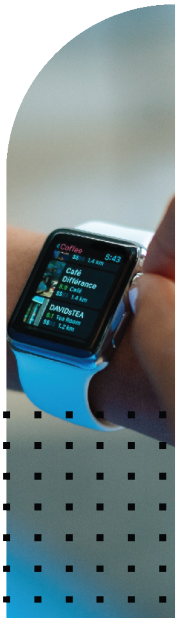
Disaster Recovery Procedures in EventDB Based Deployments

FortiSIEM 6.4.1



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

09/15/2022
FortiSIEM 6.4.1 Disaster Recovery Procedures in EventDB Based Deployments

TABLE OF CONTENTS

Change Log

Date	Change Description
04/25/2018	Initial version of FortiSIEM - Disaster Recovery Procedures
08/19/2019	Revision 1: Updated the location of the image download site.
11/25/2019	Revision 2: Updated the recovery procedures.
03/30/2020	Release of Disaster Recovery Procedures for 5.3.0.
08/15/2020	Revision 3: All new content for Disaster Recovery.
08/26/2021	Release of Disaster Recovery for 6.3.1 (revised/new feature).
10/05/2021	Updated "Step 3. Set up Disaster Recovery on Primary (Site 1)" instructions for 6.3.1 Guide.
10/15/2021	Release of Disaster Recovery for 6.3.2.
12/22/2021	Release of Disaster Recovery for 6.3.3.
01/18/2022	Release of Disaster Recovery for 6.4.0.
09/15/2022	Updated Prerequisites for a Successful DR Implementation section.

Disaster Recovery in EventDB Based Deployments

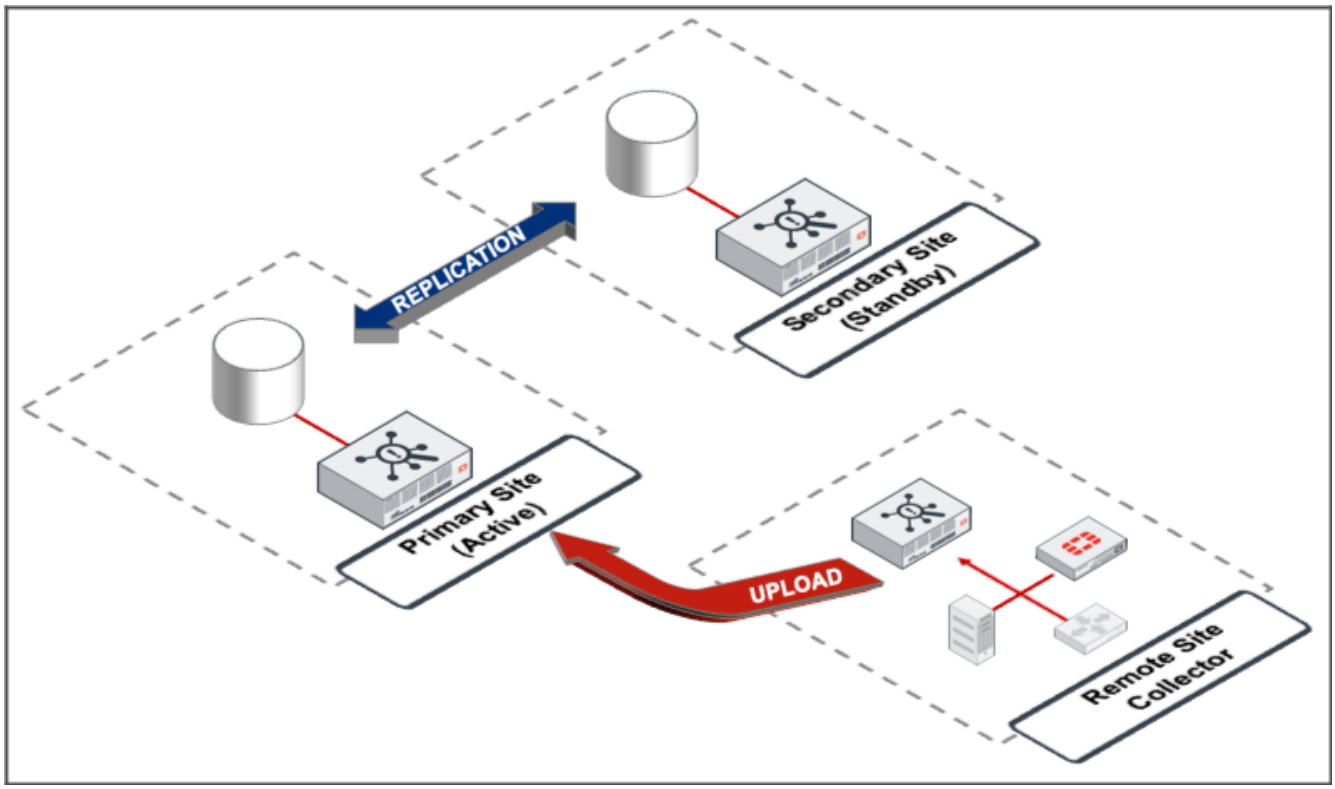
The following sections describe how to configure and work with FortiSIEM Disaster Recovery (DR) in EventDB based deployments.

Introduction

Understanding the FortiSIEM DR Feature

FortiSIEM has a replication feature, designed for those customers who require full disaster recovery capabilities, where one site is designated to be the Primary (active), Site 1, and the other the Secondary (hot standby) site, Site 2. The two systems replicate the Primary site (Site 1) database.

This requires a second fully licensed FortiSIEM system, where Site 1 (Primary) and Site 2 (Secondary) are identically setup in terms of Supervisor, Workers, and event storage.

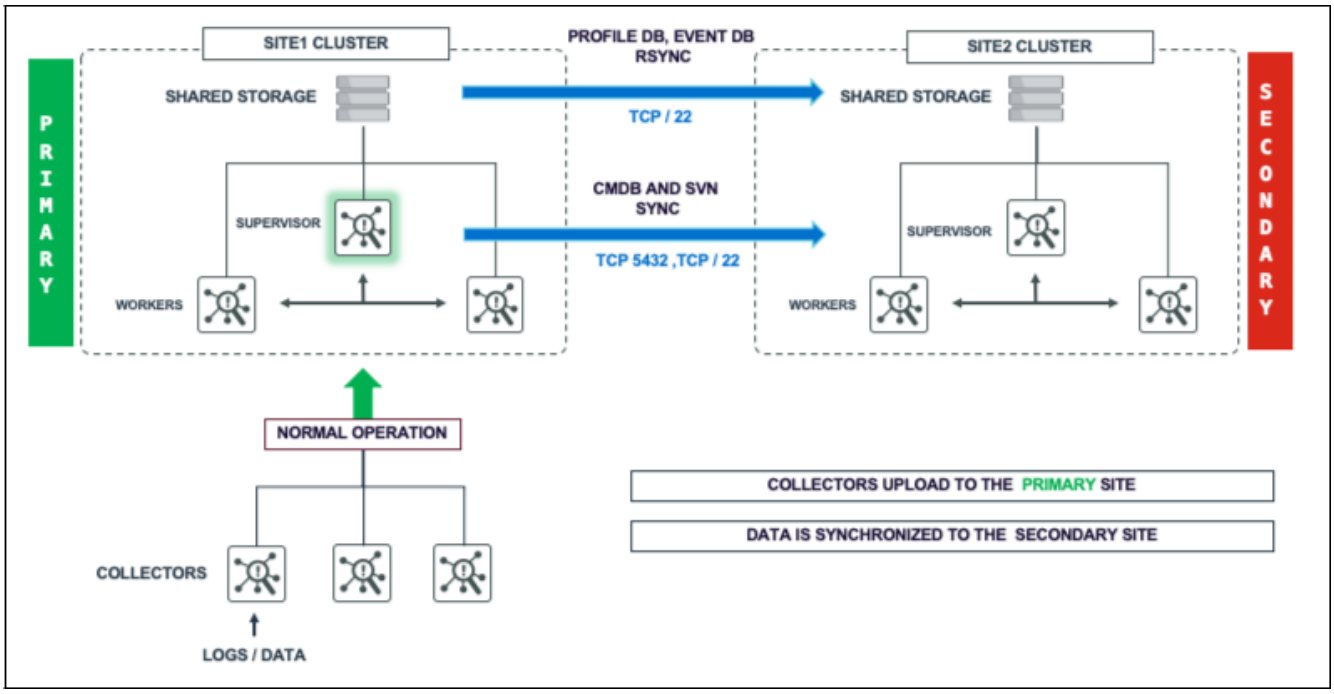


Under normal operations, if collectors are being used, these upload to Site 1, the Primary site, and will buffer by design when this site is not available. If DR is set up and a disaster occurs, then these same collectors will revert to uploading to Site 2, the Secondary site, which will now be designated as the Primary/Active site.

FortiSIEM runs as a cluster (or single node for a SMB) with Super, Worker, and Collectors nodes.

