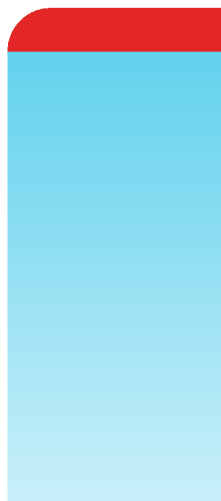


Upgrade Guide

FortiSIEM 6.4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



02/15/2024

FortiSIEM 6.4.0 Upgrade Guide

TABLE OF CONTENTS

Upgrade Paths	6
Important Notes	8
Pre-Upgrade Checklist	8
6.2.0 to 6.4.0 Upgrade Notes	8
6.1.x to 6.4.0 Upgrade Notes	8
General Upgrade Notes	9
Upgrade Pre-5.3.0 Deployment	10
Upgrade 5.3.x or 5.4.0 Deployment	13
Upgrade 6.x Deployment	15
Upgrade 6.x Single Node Deployment	16
Upgrade Supervisor	16
Upgrade Collectors	17
Extra Upgrade Steps from 6.2.0 to 6.4.0	17
Main Upgrade Steps	18
Upgrade 6.x Cluster Deployment	19
Overview	19
Detailed Steps	19
Upgrade Supervisor	20
Upgrade Workers	21
Upgrade Collectors	22
Extra Upgrade Steps from 6.2.0 to 6.4.0	22
Main Upgrade Steps	22
Restoring Hardware from Backup After a Failed Upgrade	24
Background Information	24
Restoring from Backup	24
Upgrading with Disaster Recovery Enabled	30
Post Upgrade Health Check	31
Upgrade via Proxy	36
Upgrade Log	37
Migrate Log	38
Reference	39
Steps for Expanding /opt Disk	39
Fix After Upgrading 2000F, 3500F, 3500G from 5.3.x or 5.4.0 to 6.1.2	40
Post Upgrade Health Check get-fsm-health.py --local Example Output	40

Change Log

Date	Change Description
03/22/2021	Initial version of the 6.2.0 Upgrade Guide.
03/29/2021	Added Upgrade via Proxy and Post Upgrade Health Check.
03/31/2021	Added Reference section with additional DNS information.
04/05/2021	Updated Pre-Upgrade Checklist.
04/22/2021	Added Upgrade and Migrate Log sections.
05/06/2021	Initial version of the 6.2.1 Upgrade Guide.
05/12/2021	Updated Upgrade via Proxy section.
05/17/2021	Updated existing heading, added Sizing Guide link, removed DNS check for 6.2.1 Upgrade Guide.
05/19/2021	Added "Fix After Upgrading 2000F or 3500F From 5.3.x or 5.4.0 to 6.1.2" section for 6.2.x Upgrade Guides.
05/21/2021	Update to "After Upgrading 2000F or 3500F From 5.3.x or 5.4.0 to 6.1.2" section for 6.2.x Upgrade Guides.
05/24/2021	Update to "Upgrade Collectors" sections for 6.2.x Upgrade Guides.
06/03/2021	Known Issue after 6.2.1 Upgrade added to 6.2.1 Upgrade Guide.
06/07/2021	Update to "Upgrade Collectors" sections for 6.2.1 Upgrade Guide.
07/08/2021	Initial version of the 6.3.0 Upgrade Guide.
07/21/2021	Updated Pre-Upgrade Checklist section.
07/22/2021	Updated Upgrade via Proxy section.
07/30/2021	Updated Upgrade 6.x Deployment section.
08/26/2021	Initial version of the 6.3.1 Upgrade Guide.
10/15/2021	Initial version of the 6.3.2 Upgrade Guide.
12/01/2021	Updated Pre-Upgrade Checklist section.
12/22/2021	Initial version of the 6.3.3 Upgrade Guide.
01/18/2022	Initial version of the 6.4.0 Upgrade Guide.
02/02/2022	Updated Pre-Upgrade Checklist and Upgrade via Proxy sections for the 6.4.0 Upgrade Guide.
05/23/2022	Initial version of the 6.4.1 Upgrade Guide.
06/03/2022	Updated Post Upgrade Health Check section.

Date	Change Description
09/15/2022	Updated Upgrade Supervisor and Upgrade Workers sections.
12/14/2022	Initial version of the 6.4.2 Upgrade Guide.
09/05/2023	Initial version of the 6.4.3 Upgrade Guide.
10/09/2023	Important Notes Pre-Upgrade Checklist section updated. Upgrade Path diagrams updated.
02/15/2024	Initial version of the 6.4.4 Upgrade Guide.

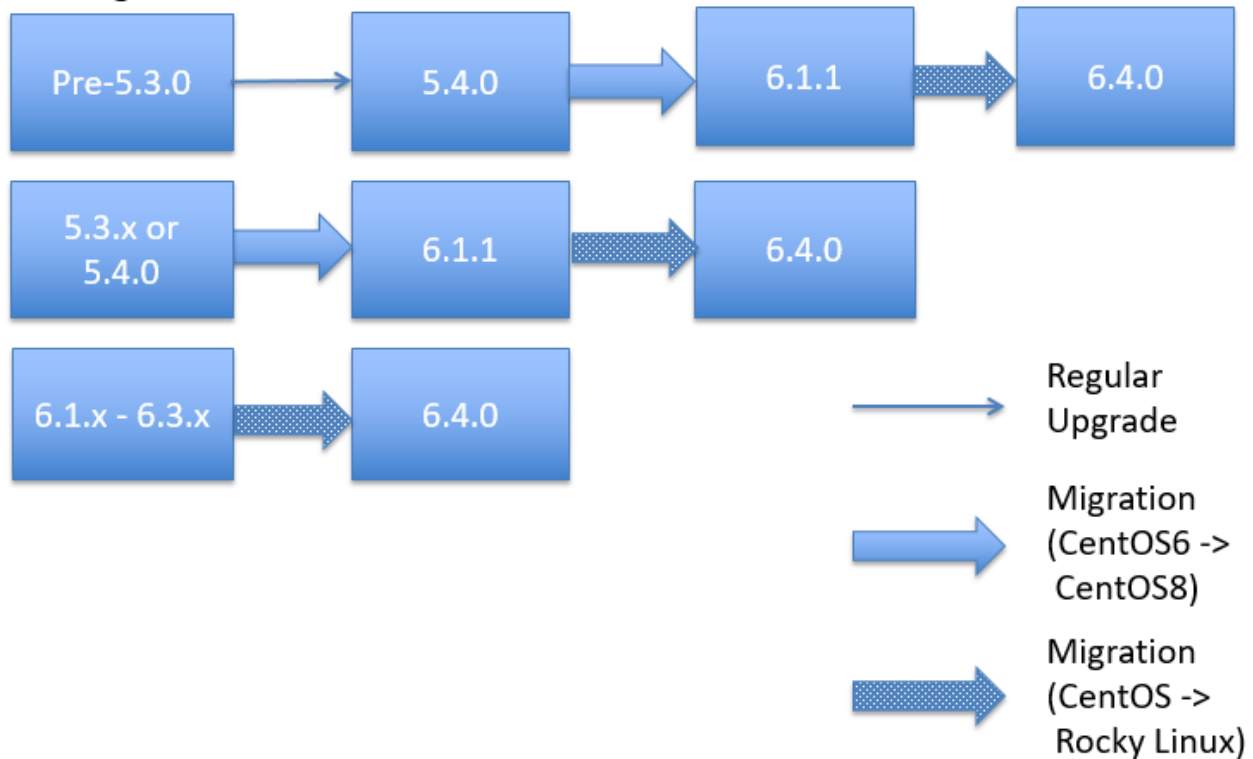
Upgrade Paths

If you are running 6.4.0, 6.4.1, or 6.4.2, Fortinet highly recommends upgrading to 6.7.7 or 7.0.1 or later, instead of upgrading to 6.4.3. If you must upgrade to 6.4.3, then the next upgrade should be to 6.7.7 or 7.0.1 or later, otherwise the Supervisor/Worker upgrade will fail. This is because of bug fix to 915077 which is in 6.7.5 or later, but not back ported to 6.6.4.

Please follow the proceeding upgrade paths to upgrade existing FortiSIEM installs to the latest 6.4.0 release.

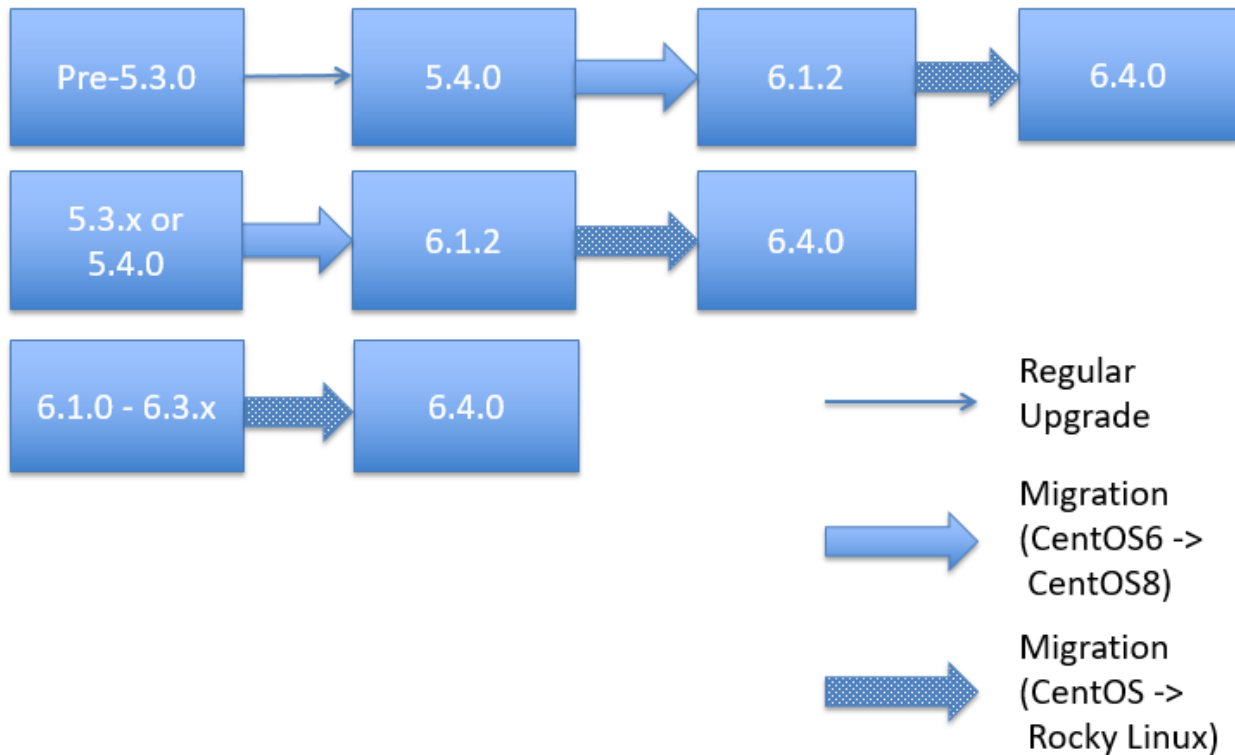
Upgrade for VM Installs

Starting release



Upgrade for 3500G, 3500F, 2000F, 500F

Starting release



Important Notes

Pre-Upgrade Checklist

To perform an upgrade, the following prerequisites must be met.

