FortiSIEM - Upgrade Guide

Version 6.1.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

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

12/01/2021
FortiSIEM 6.1.1 Upgrade Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
11/05/2020	Initial version of the 6.1.1 Upgrade Guide.
12/01/2021	Updated Pre-Upgrade Steps section.

Upgrading to FortiSIEM 6.1.1

If you are running FortiSIEM 6.x then use these instructions to upgrade to the latest FortiSIEM 6.x version.

Pre-Upgrade Steps

If you are running FortiSIEM 6.1.0, then you will need a simple step before you proceed to upgrade. This involves copying a file into a specific location on the Supervisor node. Please complete this step before you proceed to upgrade to the latest FortiSIEM version.

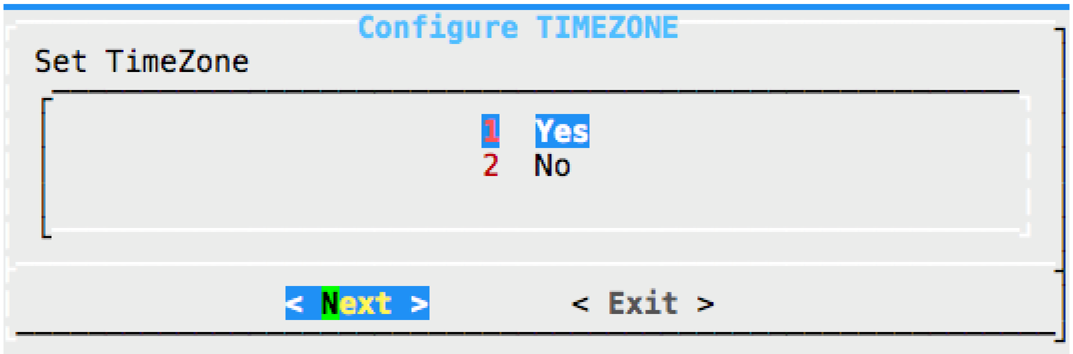
1. Carefully consider the known issues, if any, in the Release Notes.
2. Download the file `FSM_Upgrade_Script_Patch_6.1.1_build0118.zip` from the Fortinet Support website.
3. Login to the Supervisor as `root`.
4. Extract the `upgrade.py` script.
5. Copy it to `/usr/local/syslib/`.
6. Continue with the upgrade instructions below.

Upgrade Single Node Deployment

These instructions cover the upgrade process for the FortiSIEM deployment consisting of a single Supervisor node.

1. Download the upgrade image `FSM_Upgrade_All_6.1.1_build0118.zip` from Fortinet Support website.
2. Copy the file to Supervisor:
   a. Login as `root`.
   b. Run `mkdir -p /opt/upgrade`.
   c. Run `cd /opt/upgrade`.
   d. Copy `FSM_Upgrade_All_6.1.1_build0118.zip` to `/opt/upgrade`.
3. To avoid issues with SSH connection timeouts, disconnects etc.:
   a. Run the upgrade using the following command:
      ```
      screen -S upgrade
      ```
   b. To connect the screen after failure, run:
      ```
      run screen -r
      ```

4. Upgrade by running `configFSM.sh`:
   a. Setup **Timezone** with **Country** and **Region** and click **Next**.

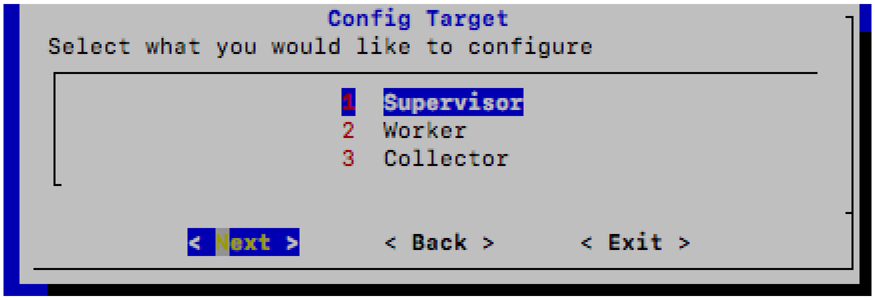


```
                 Configure TIMEZONE
 Set TimeZone

                    1  Yes
                    2  No

        < Next >            < Exit >
```

   b. Select **Supervisor** and click **Next**.

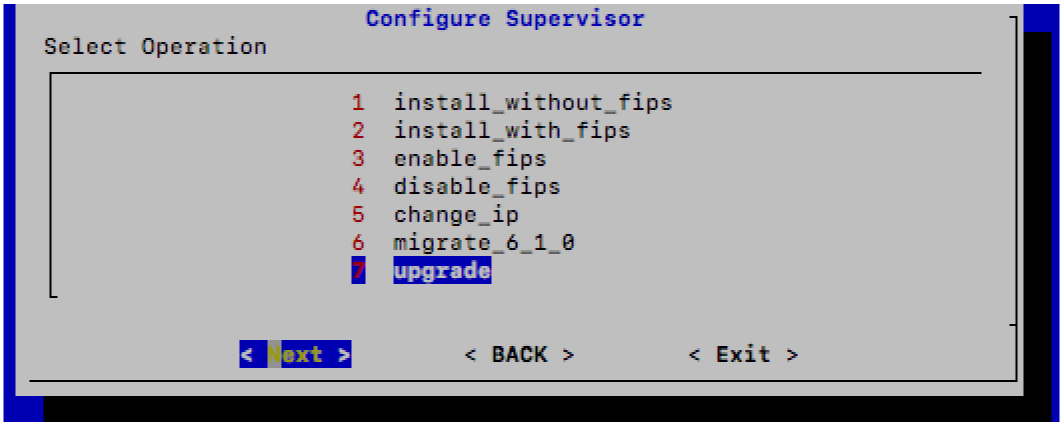


```
                 Config Target
 Select what you would like to configure

                    1  Supervisor
                    2  Worker
                    3  Collector

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

   c. Select **Upgrade** operation and click **Next**.

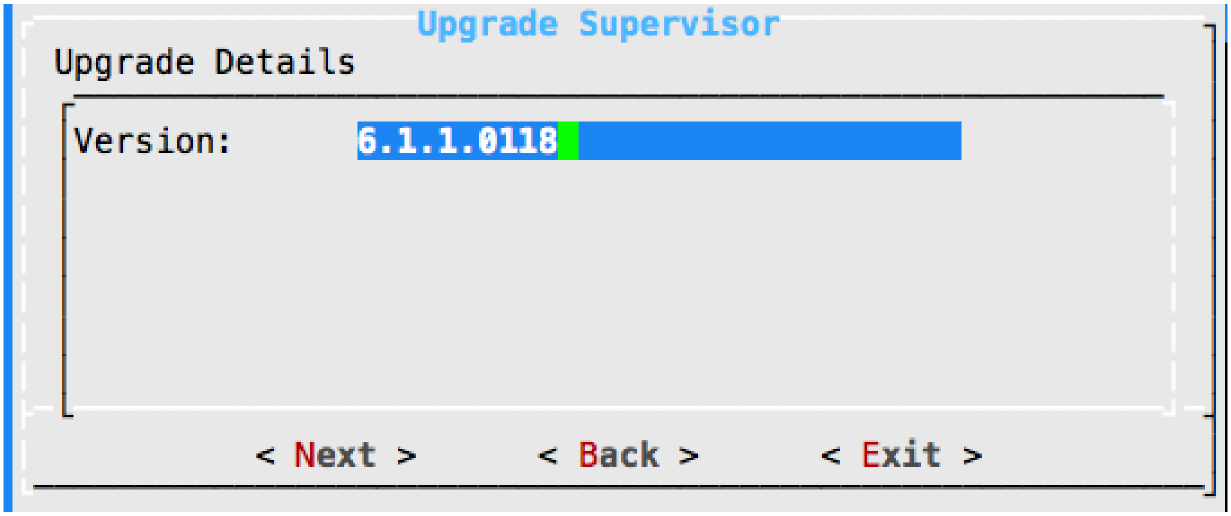