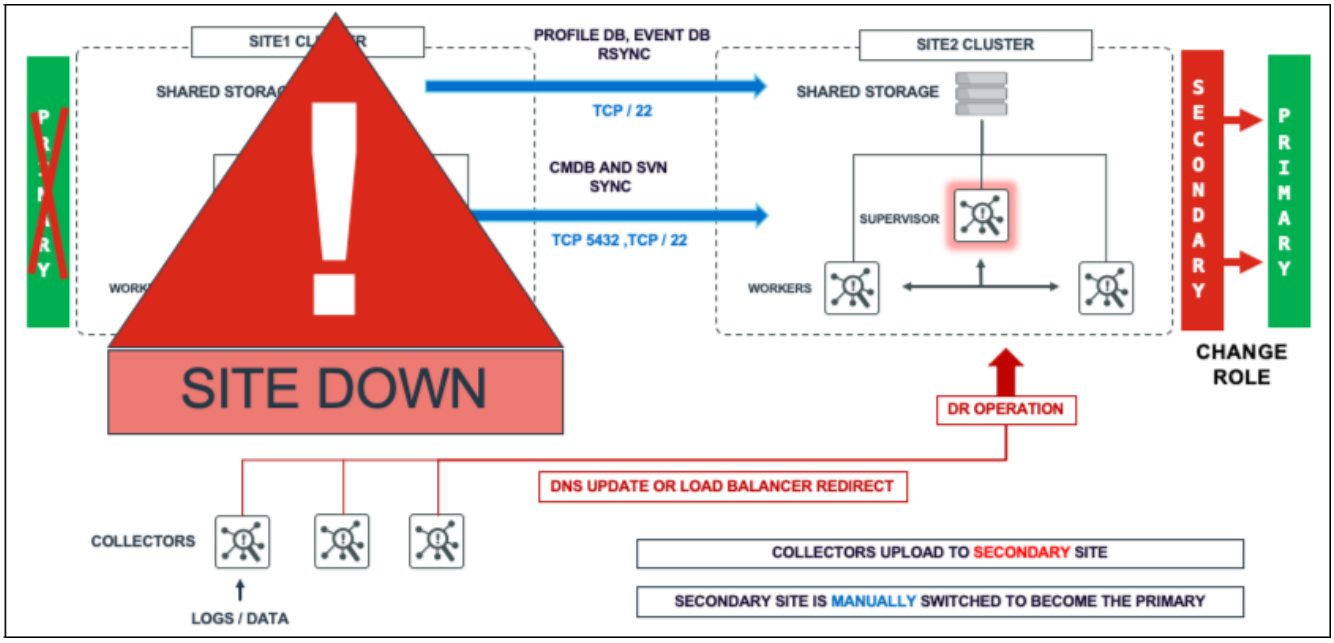
To provide DR features, FortiSIEM must have a Secondary system ready on standby to take over operations, with the following databases replicated from the Primary site:

- The CMDB residing in a PostgresSQL database.
- Device configurations residing in SVN-lite on the Supervisor node.
- Profile data residing on SQLite databases on the Supervisor node.
- Event database stored in FortiSIEM EventDB (on local disk or NFS). Disaster recovery for Elasticsearch is discussed in another document. (See Disaster Recovery for Elasticsearch here).



When disaster strikes:

1. The Secondary (Site 2) must become the Primary FortiSIEM.
2. DNS Changes must be made so that users will logon to Secondary Supervisor (Site 2), and that Collectors will send events to Secondary Workers.



When the Old Primary (Site 1) is recovered and powered up, it will sync missing data with the Secondary site (Site 2, the Active Primary FortiSIEM) once it is added back as a new Secondary site.

When the user decides to return to the pre-disaster setup, the user can switch the roles of Primary (Site 2) and Secondary (Site 1).

Prerequisites for a Successful DR Implementation

- Two separate FortiSIEM licenses - one for each site.
- The installation at both sites must be identical - workers, storage type, archive setup, hardware resources (CPU, Memory, Disk) of the FortiSIEM nodes.
- DNS Names are used for the Supervisor nodes at the two sites. Make sure that users, collectors, and agents can access both Supervisor nodes by their DNS names.
- DNS Names are used for the Worker upload addresses.
- TCP Ports for HTTPS (TCP/443), SSH (TCP/22), PostgresSQL (TCP/5432), and Private SSL Communication port between phMonitor (TCP/7900) are open between both sites.

Understanding the Requirements for DNS Names

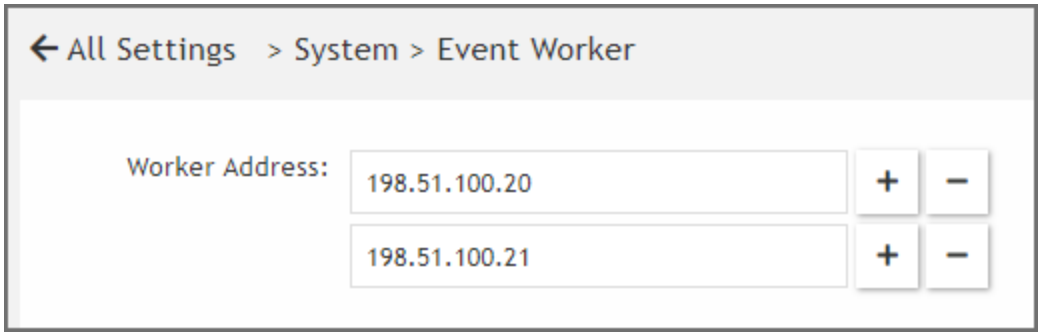
It is important to understand your FortiSIEM environment and plan ahead in terms of communications from users, agents and collectors.

Worker Event

- Performing Collector Registration
- Agent Communications

Each entry in the **Worker Event** address list is given to Collectors at registration (and periodically in communication to the Supervisor) to instruct where to upload customer event data.

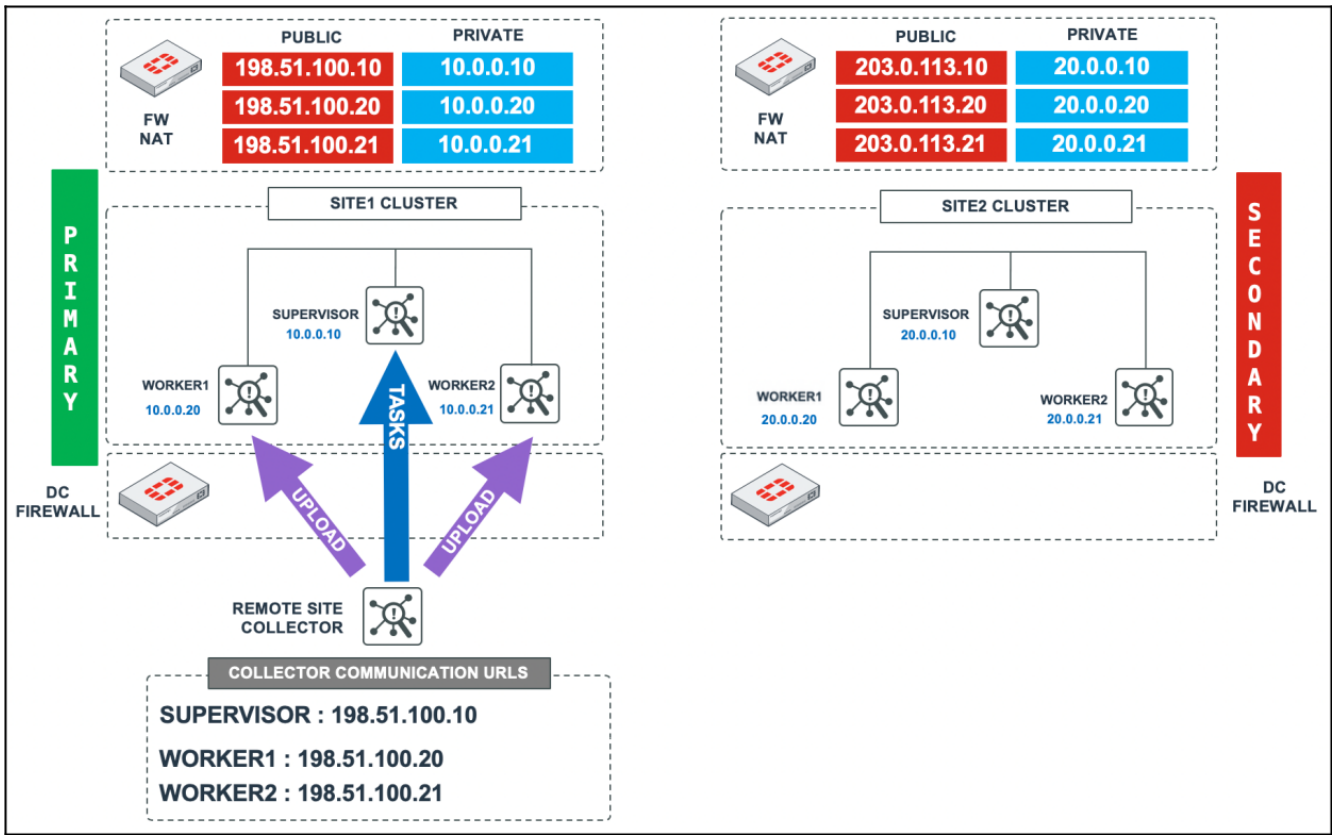
An example is shown below, where the customer has *not* followed best practice advice and used IP Addresses and not FQDNs.