1. Carefully consider the known issues, if any, in the Release Notes.
2. Make sure the Supervisor processes are all up.
3. Make sure you can login to the FortiSIEM GUI and successfully discover your devices.
4. Take a snapshot of the running FortiSIEM instance.
5. If you running FortiSIEM versions 6.2.0 or earlier and using Elasticsearch, then navigate to **ADMIN > Setup > Storage > Online >** and perform a **Test** and **Save** after the upgrade. This step is not required while upgrading from versions 6.2.1 or later.
6. From version 6.4.0 onwards, FortiSIEM runs on Rocky Linux. If upgrading from a release prior to 6.4.0, then FortiSIEM will automatically migrate the operating system from CentOS to Rocky Linux during the upgrade process. If upgrading from a FortiSIEM 6.4.0 release or later, then FortiSIEM will already be running Rocky Linux, so no additional migration is needed.
7. Make sure the FortiSIEM license is not expired.
8. Make sure the Supervisor, Workers and Collectors can connect to the Internet on port 443 to the Rocky Linux 8 OS repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) hosted by Fortinet, to get the latest OS packages. Connectivity can be either directly or via a proxy. For proxy based upgrades, see [Upgrade via Proxy](#). If Internet connectivity is not available, then follow the [Offline Upgrade Guide](#).

6.2.0 to 6.4.0 Upgrade Notes

This note applies only if you are upgrading from 6.2.0.

Before upgrading Collectors to 6.4.0, you will need to copy the `phcollectorimageinstaller.py` file from the Supervisor to the Collectors. See steps 1-3 in [Upgrade Collectors](#).

6.1.x to 6.4.0 Upgrade Notes

These notes apply only if you are upgrading from 6.1.x to 6.4.0.

1. The 6.4.0 upgrade will attempt to migrate existing SVN files (stored in `/svn`) from the old svn format to the new svn-lite format. During this process, it will first export `/svn` to `/opt` and then import them back to `/svn` in the new svn-lite format. If your `/svn` uses a large amount of disk space, and `/opt` does not have enough disk space left, then migration will fail. Fortinet recommends doing the following steps before upgrading:
 - Check `/svn` usage
 - Check if there is enough disk space left in `/opt` to accommodate `/svn`
 - Expand `/opt` by the size of `/svn`

- Begin upgrade
See [Steps for Expanding /opt Disk](#) for more information.
- 2. If you are using AWS Elasticsearch, then after upgrading to 6.4.0, take the following steps:
 - a. Go to **ADMIN > Setup > Storage> Online**.
 - b. Select "ES-type" and re-enter the credential.

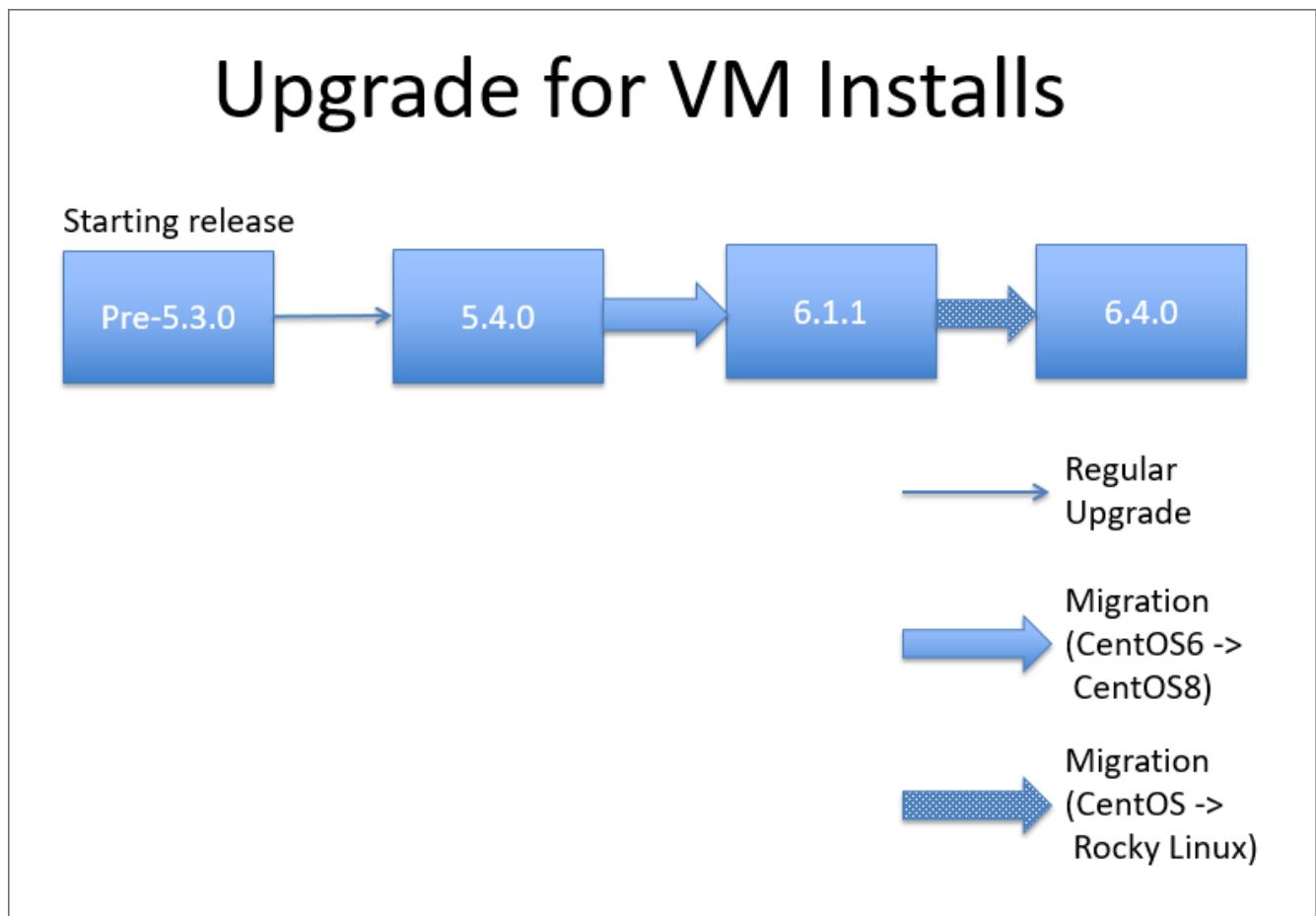
General Upgrade Notes

These notes apply to all upgrades in general.

1. For the Supervisor and Worker, do not use the upgrade menu item in configFSM.sh to upgrade from 6.2.0 to 6.4.0. This is deprecated, so it will not work. Use the new method as instructed in this guide (See **Upgrade Supervisor** for the appropriate deployment under [Upgrade Single Node Deployment](#) or [Upgrade Cluster Deployment](#)).
2. In 6.1.x releases, new 5.x collectors could not register to the Supervisor. This restriction has been removed in 6.2.x so long as the Supervisor is running in non-FIPS mode. However, 5.x collectors are not recommended since CentOS 6 has been declared End of Life.
3. Remember to remove the browser cache after logging on to the 6.4.0 GUI and before doing any operations.
4. Make sure to follow the listed upgrade order.
 - a. Upgrade the Supervisor first. It must be upgraded prior to upgrading any Workers or Collectors.
 - b. Upgrade all existing Workers next, after upgrading the Supervisor. The Supervisor and Workers must be on the same version.
 - c. Older Collectors will work with the upgraded Supervisor and Workers. You can decide to upgrade Collectors to get the full feature set in 6.4.0 after you have upgraded all Workers.
5. If you are running FortiSIEM versions 6.2.0 or earlier and using Elasticsearch, then you must redo your Elasticsearch configuration after your upgrade by taking the following steps:
 - a. Navigate to **ADMIN > Setup > Storage > Online**.
 - b. Redo your configuration.
 - c. Click **Test** to verify.
 - d. Click **Save**.

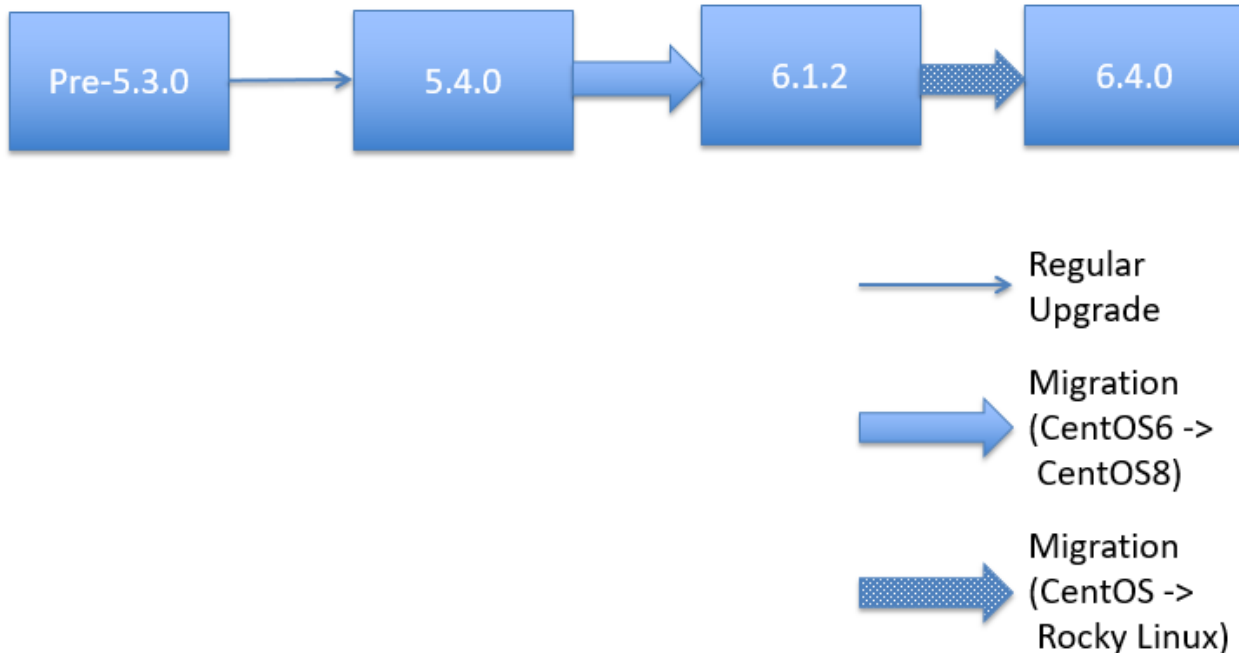
Note: These steps (5a-d) are not required while upgrading from versions 6.2.1 or later.