```
                   Configure Supervisor
 Select Operation

                    1  install_without_fips
                    2  install_with_fips
                    3  enable_fips
                    4  disable_fips
                    5  change_ip
                    6  migrate_6_1_0
                    7  upgrade

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

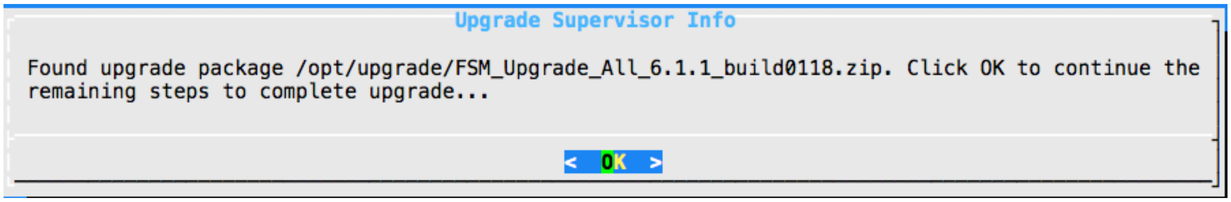
   d. Enter the version you want to upgrade to and click **Next**.



Upgrade Details

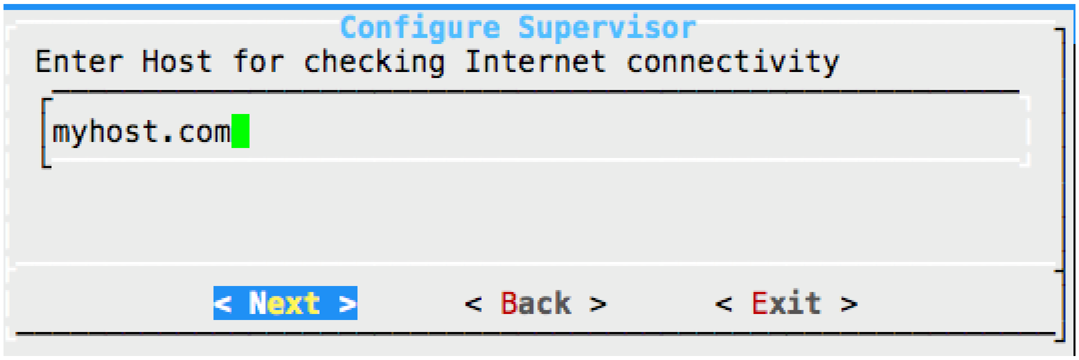
Version: 6.1.1.0118

e. Once FortiSIEM finds the matching upgrade package, click **OK**.



```
Found upgrade package /opt/upgrade/FSM_Upgrade_All_6.1.1_build0118.zip. Click OK to continue the
remaining steps to complete upgrade...
```

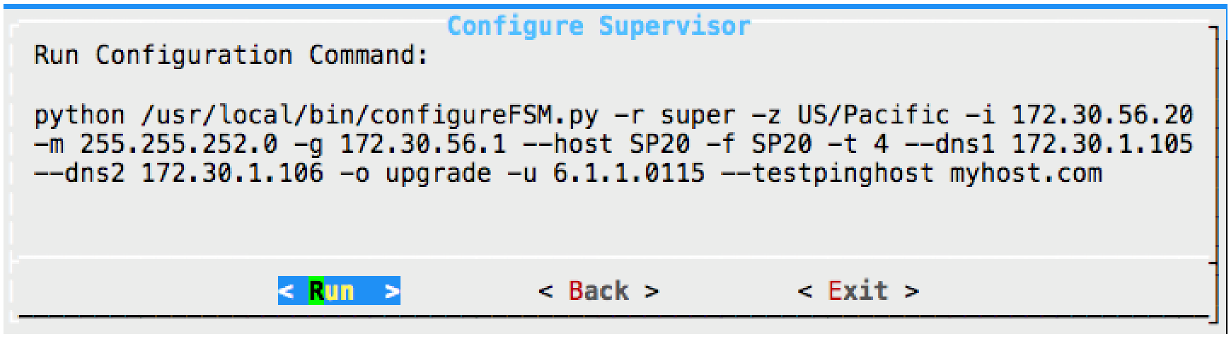
f. Enter a host name (`myhost.com` as an example) that can be resolved from the **Supervisor**, then click **Next**. Note: Internet connectivity is the same as network connectivity.



Enter Host for checking Internet connectivity

myhost.com

g. Click **Run**.

