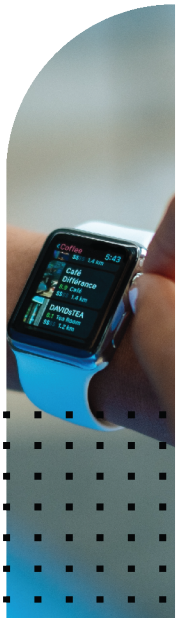
Upgrade Guide

FortiSIEM 6.3.0



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

NSE 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

09/15/2022
FortiSIEM 6.3.0 Upgrade Guide

TABLE OF CONTENTS

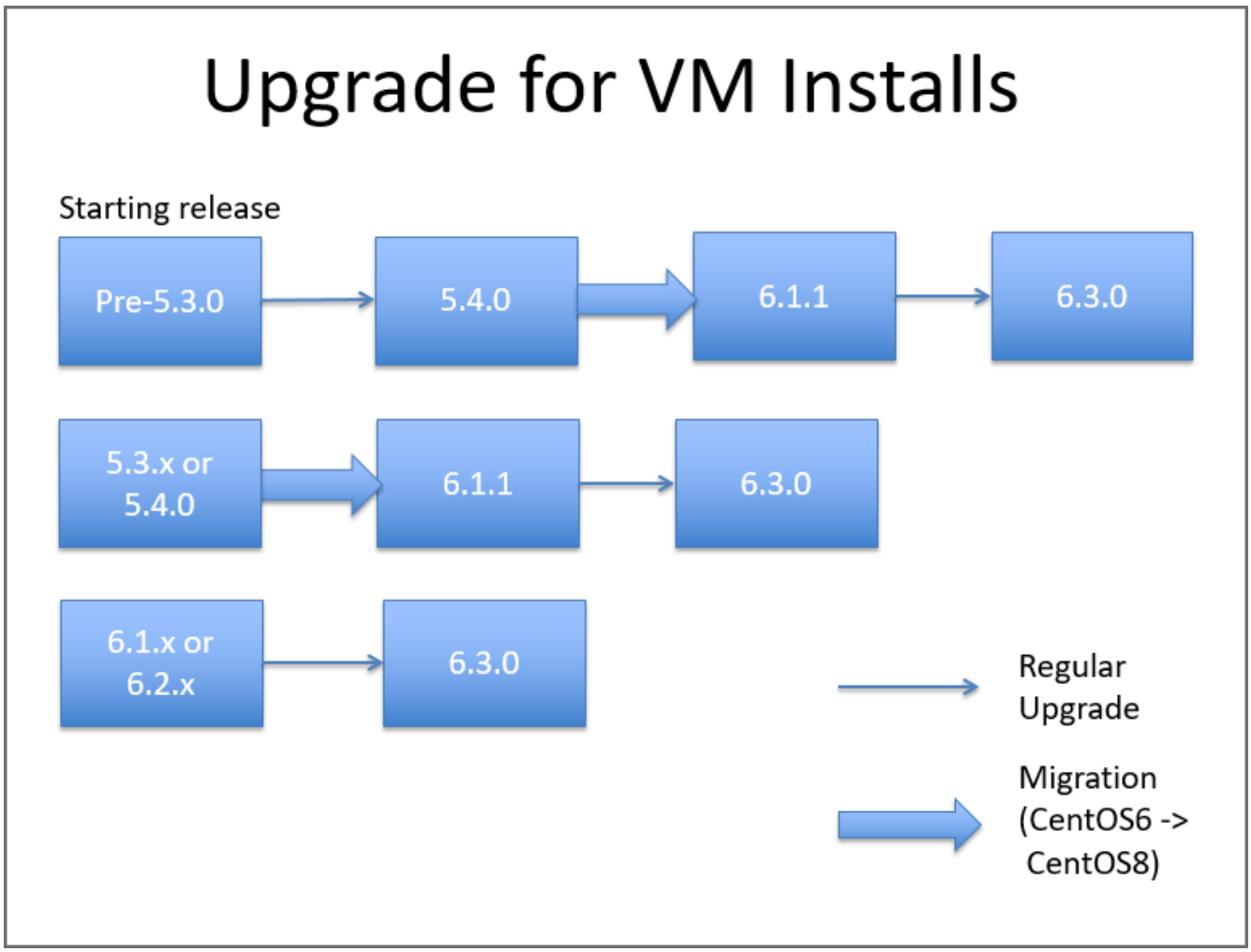
Upgrade Paths **5**
Important Notes **7**
Pre-Upgrade Checklist 7
6.2.0 to 6.3.0 Upgrade Notes 7
6.1.x to 6.3.0 Upgrade Notes 7
General Upgrade Notes 8
Upgrade Pre-5.3.0 Deployment **9**
Upgrade 5.3.x or 5.4.0 Deployment **12**
Upgrade 6.x Deployment **14**
Upgrade 6.x Single Node Deployment **15**
Upgrade Supervisor 15
Upgrade Collectors 16
Extra Upgrade Steps from 6.2.0 to 6.3.0 16
Main Upgrade Steps 17
Upgrade 6.x Cluster Deployment **18**
Overview 18
Detailed Steps 18
Upgrade Supervisor 19
Upgrade Workers 20
Upgrade Collectors 21
Extra Upgrade Steps from 6.2.0 to 6.3.0 21
Main Upgrade Steps 21
Post Upgrade Health Check **23**
Upgrade via Proxy **28**
Upgrade Log **29**
Migrate Log **30**
Reference **31**
Steps for Expanding /opt Disk 31
Fix After Upgrading 2000F, 3500F, 3500G from 5.3.x or 5.4.0 to 6.1.2 32
Post Upgrade Health Check get-fsm-health.py --local Example Output 32