Upgrade Pre-5.3.0 Deployment



Upgrade for 3500G, 3500F, 2000F, 500F

Starting release



If you are running FortiSIEM that is pre-5.3.0, take the following steps:

1. Upgrade to 5.4.0 by using the 5.4.0 Upgrade Guide: [Single Node Deployment / Cluster Deployment](#).
2. Perform a health check to make sure the system has upgraded to 5.4.0 successfully.
3. If you are running a Software Virtual Appliance, you must migrate to 6.1.1. Since the base OS changed from CentOS 6 to CentOS 8, the steps are platform specific. Use the appropriate 6.1.1 guide and follow the migration instructions.
 - [AWS Installation and Migration Guide](#)
 - [ESX Installation and Migration Guide](#)
 - [KVM Installation and Migration Guide](#)
 - [HyperV Installation and Migration Guide](#)
 - [Azure Installation and Migration Guide](#)

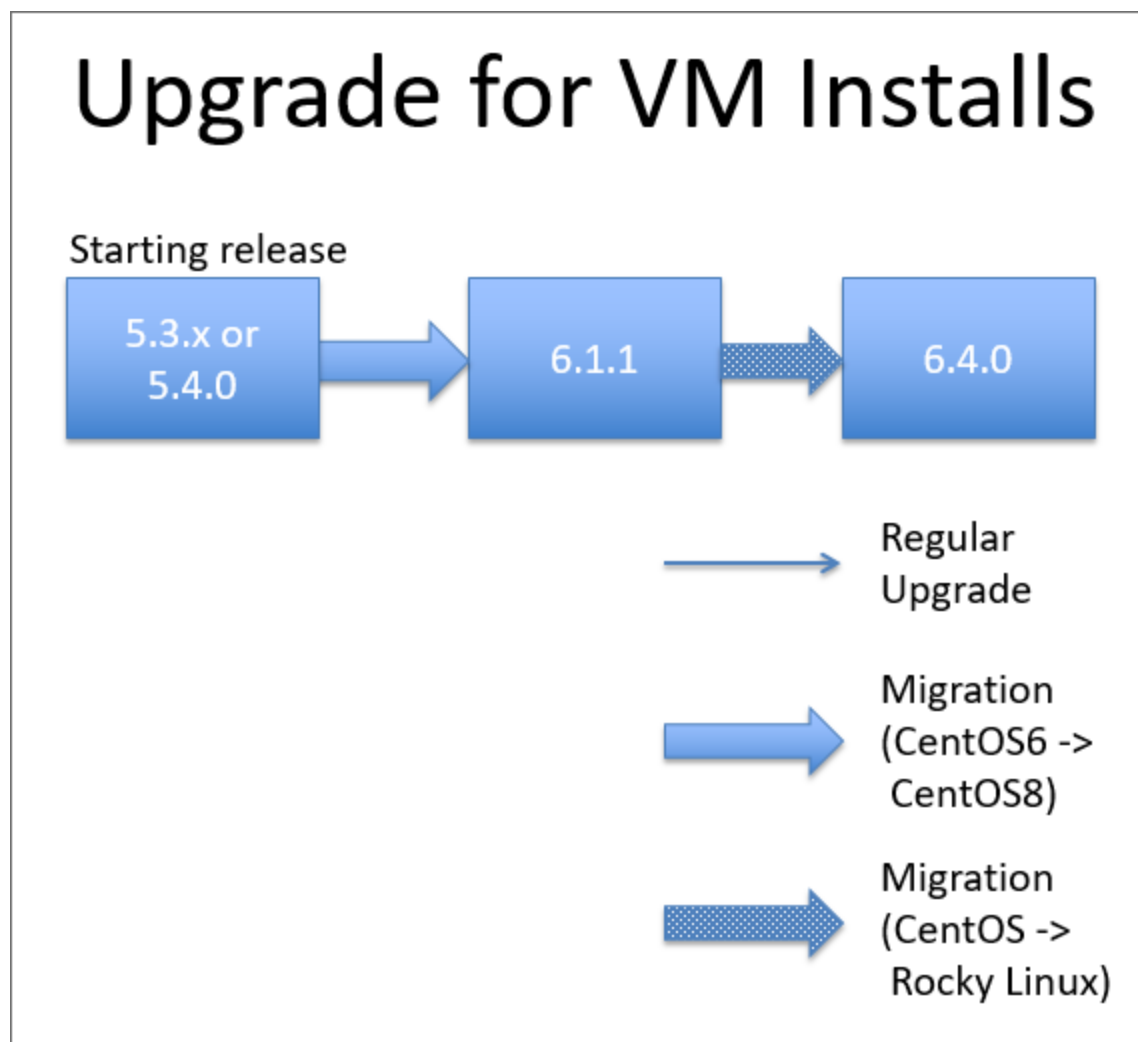
If you are running a hardware appliance (3500G, 3500F, 2000F, 500F), you must migrate to 6.1.2. Since the base OS changed from CentOS 6 to CentOS 8, the steps are platform specific. Follow the "Migrating from 5.3.x or 5.4.x to 6.1.2" instructions from the appropriate appliance specific documents listed here.

Note: If you are upgrading from a 2000F, 3500F, or 3500G appliance, make sure to follow the instructions at [Fix After Upgrading 2000F, 3500F, or 3500G From 5.3.x or 5.4.0 to 6.1.2](#) after migrating to 6.1.2.

- [3500G Hardware Configuration Guide](#)
- [3500F Hardware Configuration Guide](#)

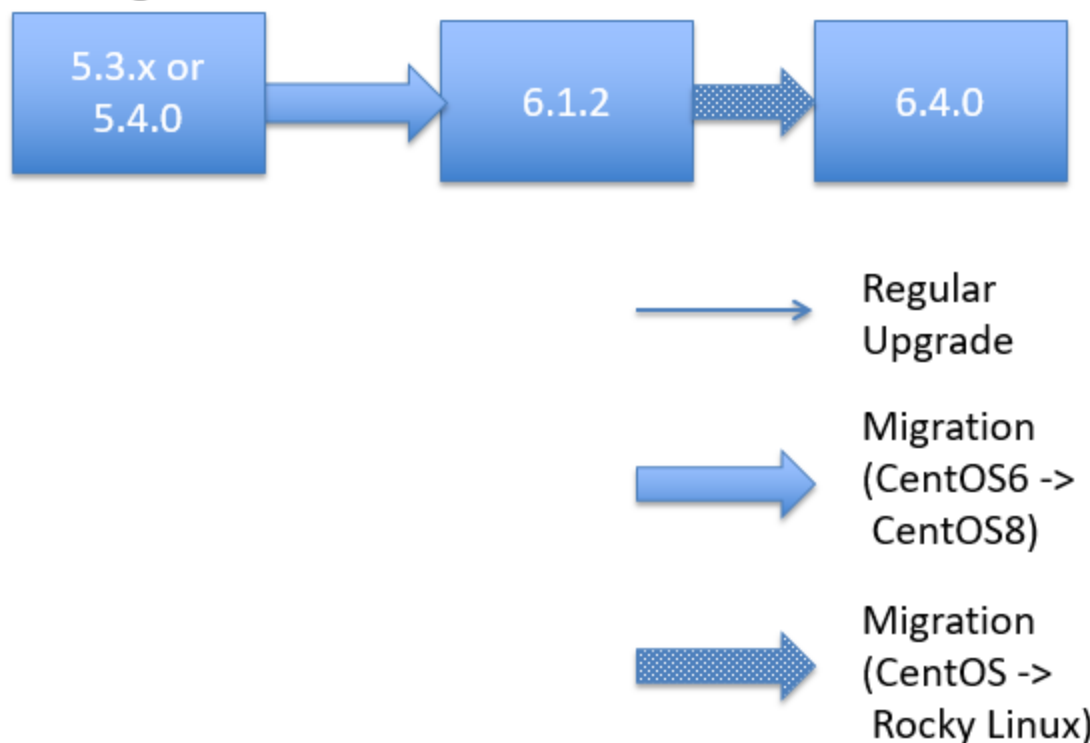
- [2000F Hardware Configuration Guide](#)
 - [500F Hardware Configuration Guide](#)
4. Perform a health check to make sure the system is upgraded to 6.1.1 or 6.1.2 successfully.
 5. Upgrade to 6.3.x by following the steps in [Upgrading From 6.x](#).

Upgrade 5.3.x or 5.4.0 Deployment



Upgrade for 3500G, 3500F, 2000F, 500F

Starting release



Start at [step 3](#) from [Upgrade Pre-5.3.0 Deployment](#), and follow the progressive steps.

Note: If you are upgrading from a 2000F, 3500F, 3500G appliance, make sure to follow the instructions at [Fix After Upgrading 2000F, 3500F, or 3500G From 5.3.x or 5.4.0 to 6.1.2](#) after migrating to 6.1.2.

Upgrade 6.x Deployment

Note: Prior to the 6.x Deployment 6.4.0 upgrade, ensure that the Supervisor, and all Workers are running on 6.x versions.

If a proxy is needed for the FortiSIEM Supervisor, Worker or Hardware appliances (FSM-2000F, 3500F, and 3500G) to access the Internet, please refer to [Upgrade via Proxy](#) before starting.

After completion of the upgrade, follow the appropriate steps in [Post Upgrade Health Check](#).

Follow the steps for your appropriate FortiSIEM setup for [single node deployment](#) or [cluster deployment](#).

- [Upgrade Single Node Deployment](#)
- [Upgrade Cluster Deployment](#)

Upgrade 6.x Single Node Deployment

Upgrading a single node deployment requires upgrading the Supervisor. If you have any Collectors, the Supervisor is a required upgrade before the Collectors.

- [Upgrade Supervisor](#)
- [Upgrade Collectors](#)

Upgrade Supervisor

To upgrade the Supervisor, take the following steps.

