

FortiSIEM - Disaster Recovery Procedures - NFS

Version 5.4.0



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/support-and-training/training.html

NSE INSTITUTE https://training.fortinet.com

FORTIGUARD CENTER https://fortiguard.com/

END USER LICENSE AGREEMENT https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK Email: techdoc@fortinet.com



10/13/2020 FortiSIEM 5.4.0 Disaster Recovery Procedures - NFS

TABLE OF CONTENTS

Change Log	4
Disaster Recovery	
	5
Understanding the FortiSIEM DR Feature	5
Prerequisites for a Successful DR Implementation	8
Understanding the Requirements for DNS Names	8
Configuring Disaster Recovery	14
FortiSIEM Primary Node	
FortiSIEM Secondary Node	
Troubleshooting Disaster Recovery Setup	19
Backend Logs	19
Alternative Logs	21
FortiSIEM Services Status on Primary and Secondary Node	22
Understanding FortiSIEM Operations in DR Mode	23
DR Change When the Primary site is Unavailable	25
Change-Over Where Both Systems are Operational	27
Turning Off the Disaster Recovery Feature	

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.

Disaster Recovery

The following sections describe how to enable and work with the FortiSIEM Disaster Recovery (DR) feature.

- Introduction
- Configuring Disaster Recovery
- Troubleshooting Disaster Recovery Setup
- DR Change When the Primary Site is Unavailable
- Change-Over Where Both Systems are Operational
- Turning Off the Disaster Recovery Feature

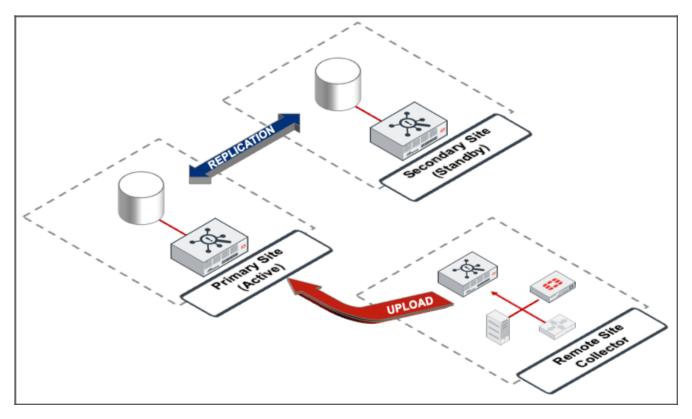
Introduction

- Understanding the FortiSIEM DR Feature
- Prerequisites for a Successful DR Implementation
- Understanding the Requirements for DNS Names

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) and the other the Secondary (standby) site. The two systems replicate the Primary sites databases.

This requires a second fully licensed FortiSIEM system, where the Primary and Secondary Sites are identically setup in terms of Supervisor, Workers, and event storage.

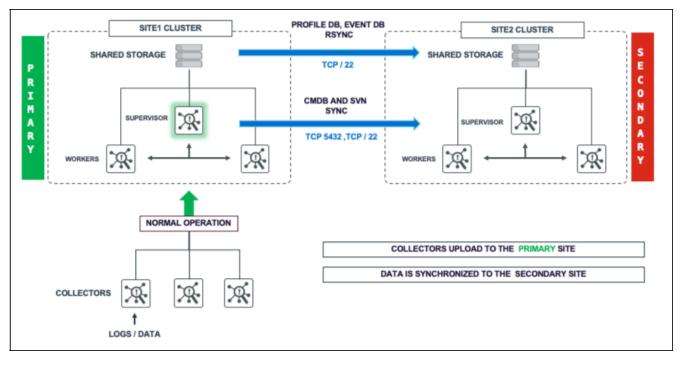


Under normal operations, if collectors are being used, these upload to the Primary site and will buffer by design when this site is not available. If DR is used, and a disaster occurs, then these same collectors will revert to uploading to the Secondary site which will now be designated as the Primary/Active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

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

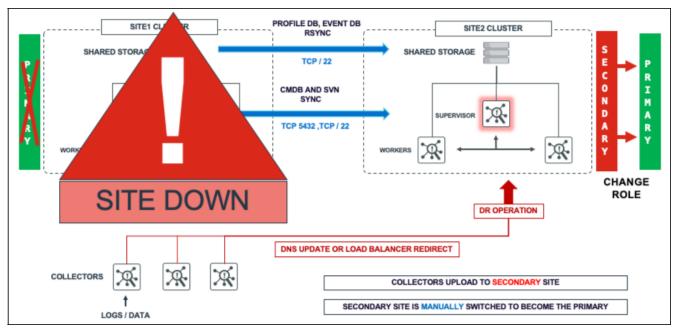
To provide DR features, FortiSIEM must have a Secondary system ready on standby to take over operations, with the following databases replicated from the Primary site:

- The CMDB residing in a PostGreSQL database.
- Device configurations residing in SVN on the Supervisor node.
- Profile data residing on SQLite databases on the Supervisor node.
- Event DB can be on a local disk (for small single node deployments) or on external storage NFS Event DB or Elasticsearch for cluster deployments.