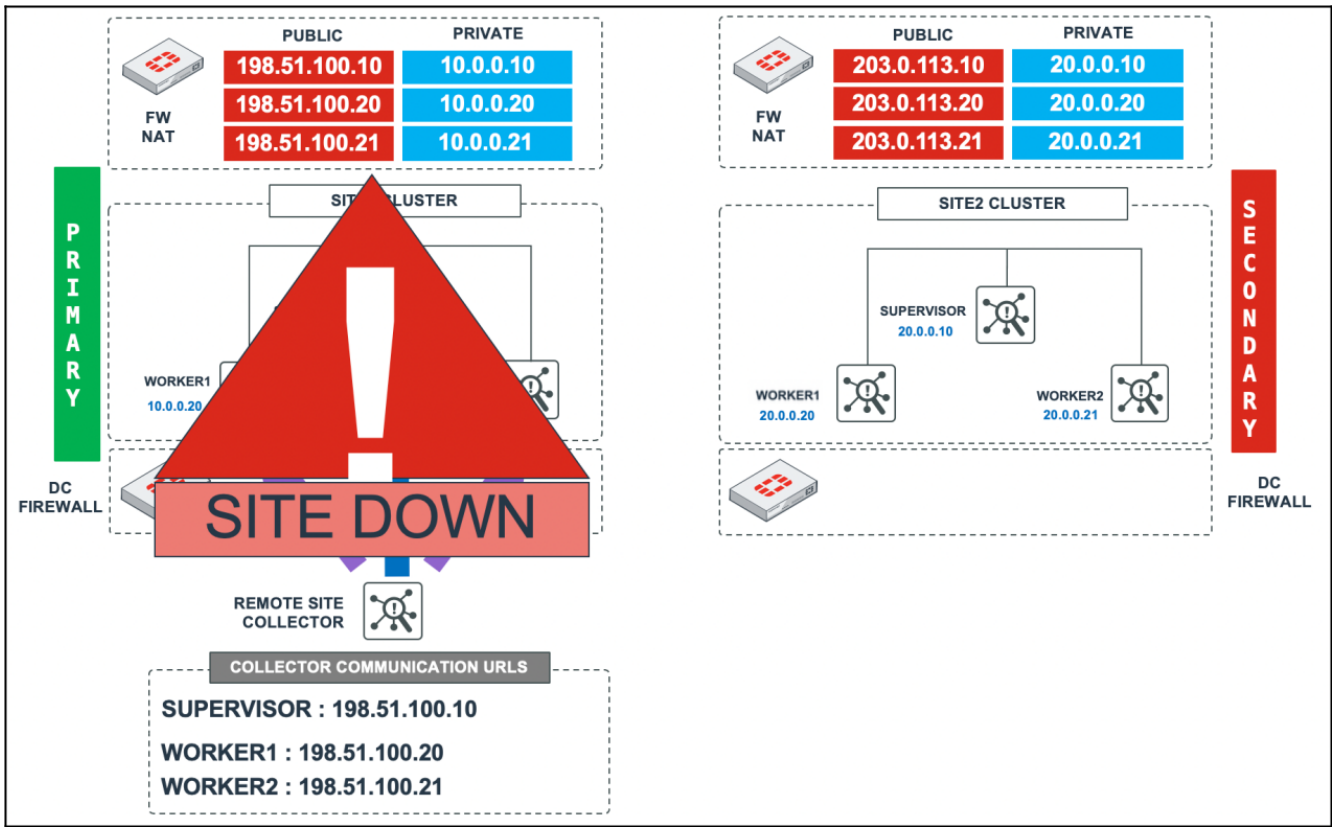
In addition to the Worker Event entries, Collectors also maintain communication with the Supervisor node, to receive jobs/tasks and report Collector health data. When Collectors register for the first time with the Supervisor node, these communication addresses are stored for this purpose.

Why is using IP addresses for Collector registration and Worker Event settings bad when it comes to DR planning?

Consider the environment below where only IP addresses have been used. During normal operations Collector traffic flows to the Workers at the Primary site (Site 1) and the Collector maintains communications with the Supervisor. This all works fine until the Primary site (Site 1) has a disaster.



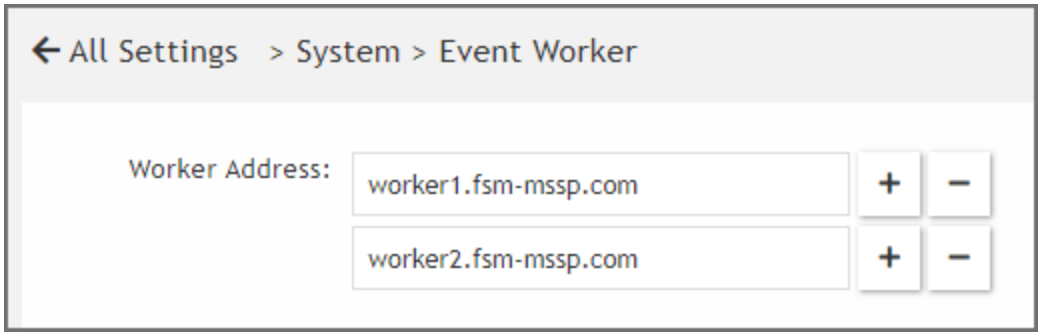
At this point, the Primary node (Site 1) is unavailable. The remote Collector nodes are essentially hard-coded (by IP) to talk to the Primary site only. Even if Site 2 (the Secondary node) is up and operational and promoted to be the Primary node, Collectors are unable to upload logs or get any tasks from the Supervisor node due to the old Primary sites IPs being used.



A much better approach is to utilize DNS.

This allows name resolution to control which Supervisor, Primary, or Secondary is currently active and which worker addresses to attempt to upload customer data to. DNS “A” records are created for the Supervisor nodes at both sites, and a “CNAME” is used to determine which is active, which has a small time to live (TTL) value.

The Worker Event settings reference DNS addresses:



External DNS Example

Node	DNS Record Type	Name	IP/Alias
Supervisor (Primary)	A	site1.fsm-mssp.com	198.51.100.10
Supervisor (Secondary)	A	site2.fsm-mssp.com	203.0.113.10

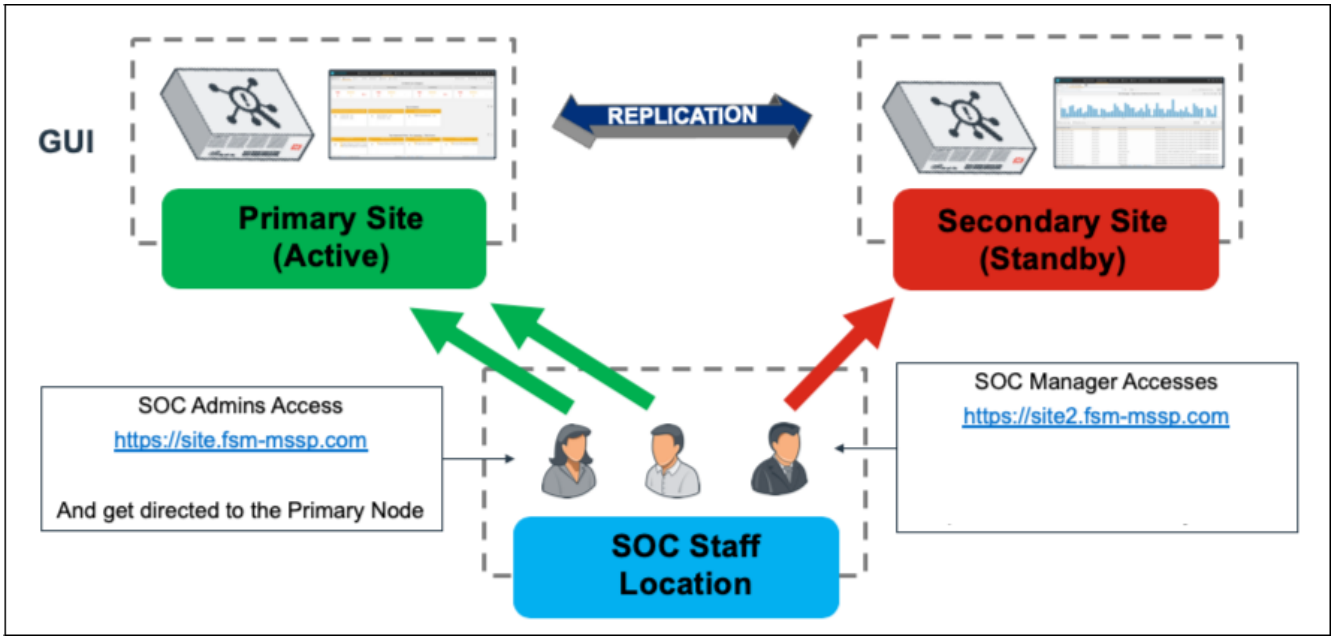
Node	DNS Record Type	Name	IP/Alias
Active Supervisor	CNAME	site.fsm-mssp.com	site1.fsm-mssp.com
Worker1 (Primary)	A	worker1.fsm-mssp.com	198.51.100.20
Worker2 (Primary)	A	worker2.fsm-mssp.com	198.51.100.21

For the internal DNS records, again both internal Supervisor addresses are listed with a CNAME to determine the current Primary GUI to logon to for SOC operators. (If public certificates are being used, then a Wildcard cert should be used to achieve this).