1. Make sure Workers are shut down. Collectors can remain up and running.
2. Login to the Supervisor via SSH as the root user directly, or SSH as admin user and then sudo to root.
For example:

```
ssh root@<IP of Supervisor>  
or  
ssh admin@<IP of Supervisor>  
sudo su -
```
3. Create the path `/opt/upgrade`.

```
mkdir -p /opt/upgrade
```
4. Download the upgrade zip package `FSM_Upgrade_All_6.4.0_build1412.zip`, then upload it to the Supervisor node under the `/opt/upgrade/` folder.
Example (From Linux CLI):

```
scp FSM_Upgrade_All_6.4.0_build1412.zip root@10.10.10.15:/opt/upgrade/
```
5. Go to `/opt/upgrade`.

```
cd /opt/upgrade
```
6. Unzip the upgrade zip package.

```
unzip FSM_Upgrade_All_6.4.0_build1412.zip
```
7. Go to the `FSM_Upgrade_All_6.4.0_build1412` directory.

```
cd FSM_Upgrade_All_6.4.0_build1412
```

 - a. Run a screen.

```
screen -S upgrade
```

Note: This is intended for situations where network connectivity is less than favorable. If there is any connection loss, log back into the SSH console and return to the virtual screen by using the following command.

```
screen -r
```
8. Start the upgrade process by entering the following.

```
sh upgrade.sh
```
9. After the process is completed, perform a basic health check. All processes should be up and running.

```
phstatus
```

Example output:

```
System uptime: 13:31:19 up 1 day, 2:44, 1 user, load average: 0.95, 1.00, 1.20  
Tasks: 29 total, 0 running, 29 sleeping, 0 stopped, 0 zombie  
Cpu(s): 8 cores, 15.4%us, 0.5%sy, 0.0%ni, 83.6%id, 0.0%wa, 0.4%hi, 0.1%si, 0.0%st
```


Mem: 24468880k total, 12074704k used, 10214416k free, 5248k buffers
 Swap: 26058744k total, 0k used, 26058744k free, 2931812k cached

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	23:57:06	0	2276m	695m
phQueryMaster	1-02:40:44	0	986m	99m
phRuleMaster	1-02:40:44	0	1315m	650m
phRuleWorker	1-02:40:44	0	1420m	252m
phQueryWorker	1-02:40:44	0	1450m	113m
phDataManager	1-02:40:44	0	1195m	101m
phDiscover	1-02:40:44	0	542m	59m
phReportWorker	1-02:40:44	0	1482m	193m
phReportMaster	1-02:40:44	0	694m	84m
phIpIdentityWorker	1-02:40:44	0	1044m	85m
phIpIdentityMaster	1-02:40:44	0	505m	43m
phAgentManager	1-02:40:44	0	1526m	71m
phCheckpoint	1-02:40:44	0	305m	49m
phPerfMonitor	1-02:40:44	0	820m	82m
phReportLoader	1-02:40:44	0	826m	327m
phDataPurger	1-02:40:44	0	613m	88m
phEventForwarder	1-02:40:44	0	534m	37m
phMonitor	1-02:40:49	0	1322m	629m
Apache	1-02:43:50	0	305m	15m
Rsyslogd	1-02:43:49	0	192m	4224k
Node.js-charting	1-02:43:43	0	614m	80m
Node.js-pm2	1-02:43:41	0	681m	61m
phFortiInsightAI	1-02:43:50	0	13996m	374m
AppSvr	1-02:43:38	14	11149m	4459m
DBSvr	1-02:43:50	0	425m	37m
JavaQueryServer	1-02:40:49	0	10881m	1579m
phAnomaly	1-02:40:29	0	982m	61m
SVNLite	1-02:43:50	0	9870m	450m
Redis	1-02:43:43	0	107m	70m

Upgrade Collectors

To upgrade Collectors, take the following steps.

Extra Upgrade Steps from 6.2.0 to 6.4.0

From version 6.2.0 to 6.4.0, take the following steps before initiating the upgrade. Otherwise, go to [Main Upgrade Steps](#).

1. Login to the Collector via SSH as root.
2. Copy `/opt/phoenix/phscripts/bin/phcollectorimageinstaller.py` from the Supervisor by running the following command. (**Note:** This is copied from the 6.2.1 or 6.4.0 Supervisor.)

```
scp root@<SupervisorIP>:/opt/phoenix/phscripts/bin/phcollectorimageinstaller.py
/opt/phoenix/phscripts/bin/
```

3. Change permission by running the following command.

```
chmod 755 /opt/phoenix/phscripts/bin/phcollectorimageinstaller.py
```

Main Upgrade Steps

To upgrade your FortiSIEM Collectors, follow the steps in [Installation Through Image Server Page](#).

Note: Installation through Image Server requires FortiSIEM 6.4.0 or higher.

Installation Through Image Server Page

To install through the Image Server GUI, take the following steps:

Note: Installation through Image Server requires FortiSIEM 6.4.0 or higher.

1. Navigate to Click **ADMIN > Settings > System > Image Server**.
2. Follow the instructions [here](#).

Upgrade 6.x Cluster Deployment

It is critical to review [Overview](#) prior to taking the detailed steps to upgrade your FortiSIEM cluster.

- [Overview](#)
- [Detailed Steps](#)
- [Upgrade Supervisor](#)
- [Upgrade Workers](#)
- [Upgrade Collectors](#)

Overview

1. Shut down all Workers.
 - Collectors can be up and running.
2. Upgrade the Supervisor first, while all Workers are shut down.
3. After the Supervisor upgrade is complete, verify the Supervisor's health.
4. Upgrade each Worker individually, then verify the Worker's health.
5. If your online storage is Elasticsearch, take the following steps:
 - a. Navigate to **ADMIN > Setup > Storage > Online**.
 - b. Click **Test** to verify the space.
 - c. Click **Save** to save.
6. Upgrade each Collector individually.

Notes:

- Step 1 prevents the accumulation of Report files when the Supervisor is not available during its upgrade. If these steps are not followed, the Supervisor may not come up after the upgrade because of excessive unprocessed report file accumulation.
- Both the Supervisor and Workers must be on the same FortiSIEM version, otherwise various software modules may not work properly. However, Collectors can be in an older version, one version older to be exact. These Collectors will work, however they may not have the latest discovery and performance monitoring features offered in the latest Supervisor/Worker versions. FortiSIEM recommends that you upgrade the Collectors as soon as possible. If you have Collectors in your deployment, make sure you have configured an image server to use as a repository for them.

Detailed Steps

Take the following steps to upgrade your FortiSIEM cluster.

1. Shutdown all Worker nodes.
`# shutdown now`
2. Upgrade the Supervisor using the steps in [Upgrade Supervisor](#). Make sure the Supervisor is running the version you have upgraded to and that all processes are up and running.

```
# phshowVersion.sh
# phstatus
```

3. If you are running Elasticsearch, and upgrading from 6.1.x to 6.4.0, then take the following steps, else skip this step and proceed to Step 4.
 - a. Navigate to **ADMIN > Storage > Online > Elasticsearch**.
 - b. Verify that the Elasticsearch cluster has enough nodes (each type node \geq replica + 1).
 - c. Go to **ADMIN > Setup > Storage > Online**.
 - d. Select "ES-type" and re-enter the credential of the Elasticsearch cluster.
 - e. Click **Test and Save**. This important step pushes the latest event attribute definitions to Elasticsearch.
4. Upgrade each Worker one by one, using the procedure in [Upgrade Workers](#).
5. Login to the Supervisor and go to **ADMIN > Health > Cloud Health** to ensure that all Workers and Supervisor have been upgraded to the intended version.

Note: The Supervisor and Workers must be on the same version.
6. Upgrade Collectors using the steps in [Upgrade Collectors](#).

Upgrade Supervisor

To upgrade the Supervisor, take the following steps.

1. Make sure Workers are shut down. Collectors can remain up and running.
2. Login to the Supervisor via SSH as the root user directly, or SSH as admin user and then sudo to root.
For example:


```
ssh root@<IP of Supervisor>
or
ssh admin@<IP of Supervisor>
sudo su -
```
3. Create the path /opt/upgrade.


```
mkdir -p /opt/upgrade
```
4. Download the upgrade zip package `FSM_Upgrade_All_6.4.0_build1412.zip`, then upload it to the Supervisor node under the /opt/upgrade/ folder.
Example (From Linux CLI):


```
scp FSM_Upgrade_All_6.4.0_build1412.zip root@10.10.10.15:/opt/upgrade/
```
5. Go to /opt/upgrade.


```
cd /opt/upgrade
```
6. Unzip the upgrade zip package.


```
unzip FSM_Upgrade_All_6.4.0_build1412.zip
```
7. Go to the `FSM_Upgrade_All_6.4.0_build1412` directory.


```
cd FSM_Upgrade_All_6.4.0_build1412
```

 - a. Run a screen.


```
screen -S upgrade
```

Note: This is intended for situations where network connectivity is less than favorable. If there is any connection loss, log back into the SSH console and return to the virtual screen by using the following command.

```
screen -r
```
8. Start the upgrade process by entering the following.


```
sh upgrade.sh
```
9. After the process is completed, perform a basic health check. All processes should be up and running.


```
phstatus
```

Example output:

```
System uptime: 13:31:19 up 1 day, 2:44, 1 user, load average: 0.95, 1.00, 1.20
Tasks: 29 total, 0 running, 29 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 15.4%us, 0.5%sy, 0.0%ni, 83.6%id, 0.0%wa, 0.4%hi, 0.1%si, 0.0%st
Mem: 24468880k total, 12074704k used, 10214416k free, 5248k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2931812k cached
```

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	23:57:06	0	2276m	695m
phQueryMaster	1-02:40:44	0	986m	99m
phRuleMaster	1-02:40:44	0	1315m	650m
phRuleWorker	1-02:40:44	0	1420m	252m
phQueryWorker	1-02:40:44	0	1450m	113m
phDataManager	1-02:40:44	0	1195m	101m
phDiscover	1-02:40:44	0	542m	59m
phReportWorker	1-02:40:44	0	1482m	193m
phReportMaster	1-02:40:44	0	694m	84m
phIpIdentityWorker	1-02:40:44	0	1044m	85m
phIpIdentityMaster	1-02:40:44	0	505m	43m
phAgentManager	1-02:40:44	0	1526m	71m
phCheckpoint	1-02:40:44	0	305m	49m
phPerfMonitor	1-02:40:44	0	820m	82m
phReportLoader	1-02:40:44	0	826m	327m
phDataPurger	1-02:40:44	0	613m	88m
phEventForwarder	1-02:40:44	0	534m	37m
phMonitor	1-02:40:49	0	1322m	629m
Apache	1-02:43:50	0	305m	15m
Rsyslogd	1-02:43:49	0	192m	4224k
Node.js-charting	1-02:43:43	0	614m	80m
Node.js-pm2	1-02:43:41	0	681m	61m
phFortiInsightAI	1-02:43:50	0	13996m	374m
AppSvr	1-02:43:38	14	11149m	4459m
DBSvr	1-02:43:50	0	425m	37m
JavaQueryServer	1-02:40:49	0	10881m	1579m
phAnomaly	1-02:40:29	0	982m	61m
SVNLite	1-02:43:50	0	9870m	450m
Redis	1-02:43:43	0	107m	70m

Upgrade Workers

To upgrade Workers, take the following steps for each Worker.

1. Login to a worker via SSH as the root user directly, or SSH as admin user and then sudo to root.

For example:

```
ssh root@<IP of Worker>
or
ssh admin@<IP of Worker>
sudo su -
```

2. Create the path /opt/upgrade.

```
mkdir -p /opt/upgrade
```

3. Download the upgrade zip package `FSM_Upgrade_All_6.4.0_build1412.zip` to `/opt/upgrade`.
4. Go to `/opt/upgrade`.
`cd /opt/upgrade`
5. Unzip the upgrade zip package.
`unzip FSM_Upgrade_All_6.4.0_build1412.zip`
6. Go to the `FSM_Upgrade_All_6.4.0_build1412` directory.
`cd FSM_Upgrade_All_6.4.0_build1412`
 - a. Run a screen.
`screen -S upgrade`

Note: This is intended for situations where network connectivity is less than favorable. If there is any connection loss, log back into the SSH console and return to the virtual screen by using the following command.
`screen -r`
7. Start the upgrade process by entering the following.
`sh upgrade.sh`
8. After the process is completed, perform a basic health check. All processes should be up and running.
9. After all Workers are upgraded, perform this extra set of steps if you were running FortiSIEM versions 6.2.0 or earlier and using Elasticsearch after the upgrade.
 - a. Navigate to **ADMIN > Setup > Storage > Online**.
 - b. Redo your configuration.
 - c. Perform a **Test** to verify it is working.
 - d. Click **Save**.