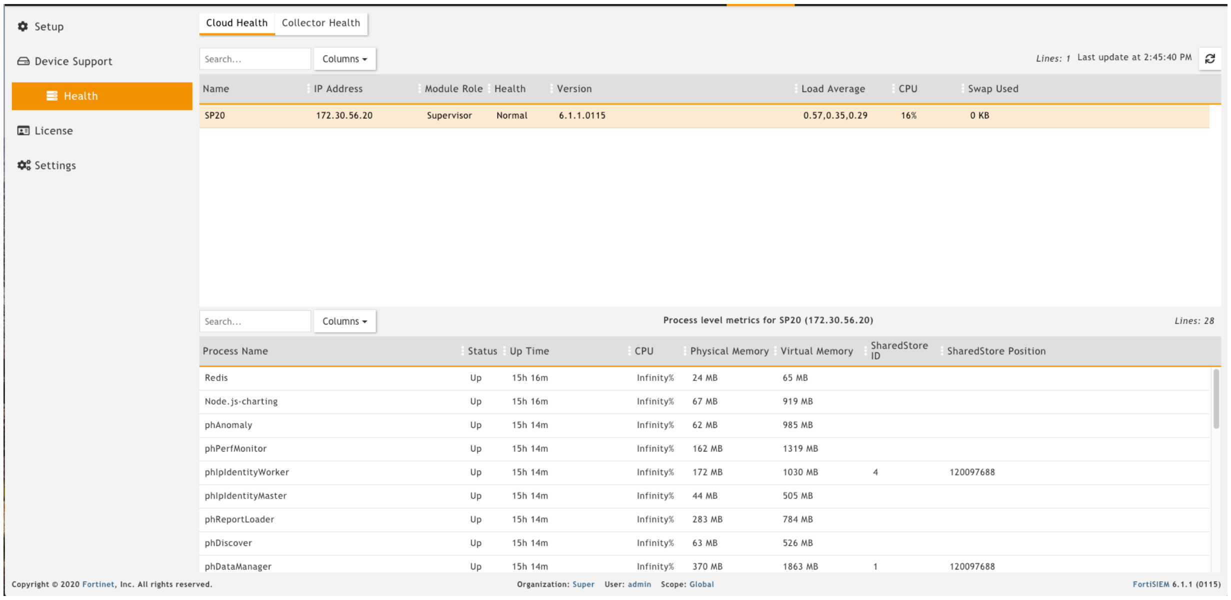


Run Configuration Command:

```
python /usr/local/bin/configureFSM.py -r super -z US/Pacific -i 172.30.56.20
-m 255.255.252.0 -g 172.30.56.1 --host SP20 -f SP20 -t 4 --dns1 172.30.1.105
--dns2 172.30.1.106 -o upgrade -u 6.1.1.0115 --testpinghost myhost.com
```

5. Login to the Supervisor and make sure the upgrade succeeded.

   a. In the GUI, go to **Admin > Health > Cloud Health** to make sure it is running the upgraded version and that all processes are up and running.



Lines: 1 Last update at 2:45:40 PM

Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used
SP20	172.30.56.20	Supervisor	Normal	6.1.1.0115	0.57,0.35,0.29	16%	0 KB

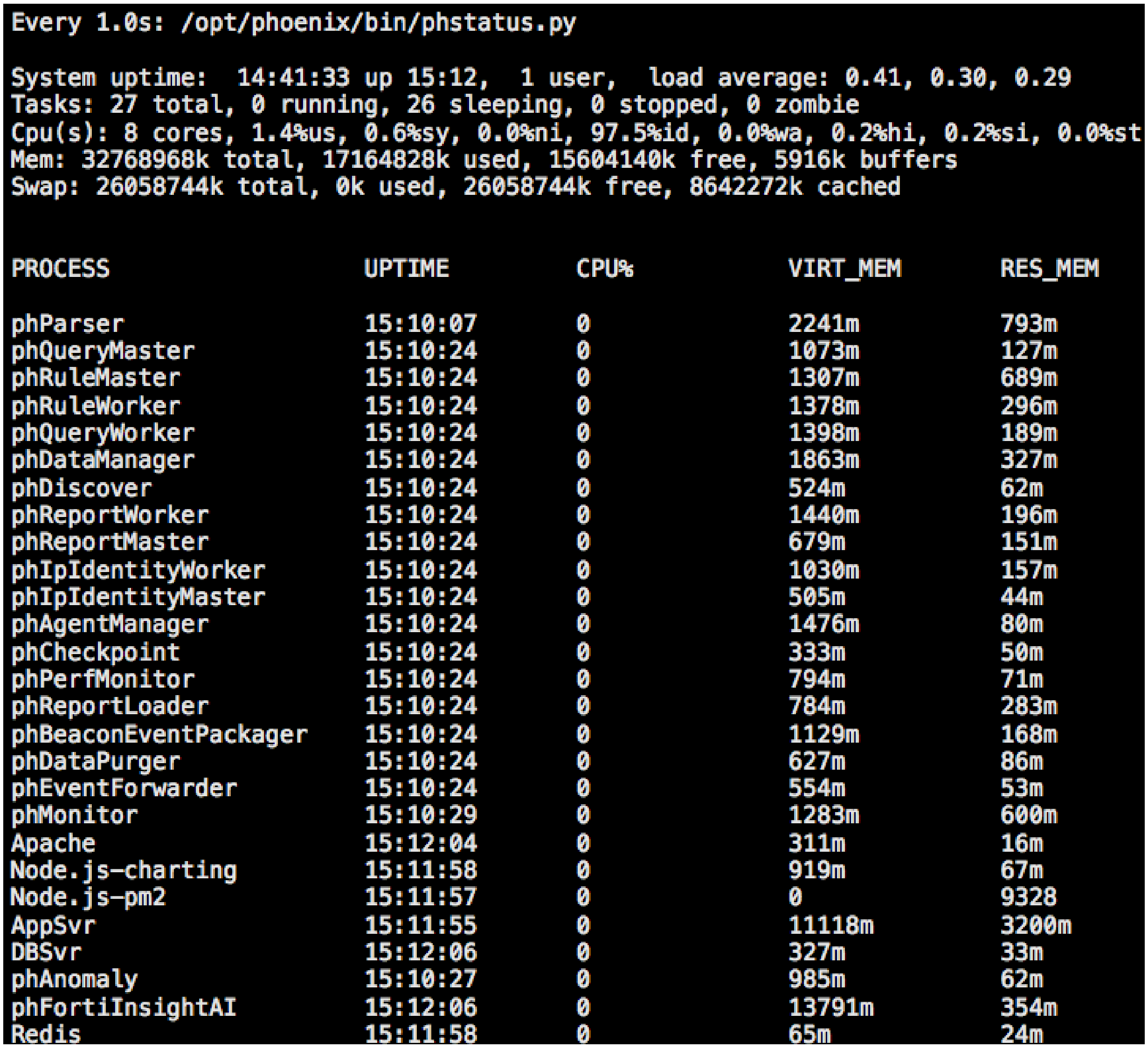
Process level metrics for SP20 (172.30.56.20)