Internal DNS Example

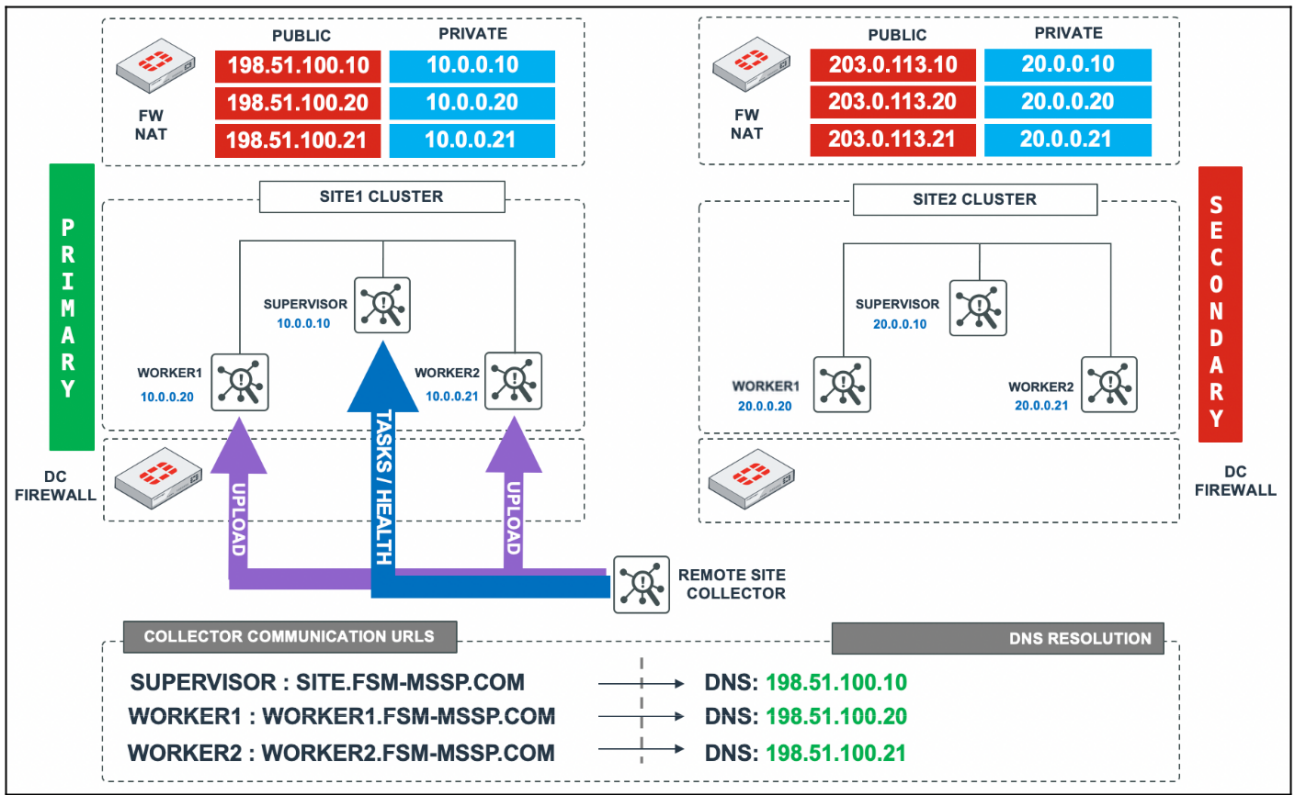
Node	DNS Record Type	Name	IP/Alias
Supervisor (Primary)	A	site1.fsm-mssp.com	10.0.0.10
Supervisor (Secondary)	A	site2.fsm-mssp.com	20.0.0.10
Active Supervisor	CNAME	site.fsm-mssp.com	site1.fsm-mssp.com

By utilizing internal DNS, then SOC operators can always access the active Supervisor GUI via `site.fsm-mssp.com`, but as will be discussed later, the Secondary Standby Supervisor can always be accessed if required.

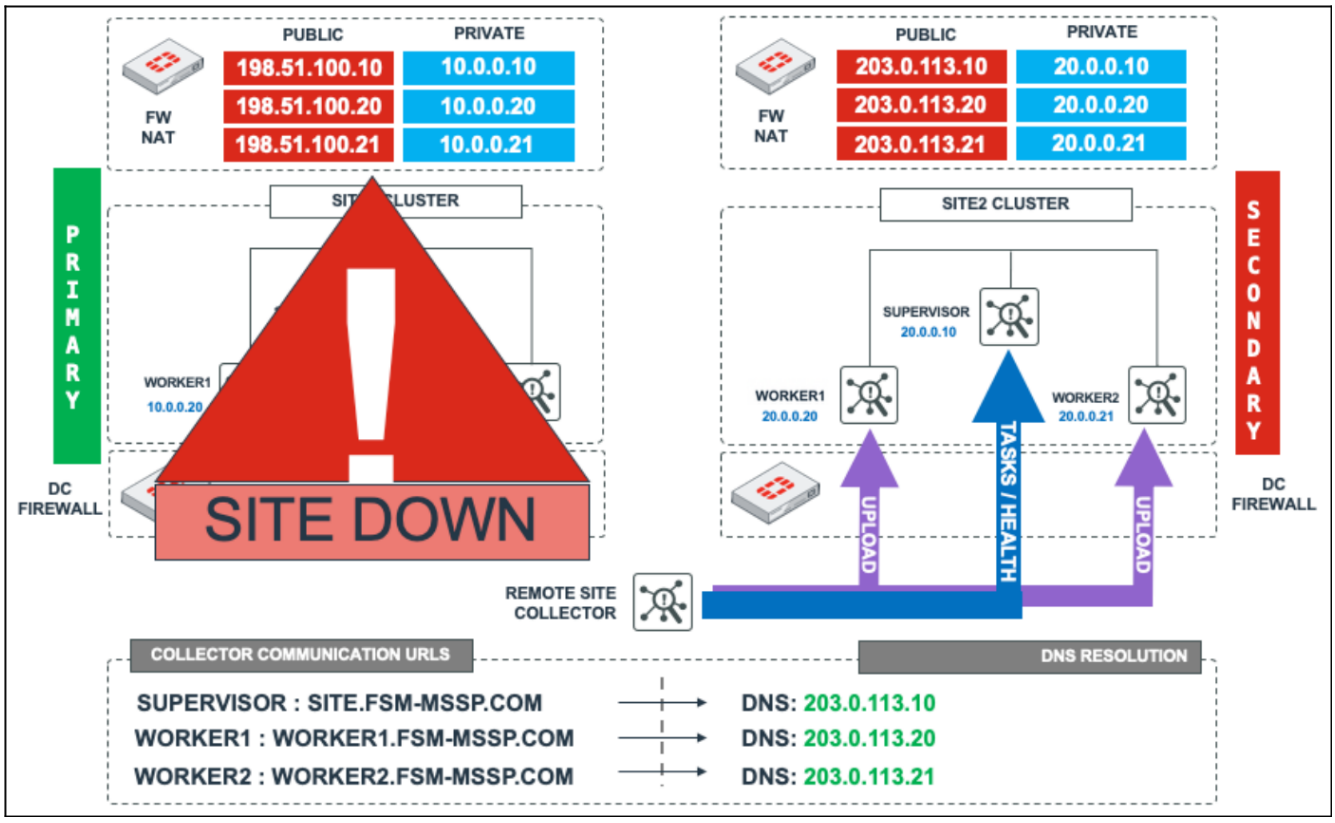


Note: Any DNS changes, are made **manually** in the event of a failover.

As can be seen below, using DNS the Collectors are instructed to talk to the Active site.



And in the event of a failure at the Primary Site, they can be easily instructed to communicate with the Supervisor and Workers at the Secondary site which will be manually switched to be the Primary Role site.



Note : In addition to DNS changes being made manually, the process for promoting the Secondary Supervisor to be the Primary Role Supervisor node is also made manually in the FortiSIEM Command Line.

Performing Collector Registration

When registering Collectors, you should ignore the Supervisor-IP requirement, and instead use the CNAME for the Active Supervisor node.

```
[root@collector ~]# phProvisionCollector

Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password>
     <Supervisor-IP> <Organization-name> <Collector-name>
```

An example using `site.fsm-mssp.com` is shown below. Since Collectors always communicate with the Supervisor node, communications can be easily restored to the Primary via a simple DNS change.