Note: These steps (9a-d) are not required while upgrading from versions 6.2.1 or later.

Upgrade Collectors

Extra Upgrade Steps from 6.2.0 to 6.4.0

From version 6.2.0 to 6.4.0, take the following steps before initiating the upgrade. Otherwise, go to [Main Upgrade Steps](#).

1. Login to the Collector via SSH as root.
2. Copy `/opt/phoenix/phscripts/bin/phcollectorimageinstaller.py` from the Supervisor by running the following command. (**Note:** This is copied from the 6.2.1 or 6.4.0 Supervisor.)
`scp root@<SupervisorIP>:/opt/phoenix/phscripts/bin/phcollectorimageinstaller.py /opt/phoenix/phscripts/bin/`
3. Change permission by running the following command.
`chmod 755 /opt/phoenix/phscripts/bin/phcollectorimageinstaller.py`

Main Upgrade Steps

- [Installation Through Image Server Page](#)

Note: Installation through Image Server requires FortiSIEM 6.4.0 or higher.

Installation Through Image Server Page

To install through the Image Server GUI, take the following steps:

Note: Installation through Image Server requires FortiSIEM 6.4.0 or higher.

1. Navigate to Click **ADMIN > Settings > System > Image Server**.
2. Follow the instructions [here](#).

Restoring Hardware from Backup After a Failed Upgrade

Background Information

When you upgrade a FortiSIEM system running on hardware (2000F, 3500F, 3500G, 500F) to 6.3.1 and later, the upgrade automatically makes a system backup of root disk, boot disk, opt disk, and in case of the Supervisor, also CMDB disk, and SVN disks.

This backup is stored in `/opt/hwbackup` if the `/opt` partition has 300GB or more free space. Once the backup pre-upgrade task is complete, the logs are stored at `/opt/phoenix/log/backup-upg.stdout.log` and `/opt/phoenix/log/backup-upg.stderr.log`.

The actual backup may be much smaller depending on the size of your CMDB and SVN partitions. Backups are also compressed using XZ compression. The partition itself is 500GB in size, so in most installations, you will have this much available space.

In case you do not have 300GB free space in `/opt`, the upgrade will abort quickly. In this case, you can also externally store the backup. For this, you will need to mount an external disk and create a symlink like this:

```
ln -s <external-disk-mount-point> /opt/hwbackup
```

Here is a sample listing of `/opt/hwbackup`:

```
[root@sp5747 hwbackup]# pwd
/opt/hwbackup
[root@sp5747 hwbackup]# ls -lh
total 19G
-rw-r--r-- 1 root root 824 Aug 24 17:08 fsm_backup_sha256sum_6.3.0.0331_2021-08-24-17-01.txt
-rw-r--r-- 1 root root 803M Aug 24 17:05 fsm_boot_disk_6.3.0.0331_2021-08-24-17-01.img.xz
-rw-r--r-- 1 root root 61M Aug 24 17:07 fsm_cmdb_6.3.0.0331_2021-08-24-17-01.xfsdump.xz
-rwxr-xr-x 1 root root 6.0K Aug 19 16:12 fsm_hw_restore_from_backup.sh
-rw-r--r-- 1 root root 14G Aug 24 17:05 fsm_opt_6.3.0.0331_2021-08-24-17-01.tar.xz
-rw-r--r-- 1 root root 5.0G Aug 24 17:07 fsm_root_disk_6.3.0.0331_2021-08-24-17-01.xfsdump.xz
-rw-r--r-- 1 root root 192 Aug 24 17:07 fsm_root_disk_partition_table_6.3.0.0331_2021-08-24-17-01.txt
-rw-r--r-- 1 root root 1.8K Aug 24 17:07 fsm_root_disk_vg_cfg_backup_6.3.0.0331_2021-08-24-17-01.txt
-rw-r--r-- 1 root root 13K Aug 24 17:07 fsm_svn_6.3.0.0331_2021-08-24-17-01.xfsdump.xz
-rw-r--r-- 1 root root 30K Aug 24 17:08 MegaSAS.log
[root@sp5747 hwbackup]# ./fsm_hw_restore_from_backup.sh
```

If there was a previous attempt at an upgrade, then there will already be a `/opt/hwbackup` directory. A new attempt will rename `/opt/hwbackup` to `/opt/hwbackup.1` and continue the new backup and upgrade. This means that the system will keep at most 2 backups. For instance, if you upgrade from 6.3.0 to 6.3.1 and in the future to 6.3.2, then you will have a backup of both the 6.3.0 system as well as 6.3.1 system.

Restoring from Backup

To restore from a backup, take the following steps:

1. Switch the running system to rescue mode. You will need do the following on the VGA or serial console of the hardware.

2. Switch to rescue mode as follows after logging into the system as the 'root' user.

```
systemctl isolate rescue.target
```

3. You will be prompted to type the root administrator password as shown here.

```
Give root password for maintenance
(or press Control-D to continue):
[root@sp5747 ~]# cd /opt/hwbackup/
[root@sp5747 hwbackup]# ./fsm_hw_restore_from_backup.sh
```

4. If the backup is stored on /opt/hwbackup, you can `chdir` to this. If the backup is stored on an external disk, mount the disk and symlink it again to /opt/hwbackup.
5. Run the restore command:

```
cd /opt/hwbackup
```

```
./fsm_hw_restore_from_backup.sh
```

Note: If you run the restore program in normal multi-user mode, the script exits with an error like this:

```
[root@sp5747 hwbackup]# ./fsm_hw_restore_from_backup.sh
./fsm_hw_restore_from_backup.sh: System is not running in rescue mode, so restore will be aborted...
You can switch to rescue mode using 'systemctl isolate rescue.target' command
Restore script ./fsm_hw_restore_from_backup.sh ran for a period of 1 seconds
[root@sp5747 hwbackup]# _
```

The whole restore may take anywhere from 15 minutes to more than an hour depending on how large the CMDb/SVN partitions are. The restore script will make sure that the SHA 256 checksums for the backup files match and only then, will it proceed. If this fails, then it will stop the restore process immediately. Here are screenshots for a sample Supervisor restore from 6.3.1 to 6.3.0.0331:

```
[root@sp5747 hwbackup]# ./fsm_hw_restore_from_backup.sh
Checking the integrity of the backup files using sha256 checksums...
fsm_boot_disk_6.3.0.0331_2021-08-24-17-01.img.xz: OK
fsm_cmdb_6.3.0.0331_2021-08-24-17-01.xfsdump.xz: OK
fsm_opt_6.3.0.0331_2021-08-24-17-01.tar.xz: OK
fsm_root_disk_6.3.0.0331_2021-08-24-17-01.xfsdump.xz: OK
fsm_root_disk_partition_table_6.3.0.0331_2021-08-24-17-01.txt: OK
fsm_root_disk_vg_cfg_backup_6.3.0.0331_2021-08-24-17-01.txt: OK
fsm_svn_6.3.0.0331_2021-08-24-17-01.xfsdump.xz: OK
Stopping all processes to perform a restore...
Restoring HW backup with FSM version: 6.3.0.0331 created on the date 2021-08-24 and at time 17:01 hrs...
Restoring / (root) disk...
```

```
Restoring HW backup with FSM version: 6.3.0.0331 created on the date 2021-08-24 and at time 17:01 hrs...
Restoring / (root) disk...
xfsrestore: using file dump (drive_simple) strategy
xfsrestore: version 3.1.8 (dump format 3.0)
xfsrestore: searching media for dump
xfsrestore: examining media file 0
xfsrestore: dump description:
xfsrestore: hostname: sp5747.fortinet.com
xfsrestore: mount point: /
xfsrestore: volume: /dev/mapper/cl-root
xfsrestore: session time: Tue Aug 24 17:05:16 2021
xfsrestore: level: 0
xfsrestore: session label: "cl-root"
xfsrestore: media label: "cl-root"
xfsrestore: file system id: 511c435d-0ada-4b94-8125-6b80a63574ad
xfsrestore: session id: a9b57771-ac25-40c2-b453-a4b79e5b5ed3
xfsrestore: media id: 07670986-ce72-4f66-a4c0-2c1f74a52e0d
xfsrestore: searching media for directory dump
xfsrestore: reading directories
xfsrestore: 19595 directories and 175075 entries processed
xfsrestore: directory post-processing
xfsrestore: WARNING: unable to set secure extended attribute for proc: Operation not supported (95)
xfsrestore: restoring non-directory files
xfsrestore: status at 20:46:28: 21442/146457 files restored, 14.0% complete, 30 seconds elapsed
xfsrestore: status at 20:46:58: 38507/146457 files restored, 57.5% complete, 60 seconds elapsed
xfsrestore: status at 20:47:28: 38546/146457 files restored, 57.5% complete, 90 seconds elapsed
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of run/blkid/blkid.tab failed
Inappropriate ioctl for device
xfsrestore: status at 20:47:58: 53052/146457 files restored, 65.0% complete, 120 seconds elapsed
xfsrestore: status at 20:48:28: 68008/146457 files restored, 68.7% complete, 150 seconds elapsed
xfsrestore: status at 20:48:58: 72511/146457 files restored, 70.2% complete, 180 seconds elapsed
xfsrestore: status at 20:49:28: 73913/146457 files restored, 73.6% complete, 210 seconds elapsed
xfsrestore: status at 20:49:58: 87298/146457 files restored, 85.1% complete, 240 seconds elapsed
xfsrestore: status at 20:50:28: 105103/146457 files restored, 88.2% complete, 270 seconds elapsed
xfsrestore: status at 20:50:58: 127998/146457 files restored, 97.4% complete, 300 seconds elapsed
xfsrestore: WARNING: open_by_handle of data failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of data failed: Bad file descriptor
xfsrestore: WARNING: open_by_handle of querydata failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of querydata failed: Bad file descriptor
xfsrestore: WARNING: open_by_handle of cmdb failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of cmdb failed: Bad file descriptor
xfsrestore: WARNING: open_by_handle of svn failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of svn failed: Bad file descriptor
xfsrestore: WARNING: open_by_handle of opt failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of opt failed: Bad file descriptor
xfsrestore: WARNING: path_to_handle of var/lib/nfs/rpc_pipefs failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of var/lib/nfs/rpc_pipefs failed: Bad file descriptor
xfsrestore: WARNING: path_to_handle of sys failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x00000000, extsize = 0x0, projid = 0x0) of sys failed: Bad file descriptor
xfsrestore: WARNING: path_to_handle of run/blkid failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of run/blkid failed: Bad file descriptor
```

Note: These WARNING messages can be ignored. These are likely to be temporary system files at the Linux level when the backup was taken. At the time of backup, all FSM services are stopped.

```

xfsrestore: WARNING: open_by_handle of data failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of data failed: Bad file descr
iptor
xfsrestore: WARNING: open_by_handle of querydata failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of querydata failed: Bad file
descriptor
xfsrestore: WARNING: open_by_handle of cmdb failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of cmdb failed: Bad file descr
iptor
xfsrestore: WARNING: open_by_handle of svn failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of svn failed: Bad file descri
ptor
xfsrestore: WARNING: open_by_handle of opt failed:Bad file descriptor
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of opt failed: Bad file descri
ptor
xfsrestore: WARNING: path_to_handle of var/lib/nfs/rpc_pipefs failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of var/lib/nfs/rpc_pipefs fail
ed: Bad file descriptor
xfsrestore: WARNING: path_to_handle of sys failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x00000000, extsize = 0x0, projid = 0x0) of sys failed: Bad file
descriptor
xfsrestore: WARNING: path_to_handle of run/blkid failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of run/blkid failed: Bad file
descriptor
xfsrestore: WARNING: path_to_handle of run/lock/lvm failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of run/lock/lvm failed: Bad fi
le descriptor
xfsrestore: WARNING: path_to_handle of run/lock failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x0, extsize = 0x0, projid = 0x0) of run/lock failed: Bad file d
escriptor
xfsrestore: WARNING: path_to_handle of run failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x00000000, extsize = 0x0, projid = 0x0) of run failed: Bad file
descriptor
xfsrestore: WARNING: path_to_handle of proc failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x00000000, extsize = 0x0, projid = 0x0) of proc failed: Bad fil
e descriptor
xfsrestore: WARNING: path_to_handle of dev failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x00000000, extsize = 0x0, projid = 0x0) of dev failed: Bad file
descriptor
xfsrestore: WARNING: path_to_handle of boot failed:Inappropriate ioctl for device
xfsrestore: WARNING: attempt to set extended attributes (xflags 0x00000000, extsize = 0x0, projid = 0x0) of boot failed: Bad fil
e descriptor
xfsrestore: restore complete: 387 seconds elapsed
xfsrestore: Restore Status: SUCCESS
Restoring /opt...
.....
.....
.....