Lines: 28

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
Redis	Up	15h 16m	Infinity%	24 MB	65 MB		
Node.js-charting	Up	15h 16m	Infinity%	67 MB	919 MB		
phAnomaly	Up	15h 14m	Infinity%	62 MB	985 MB		
phPerfMonitor	Up	15h 14m	Infinity%	162 MB	1319 MB		
phIpIdentityWorker	Up	15h 14m	Infinity%	172 MB	1030 MB	4	120097688
phIpIdentityMaster	Up	15h 14m	Infinity%	44 MB	505 MB		
phReportLoader	Up	15h 14m	Infinity%	283 MB	784 MB		
phDiscover	Up	15h 14m	Infinity%	63 MB	526 MB		
phDataManager	Up	15h 14m	Infinity%	370 MB	1863 MB	1	120097688

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.1.1 (0115)

b. Login via SSH and run `phstatus` to make sure that all processes are up and running.



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

System uptime:  14:41:33 up 15:12,  1 user,  load average: 0.41, 0.30, 0.29
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 1.4%us, 0.6%sy, 0.0%ni, 97.5%id, 0.0%wa, 0.2%hi, 0.2%si, 0.0%st
Mem: 32768968k total, 17164828k used, 15604140k free, 5916k buffers
Swap: 26058744k total, 0k used, 26058744k free, 8642272k cached


PROCESS                 UPTIME        CPU%          VIRT_MEM      RES_MEM

phParser                15:10:07      0             2241m         793m
phQueryMaster           15:10:24      0             1073m         127m
phRuleMaster            15:10:24      0             1307m         689m
phRuleWorker            15:10:24      0             1378m         296m
phQueryWorker           15:10:24      0             1398m         189m
phDataManager           15:10:24      0             1863m         327m
phDiscover              15:10:24      0             524m          62m
phReportWorker          15:10:24      0             1440m         196m
phReportMaster          15:10:24      0             679m          151m
phIpIdentityWorker      15:10:24      0             1030m         157m
phIpIdentityMaster      15:10:24      0             505m          44m
phAgentManager          15:10:24      0             1476m         80m
phCheckpoint            15:10:24      0             333m          50m
phPerfMonitor           15:10:24      0             794m          71m
phReportLoader          15:10:24      0             784m          283m
phBeaconEventPackager   15:10:24      0             1129m         168m
phDataPurger            15:10:24      0             627m          86m
phEventForwarder        15:10:24      0             554m          53m
phMonitor               15:10:29      0             1283m         600m
Apache                  15:12:04      0             311m          16m
Node.js-charting        15:11:58      0             919m          67m
Node.js-pm2             15:11:57      0             0             9328
AppSvr                  15:11:55      0             11118m        3200m
DBSvr                   15:12:06      0             327m          33m
phAnomaly               15:10:27      0             985m          62m
phFortiInsightAI        15:12:06      0             13791m        354m
Redis                   15:11:58      0             65m           24m
```

Upgrade Cluster Deployment

- Overview
- Detailed Steps - Local Disk or NFS Storage
- Detailed Steps - Elasticsearch Storage

These instructions cover the upgrade process for FortiSIEM cluster deployment consisting the Supervisor, Workers and Collectors.

Overview

It is important to be aware of these steps while upgrading the FortiSIEM cluster. This is a general overview only; detailed steps will follow.

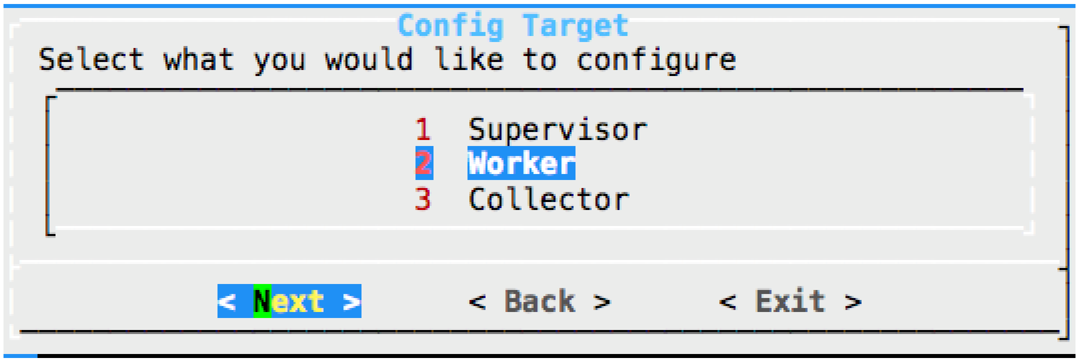
1. Shut down all Workers. Collectors can be up and running.
2. Upgrade Supervisor first (while all Workers are shutdown).
3. After Supervisor is up and running, upgrade Workers one by one.
4. Upgrade Collectors.

Step #1 prevents the accumulation of **Report** files while the Supervisor is not available during upgrade. If these steps are not followed, the Supervisor may not be able to come up after the upgrade because of excessive unprocessed report file accumulation.

Note: Both the Supervisor and the Worker must be on the same FortiSIEM version, or else various software modules may not work properly. However, Collectors can be in an older version (one version older) - they will work, however they may not have the latest discovery and performance monitoring features in the Supervisor/Worker versions. So FortiSIEM recommends that you also upgrade Collectors within a short period of time. If you have Collectors in your deployment, make sure you have configured an image server to use as a repository for the Collector.

Detailed Steps - Local Disk or NFS Storage

1. Shutdown all Worker nodes.
2. Upgrade Supervisor using the previous step. Make sure the Supervisor is running the version you have upgraded to and that all processes are up and running.
3. After upgrading the Supervisor, you can upgrade Workers one by one, the same way as the Supervisor. In this case, choose **Worker**.

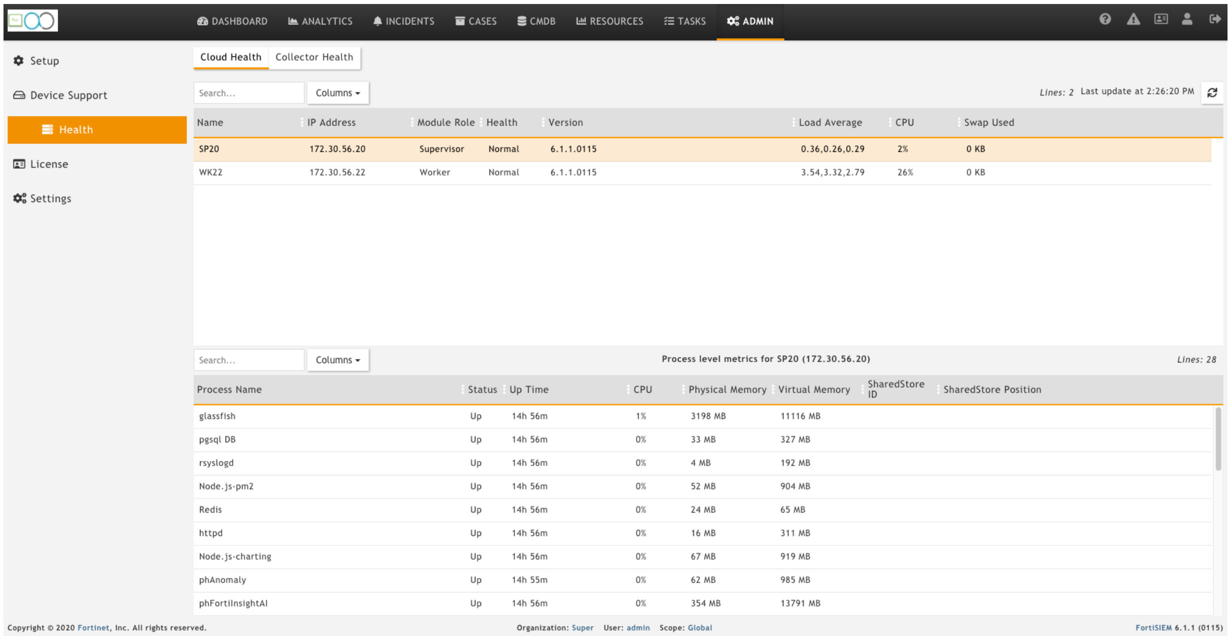


