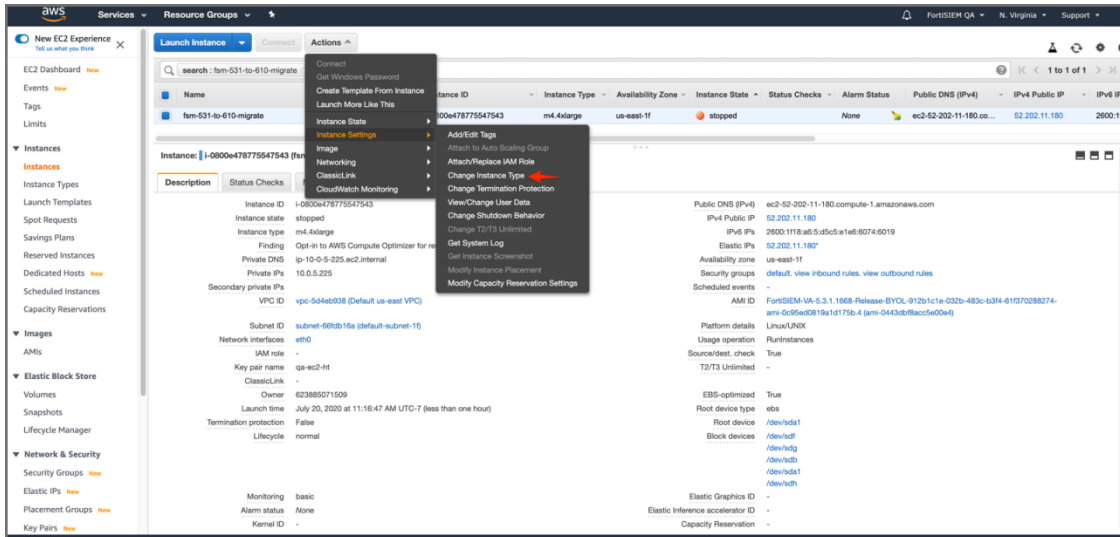
- h. Remove the restored settings directories because you no longer need them, for example:

```
# rm -rf /restore-53x-settings
# rm -rf /svn/53x-settings
# rm -f /images
```

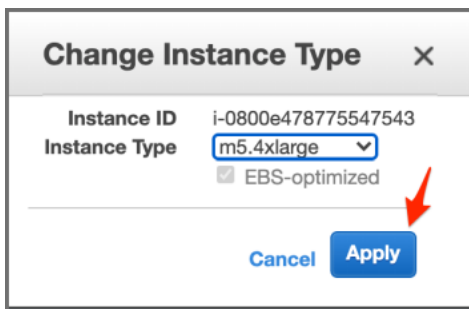
(Optional) Change Instance Type to the Latest Generation

If you would like to change the instance type to one in the current generation for higher performance, this is a good time to do it. 5.3.0, 5.3.1 or 5.3.2 and earlier versions do not support m5 (AWS Nitro) instance types. FSM 6.1.0 supports all instance types that have the recommended vCPU/memory levels. This step may require a reset of FortiSIEM license for the UUID change.

To do this, stop the instance and change instance type as follows, then start the instance again.



Select the **Instance Type** from the drop-down list and click **Apply**.



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 6.1.0 Collectors
- Register 6.1.0 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 6.1.0 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 6.1.0 Workers to the 6.1.0 Supervisor. The 6.1.0 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 6.1.0 Supervisor and Workers. You can install 6.1.0 collectors at your convenience.

Install 6.1.0 Collectors

FortiSIEM does not support Collector migration to 6.1.0. You can install new 6.1.0 Collectors and register them to 6.1.0 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-6.1.0 Collector.
3. Install the 6.1.0 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 6.1.0 Collector. This step is needed for Agents to work seamlessly with 6.1.0 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 6.1.0 migration, this password is lost.

Register 6.1.0 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-6.1.0 Collector. Specifically, use this form of the

`phProvisionCollector` command to register a 6.1.0 Collector and keep the old associations:

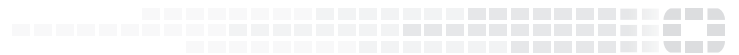
```
# /opt/phoenix/bin/phProvisionCollector --update <user> '<password>' <Super IP or Host>
  <Organization> <CollectorName>
```

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.



FORTINET®



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.