```

```
Restoring /opt...
.....
Removing existing directories in cmdb
Restoring /cldb disk...
xsrestore: using file dump (drive_simple) strategy
xsrestore: version 3.1.8 (dump format 3.0)
xsrestore: searching media for dump
xsrestore: examining media file 0
xsrestore: dump description:
xsrestore: hostname: sp5747.fortinet.com
xsrestore: mount point: /cldb
xsrestore: volume: /dev/mapper/FSIEM3500F-phx_cldb
xsrestore: session time: Tue Aug 24 17:07:23 2021
xsrestore: level: 0
xsrestore: session label: "cldb"
xsrestore: media label: "cldb"
xsrestore: file system id: c9c48a15-b50e-4ff4-ad98-0b2b9fba0840
xsrestore: session id: 210640e6-9f98-4cbe-96ca-5efd3c209206
xsrestore: media id: 555b095a-1b3e-4bf8-b49f-432021e70e07
xsrestore: searching media for directory dump
xsrestore: reading directories
xsrestore: 30 directories and 2643 entries processed
xsrestore: directory post-processing
xsrestore: restoring non-directory files
xsrestore: restore complete: 6 seconds elapsed
xsrestore: Restore Status: SUCCESS
Removing existing directories in svn
Restoring /svn disk...
xsrestore: using file dump (drive_simple) strategy
xsrestore: version 3.1.8 (dump format 3.0)
xsrestore: searching media for dump
xsrestore: examining media file 0
xsrestore: dump description:
xsrestore: hostname: sp5747.fortinet.com
xsrestore: mount point: /svn
xsrestore: volume: /dev/mapper/FSIEM3500F-phx_svn
xsrestore: session time: Tue Aug 24 17:07:39 2021
xsrestore: level: 0
xsrestore: session label: "svn"
xsrestore: media label: "svn"
xsrestore: file system id: 5dbb7da5-e17b-40cb-a3f4-5b0e59496b3d
xsrestore: session id: 429b02ec-e8ea-4004-9590-cde65b467384
xsrestore: media id: 26273d79-9025-4108-89f6-4616e6ad4e1b
xsrestore: searching media for directory dump
xsrestore: reading directories
xsrestore: 12 directories and 43 entries processed
xsrestore: directory post-processing
xsrestore: restoring non-directory files
xsrestore: restore complete: 0 seconds elapsed
xsrestore: Restore Status: SUCCESS
Restoring /boot disk after umount...
1033060352 bytes (1.0 GB, 985 MiB) copied, 10 s, 103 MB/s
0+130005 records in
0+130005 records out
[root@sp5747 hwbackup]# 1073741024 bytes (1.1 GB, 1.0 GiB) copied, 29.1323 s, 36.9 MB/s
Restore 6.3.0.0331 complete.
Please reboot the system...
Restore script /fsm_hw_restore_from_backup.sh ran for a period of 9 minutes and 27 seconds
[root@sp5747 hwbackup]#
```

```
Restoring /boot disk after umount...
1033060352 bytes (1.0 GB, 985 MiB) copied, 10 s, 103 MB/s
0+130005 records in
0+130005 records out
[root@sp5747 hwbakup1# 1073741824 bytes (1.1 GB, 1.0 GiB) copied, 29.1323 s, 36.9 MB/s
Restore 6.3.0.0331 complete.
Please reboot the system...
Restore script ./fsm_hw_restore_from_backup.sh ran for a period of 9 minutes and 27 seconds
[root@sp5747 hwbakup1# _
```

6. Once the restore is complete, it will print how long the restore took and will ask you to reboot the system. Run the command to reboot your system:

```
reboot
```

The system should now come up with your pre-upgrade version. Wait at least 15 minutes for all processes to come up.

If you are using 3500F, 2000F, or 3500G as a worker node, or 500F as a collector node, then the restore of CMDB and SVN is skipped.

The restore logs are stored in this location

```
/opt/hwbakup/fsm-hw-restore-<date>-<hour-minute>.log
```

If the restore fails for any reason or if processes do not come up after reboot, then please contact technical support.

Upgrading with Disaster Recovery Enabled

To upgrade your FortiSIEMs in a Disaster Recovery environment, take the following steps.

1. Upgrade the Primary Supervisor and Workers
2. After the Primary is fully upgraded, upgrade the Secondary Supervisor and Workers.

After Step 1, the Secondary Supervisor database schema is already upgraded. Step 2 simply upgrades the executables in Site 2.

Post Upgrade Health Check

Note: If any of the checks fail, then the upgrade might have failed. In this case, contact Fortinet Support.

1. Check Cloud health and Collector health from the FortiSIEM GUI:

- Versions display correctly.
- All processes are up and running.
- Resource usage is within limits.

The first screenshot shows the 'Cloud Health' tab in the FortiSIEM GUI. It displays a table with columns: Name, IP Address, Module Role, Health, Version, Load Average, CPU, Swap Used, Memory Size, and Memory Used. The table lists two processes: 'super' and 'worker', both with a health status of 'Normal' and version '6.3.0.0330'. Below this, there is a section for 'Process level metrics for offline super (172.30.57.230)' with columns: Process Name, Status, Uptime, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. The table lists various processes like 'gssmsh', 'phMonitorSupervisor', 'phParser', etc., all with a status of 'Up'.

The second screenshot shows the 'Collector Health' tab in the FortiSIEM GUI. It displays a table with columns: Organization, Name, IP Address, Status, Collector Type, Health, Uptime, CPU, Memory, Allocated EPS, Incoming EPS, Version, and Collector ID. The table lists one collector: 'org1' with name 'col1', IP address '172.30.57.232', status 'up', collector type 'VM', health 'Normal', and version '6.3.0...'. Below this, there is a section for 'Process level metrics for offline super (172.30.57.230)' with columns: Process Name, Status, Uptime, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. The table lists various processes like 'phMonitorAgent', 'phParser', 'phPerfMonitor', etc., all with a status of 'Up'.

2. Check that the Redis passwords match on the Supervisor and Workers:

- Supervisor: run the command `phLicenseTool --showRedisPassword`
- Worker: run the command `grep -i auth /opt/node-rest-service/ecosystem.config.js`

```
[root@offlinesuper ~]# grep -i auth /opt/node-rest-service/ecosystem.config.js
REDIS_AUTH: '4CiVtA9n1Fh2KPlkDWCjsLTzJCwiwg7F3Yok@5WhVYAnGjSB66pR1v743v5zGNJYXy8%ZB5ScQFk6ihx8L^Dzhj^YONtWQff554ERhEXU1jBtBZ%chxCLYqcvqvzswQ9',
REDIS_AUTH: '4CiVtA9n1Fh2KPlkDWCjsLTzJCwiwg7F3Yok@5WhVYAnGjSB66pR1v743v5zGNJYXy8%ZB5ScQFk6ihx8L^Dzhj^YONtWQff554ERhEXU1jBtBZ%chxCLYqcvqvzswQ9',
[root@offlinesuper ~]# ssh root@172.30.57.231
root@172.30.57.231's password:
Last login: Thu Jul 1 13:17:46 2021 from 172.30.57.230
[root@offlineworker ~]# grep -i auth /opt/node-rest-service/ecosystem.config.js
REDIS_AUTH: '4CiVtA9n1Fh2KPlkDWCjsLTzJCwiwg7F3Yok@5WhVYAnGjSB66pR1v743v5zGNJYXy8%ZB5ScQFk6ihx8L^Dzhj^YONtWQff554ERhEXU1jBtBZ%chxCLYqcvqvzswQ9',
REDIS_AUTH: '4CiVtA9n1Fh2KPlkDWCjsLTzJCwiwg7F3Yok@5WhVYAnGjSB66pR1v743v5zGNJYXy8%ZB5ScQFk6ihx8L^Dzhj^YONtWQff554ERhEXU1jBtBZ%chxCLYqcvqvzswQ9',
```

3. Check that the database passwords match on the Supervisor and Workers:

- Supervisor: run the command `phLicenseTool --showDatabasePassword`
- Worker: run the command `grep Auth_PQ_dbpass /etc/httpd/conf/httpd.conf`

```
[root@offlineworker ~]# grep Auth_PQ_dbpass /etc/httpd/conf/httpd.conf
Auth_PQ_dbpass Mhp0YzN^riB6
Auth_PQ_dbpass Mhp0YzN^riB6
```

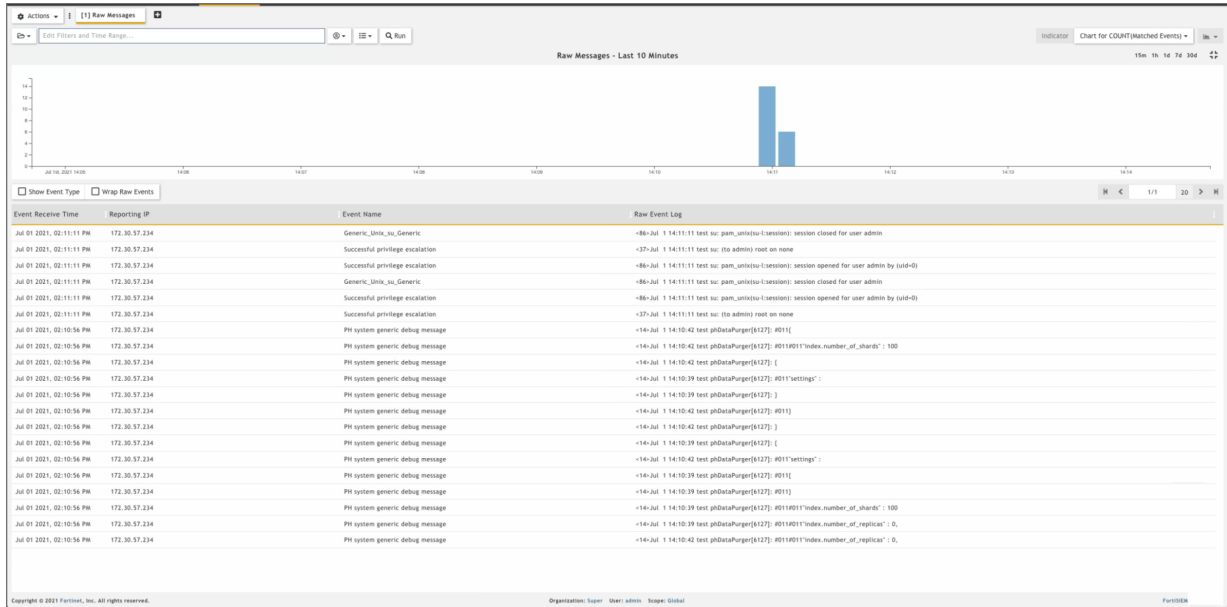
4. Elasticsearch case: check the Elasticsearch health

The screenshot shows the FortiSIEM dashboard with the 'Elasticsearch Health' section active. The top navigation bar includes links to Dashboard, Analytics, Incidents, Cases, Cases, Case, Resources, Tasks, and Admin. The left sidebar has links to Setup, Device Support, Health, License, and Settings. The main content area displays the 'Elasticsearch Health' section, which includes a table of cluster status and a detailed table of node information.