```
                    Config Target
 Select what you would like to configure

                  1  Supervisor
                  2  Worker
                  3  Collector

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

4. After you have upgraded all of the Workers, login to the Supervisor. Go to **Admin > Health > Cloud health** and make sure that all Workers are running the version you have upgraded to and that all processes are up and running. Note: Supervisor and Workers must be on the same version.



Lines: 2 Last update at 2:26:20 PM

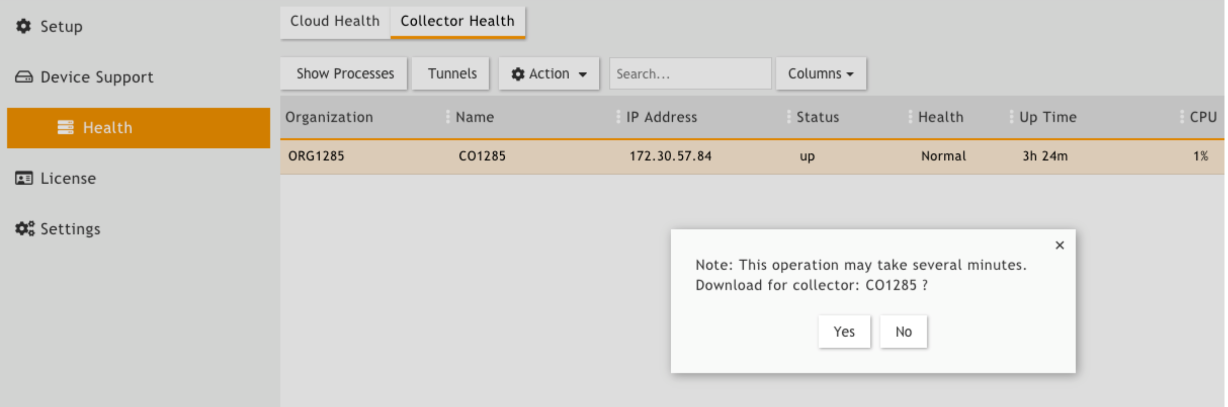
Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used
SP20	172.30.56.20	Supervisor	Normal	6.1.1.0115	0.36,0.26,0.29	2%	0 KB
WK22	172.30.56.22	Worker	Normal	6.1.1.0115	3.54,3.32,2.79	26%	0 KB

Process level metrics for SP20 (172.30.56.20) *Lines: 28*

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
glassfish	Up	14h 56m	1%	3198 MB	11116 MB		
pgsql DB	Up	14h 56m	0%	33 MB	327 MB		
rsyslogd	Up	14h 56m	0%	4 MB	192 MB		
Node.js-pm2	Up	14h 56m	0%	52 MB	904 MB		
Redis	Up	14h 56m	0%	24 MB	65 MB		
httpd	Up	14h 56m	0%	16 MB	311 MB		
Node.js-charting	Up	14h 56m	0%	67 MB	919 MB		
phAnomaly	Up	14h 55m	0%	62 MB	985 MB		
phFortiInsightAI	Up	14h 56m	0%	354 MB	13791 MB		

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.1.1 (0115)