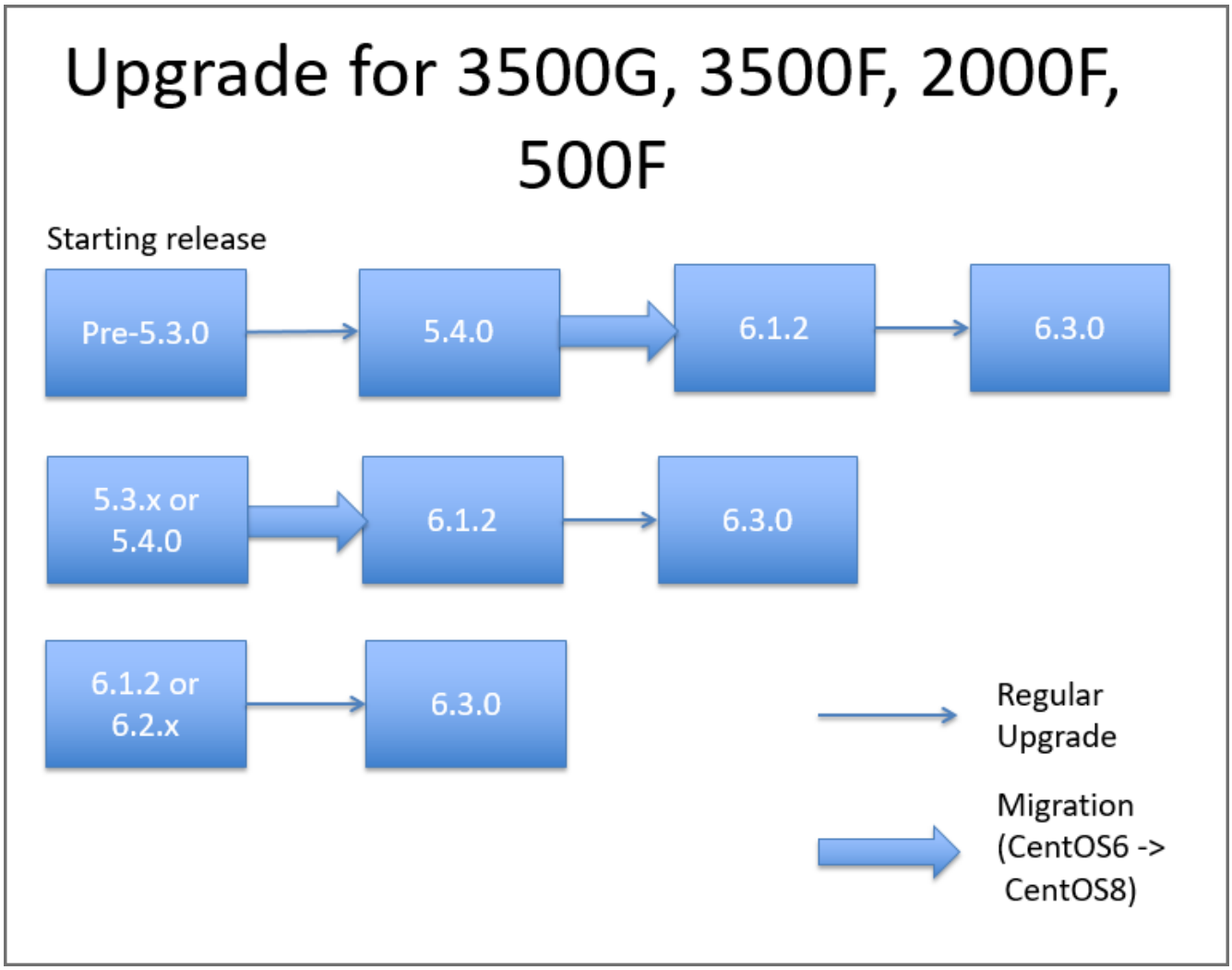
Change Log

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.
09/15/2022	Updated Upgrade Supervisor and Upgrade Workers sections.

Upgrade Paths

Please follow the proceeding upgrade paths to upgrade existing FortiSIEM installs to the latest 6.3.0 release.




Upgrade for 3500G, 3500F, 2000F, 500F
Starting release
Pre-5.3.0
5.4.0
6.1.2
6.3.0
5.3.x or 5.4.0
6.1.2
6.3.0
6.1.2 or 6.2.x
6.3.0
Regular Upgrade
Migration (CentOS6 -> CentOS8)

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. Make sure the FortiSIEM license is not expired.
7. Make sure the Supervisor, Workers and Collectors can connect to the Internet on port 443 to the CentOS OS repositories (os-pkgs-cdn.fortisiem.fortinet.com and os-pkgs.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 6.3.0 Upgrade Notes

This note applies only if you are upgrading from 6.2.0.

Before upgrading Collectors to 6.3.0, 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 6.3.0 Upgrade Notes

These notes apply only if you are upgrading from 6.1.x to 6.3.0.

1. The 6.3.0 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 6.3.0, take the following steps:

a. Go to **ADMIN > Setup > Storage> Online**.
b. Select "ES-type" and re-enter the credential.