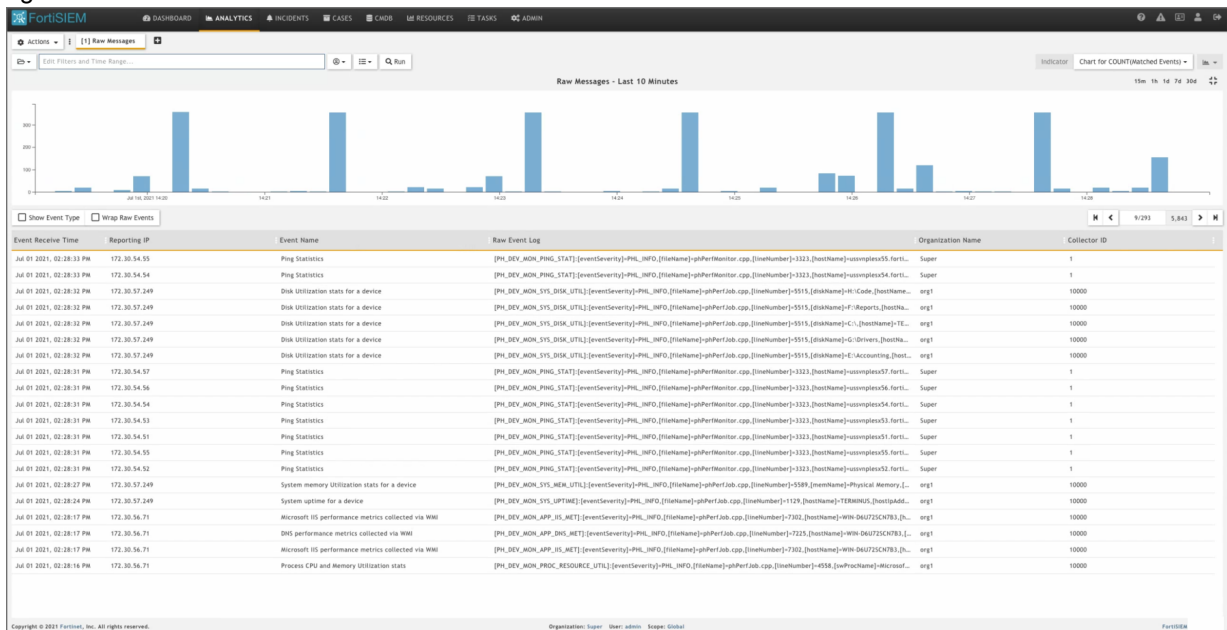
Cluster	IP Address	Status	Nodes	Data Nodes	Active Shards
FSM_CLSTR	172.30.57.181 172.30.57.190 172.30.57.189 172.30.57.193	Normal	4	4	3496

Name	IP Address	Role	Version	Load	OS	Total Memory	Used Memory	Used Swap
FSM_CLSTR0	172.30.57.181	data,ingest	6.8.13	0.1/0.06/0.02	Linux	15 GB	8 GB	0B
FSM_CLSTR1	172.30.57.190	data,ingest	6.8.13	0.43/0.21/0.07	Linux	15 GB	5 GB	0B
FSM_CLSTR2	172.30.57.189	data,ingest	6.8.13	0.2/0.07/0.02	Linux	15 GB	5 GB	0B
FSM_CLSTR_MSTR	172.30.57.193	master,data,ingest	6.8.13	0.27/0.08/0.03	Linux	15 GB	5 GB	0B

5. Check that events are received correctly:
- a. Search All Events in last 10 minutes and make sure there is data.



- b. Search for events from Collector and Agents and make sure there is data. Both old and new collectors and agents must work.



- c.** Search for events using CMDB Groups (Windows, Linux, Firewalls, etc.) and make sure there is data.

Edit Filters and Time Range...

Load Save Clear All

Filter

☐ Event Keyword
☒ Event Attribute

Paren	Attribute	Operator	Value	Paren	Next	Row
+ -	Reporting IP	IN	Group: Windows	+ -	AND	+ -

☐ CMDB Attribute

Time Range

☐ Real-time
 ☒ Relative Last 10 Minutes
☐ Absolute

Trend Interval: Auto

Apply & Run Apply Cancel

Voltage measurement

Actions | [1] Search

Reported IP In Group: Windows

Indicator Chart for COUNT(Matched Events)

Search - Last 10 Minutes

☐ Show Event Type

Reporting IP	Event Name	Organization Name	Collector ID	COUNT(Matched Events)
<input checked="" type="checkbox"/> 172.30.56.71	Windows Manual Windows Service stopped	eng1	10000	239
<input checked="" type="checkbox"/> 172.30.57.249	Windows Manual Windows Service stopped	eng1	10000	225
<input checked="" type="checkbox"/> 172.30.57.249	Windows login success	eng1	10000	96
<input checked="" type="checkbox"/> 172.30.57.249	Group membership information	eng1	10000	96
<input checked="" type="checkbox"/> 172.30.57.249	Windows logoff	eng1	10000	95
<input checked="" type="checkbox"/> 172.30.57.249	Windows local or domain via NTLM authentication successful	eng1	10000	88
<input type="checkbox"/> 172.30.56.71	Process CPU and Memory Utilization stats	eng1	10000	50
<input type="checkbox"/> 172.30.56.71	System per CPU Utilization for a device	eng1	10000	24
<input type="checkbox"/> 172.30.56.71	Network interface utilization stats for a device	eng1	10000	20
<input type="checkbox"/> 172.30.57.249	Process CPU and Memory Utilization stats	eng1	10000	17
<input type="checkbox"/> 172.30.56.71	Windows Auto Service stopped	eng1	10000	12
<input type="checkbox"/> 172.30.56.71	The state of a transaction has changed	eng1	10000	12
<input type="checkbox"/> 172.30.59.253	Network IO stats for a Virtual Machine	Super	1	12
<input type="checkbox"/> 172.30.56.71	System uptime for a device	eng1	10000	11
<input type="checkbox"/> 172.30.56.170	Network IO stats for a Virtual Machine	Super	1	11
<input type="checkbox"/> 172.30.52.13	Network IO stats for a Virtual Machine	Super	1	10
<input type="checkbox"/> 172.30.52.29	Network IO stats for a Virtual Machine	Super	1	10
<input type="checkbox"/> 172.30.52.31	Network IO stats for a Virtual Machine	Super	1	10
<input type="checkbox"/> 172.30.52.135	Network IO stats for a Virtual Machine	Super	1	10
<input type="checkbox"/> 172.30.53.128	Network IO stats for a Virtual Machine	Super	1	10

Copyright © 2021 Fortinet, Inc. All rights reserved. Organization: Super User: admin Source: Global FORTINET

6. Make sure there are no SVN authentication errors in CMDB when you click any device name.

0

Routers

0

Firewalls

2

Windows

1

Unix

0

ESX

0

AWS

0

Azure

CMDB > Devices > Server

New

Edit

Delete

org1

Discovered by all

Q

Name	IP	Device Type	Status	Discovered	Method	Organization	Agent Policy	Agent Status	Monitor Status	Event Status	Agent Type	AWS Account	AWS Instance	Parser Name	Agent V
es5721a-reisa	172.30.57.214	Generic Unix	Pending	Jun 29 2021, 02:06:20 PM	LOG	org1				Critical					
TERMINUS	172.30.57.249	Windows Server 2016	Pending	Jul 01 2021, 02:26:30 PM	WMI_PING	org1			Normal	Normal					
WIN-DAGU72SCN7B3	172.30.56.71	Windows Server 2008 R2	Pending	Jun 30 2021, 02:40:24 PM	WMI_PING	org1				Normal					

Summary

Properties

Monitor

Software > Running Applications

Hardware

Configuration

Relationships

File

Auto expand

Apply

Q

Search...

▼

▼

Critical	Monitor	Name	Process Name	Process Params	Path	Port/Protocol	Status	Uptime	Last Updated
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft IIS	svchost.exe	-IISvcs	C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft DNS	dns.exe		C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft IAS	iadhost.exe	{8BD46741-18F0-4A44-B325-29D86C7...}	C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Windows SNMP Service	snmp.exe		C:\Windows\System32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Terminal Server	svchost.exe	-4 termcons	C:\Windows\System32\		running	5d th ago	Jul 01 2021, 02:26:51 PM
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft RPC service	svchost.exe	-4 RPCSS	C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:51 PM
<input type="checkbox"/>	<input type="checkbox"/>	Windows DHCP Client	svchost.exe	-4 NetworkServiceNetworkRestricted	C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Windows DHCP Client	svchost.exe	-4 NetworkService	C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Windows Distributed File System Ser...	lsass.exe		C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Distributed Transaction Coor...	mofc.exe		C:\Windows\System32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Windows Internet Messaging Service	lsass.exe		C:\Windows\System32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Network Services	svchost.exe	-4 netwscs	C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:52 PM
<input type="checkbox"/>	<input type="checkbox"/>	DCOM Process Launcher	svchost.exe	-4 DcomLaunch	C:\Windows\system32\		running	5d th ago	Jul 01 2021, 02:26:51 PM

Copyright © 2021 Fortinet, Inc. All rights reserved.