When disaster strikes:

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



When the Old Primary is recovered and powered up, it will sync missing data with the Secondary site (the Active Primary FortiSIEM).

When the user decides to return to the pre-disaster setup, the user can switch the roles of Primary and Secondary.

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, report server 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) and PostGreSQL (TCP/5432) 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 Upload

- Performing Collector Registration
- Agent Communications

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

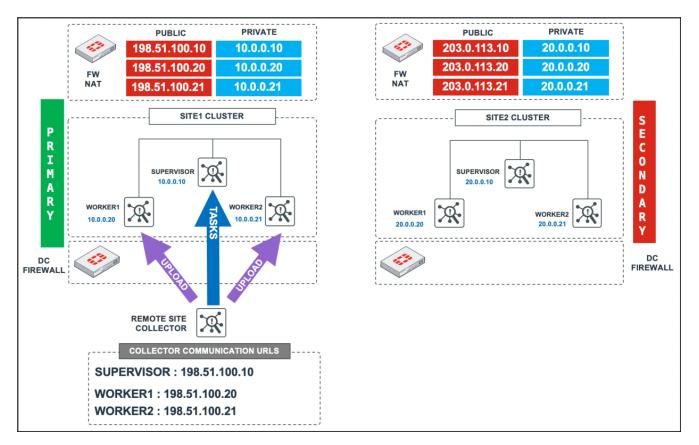
An example is shown below, where the customer has *not* followed best practice advice and used IP Addresses and not FQDNs.

← All Settings > Syst	em > Worker Upload			
Worker Address:	198.51.100.20	+	-	
	198.51.100.21	+	-	

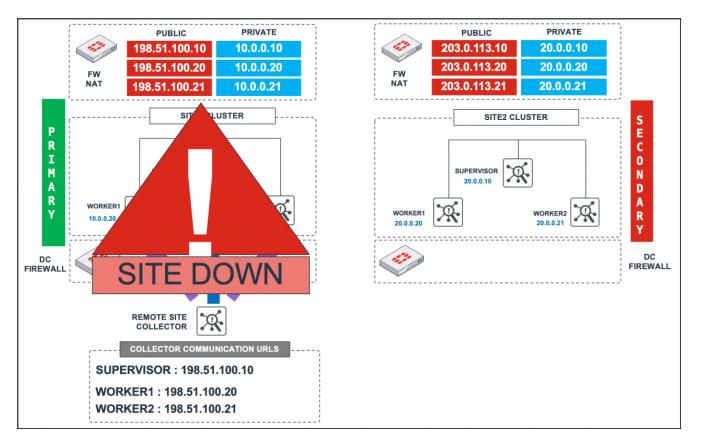
In addition to the Worker Upload entries, Collectors also maintain communication with the Supervisor node, to receive jobs/tasks and report Collector health data. When Collectors register for the first time with the Supervisor node, these communication addresses are stored for this purpose.

Why is using IP addresses for Collector registration and Worker Upload 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 and the Collector maintains communications with the Supervisor. This all works fine until the Primary site has a disaster.



At this point, when the Primary node is unavailable. The remote Collector nodes are essentially hard-coded (by IP) to talk to the Primary site only. Even if 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 Upload settings reference DNS addresses:

← All Settings > Syst	tem > Worker Upload		
Worker Address:	worker1.fsm-mssp.com	+	-
	worker2.fsm-mssp.com	+	-
	worker2.tsm-mssp.com	+	_

External DNS Example

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

Disaster Recovery

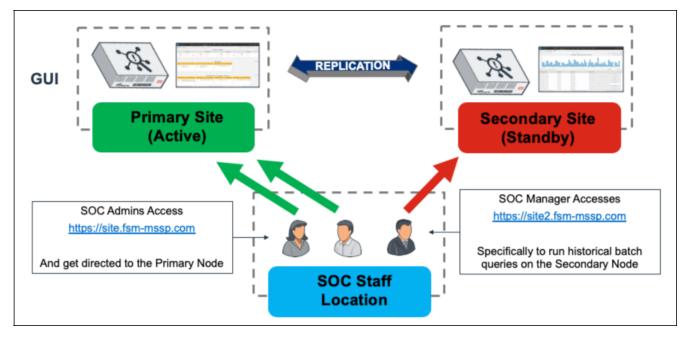
Node	DNS Record Type	Name	IP/Alias
Worker1 (Primary)	А	worker1.fsm-mssp.com	198.51.100.20
Worker2 (Primary)	А	worker2.fsm-mssp.com	198.51.100.21