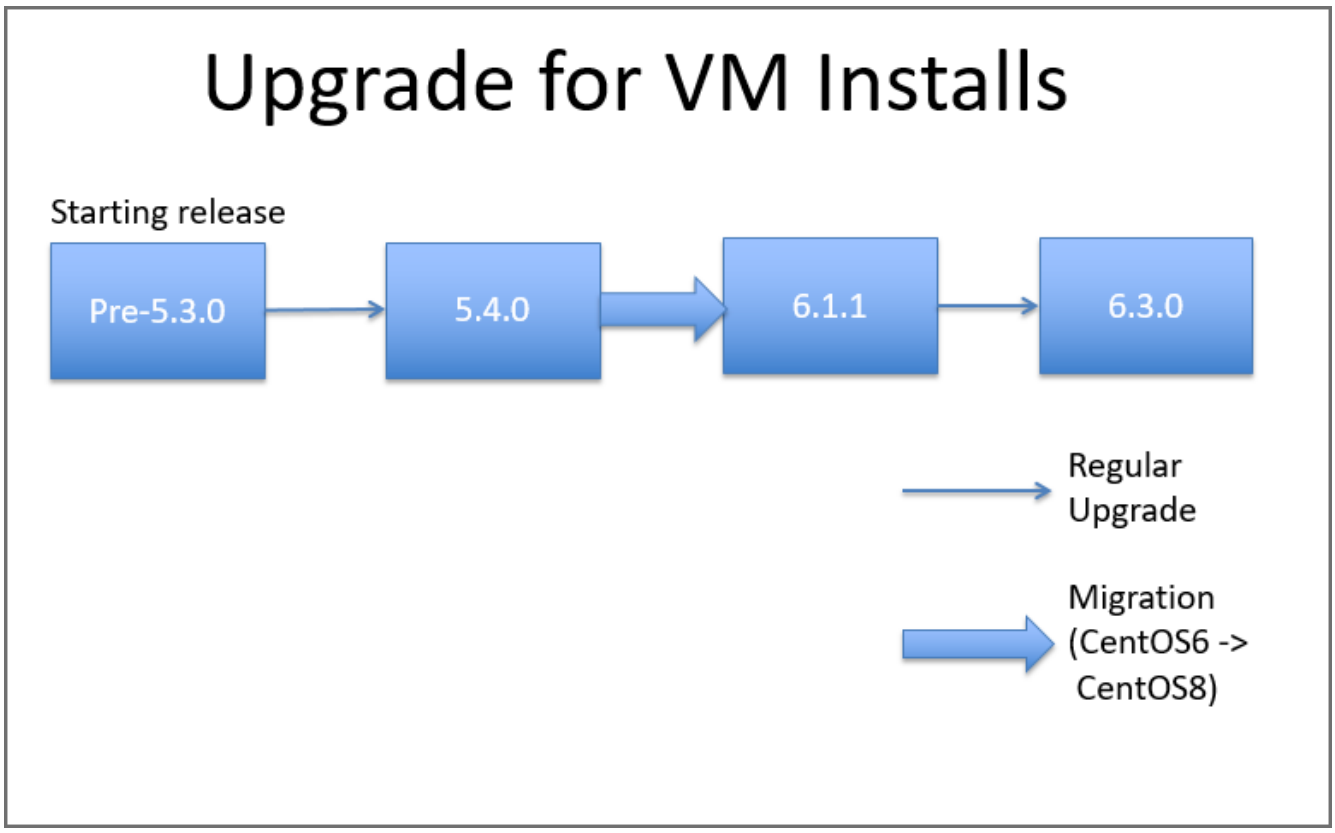
General Upgrade Notes

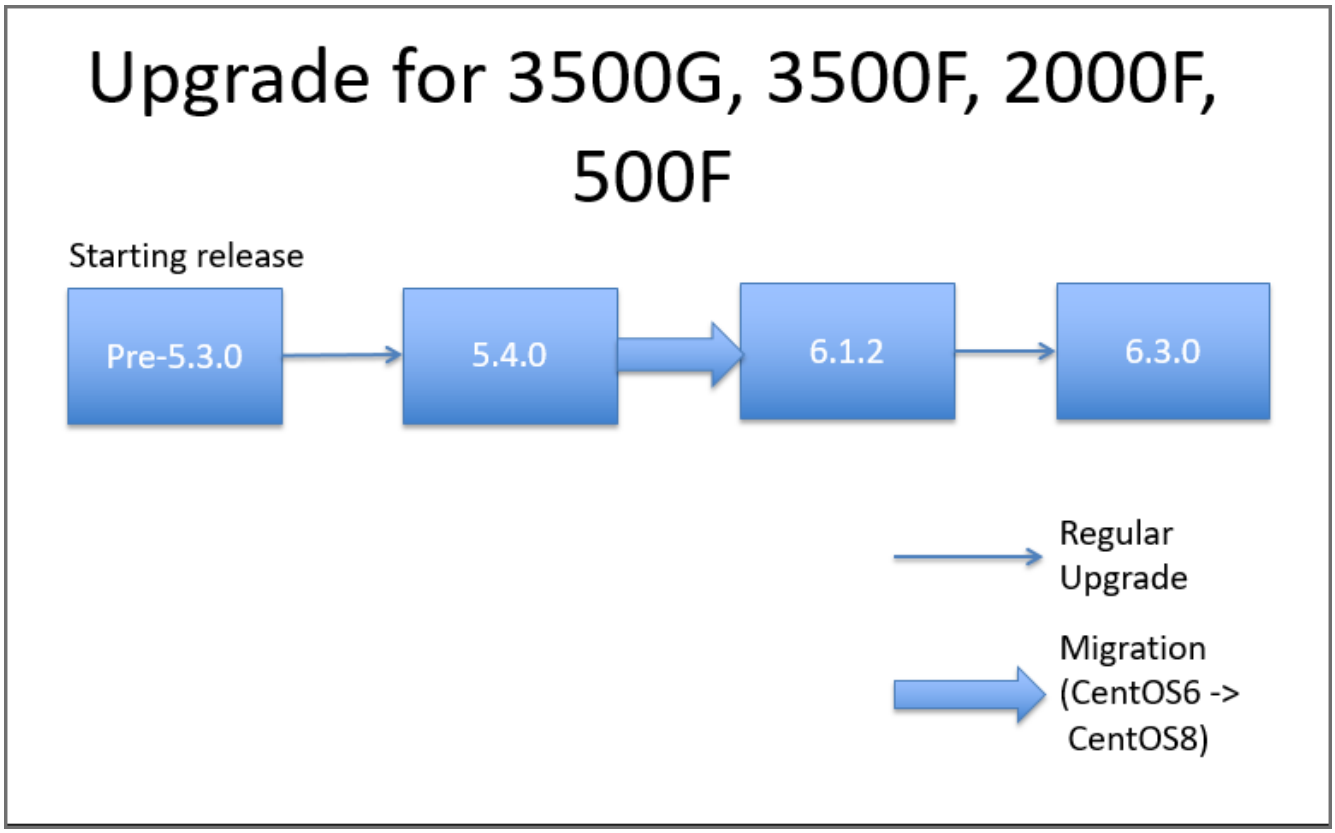
These notes apply to all upgrades in general.

1. For the Supervisor and Worker, do not use the upgrade menu item in configFSM.sh to upgrade from 6.2.0 to 6.3.0. 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. If you have more than 5 Workers, Fortinet recommends using at least 16 vCPU for the Supervisor and to increase the number of notification threads for RuleMaster (See the sizing guide for more information). To do this, SSH to the Supervisor and take the following steps:
   a. Modify the `phoenix_config.txt` file, located at `/opt/phoenix/config/` with
      ```
      #notification will open threads to accept connections
      #FSM upgrade preserves customer changes to the parameter value notification_
      server_thread_num=50
      ```
      Note: The default `notification_server_thread_num` is 20.
   b. Restart `phRuleMaster` using the following commands:
      ```
      #phtools --stop phRuleMaster
      #phtools --start phRuleMaster
      ```
4. Remember to remove the browser cache after logging on to the 6.3.0 GUI and before doing any operations.
5. 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 6.3.0 after you have upgraded all Workers.
6. 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 (6a-d) are not required while upgrading from versions 6.2.1 or later.

Upgrade Pre-5.3.0 Deployment





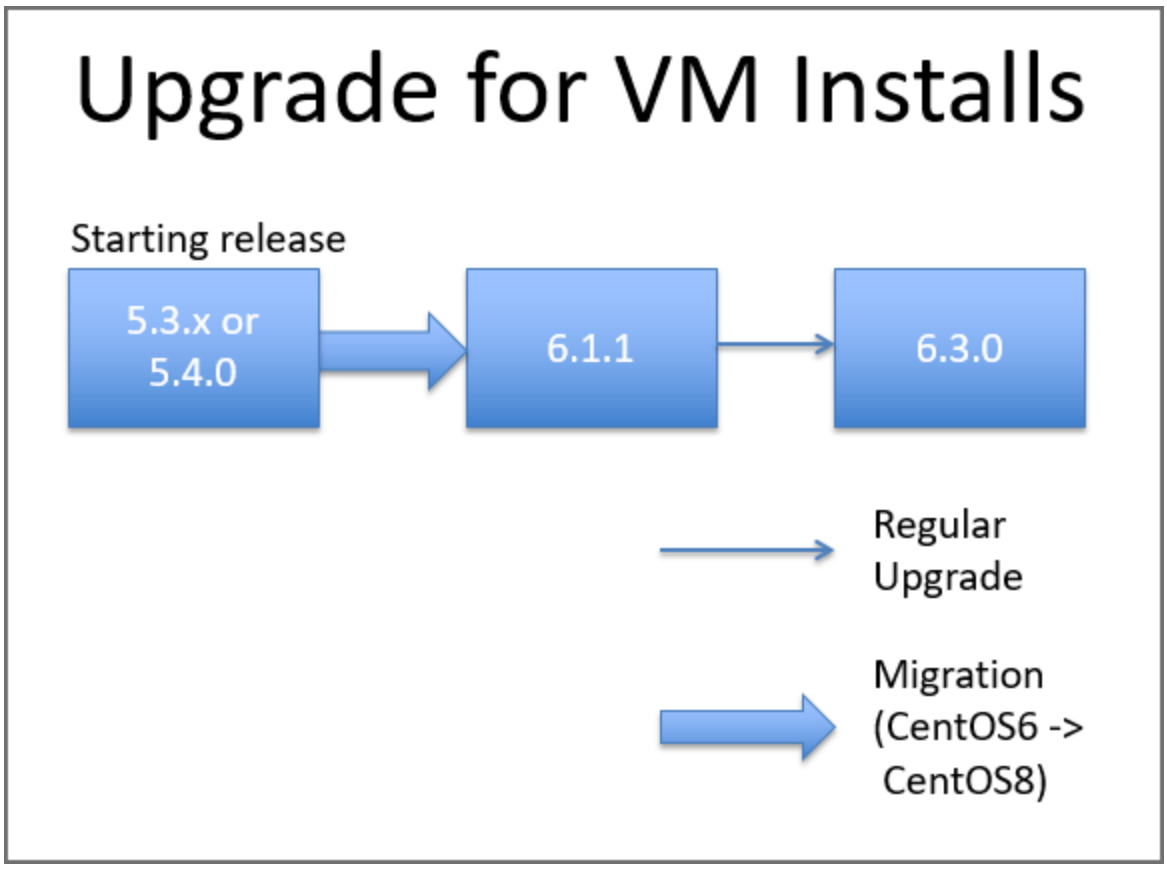
If you are running FortiSIEM that is pre-5.3.0, take the following steps:

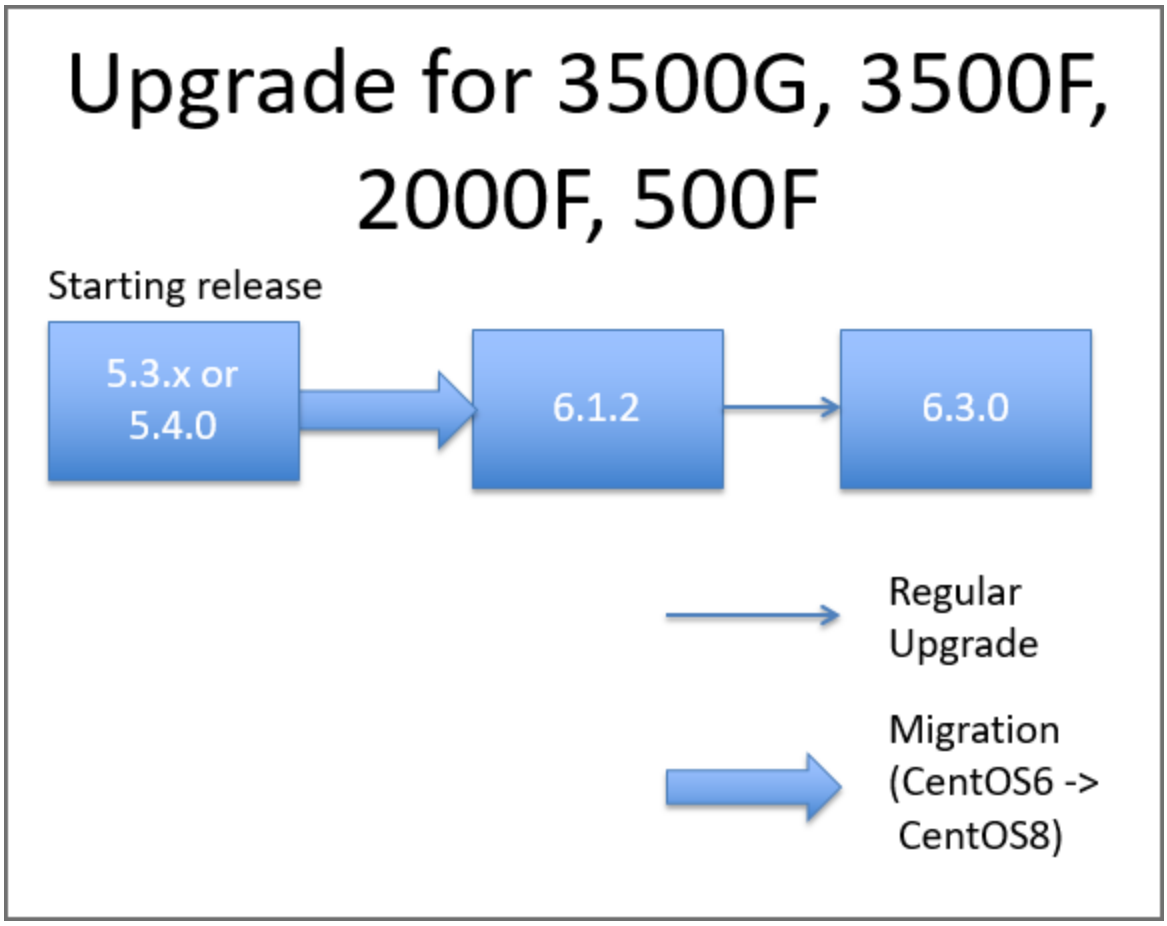
1. Upgrade to 5.4.0 by using the 5.4.0 Upgrade Guide: Single Node Deployment / Cluster Deployment.
2. Perform a health check to make sure the system has upgraded to 5.4.0 successfully.
3. If you are running a Software Virtual Appliance, you must migrate to 6.1.1. Since the base OS changed from CentOS 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





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 6.3.0 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_6.3.0_build0331.zip`, then upload it to the Supervisor node under the `/opt/upgrade/` folder.
   Example (From Linux CLI):
   `scp FSM_Upgrade_All_6.3.0_build0331.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_6.3.0_build0331.zip`
7. Go to the FSM_Upgrade_All_6.3.0_build0331 directory.
   `cd FSM_Upgrade_All_6.3.0_build0331`
   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 6.3.0

From version 6.2.0 to 6.3.0, 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 6.3.0 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

1. Login to the Supervisor via SSH as root.
2. Prepare the Collector upgrade image by running the following command on the Supervisor.
   `phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.3.0_build0331.zip <SupervisorFQDN>`

   Note: Replace <*SupervisorFQDN*> with the fully qualified domain name of the Supervisor.

   Example:

   `# phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.3.0_build0331.zip supervisor.fortinet.com`

   or

   `# phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.3.0_build0331.zip 10.10.10.15`
3. Login to the FortiSIEM Supervisor GUI and navigate to **ADMIN > Health > Collector Health**.
4. Select a Collector.
   a. Download the image by selecting the **Action** drop-down list and clicking **Download Image**.
   b. Upgrade the image by selecting the **Action** drop-down list and clicking **Install Image**.
5. Make sure the Collector and all its processes are up by taking the following steps:
   a. Go to the Task panel by clicking "Jobs and Errors" on the top right corner.
   b. Check the collector upgrade task status.
      The status should be **Done**, and progress should be **100%**.
6. Repeat steps 3 through 5 for all Collectors.