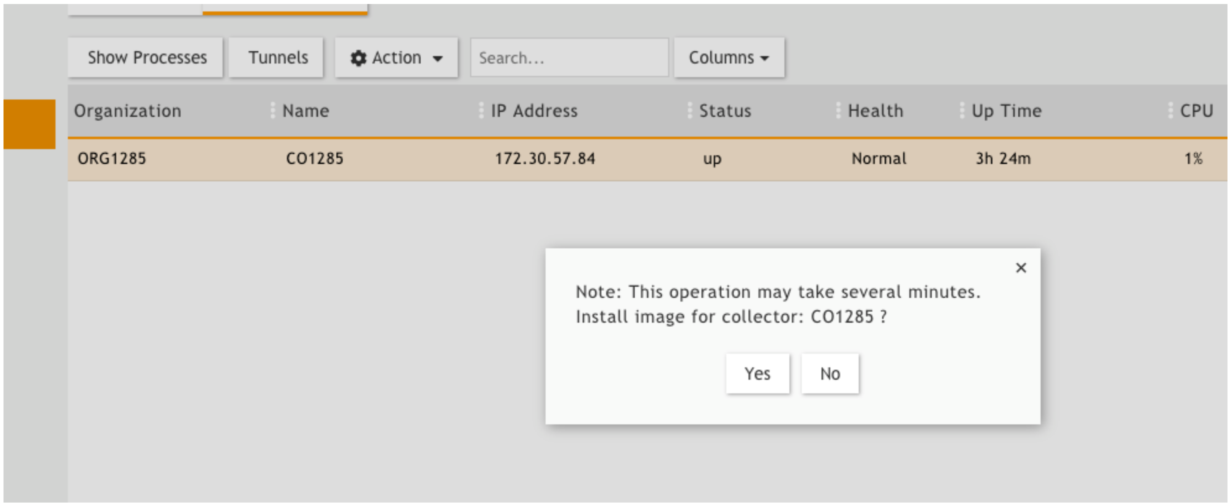
5. Upgrade Collectors running 6.1.0 or later.
   a. Login to the Supervisor via SSH as `root`.
   b. Setup upgrade by running `phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.1.1_build0118.zip <superIP>`.The command will copy the upgrade files to the right location and prepare collector download:
   c. Login to the FortiSIEM GUI.
   d. Go to the **ADMIN > Health > Collector Health** page.
   e. Select a Collector, then choose **Actions > Download Image**, then wait for completion.



Organization	Name	IP Address	Status	Health	Up Time	CPU
ORG1285	CO1285	172.30.57.84	up	Normal	3h 24m	1%

Note: This operation may take several minutes.
Download for collector: CO1285 ?

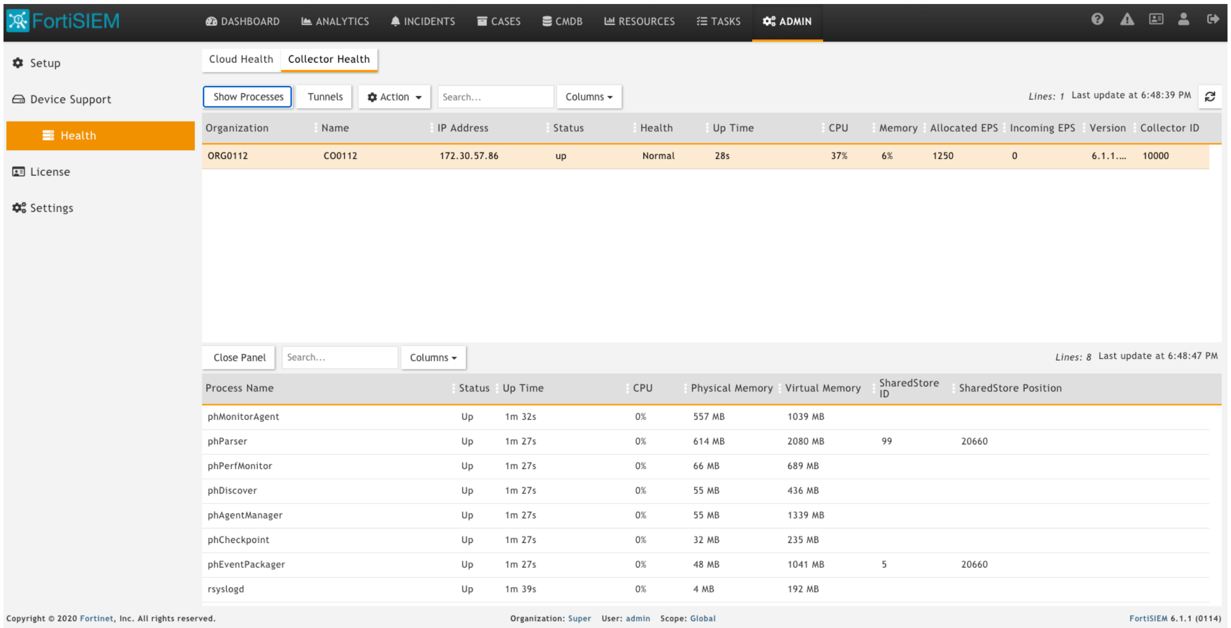
   f. Select a Collector, then choose **Actions > Install Image**, then wait for completion.



Organization	Name	IP Address	Status	Health	Up Time	CPU
ORG1285	CO1285	172.30.57.84	up	Normal	3h 24m	1%

Note: This operation may take several minutes.
Install image for collector: CO1285 ?

g. Collector will upgrade, reboot and re-connect to the Supervisor. Check Collector Health to make sure it is running normally.



Lines: 1 Last update at 6:48:39 PM

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Collector ID
ORG0112	CO0112	172.30.57.86	up	Normal	28s	37%	6%	1250	0	6.1.1....	10000

Lines: 8 Last update at 6:48:47 PM

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	1m 32s	0%	557 MB	1039 MB		
phParser	Up	1m 27s	0%	614 MB	2080 MB	99	20660
phPerfMonitor	Up	1m 27s	0%	66 MB	689 MB		
phDiscover	Up	1m 27s	0%	55 MB	436 MB		
phAgentManager	Up	1m 27s	0%	55 MB	1339 MB		
phCheckpoint	Up	1m 27s	0%	32 MB	235 MB		
phEventPackager	Up	1m 27s	0%	48 MB	1041 MB	5	20660
rsyslogd	Up	1m 39s	0%	4 MB	192 MB		

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.1.1 (0114)

6. For pre-6.1.0 Collectors, FortiSIEM does not support Collector migration to 6.1.0 for VM based collectors. You will need to install new 6.1.1 Collectors and register them to 6.1.1 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. To do this follow these steps:

   a. Preparation steps:

      i. Copy the http hashed password file `/etc/httpd/accounts/passwds` from the old Collector.

      ii. Disconnect the pre-6.1.0 Collector.

      iii. Install the 6.1 Collector with the old IP address by the following the steps in **Cluster Installation > Install Collectors**.

      iv. Copy the saved http hashed password file `/etc/httpd/accounts/passwds` from the old Collector to the 6.1.0 Collector. This step is needed for Agents to work seamlessly with 6.1.0 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.0 migration, this password is lost.