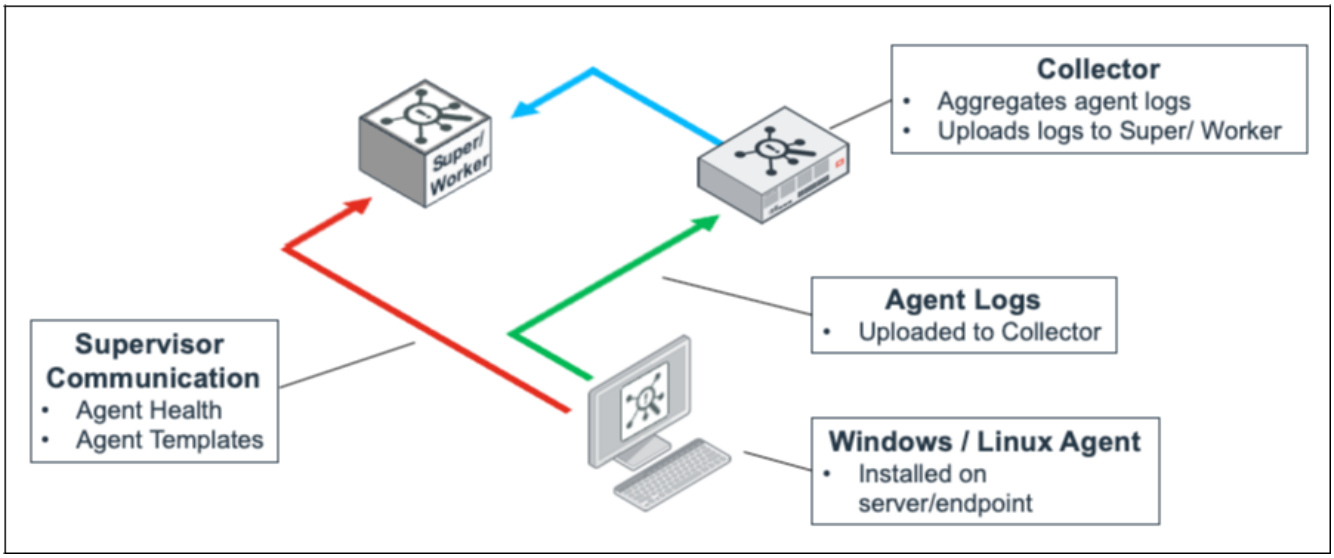
```
[root@collector ~]# phProvisionCollector --add admin admin*1 site.fsm-mssp.com super
     collector.fsm-mssp.com

Continuing to provision the Collector
Adding Collector (collector.fsm-mssp.com) to Super (site.fsm-mssp.com) with Organization
     (super)
This collector is registered successfully, and will be rebooted soon.
```

Agent Communications

The communications for FortiSIEM Windows and Linux agents follow a similar path to the above. Agents register with the Supervisor node, and maintain this communication to receive updated templates and report health. One or more

Collectors are assigned to each agent as the node or nodes to deliver event data.



For best practice, agent registration should use the Supervisor CNAME. This way, if the Primary Site is a totally destroyed, you can still easily ensure agent communication to the DR site Supervisor via a simple DNS change and still make template changes etc.

The Windows installation file `installSettings.xml` is shown:

```
<?xml version="1.0" encoding="utf-8"?>
<InstallConfig Version="1">
  <Org>
    <ID>1</ID>
    <Name>Super</Name>
  </Org>
  <Super>
    <Name>site.fsm-mssp.com</Name>
    <Port>443</Port>
  </Super>
  <Registration>
    <Username>super/agent_admin</Username>
    <Password>admin*2</Password>
  </Registration>
  <Proxy/>
  <SSLCertificate>ignore</SSLCertificate>
</InstallConfig>
```

The same concept also applies to deploying Linux agents.

Configuring Disaster Recovery

Ensure you have followed the Prerequisites for a Successful DR Implementation prior to this configuration.

Assume there are two sites, Site 1 needs to be set up as Primary, and Site 2 as Secondary.

Step 1. Collect UUID and SSH Public Key from Primary (Site 1)

1. For the UUID, obtain the Hardware ID value through an SSH session by running the following command on Site 1.

   ```
   /opt/phoenix/bin/phLicenseTool --show
   ```

   For example:

   ```
   [root@site1 ~]# /opt/phoenix/bin/phLicenseTool --show
   License Information:
   Attribute                       Value                                   Expiration Date
   Serial Number                   FSMS0100[redacted]
   Hardware ID                     564[redacted]C-0247-87C2-[redacted]3B56EFFF
   License Type                    Enterprise
   Devices                         1500                                    Mar 17, 2021
   Endpoint Devices                N/A                                     N/A
   Additional EPS                  N/A                                     N/A
   ```

2. Enter/paste the Hardware ID into the **UUID** field for the Site 1 FortiSIEM.
3. Under **Configuration and Profile Replication**, generate the **SSH Public Key** and **SSH Private Key Path** by entering the following in your SSH session from Site 1:

   ```
   su - admin
   ssh-keygen -t rsa -b 4096
   ```

   Leave the file location as default, and press enter at the passphrase prompt.

   The output will appear similar to the following:

   ```
   Generating public/private rsa key pair.
   Enter file in which to save the key (/opt/phoenix/bin/.ssh/id_rsa):
   Created directory '/opt/phoenix/bin/.ssh'.
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /opt/phoenix/bin/.ssh/id_rsa.
   Your public key has been saved in /opt/phoenix/bin/.ssh/id_rsa.pub.
   The key fingerprint is:
   a9:43:88:d1:ed:b0:99:b5:bb:e7:6d:55:44:dd:3e:48 admin@site1.fsmtesting.com
   The key's randomart image is:
   +--[ RSA 4096]----+
   |  ....|
   |  . . E. o|
   ```

4. For the **SSH Public Key** enter the following command, and copy **all** of the output.

   ```
   cat /opt/phoenix/bin/.ssh/id_rsa.pub
   ```

Step 2. Collect UUID and SSH Public Key from Secondary (Site 2)

1. On the Site 2 FortiSIEM node, SSH as root.
2. Run the following command to get the **Hardware ID**, also known as the **UUID**. Record this Site 2 Hardware ID, as you will need it later.

   ```
   /opt/phoenix/bin/phLicenseTool --show
   ```

```
[root@site1 ~]# /opt/phoenix/bin/phLicenseTool --show
License Information:
Attribute                          Value                                  Expiration Date
Serial Number                      FSMS0100[redacted]
Hardware ID                        564[redacted]C-0247-87C2-[redacted]3B56EFFF
License Type                       Enterprise
Devices                            1500                                   Mar 17, 2021
Endpoint Devices                   N/A                                    N/A
Additional EPS                     N/A                                    N/A
```

3. Generate a public key for **Site 2** by running the following commands.

   ```
   su - admin
   ssh-keygen -t rsa -b 4096
   ```

   Leave the file location as default, and press enter at the passphrase prompt. Your output will appear similar to the following.

   ```
   Generating public/private rsa key pair.
   Enter file in which to save the key (/opt/phoenix/bin/.ssh/id_rsa):
   Created directory '/opt/phoenix/bin/.ssh'.
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /opt/phoenix/bin/.ssh/id_rsa.
   Your public key has been saved in /opt/phoenix/bin/.ssh/id_rsa.pub.
   The key fingerprint is:
   a9:43:88:d1:ed:b0:99:b5:bb:e7:6d:55:44:dd:3e:48 admin@site2.fsmtesting.com
   The key's randomart image is:
   +--[ RSA 4096]----+
   | ....|
   | . . E. o|
   ```

4. Enter the following command, and copy **all** of the output.

   ```
   cat /opt/phoenix/bin/.ssh/id_rsa.pub
   ```

   You will use the output as your **SSH Public Key** for Site 2 in later set up.

5. Exit the admin user in the SSH session by entering the following command:

   ```
   exit
   ```

Step 3. Set up Disaster Recovery on Primary (Site 1)

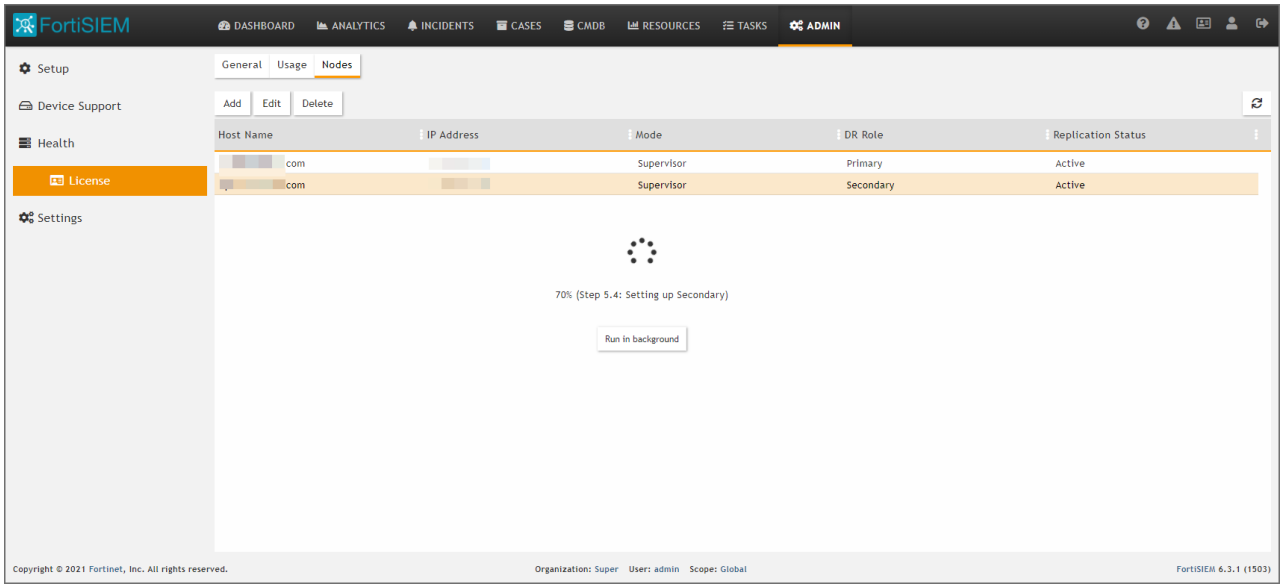
1. Navigate to **ADMIN > License > Nodes**.
2. Click **Add**.
3. On the **Add Node** window, in the **Type** drop-down list, select **Secondary (DR)**.
   The primary (Site 1) node configuration fields appear in the left column, and the secondary (Site 2) node configuration fields appear in the right column.
4. Under the Host Info Role **Primary** column, take the following steps:
   a. In the **Host** field, enter the host name of the Site 1 FortiSIEM.
   b. In the **IP** field, enter the IP of the Site 1 FortiSIEM.
   c. In the **SSH Public Key** field, enter/paste the SSH Public Key of the Site 1 FortiSIEM that you obtained earlier.
   d. For the **SSH Private Key Path**, enter the following into the field:
      `/opt/phoenix/bin/.ssh/id_rsa`
   e. For **Replication Frequency**, select a value for the Site 1 FortiSIEM.
   f. Select the **EventDB Replication** check box if you would also like the Event Database to be replicated. This is **NOT** required for Elasticsearch.