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 6.3.0, 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 >= 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_6.3.0_build0331.zip`, then upload it to the Supervisor node under the `/opt/upgrade/` folder.
   Example (From Linux CLI):
   `scp FSM_Upgrade_All_6.3.0_build0331.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_6.3.0_build0331.zip`
7. Go to the FSM_Upgrade_All_6.3.0_build0331 directory.
   `cd FSM_Upgrade_All_6.3.0_build0331`
   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_6.3.0_build0331.zip` to `/opt/upgrade`.
4. Go to `/opt/upgrade`.
   ```
   cd /opt/upgrade
   ```
5. Unzip the upgrade zip package.
   ```
   unzip FSM_Upgrade_All_6.3.0_build0331.zip
   ```
6. Go to the FSM_Upgrade_All_6.3.0_build0331 directory.
   ```
   cd FSM_Upgrade_All_6.3.0_build0331
   ```
   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) is not required while upgrading from versions 6.2.1 or later.

Upgrade Collectors

Extra Upgrade Steps from 6.2.0 to 6.3.0

From version 6.2.0 to 6.3.0, 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 6.3.0 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 Collectors, take the following steps.

1. Login to the Supervisor via SSH as root.
2. Prepare the Collector upgrade image by running the following command on the Supervisor.

```
phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.3.0_build0331.zip
<SupervisorFQDN>
```

Note: Replace <*SupervisorFQDN*> with the fully qualified domain name of the Supervisor.

Example:

```
# phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.3.0_build0331.zip
supervisor.fortinet.com
```

or

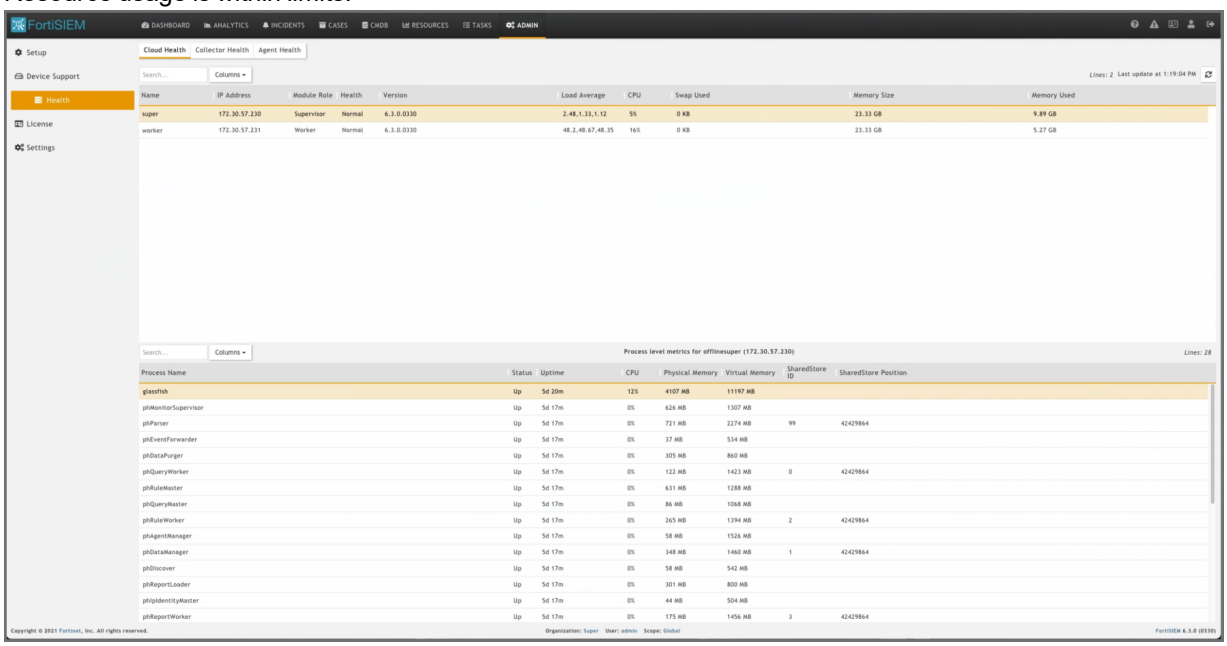
```
# phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.3.0_build0331.zip
10.10.10.15
```

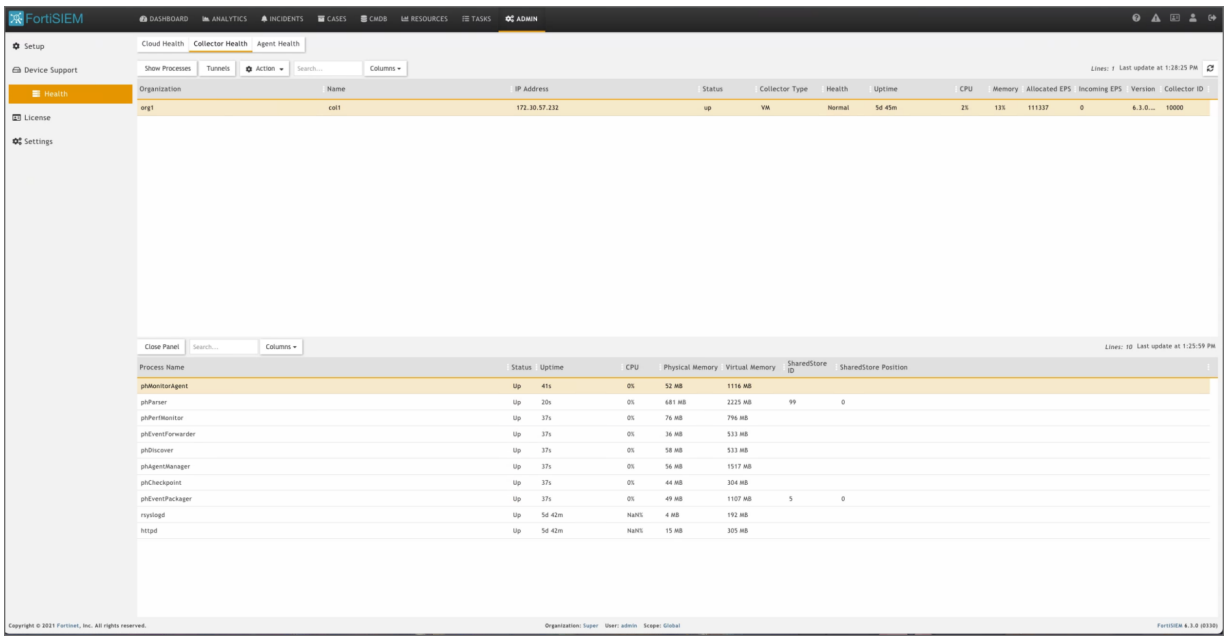
3. Login to the FortiSIEM Supervisor GUI and navigate to **ADMIN > Health > Collector Health**.
4. Select a Collector.
   a. Download the image by selecting the **Action** drop-down list and clicking **Download Image**.
   b. Upgrade the image by selecting the **Action** drop-down list and clicking **Install Image**.
5. Make sure the Collector and all its processes are up by taking the following steps:
   a. Go to the Task panel by clicking "Jobs and Errors" on the top right corner.
   b. Check the collector upgrade task status.
      The status should be **Done**, and progress should be **100%**.
6. Repeat steps 3 through 5 for all Collectors.