Organization: Super User: admin Scope: Global

Part006M

7. Make sure recent incidents and their triggering events are displayed.

Actions

Overview

List by Time

Inc Risk

Exp Explorer

Alerts

NITRE ATTACKER -

1 minute

Search

Mon 16 Jul 2024

All Active Incidents

H < 1/1 13 > H

Severity Category	Last Occurred	Incident	Tactics	Technique	Reporting	Source	Target	Detail	Incident Status	Resolution	
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: PYYol_8008 Datascanner Type: VMW's Disk Capacity Util: 75.40	Datascanner: PYYol_8006 Datascanner Type: VMW's Disk Capacity Util: 75.40	Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Server Memory Warning	Impact	Endpoint Denial of Service: OS ...	usomplex57.fortinet-us.com		172.30.54.57 usomplex57.fortine...	Memory Util: 81.24		Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: PYYol_8012 Datascanner Type: VMW's Disk Capacity Util: 75.93		Active	Open
INFO	Jul 01 2021, 02:20:00 PM	Server Down: No Ping Response	Impact	System Shutdowns/Reboot	vc-devops		172.30.52.10 vc-devops			Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: _templates Datascanner Type: VMW's Disk Capacity Util: 93.48		Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: PYYol_A003 Datascanner Type: VMW's Disk Capacity Util: 77.55		Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: PYYol_8001 Datascanner Type: VMW's Disk Capacity Util: 76.13		Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: PYYol_8008 Datascanner Type: VMW's Disk Capacity Util: 76.34		Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: PYYol_8003 Datascanner Type: VMW's Disk Capacity Util: 79.89		Active	Open
MEDIUM	Jul 01 2021, 02:20:00 PM	Datstore Space Warning	Impact	Endpoint Denial of Service: OS ...	vc-devops		vc-devops Datascanner: US-NPL	Datascanner: PYYol_8011 Datascanner Type: VMW's Disk Capacity Util: 77.06		Active	Open
MEDIUM	Jul 01 2021, 02:12:00 PM	No performance metrics from a device		wlr57213-resna			vc-devops			Active	Open
MEDIUM	Jul 01 2021, 01:32:00 PM	No logs from a device		cso57214-resna			172.30.57.214	Job Name: Syslog		Active	Open
MEDIUM	Jul 01 2021, 12:32:00 PM	No logs from a device		gs57212-resna			172.30.57.212	Job Name: Syslog		Active	Open

Details

Events

Rule

Auto expand

Copyright © 2021 Fortinet, Inc. All rights reserved.

Organization: super User: admin Scope: Global

FortiSD-WAN

8. Check Worker for Collector Credentials by running the following command:

```
cat /etc/httpd/accounts/passwds
```

This validates that all workers contain collector credentials to log in and upload logs.

9. Run the following script on the Supervisor.

```
get-fsm-health.py --local
```

Your output should appear similar to the example output in [Post Upgrade Health Check get-fsm-health.py --local](#)
[Example Output](#).

Upgrade via Proxy

During upgrade, the FortiSIEM Supervisor, Worker, or Hardware appliances (FSM-2000F, 3500F, or 3500G) must be able to communicate with Rocky Linux 8 OS repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-r8.fortisiem.fortinet.com`) hosted by Fortinet, to get the latest OS packages. Follow these steps to set up this communication via proxy, before initiating the upgrade.

1. SSH to the node.
2. Create this file `etc/profile.d/proxy.sh` with the following content and then save the file.

```
PROXY_URL="<proxy-ip-or-hostname>:<proxy-port>"
export http_proxy="$PROXY_URL"
export https_proxy="$PROXY_URL"
export ftp_proxy="$PROXY_URL"
export no_proxy="127.0.0.1,localhost"
```

3. Run `source /etc/profile.d/proxy.sh`.
4. Test that you can use the proxy to successfully communicate with the two sites here:
`os-pkgs-cdn.fortisiem.fortinet.com`
`os-pkgs.fortisiem.fortinet.com`.
5. Begin the upgrade.

Upgrade Log

The 6.4.0.1412 Upgrade ansible log file is located here: `/usr/local/upgrade/logs/ansible.log`.

Errors can be found at the end of the file.

Migrate Log

The 5.3.x/5.4.x to 6.1.x Migrate ansible log file is located here: `/usr/local/migrate/logs/ansible.log`.

Errors can be found at the end of the file.

Reference

Steps for Expanding /opt Disk

1. Go to the Hypervisor and increase the size of /opt disk or the size of /svn disk
2. # ssh into the supervisor as root
3. # lsblk

```
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
...
sdb                  8:16   0 100G  0 disk                << old size
└─sdb1                8:17   0 22.4G  0 part [SWAP]
└─sdb2                8:18   0 68.9G  0 part /opt
...
```

4. # yum -y install cloud-utils-growpart gdisk
5. # growpart /dev/sdb 2
CHANGED: partition=2 start=50782208 old: size=144529408 end=195311616 new:
size=473505759 end=524287967
6. # lsblk

```
Changed the size to 250GB for example:
#lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
...
sdb                  8:16   0 250G  0 disk                <<< NOTE the new size for the disk in
/opt
└─sdb1                8:17   0 22.4G  0 part [SWAP]
└─sdb2                8:18   0 68.9G  0 part /opt
...
```

7. # xfs_growfs /dev/sdb2

```
meta-data=/dev/sdb2          isize=512    agcount=4, agsize=4516544 blks
=                               sectsz=512   attr=2, projid32bit=1
=                               crc=1       finobt=1, sparse=1, rmapbt=0
=                               reflink=1
data      =                   bsize=4096   blocks=18066176, imaxpct=25
=                               sunit=0       swidth=0 blks
naming    =version 2          bsize=4096   ascii-ci=0, ftype=1
log       =internal log      bsize=4096   blocks=8821, version=2
=                               sectsz=512   sunit=0 blks, lazy-count=1
realtime  =none              extsz=4096   blocks=0, rtextents=0
data blocks changed from 18066176 to 59188219
```

8. # df -hz

```
Filesystem            Size  Used Avail Use% Mounted on
...
/dev/sdb2              226G  6.1G  220G   3% / << NOTE the new disk size
```

Fix After Upgrading 2000F, 3500F, 3500G from 5.3.x or 5.4.0 to 6.1.2

After upgrading hardware appliances 2000F, 3500F, or 3500G from 5.3.x or 5.4.0 to 6.1.2, the swap is reduced from 24GB to 2GB. Note that the upgrade from 6.1.2 to 6.2.x does not have this problem. This will impact performance. To fix this issue, take the following steps.

1. First, run the following command based on your hardware appliance model.

For 2000F

```
swapon -s /dev/mapper/FSIEM2000F-phx_swap
```

For 3500F

```
swapon -s /dev/mapper/FSIEM3500F-phx_swap
```

For 3500G

```
swapon -s /dev/mapper/FSIEM3500G-phx_swap
```

2. Add the following line to `/etc/fstab` for the above swap partition based on your hardware appliance model.

For 2000F

```
/dev/FSIEM2000F/phx_swap /swapfile swap defaults 0 0
```

For 3500F

```
/dev/FSIEM3500F/phx_swap /swapfile swap defaults 0 0
```

For 3500G

```
/dev/FSIEM3500G/phx_swap /swapfile swap defaults 0 0
```

3. Reboot the hardware appliance.

4. Run the following command

```
swapon --show
```

and make sure there are 2 swap partitions mounted instead of just 1, as shown here.

```
[root@sp5753 ~]# swapon --show
```

```
NAME      TYPE      SIZE USED  PRIO
/dev/dm-5 partition 30G   0B    -3
/dev/dm-0 partition 2.5G   0B    -2
```

Post Upgrade Health Check `get-fsm-health.py --local` Example Output

Here is an example of a successful output when running `get-fsm-health.py --local`.

```

Health Check
=====
Wed Jul 07 17:35:26 PDT 2021
-----
Fetching Information from Local.
- Host Info ..... succeeded.
- FortiSIEM Version ..... succeeded.
- FortiSIEM License Info ..... succeeded.
- Configuration ..... succeeded.
- CMDB Info ..... succeeded.
- Largest CMDB Tables ..... succeeded.
```



```

- EPS Info ..... succeeded.
- Worker Upload Event Queue Info ..... succeeded.
- Inline Report Queue ..... succeeded.
- Active Queries ..... succeeded.
- Load Average ..... succeeded.
- CPU Usage Details ..... succeeded.
- Top 5 Processes by CPU ..... succeeded.
- Memory Usage ..... succeeded.
- Swap Usage ..... succeeded.
- Top 5 Processes by Resident Memory ..... succeeded.
- Disk Usage ..... succeeded.
- IOStat ..... succeeded.
- Top 5 Processes by IO ..... succeeded.
- NFSIOStat ..... succeeded.
- NFS Disk Operations Time (second) ..... succeeded.
- Top 10 Slow EventDB Queries ( > 1 min) Today ..... succeeded.
- Top 5 Rule with Large Memory Today ..... succeeded.
- FortiSIEM Process Uptime Less Than 1 day ..... succeeded.
- Top 5 log files in /var/log ..... succeeded.
- FortiSIEM Shared Store Status ..... succeeded.
- App Server Exceptions Today ..... succeeded.
- Backend Errors Today ..... succeeded.
- Backend Segfaults Today ..... succeeded.
- Patched files ..... succeeded.
- Outstanding Discovery Jobs ..... succeeded.
- FortiSIEM Log File Size ..... succeeded.
- FortiSIEM Fall Behind Jobs ..... succeeded.
- FortiSIEM Jobs Distribution ..... succeeded.

```

```

-----
Data Collection
=====

```

```

All data was collected.

```

```

-----
Health Assessment
=====

```

```

Overall health: **Critical**

```

```

CPU Utilization: Normal

```

- 15 min Load average: 1.05
- System CPU: 4.5%

```

Memory Utilization: Normal

```

- Memory utilization: 48%
- Swap space utilization: 0.0%
- Swap in rate: 0B/s
- Swap out rate: 0B/s

```

I/O Utilization: Normal

```

- CPU Idle Wait: 0.0%
- Local disk IO util: 0.2%
- NFS latency (/data): 2.2ms

```

Disk Utilization: Normal

```

- Disk Utilization: 33%

```

Event Ingestion: Normal

```

```

- Worker event upload queue: 1
- Shared store status: Nobody is falling behind
Event Analysis: Normal
- Inline report queue: 4
- Active query queue: 0
System Errors: Normal
- Process down. See details.
- App server errors: 0
- Backend error: 2
Performance Monitoring: **Critical**
- 1250 jobs are falling behind. (Super) *****

```

 Details
 =====

Host Info

NodeType	Host Name	IP Address
----------	-----------	------------

Super	sp156	172.30.56.156
-------	-------	---------------

FortiSIEM Version

NodeType	Version	Commit Hash	Built On
----------	---------	-------------	----------

Super	6.3.0.0331	6e29f46b382	Thu Jul 01 15:58:02 PDT 2021
-------	------------	-------------	------------------------------

FortiSIEM License Info

License Information:

Attribute	Value	Expiration
Date		
Serial Number	FSMTEST8888888888	
Hardware ID	88888888-8888-8888-8888-888888888888	
License Type	Service Provider	
Devices	1000	Dec 31, 2021
Endpoint Devices	1000	Dec 31, 2021
Additional EPS	10000	Dec 31, 2021
Total EPS	22000	Dec 31, 2021
Agents	2000	Dec 31, 2021
UEBA Telemetry License	1000	Dec 31, 2021
IOC Service	Valid	Dec 31, 2021
Maintenance and Support	Valid	Dec 31, 2021

.....



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.