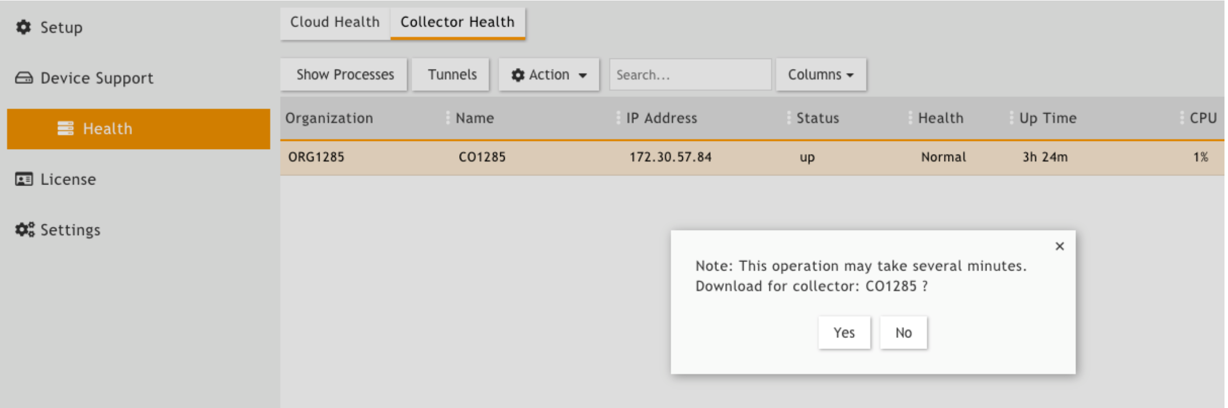
   b. Register Collectors steps:
      i. Follow the steps in **Cluster Installation > Register Collectors**, with the following difference: in the `phProvisionCollector` command, use `--update` option instead of `--add`. Other than this, use the same parameters that were used to register the pre-6.1.0 Collector. Specifically, use the `phProvisionCollector` command to register a 6.1.0 Collector and keep the old associations: `# /opt/phoenix/bin/phProvisionCollector --update <user> <password> <Super IP or Host> <Organization> <CollectorName>`. Then, re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.

7. Follow steps in the 500F Collector Configuration Guide to upgrade 500F hardware based Collectors to 6.1.1.

Detailed steps – Elasticsearch Storage

For Elasticsearch, 6.1.0 Workers cannot be upgraded to 6.1.1. You must delete the Workers from the Supervisor, upgrade the Supervisor, and then add back the Workers.

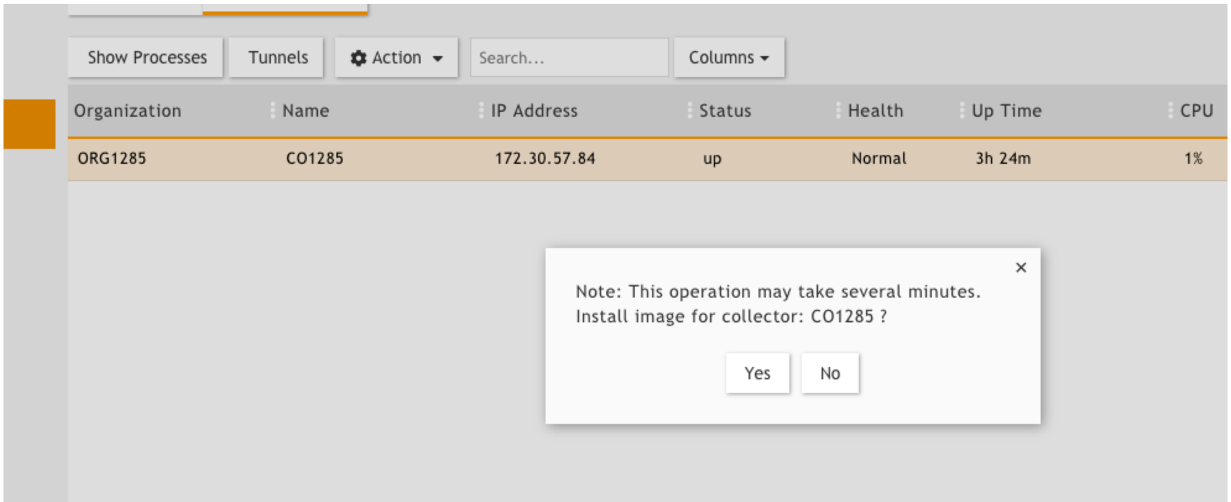
1. Delete the Workers as follows:
   a. Login to Supervisor.
   b. Go to **Admin > License > Nodes** and delete Workers one by one.
   c. Go to **Admin > Health > Cloud health** and make sure Workers do not appear.
   d. Go to **Admin > Event Worker** and delete the Workers.
   e. Shutdown the Workers.
2. Upgrade the Supervisor as in the Single node install. Then go to **Admin > Storage > Online > Elasticsearch** and click **Test and Save**. This important step pushes the latest event attribute definitions to Elasticsearch.
3. Install fresh Worker nodes based on your platform. See the appropriate Installation and Migration Guide for your platform here.
4. Add back the Workers to the Supervisor as follows:
   a. Login to Supervisor.
   b. Go to **Admin > License > Nodes** and add Workers one by one.
   c. Go to **Admin > Health > Cloud health** and make sure Workers appear.
   d. Go to **Admin > Event Worker** and add the Workers.
5. At this point, both Super and Worker must be running 6.1.0. Collectors must be sending events. Verify this from **Admin > Health > Cloud health**, **Admin > Health > Collector health**, and by running some reports.
6. Upgrade Collectors running 6.1.0 or later.
   a. Login to the Supervisor via SSH as `root`.
   b. Setup upgrade by running `phSetupCollectorUpgrade.sh /opt/upgrade/FSM_Upgrade_All_6.1.1_build0118.zip <superIP>`.The command will copy the upgrade files to the right location and prepare collector download:
   c. Login to the FortiSIEM GUI.
   d. Go to the **ADMIN > Health > Collector Health** page.
   e. Select a Collector, then choose **Actions > Download Image**, then wait for completion.