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.





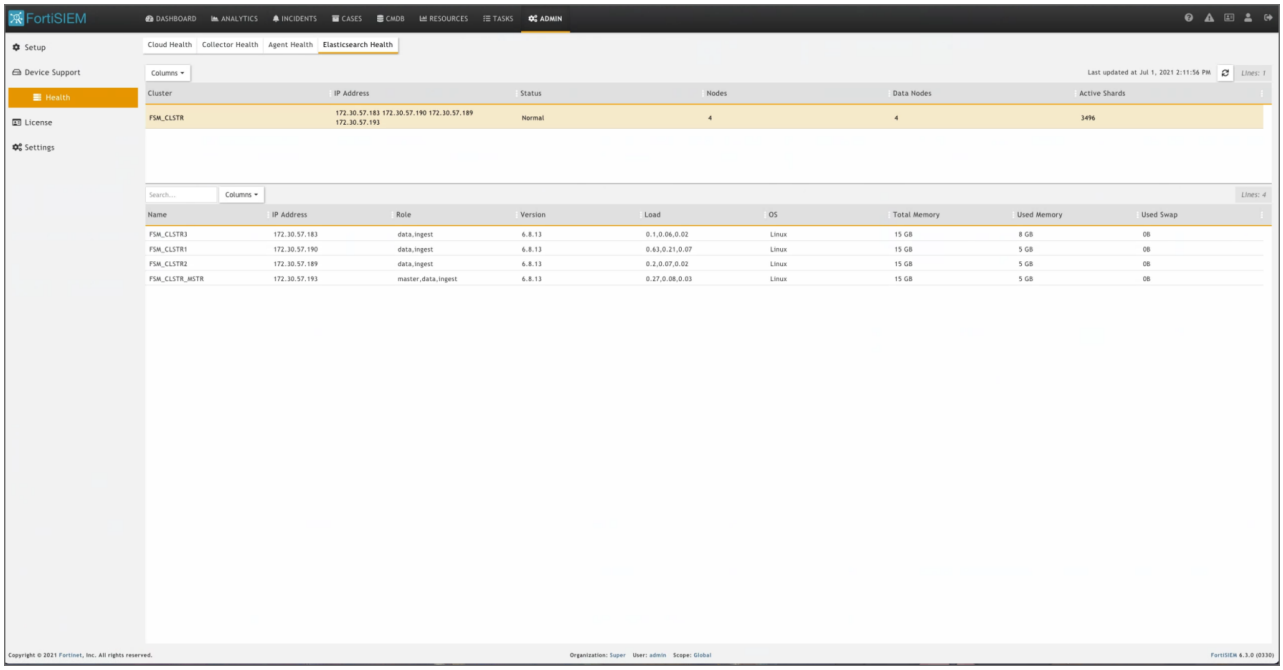
2. Check that the Redis passwords match on the Supervisor and Workers:
   - Supervisor: run the command `phLicenseTool --showRedisPassword`
   - Worker: run the command `grep -i auth /opt/node-rest-service/ecosystem.config.js`

```
[root@offlinesuper ~]# grep -i auth /opt/node-rest-service/ecosystem.config.js
      REDIS_AUTH: '4CiVtA9n1Fh2KPlkDWCjsLTzJCwiwg7F3Yok@5WhVYAnGjSB66pR1v743v5zGNJYXyB%ZB5ScQfk6ihx8L^Dzhj^YO%tWQff554ERhE%U1jBtBZ%chxCLYqcvqvzswQ9',
      REDIS_AUTH: '4CiVtA9n1Fh2KPlkDWCjsLTzJCwiwg7F3Yok@5WhVYAnGjSB66pR1v743v5zGNJYXyB%ZB5ScQfk6ihx8L^Dzhj^YO%tWQff554ERhE%U1jBtBZ%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@5WhVYAnGjSB66pR1v743v5zGNJYXyB%ZB5ScQfk6ihx8L^Dzhj^YO%tWQff554ERhE%U1jBtBZ%chxCLYqcvqvzswQ9',
      REDIS_AUTH: '4CiVtA9n1Fh2KPlkDWCjsLTzJCwiwg7F3Yok@5WhVYAnGjSB66pR1v743v5zGNJYXyB%ZB5ScQfk6ihx8L^Dzhj^YO%tWQff554ERhE%U1jBtBZ%chxCLYqcvqvzswQ9',
```

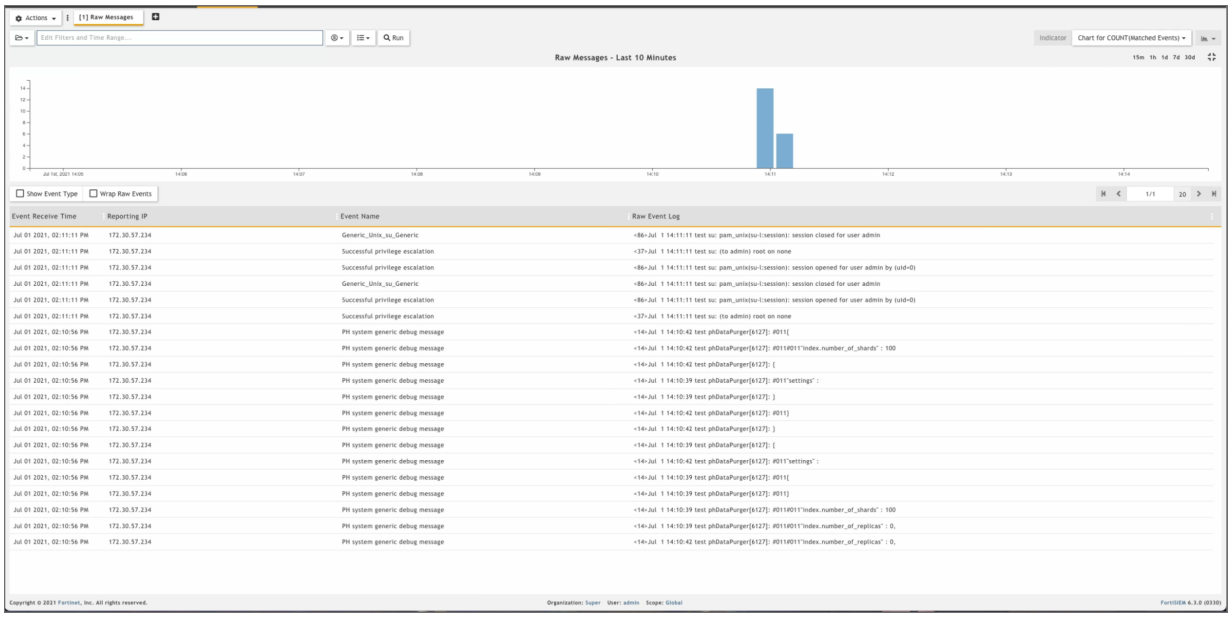
3. Check that the database passwords match on the Supervisor and Workers:
   - Supervisor: run the command `phLicenseTool --showDatabasePassword`
   - Worker: run the command `grep Auth_PQ_dbpass /etc/httpd/conf/httpd.conf`

```
[root@offlineworker ~]# grep Auth_PQ_dbpass /etc/httpd/conf/httpd.conf
      Auth_PQ_dbpass      MHp0YzN^riB6
      Auth_PQ_dbpass      MHp0YzN^riB6
```