Note 1: For Local/NFS Event DB installs, this value is used for SVN and ProfileDB synchronization.

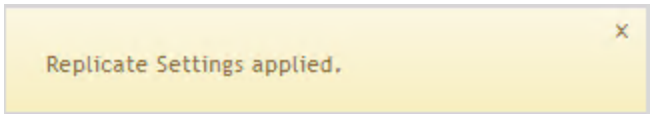
Note 2: For Local/NFS Event DB installs, `rsync` is used, and this runs continually in the background.

5. Under the Host Info Role **Secondary** column, take the following steps:
   a. In the **Host** field, enter the host name of the Site 2 FortiSIEM.
   b. In the **IP** field, enter the IP address of the Site 2 FortiSIEM.
   c. In the **UUID** field, enter/paste the Hardware ID of the Site 2 FortiSIEM that you obtained earlier.
   d. In the **SSH Public Key** field, enter/paste the SSH Public Key of the Site 2 FortiSIEM that you obtained earlier.
   e. For the **SSH Private Key Path**, enter the following into the field:
   `/opt/phoenix/bin/.ssh/id_rsa`
   f. Select the **EventDB Replication** check box if you would also like the Event Database to be replicated. If you are running Elasticsearch, then see the Disaster Recovery for Elasticsearch Guide here.
   g. Click **Export** and download a file named `replicate.json`.
   Note: This file contains all of the Disaster Recovery settings, and can be used as a backup.
6. Click **Save**.

   At this point, the Site 1 (Primary) node will begin configuration and the step and progress of the Disaster Recovery is displayed in the GUI.



When completed, the message "Replicate Settings applied." will appear.

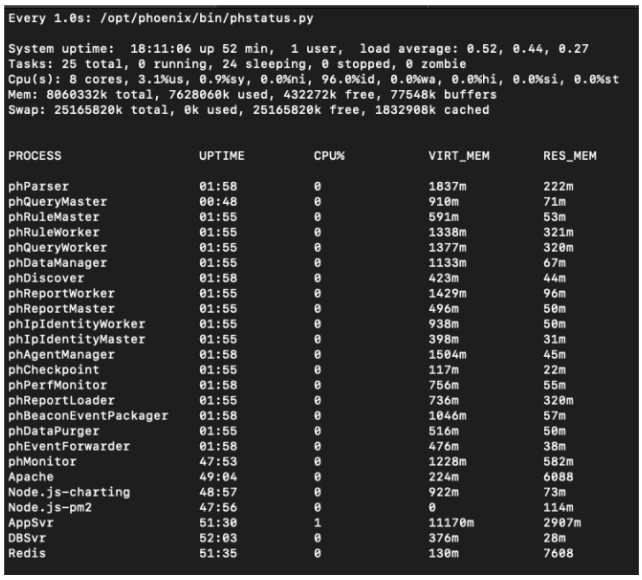


Service Status on Primary and Secondary

On the Primary node, all FortiSIEM `ph*` services will be in an "up" state.

On the Secondary node, most `ph*` services will be "down" except for `phQueryMaster`, `phQueryWorker`, `phDataPurger`, and `phMonitor`.

This can be seen in the following images. They illustrate the Primary Node and Secondary Node after a full CMDB sync:

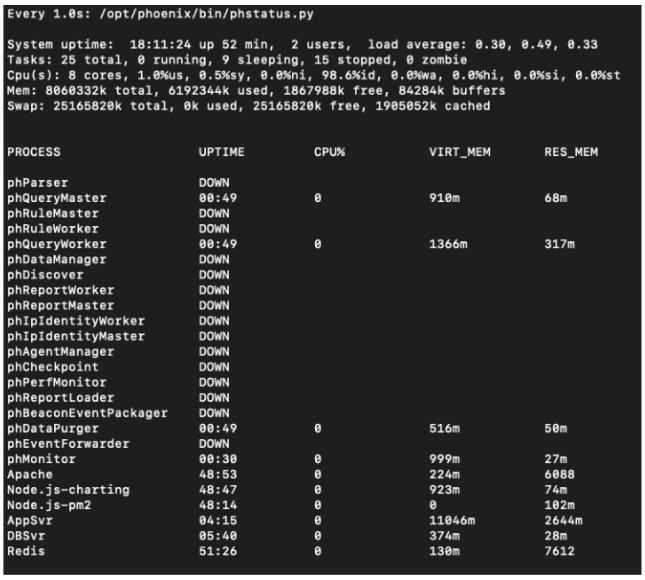


```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime:  18:11:06 up 52 min,  1 user,  load average: 0.52, 0.44, 0.27
Tasks: 25 total, 0 running, 24 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 3.1%us, 0.9%sy, 0.0%ni, 96.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 8060332k total, 7628060k used, 432272k free, 77548k buffers
Swap: 25165820k total, 0k used, 25165820k free, 1832908k cached


PROCESS                 UPTIME          CPU%            VIRT_MEM        RES_MEM

phParser                01:58           0               1837m           222m
phQueryMaster           00:48           0               910m            71m
phRuleMaster            01:55           0               591m            53m
phRuleWorker            01:55           0               1338m           321m
phQueryWorker           01:55           0               1377m           320m
phDataManager           01:55           0               1133m           67m
phDiscover              01:58           0               423m            44m
phReportWorker          01:55           0               1429m           96m
phReportMaster          01:55           0               496m            50m
phIpIdentityWorker      01:55           0               938m            50m
phIpIdentityMaster      01:55           0               398m            31m
phAgentManager          01:58           0               1504m           45m
phCheckpoint            01:55           0               117m            22m
phPerfMonitor           01:58           0               756m            55m
phReportLoader          01:55           0               736m            320m
phBeaconEventPackager   01:58           0               1046m           57m
phDataPurger            01:55           0               516m            50m
phEventForwarder        01:58           0               476m            38m
phMonitor               47:53           0               1228m           582m
Apache                  49:04           0               224m            6088
Node.js-charting        48:57           0               922m            73m
Node.js-pm2             47:56           0               0               114m
AppSvr                  51:30           1               11170m          2907m
DBSvr                   52:03           0               376m            28m
Redis                   51:35           0               130m            7608
```



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

System uptime:  18:11:24 up 52 min,  2 users,  load average: 0.30, 0.49, 0.33
Tasks: 25 total, 0 running, 9 sleeping, 15 stopped, 0 zombie
Cpu(s): 8 cores, 1.0%us, 0.5%sy, 0.0%ni, 98.6%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 8060332k total, 6192344k used, 1867988k free, 84284k buffers
Swap: 25165820k total, 0k used, 25165820k free, 1905052k cached


PROCESS                 UPTIME          CPU%            VIRT_MEM        RES_MEM

phParser                DOWN
phQueryMaster           00:49           0               910m            68m
phRuleMaster            DOWN
phRuleWorker            DOWN
phQueryWorker           00:49           0               1366m           317m
phDataManager           DOWN
phDiscover              DOWN
phReportWorker          DOWN
phReportMaster          DOWN
phIpIdentityWorker      DOWN
phIpIdentityMaster      DOWN
phAgentManager          DOWN
phCheckpoint            DOWN
phPerfMonitor           DOWN
phReportLoader          DOWN
phBeaconEventPackager   DOWN
phDataPurger            00:49           0               516m            50m
phEventForwarder        DOWN
phMonitor               00:30           0               999m            27m
Apache                  48:53           0               224m            6088
Node.js-charting        48:47           0               923m            74m
Node.js-pm2             48:14           0               0               102m
AppSvr                  04:15           0               11046m          2644m
DBSvr                   05:40           0               374m            28m
Redis                   51:26           0               130m            7612
```

On the Secondary node, all backend processes should be down on the Supervisor and Workers except for phQueryMaster, phQueryWorker, DataPurger, DBServer, and AppServer.

Viewing Replication Health

Replication progress is available by navigating to **ADMIN > Health > Replication Health**. For details see here.

Permitted User Activities on Secondary

When operating in DR Replication mode, there are a few things to bear in mind:

- Both the Primary (Site 1) and Secondary (Site 2) nodes GUI are available for login.
- The Secondary (Site 2) is only available for read-only operations. From Secondary (Site 2), expect the following:
  - Able to view CMDB, Incidents, Cases, Tasks, Resources and all settings in the ADMIN page except the License Usage Page, etc
  - Cannot run any queries on **ANALYTICS** and all widgets on Dashboards and all report related graphs such as the License Usage Page have no data.
  - Cannot do any Editing operations on all GUI pages.
  - All actions related to update operations do not work.

Troubleshooting Disaster Recovery

- GUI
- Backend Logs
- Failure to Connect to Secondary

GUI

While Replication is being set up, you can see the progress in the GUI in two locations.

1. **ADMIN > License > Nodes > Add DR**
   or
2. **Jobs/Errors > Jobs > filter on 6.3.1-DR**

Backend Logs

On both the Primary and Secondary nodes, use the `cat` command to view the backend logs (`/opt/phoenix/log/phoenix.log`):