Organization	Name	IP Address	Status	Health	Up Time	CPU
ORG1285	CO1285	172.30.57.84	up	Normal	3h 24m	1%

Note: This operation may take several minutes.
Download for collector: CO1285 ?

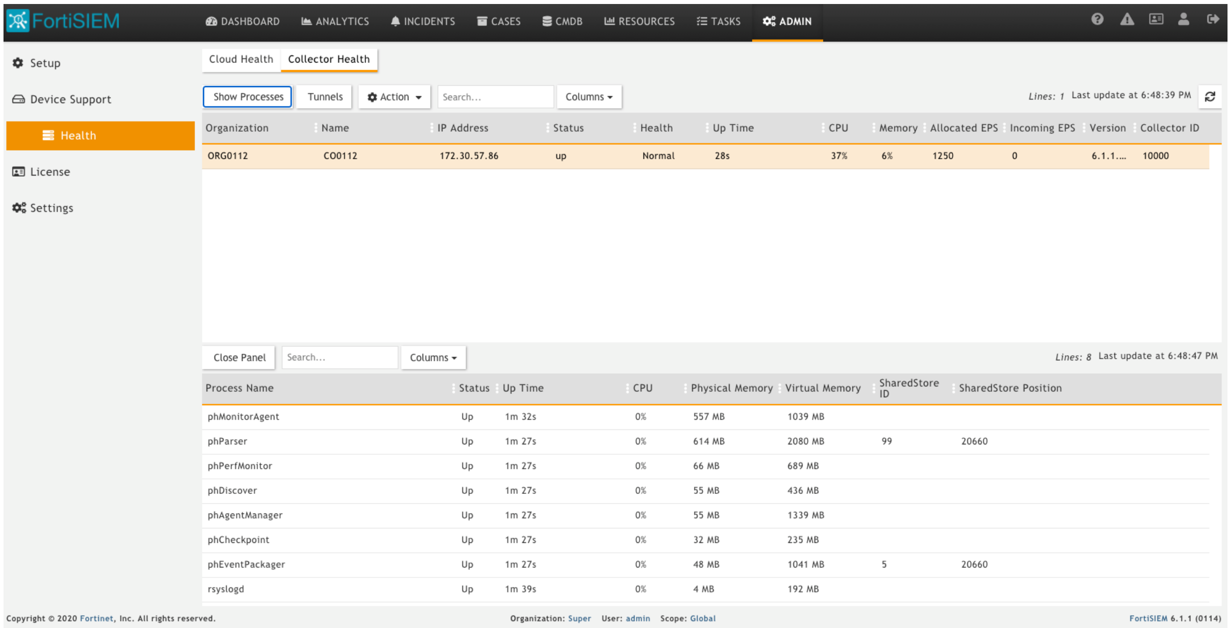
f. Select a Collector, then choose **Actions > Install Image**, then wait for completion.



Organization	Name	IP Address	Status	Health	Up Time	CPU
ORG1285	CO1285	172.30.57.84	up	Normal	3h 24m	1%

Note: This operation may take several minutes.
Install image for collector: CO1285 ?

g. Collector will upgrade, reboot and re-connect to the Supervisor. Check Collector Health to make sure it is running normally.



Lines: 1 Last update at 6:48:39 PM

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Collector ID
ORG0112	CO0112	172.30.57.86	up	Normal	28s	37%	6%	1250	0	6.1.1....	10000

Lines: 8 Last update at 6:48:47 PM

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	1m 32s	0%	557 MB	1039 MB		
phParser	Up	1m 27s	0%	614 MB	2080 MB	99	20660
phPerfMonitor	Up	1m 27s	0%	66 MB	689 MB		
phDiscover	Up	1m 27s	0%	55 MB	436 MB		
phAgentManager	Up	1m 27s	0%	55 MB	1339 MB		
phCheckpoint	Up	1m 27s	0%	32 MB	235 MB		
phEventPackager	Up	1m 27s	0%	48 MB	1041 MB	5	20660
rsyslogd	Up	1m 39s	0%	4 MB	192 MB		

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.1.1 (0114)

7. For pre-6.1.0 Collectors, FortiSIEM does not support Collector migration to 6.1.0 for VM based collectors. You will need to install new 6.1.1 Collectors and register them to 6.1.1 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. To do this follow these steps:
   a. Preparation steps:
      i. Copy the http hashed password file `/etc/httpd/accounts/passwds` from the old Collector.
      ii. Disconnect the pre-6.1.0 Collector.
      iii. Install the 6.1 Collector with the old IP address by the following the steps in **Cluster Installation > Install Collectors**.
      iv. Copy the saved http hashed password file `/etc/httpd/accounts/passwds` from the old Collector to the 6.1.0 Collector. This step is needed for Agents to work seamlessly with 6.1.0 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.0 migration, this password is lost.
   b. Register Collectors steps:
      i. Follow the steps in **Cluster Installation > Register Collectors**, with the following difference: in the `phProvisionCollector` command, use `--update option instead of --add`. Other than this, use the same parameters that were used to register the pre-6.1.0 Collector. Specifically, use the `phProvisionCollector` command to register a 6.1.0 Collector and keep the old associations: `# /opt/phoenix/bin/phProvisionCollector --update <user> <password> <Super IP or Host> <Organization> <CollectorName>`. Then, re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.
8. Follow the steps in the 500F Collector Configuration Guide to upgrade 500F hardware based Collectors to 6.1.1.

Upgrade via Proxy

During upgrade, Super/Worker and Hardware appliances FSM-2000F and 3500F 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. Edit `/etc/yum.conf` as follows:
   - If your proxy does not require authentication, then add a line like this:
     - `proxy=http://<proxy-ip-or-hostname>:<proxy-port>`
   - If your proxy requires authentication, then add `proxy_username=` and `proxy_password=` entries as well. For example, for squid proxy:
     - `proxy_username=<user>`
     - `proxy_password=<pwd>`
3. Test that you can use the proxy to successfully communicate with the two sites: `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs.fortisiem.fortinet.com`.
4. Begin the upgrade.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.