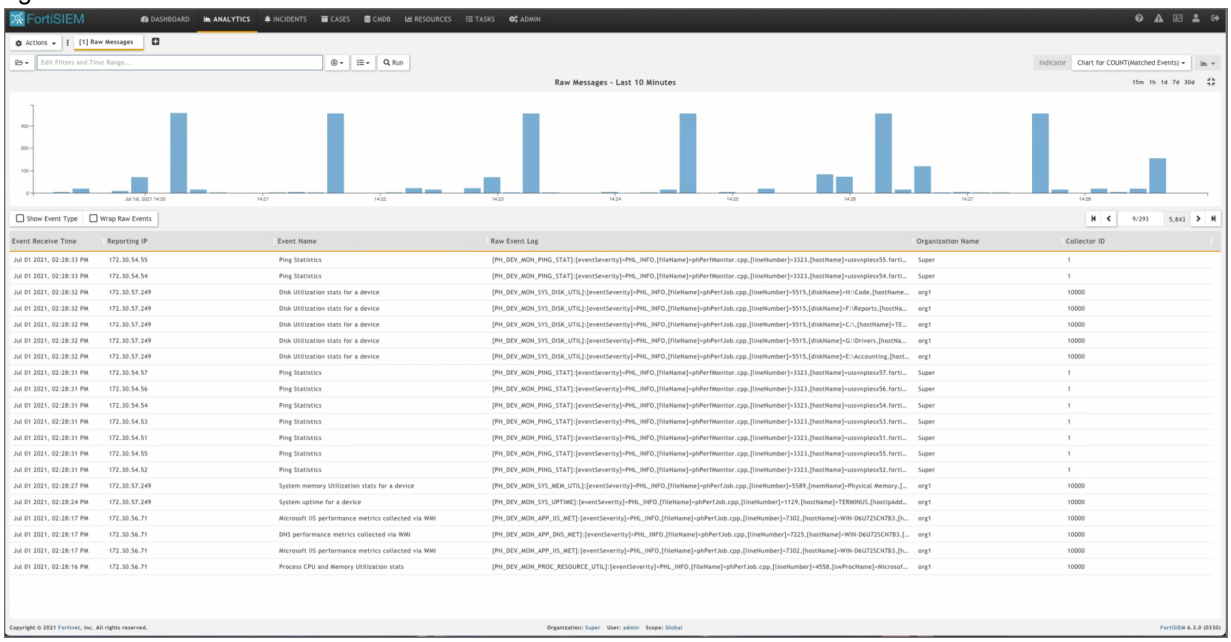
4. Elasticsearch case: check the Elasticsearch health



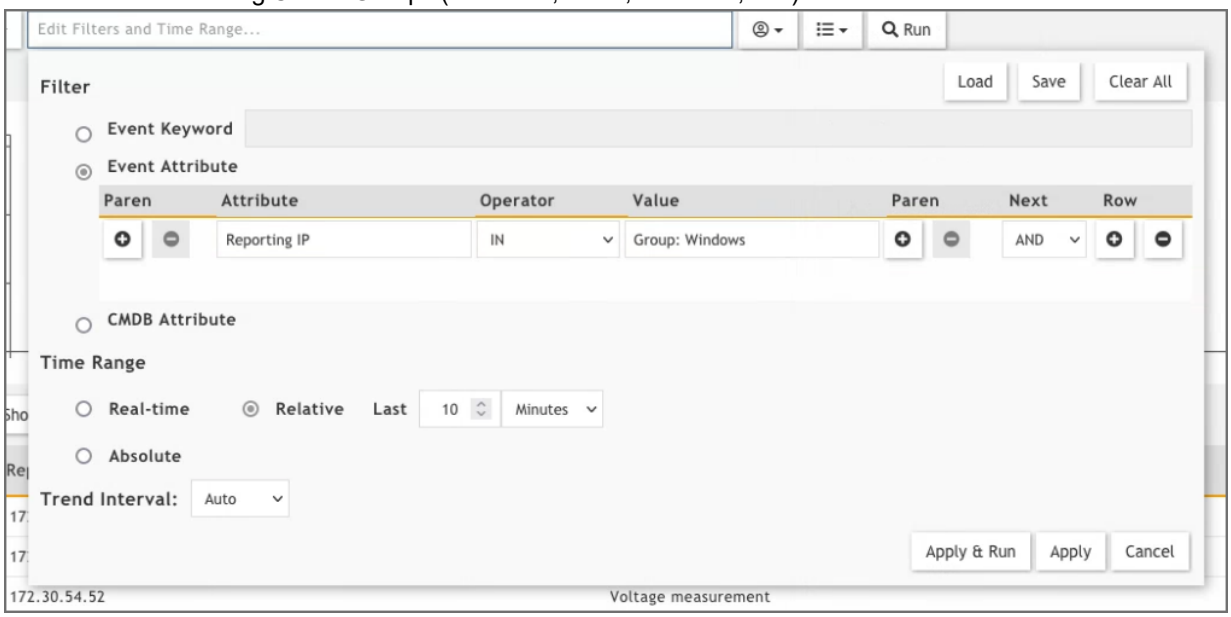
5. Check that events are received correctly:
   a. Search All Events in last 10 minutes and make sure there is data.