```
cat /opt/phoenix/config/phoenix.log
```

Successful Enablement of Disaster Recovery of the Primary node

2021-08-20T16:26:22.186396-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7398, [phLogDetail]=631-DR, Step 1: check command type

2021-08-20T16:26:22.186451-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7407, [phLogDetail]=631-DR, Step 2: check command data

2021-08-20T16:26:22.186475-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7414, [phLogDetail]=631-DR, Step 3: load replication setting

2021-08-20T16:26:22.222539-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7444, [phLogDetail]=631-DR-init-primary, Step 1: Saving Disaster Recovery Settings on Primary

2021-08-20T16:26:22.252896-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7457, [phLogDetail]=631-DR-init-primary, Step 2: Saving peer SSH public key on Primary

2021-08-20T16:26:22.291143-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7471, [phLogDetail]=631-DR-init-primary, Step 3: Updating SSH Configuration on Primary

2021-08-20T16:26:22.328987-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7486, [phLogDetail]=631-DR-init-primary, Step 4: Updating SSH Known Hosts on Primary

2021-08-20T16:26:22.503675-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7508, [phLogDetail]=631-DR-init-primary, Step 5: Initializing Disaster Recovery

2021-08-20T16:26:22.577513-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7567, [phLogDetail]=631-DR-init-primary, Step 5.1: Running phinitprimary script on Primary

2021-08-20T16:26:23.521939-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7582, [phLogDetail]=631-DR-init-primary, Step 5.2: Sending Task to Secondary

2021-08-20T16:26:23.579504-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7619, [phLogDetail]=631-DR-init-primary, Step 5.3: Initializing Secondary

2021-08-20T16:26:23.620795-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 1

2021-08-20T16:26:23.644367-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 20

2021-08-20T16:26:23.671393-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 30

2021-08-20T16:26:23.709927-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 40

2021-08-20T16:26:23.740996-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 50

2021-08-20T16:29:01.385371-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 80

2021-08-20T16:29:01.454035-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7634, [phLogDetail]=631-DR-init-primary, Step 5.5: Secondary Setup complete

2021-08-20T16:29:01.454250-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7515, [phLogDetail]=631-DR-init-primary, Step 6: Waiting for App Server to come back up on Primary

2021-08-20T16:29:01.509276-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7523, [phLogDetail]=631-DR-init-primary, Step 7: Waiting for Secondary App Server to update Service Passwords

2021-08-20T16:29:01.797224-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8187, [phLogDetail]=631-DR-init-primary, Step 7.1: get sevice user

2021-08-20T16:29:01.797257-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8195, [phLogDetail]=631-DR-init-primary, Step 7.2: get secondary host

2021-08-20T16:29:01.797440-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8214, [phLogDetail]=631-DR-init-primary, Step 7.3: send task updating Svc password to secondary

2021-08-20T16:29:01.882229-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8224, [phLogDetail]=631-DR-init-primary, Step 7.4: finish updating Svc password on secondary

2021-08-20T16:29:01.884157-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7541, [phLogDetail]=631-DR-init-primary, Step 8: Restarting processes on Primary

2021-08-20T16:29:01.923315-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7549, [phLogDetail]=631-DR-init-primary, Step 9: Broadcasting DR tasks to all processes on Primary

2021-08-20T16:29:01.962740-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7559, [phLogDetail]=631-DR-init-primary, Step 10: Disaster Recovery setup complete

2021-08-20T16:29:02.169745-07:00 va3005 phMonitorSupervisor[11908]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7432, [phLogDetail]=631-DR, Step 4: initializing DR finished.

2021-08-20T17:03:54.103262-07:00 va3005 phMonitorSupervisor[7384]: [PH_GENERIC_INFO]:[eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7712,[phLogDetail]=631-DR-init-secondary, Step 1: Initalize secondary From Primary server

2021-08-20T17:03:54.103449-07:00 va3005 phMonitorSupervisor[7384]: [PH_GENERIC_INFO]:[eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7733,[phLogDetail]=631-DR-init-secondary, Step 2: parse task info

2021-08-20T17:03:54.103689-07:00 va3005 phMonitorSupervisor[7384]: [PH_GENERIC_INFO]:[eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7757,[phLogDetail]=631-DR-init-secondary, Step 3: update SSH keys of primary on secondary

2021-08-20T17:03:54.115290-07:00 va3005 phMonitorSupervisor[7384]: [PH_GENERIC_INFO]:[eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7775,[phLogDetail]=631-DR-init-secondary, Step 4: update SSH configurations on secondary

2021-08-20T17:03:54.126466-07:00 va3005 phMonitorSupervisor[7384]: [PH_GENERIC_INFO]:[eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7793,[phLogDetail]=631-DR-init-secondary, Step 5: update SSH known hosts for primary on secondary

2021-08-20T17:03:54.148876-07:00 va3005 phMonitorSupervisor[7384]: [PH_GENERIC_INFO]:[eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7817,[phLogDetail]=631-DR-init-secondary, Step 6: run phinitsecondary script

2021-08-20T17:06:29.865977-07:00 va3005 phMonitorSupervisor[7384]: [PH_GENERIC_INFO]:[eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7881,[phLogDetail]=631-DR-init-secondary, Step 10: finish initialize secondary

Successful Enablement of Disaster Recovery of the Secondary node

2021-08-20T16:29:29.146469-07:00 andy-super-ipv6 phMonitorSupervisor[11936]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7712, [phLogDetail]=631-DR-init-secondary, Step 1: Initalize secondary From Primary server

2021-08-20T16:29:29.146829-07:00 andy-super-ipv6 phMonitorSupervisor[11936]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7733, [phLogDetail]=631-DR-init-secondary, Step 2: parse task info

2021-08-20T16:29:29.147537-07:00 andy-super-ipv6 phMonitorSupervisor[11936]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7757, [phLogDetail]=631-DR-init-secondary, Step 3: update SSH keys of primary on secondary

2021-08-20T16:29:29.160266-07:00 andy-super-ipv6 phMonitorSupervisor[11936]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7775, [phLogDetail]=631-DR-init-secondary, Step 4: update SSH configurations on secondary

2021-08-20T16:29:29.172964-07:00 andy-super-ipv6 phMonitorSupervisor[11936]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7793, [phLogDetail]=631-DR-init-secondary, Step 5: update SSH known hosts for primary on secondary

2021-08-20T16:29:29.287039-07:00 andy-super-ipv6 phMonitorSupervisor[11936]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7817, [phLogDetail]=631-DR-init-secondary, Step 6: run phinitsecondary script

2021-08-20T16:32:06.952364-07:00 andy-super-ipv6 phMonitorSupervisor[11936]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7881, [phLogDetail]=631-DR-init-secondary, Step 10: finish initialize secondary

2021-08-20T17:06:58.153075-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7398, [phLogDetail]=631-DR, Step 1: check command type

2021-08-20T17:06:58.153099-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7407, [phLogDetail]=631-DR, Step 2: check command data

2021-08-20T17:06:58.153113-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7414, [phLogDetail]=631-DR, Step 3: load replication setting

2021-08-20T17:06:58.188916-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7444, [phLogDetail]=631-DR-init-primary, Step 1: Saving Disaster Recovery Settings on Primary

2021-08-20T17:06:58.217059-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7457, [phLogDetail]=631-DR-init-primary, Step 2: Saving peer SSH public key on Primary

2021-08-20T17:06:58.260626-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7471, [phLogDetail]=631-DR-init-primary, Step 3: Updating SSH Configuration on Primary

2021-08-20T17:06:58.306178-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7486, [phLogDetail]=631-DR-init-primary, Step 4: Updating SSH Known Hosts on Primary

2021-08-20T17:06:58.353953-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7508, [phLogDetail]=631-DR-init-primary, Step 5: Initializing Disaster Recovery

2021-08-20T17:06:58.422293-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7567, [phLogDetail]=631-DR-init-primary, Step 5.1: Running phinitprimary script on Primary

2021-08-20T17:06:59.039355-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7582, [phLogDetail]=631-DR-init-primary, Step 5.2: Sending Task to Secondary

2021-08-20T17:06:59.144875-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7619, [phLogDetail]=631-DR-init-primary, Step 5.3: Initializing Secondary

2021-08-20T17:06:59.188592-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 1

2021-08-20T17:06:59.220850-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 20

2021-08-20T17:06:59.250523-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 30

2021-08-20T17:06:59.284640-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 40

2021-08-20T17:06:59.310058-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 50

2021-08-20T17:09:34.909429-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7629, [phLogDetail]=631-DR-init-primary, Step 5.4: Setting up Secondary: 80

2021-08-20T17:09:34.987417-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7634, [phLogDetail]=631-DR-init-primary, Step 5.5: Secondary Setup complete

2021-08-20T17:09:34.987610-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7515, [phLogDetail]=631-DR-init-primary, Step 6: Waiting for App Server to come back up on Primary

2021-08-20T17:09:35.042360-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7523, [phLogDetail]=631-DR-init-primary, Step 7: Waiting for Secondary App Server to update Service Passwords

2021-08-20T17:09:35.106214-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8187, [phLogDetail]=631-DR-init-primary, Step 7.1: get sevice user

2021-08-20T17:09:35.106241-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8195, [phLogDetail]=631-DR-init-primary, Step 7.2: get secondary host

2021-08-20T17:09:35.106352-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8214, [phLogDetail]=631-DR-init-primary, Step 7.3: send task updating Svc password to secondary

2021-08-20T17:09:35.180197-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=8224, [phLogDetail]=631-DR-init-primary, Step 7.4: finish updating Svc password on secondary

2021-08-20T17:09:35.182966-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7541, [phLogDetail]=631-DR-init-primary, Step 8: Restarting processes on Primary

2021-08-20T17:09:35.222909-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7549, [phLogDetail]=631-DR-init-primary, Step 9: Broadcasting DR tasks to all processes on Primary

2021-08-20T17:09:35.253335-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7559, [phLogDetail]=631-DR-init-primary, Step 10: Disaster Recovery setup complete

2021-08-20T17:09:35.276445-07:00 andy-super-ipv6 phMonitorSupervisor[38314]: [PH_GENERIC_INFO]: [eventSeverity]=PHL_INFO,[procName]=phMonitorSupervisor,[fileName]=phMonitorProcess.cpp,[lineNumber]=7432, [phLogDetail]=631-DR, Step 4: initializing DR finished.

Failure to Connect to Secondary

If the message "Failed to connect secondary" appears, after enabling Diasaster Recovery, try restarting phMonitor on the Secondary.

Working with Disaster Recovery

This section provides steps for working with various Disaster Recovery situations.

Primary (Site 1) Down, Secondary (Site 2) becomes Primary

Primary (Site 1) has failed and unavailable. The current Secondary (Site 2) needs to become Primary. The Collectors will start buffering events since the Site 1 Workers are down.

Follow the steps below to promote Site 2 to Primary.

Log on to Site 2 (Secondary) as root and run the following command:

```
phsecondary2primary
```

Site 2 (Secondary) becomes Primary, and you can log on to Site 2, which becomes the current Primary, to continue your work.

Note: The process should take approximately 10 minutes to complete. Both FortiSIEM nodes become independent after running the command.

Site 1 Up and Supervisor / Worker Recovered

Site1 has recovered after failure meaning that the Supervisor and Workers are up. You first need to make Site 1 as Secondary and then (optionally) switch roles if you want Site 1 to become Primary again.

Follow the instructions below to make Site 1 as Secondary.

1. Logon to the current Primary FortiSIEM node (this should be Site 2) using the GUI.
2. Navigate to **ADMIN > License > Nodes**.
3. Select the Secondary FortiSIEM node listed (this should be Site 1). It should appear as **Inactive** under the **Replication Status** column.
4. Click **Edit**.
5. Review the information to ensure that all the information is correct.
   Note: The information is read only.
6. When done, click **Save**. The Original Primary (Site 1) now becomes the Secondary in your Disaster Recovery configuration. The **Replication Status** changes from **Inactive** to **Active**.

Now, if you want to switch roles so Site 1 becomes Primary again, follow the instructions in Switching Primary and Secondary Roles.

Site 1 Up but Supervisor / Worker Cannot be Recovered

In this case, Site 1 is up, but the Supervisor and Workers cannot be recovered after failure.

In this situation, you need to first reinstall a Supervisor and Workers on Site 1 and make Site 1 as Secondary.

1. Logon to the current Primary FortiSIEM node (Site 2) using the GUI.
2. Navigate to **ADMIN > License > Nodes**.
3. Select the Secondary FortiSIEM node listed. It should appear with as **Inactive** under the **Replication Status** column.
4. Click **Delete** to remove it from the Disaster Recovery configuration.
5. Log out from Site 2.
6. Re-install Supervisor and Workers in Site 1.
7. Log back onto Site 2 GUI.
8. Add Site 1 as a new Secondary by following the instructions in Configuring Disaster Recovery.

Now, if you want to switch roles so Site 1 becomes Primary again, follow the instructions in Switching Primary and Secondary Roles.

Switching Primary and Secondary Roles

If you need to change your Disaster Recovery setup so that Site 2 will be Secondary, and Site 1 will be Primary, take the following steps.

1. Logon to the current Secondary FortiSIEM node (Site 1) as root, and run the following command:
   `phsecondary2primary`
   When the job is completed, Site 1 is now the Primary.
2. Logon to the Site 1 (Primary) UI.
3. Navigate to **ADMIN > License > Nodes**.
4. Select the Site 2 (Secondary) FortiSIEM node listed and click **Edit**.
5. Review the information to ensure that all the information is correct.
6. When done, click **Save**.
   Site 1 will become Primary and Site 2 will be Secondary. Remember to change the DNS addresses after this role switch so that users are logging on to the Primary and Collectors are sending to Primary Workers.

Recovering from Human Error

If, by mistake, the `phsecondary2primary` command is executed, it turns Site 2 (Secondary) node to Primary. At this point, you have two independent Primary nodes. To recover, take the following steps:

1. Logon to the FortiSIEM you wish to be the current Primary.
2. Navigate to **ADMIN > License > Nodes**.
3. Select the Secondary node.
4. Click **Edit**.
5. Review the information to ensure that all the information is correct.
6. When done, click **Save**.

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.

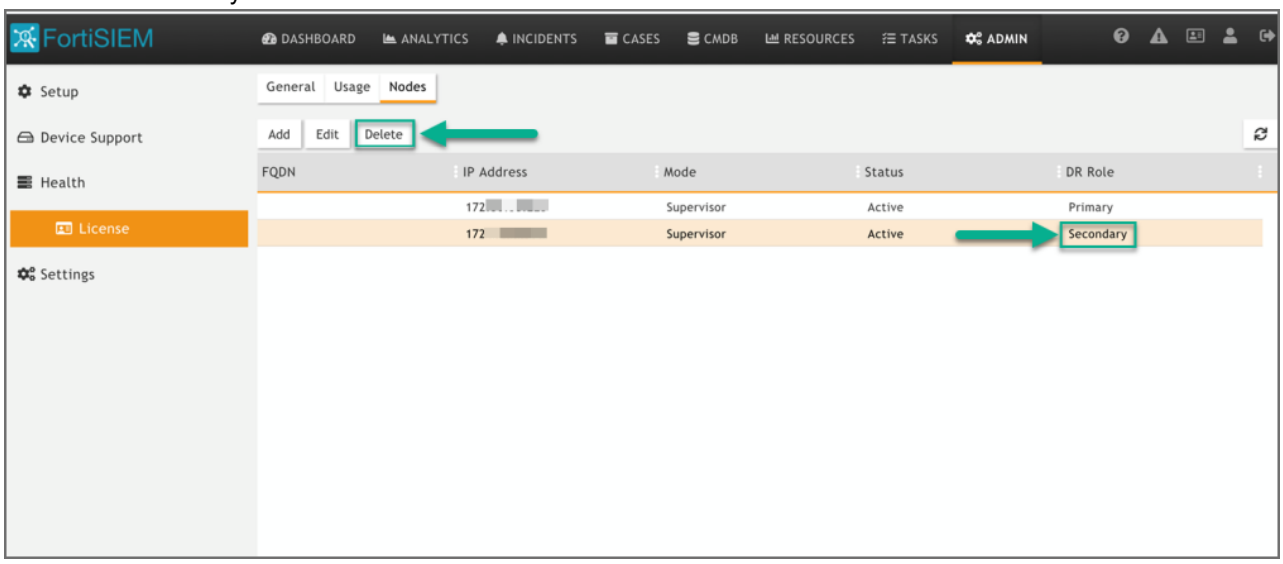
For information on upgrading, see the Upgrade Guide.

Turning Off Disaster Recovery

To turn off Disaster Recovery, take the following steps.

1. Logon to the current Primary GUI.
2. Navigate to **ADMIN > License > Nodes**.

3. Select the Secondary FortiSIEM node listed and click **Delete**.



4. Click **Yes** to confirm the operation.

Changing IP on Secondary

If, for any reason, you need to change the IP address on the Secondary (Site 2) for Disaster Recovery, take the following steps:

1. Turn off Disaster Recovery, by following the instructions in Turning Off Disaster Recovery.
2. Change the IP of your Secondary (Site 2).
3. Re-enable Disaster Recovery by following the instructions in Configuring Disaster Recovery.

www.fortinet.com