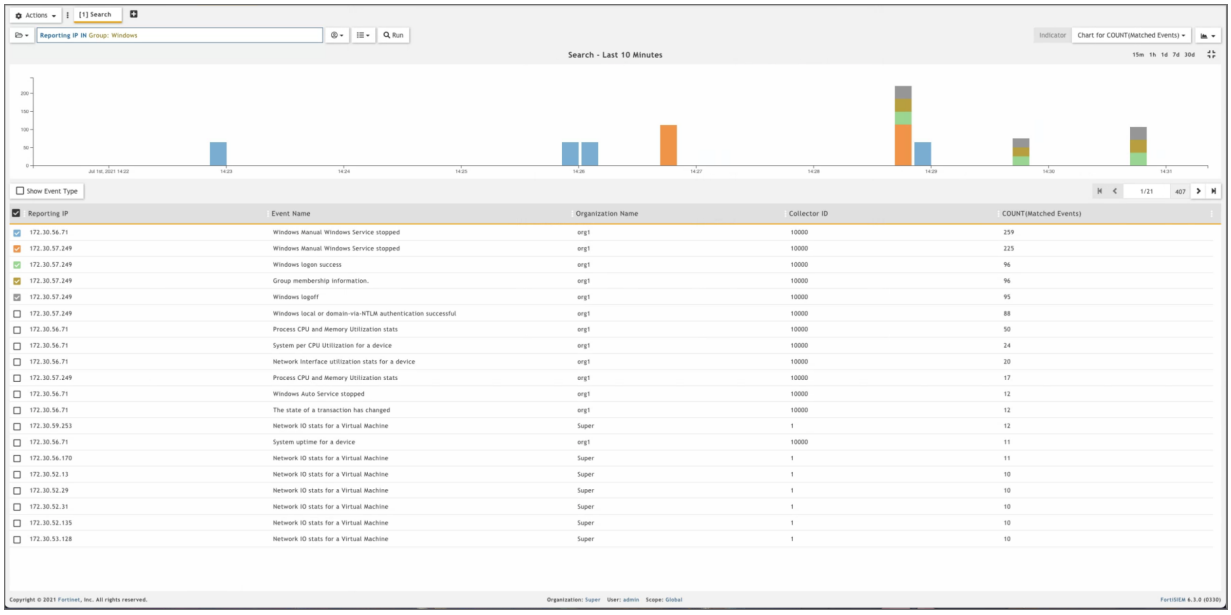


   b. Search for events from Collector and Agents and make sure there is data. Both old and new collectors and agents must work.

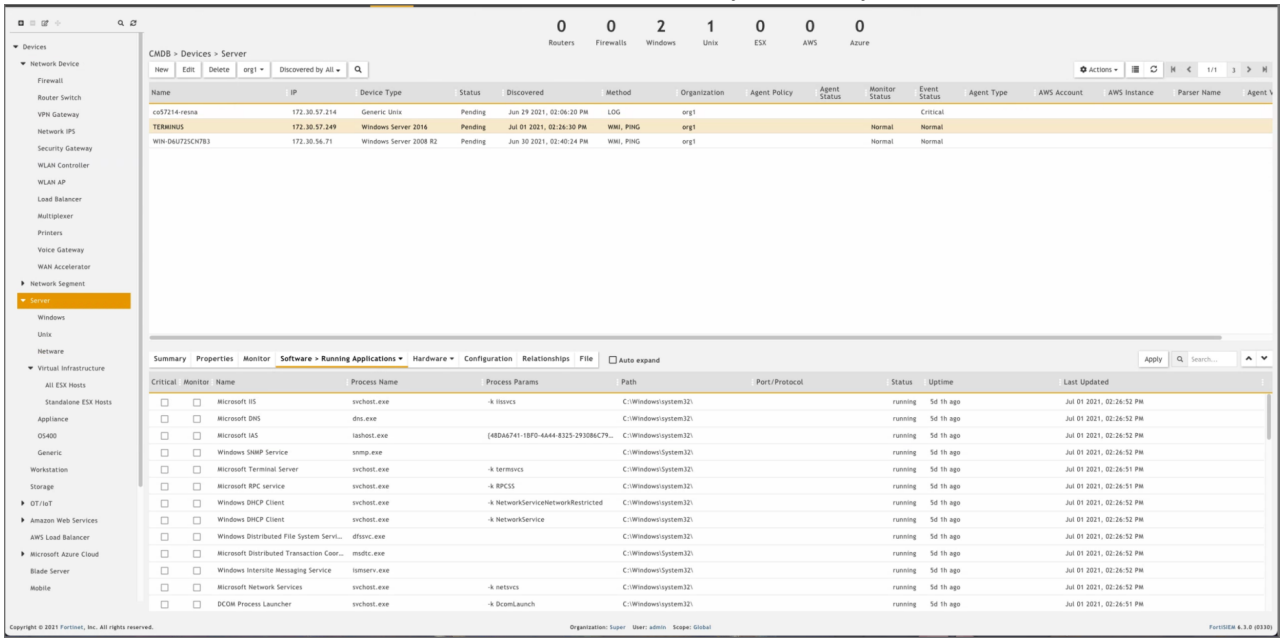


c. Search for events using CMDB Groups (Windows, Linux, Firewalls, etc.) and make sure there is data.

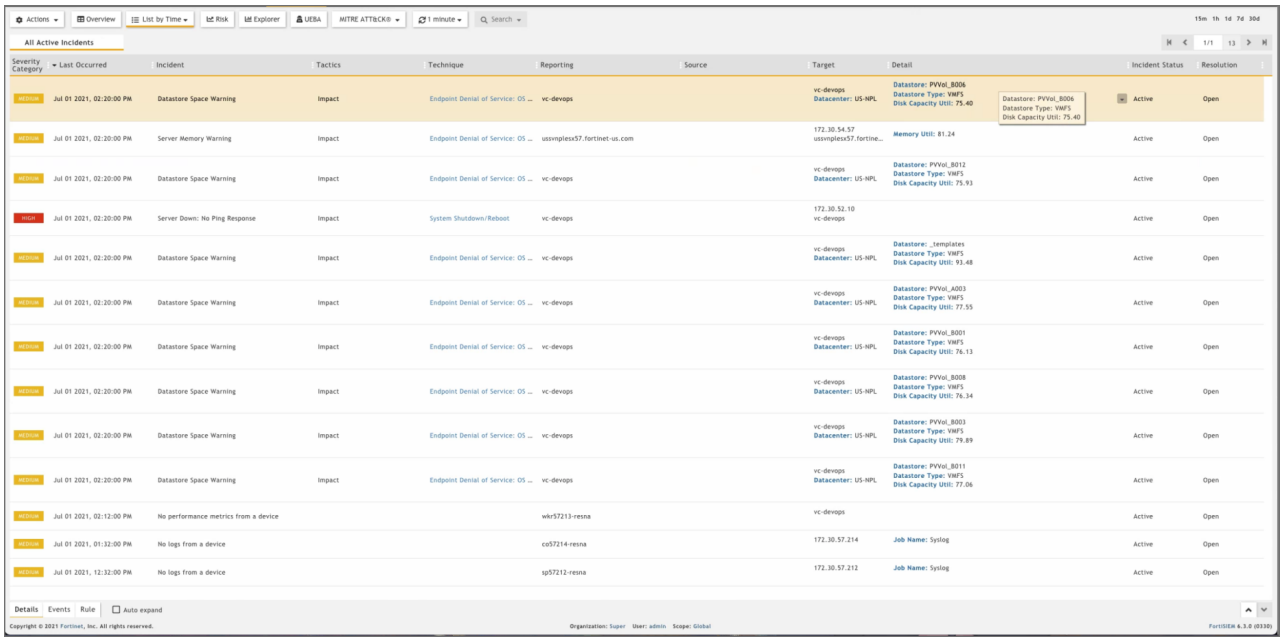




6. Make sure there are no SVN authentication errors in CMDB when you click any device name.



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



8. Check Worker for Collector Credentials by running the following command:
   `cat /etc/httpd/accounts/passwd`
   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 CentOS OS repositories (`os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs.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 6.3.0.0331 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© 2022 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.