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

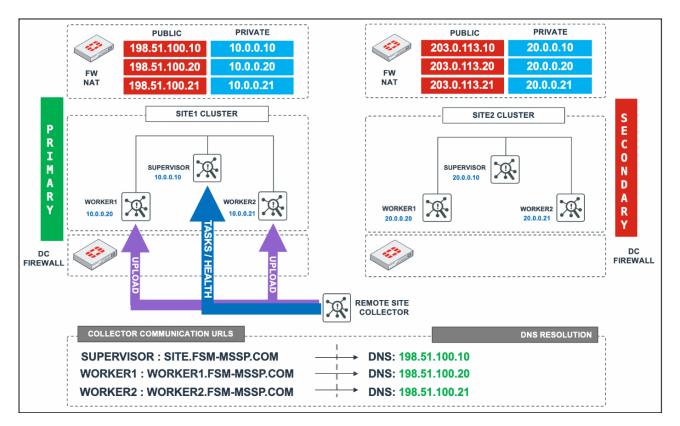
Node	DNS Record Type	Name	IP/Alias
Supervisor (Primary)	А	site1.fsm-mssp.com	10.0.0.10
Supervisor (Secondary)	Α	site2.fsm-mssp.com	20.0.0.10
Active Supervisor	CNAME	site.fsm-mssp.com	site1.fsm-mssp.com

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.

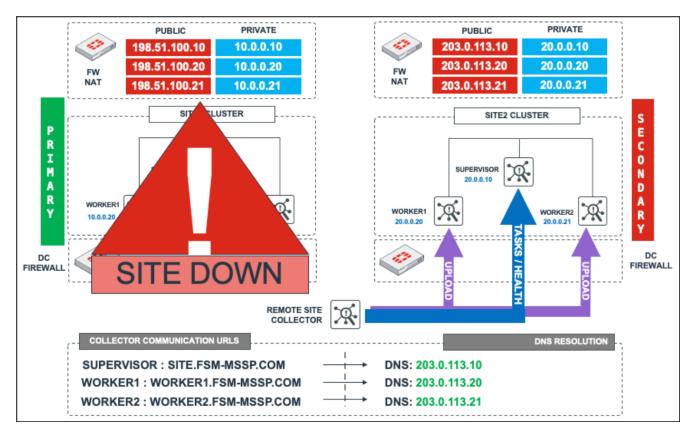


Note: Any DNS changes, are made manually in the event of a failover.

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 GUI.

Performing Collector Registration

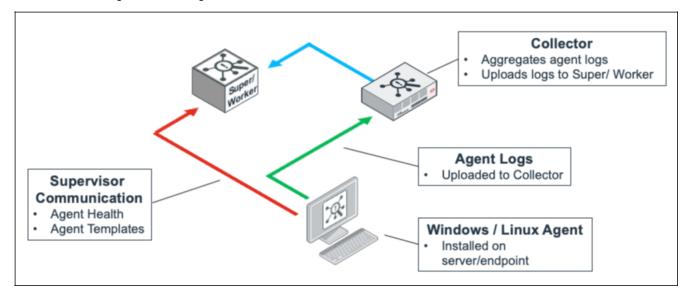
When registering Collectors, you should ignore the Supervisor-IP requirement, and instead use the CNAME for the Active Supervisor node.

```
[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.

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">
 <0rg>
    <ID>1</ID>
    <Name>Super</Name>
  </0rg>
  <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

The following sections describe how to configure FortiSIEM primary and secondary nodes for disaster recovery.

- FortiSIEM Primary Node
- FortiSIEM Secondary Node

FortiSIEM Primary Node

On the Primary FortiSIEM node in the GUI:

- 1. Navigate to Admin > Settings > Database > Replicate (or Replication in 5.3+).
- 2. Select Enable Replication.
- 3. For the **Primary**, enter the **Host** and **IP** information.
- 4. For the UUID, obtain the Hardware ID value through an SSH session on the Primary by entering the following command:

/opt/phoenix/bin/phLicenseTool --show
For example:

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

- 5. For the CMDB Replication mount point, enter / something (this can be any fake mount point). (Note: this value is not actually used today).
- 6. Under Configuration and Profile Replication, generate the SSH Public Key and SSH Private Key Path by entering the following in your SSH session:

```
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|
```

- 7. For the SSH Public Key enter the following command, and copy all of the output into the field: cat /opt/phoenix/bin/.ssh/id_rsa.pub
- 8. For the SSH Private Key Path, enter the following into the field: /opt/phoenix/bin/.ssh/id_rsa.
- **9.** Exit the admin user in the SSH session by entering the following command: exit
- Select a Replication Frequency, with a minimum of 10 minutes.
 Note: For Local/NFS Event DB installs, this value is used for SVN and ProfileDB synchronization.
- **11.** Select the EventDB Replication check box if you would also like the Event Database to be replicated. **Note:** For Local/NFS Event DB installs, rsync is used and this runs continually in the background.

12. Finally, run the following command in the primary SSH session and enter the output under the Role: Secondary, **Primary DB Password** field.

Note: The **Primary DB Password** field initially looks like it has a populated value. This is **false**, and the following step must be completed.

Primary DB Password:	•••••

/opt/phoenix/bin/phLicenseTool -showDatabasePassword

[[root@site1 ~]# /opt/phoenix/bin/phLicenseTool --showDatabasePassword EPicip@8CORi



Keep a copy of this password for Step 4 under FortiSIEM Secondary Node.

The completed Primary role details will appear similar to the following:

← All Settings >	Data	abase > Replicate				
R	ole:	Primary	¢	Role:	Secondary	¢
н	ost:	site1.fsm-mssp.com		Host:		
	IP:	10.10.2.31		IP:		
UL	JID:	564D662C 3553B56EFFF		UUID:		
				Primary DB Password:	•••••	
Schub Replic	catio	n		🗹 CMDB Replicatio	n	
Mount Po	int:	/something		Mount Point:		
🗹 Configuratio	on an	d Profile Replication		Sconfiguration an	d Profile Replication	
SSH Public K	(ey:	0+u3XGxXzxFoiJVLFXRH1cMTzvplJkViXE7Gv FxeleND&cnxM= admin@site1.fsm-mssp.com		SSH Public Key:		
SSH Private Key Pa	ath:	/opt/phoenix/bin/.ssh/id_rsa		SSH Private Key Path:		
Seplication	Freq	uency		🗹 Replication Freq	uency	
Val	lue:	10 Minutes	¢	Value:	30 Minutes	\$
🗹 EventDB Rep	plica	tion		🕑 EventDB Replica	tion	

Now move on to configuring the Secondary nodes details.

- 13. For the Secondary, enter the Host and IP information.
- **14.** For the **UUID**, obtain the **Hardware ID** value through an SSH session on the secondary node by entering the following command:

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

15. For the **CMDB Replication** mount point enter / something (this can be any fake mount point). **Note:** this value is not actually used today.

16. Under **Configuration and Profile Replication**, generate the **SSH Public Key** and **SSH Private Key Path** by entering the following in your SSH session on your secondary node:

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

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

- **17.** For the **SSH Public Key** enter the following command, and copy **all** of the output into the field: cat /opt/phoenix/bin/.ssh/id rsa.pub
- 18. For the SSH Private Key Path, enter the following into the field: /opt/phoenix/bin/.ssh/id rsa.
- **19.** Exit the admin user in the SSH session by entering the following command: exit
- 20. Select the same **Replication Frequency** as were set on the Primary node.

All Settings > Dat	abase > Replicate			
Role:	Primary	Role:	Secondary	¢
Host:	site1.fsm-mssp.com	Host:	site2.fsm-mssp.com	
IP:	10.10.2.31	IP:	10.10.2.35	
UUID:	564D662 \$553B56EFFF	UUID:	564DEFCE 731CCED	
		Primary DB Password:	•••••	
🕑 CMDB Replicatio	n	GMDB Replicatio	n	
Mount Point:	/something	Mount Point:	/something	
Sconfiguration a	nd Profile Replication	Sconfiguration ar	nd Profile Replication	
SSH Public Key:	0+u3XGxXzxFoiJYLFXRH1cMTzyplJkYiXE7Gy FxeleND8cnxM= admin@site1.fsm-mssp.com		Wd9USpwRLkLdUarRJhWp4rg7VtAesBKB9u1+jC miKP/Q782eM= admin@site2.fsm-mssp.com	
SSH Private Key Path:	/opt/phoenix/bin/.ssh/id_rsa	SSH Private Key Path:	/opt/phoenix/bin/.ssh/id_rsa	
Seplication Free	quency	Seplication Free	quency	
Value:	10 Minutes	♦ Value:	10 Minutes	¢
🗹 EventDB Replica	ation	🕑 EventDB Replica	ition	
	Ар	ply Export Import		

- 21. Click Export and download a file named replicate.json. Note: This file contains all of the DR settings, except the Primary DB Password.
- 22. Click Apply.

Note: This should result in the following message in the GUI, where it will stick at 40% until the Secondary node configuration is completed.

	Prin	nary DB Password:	•••••
	V	CMDB Replicatio	on
		Mount Point: 40%	/something
		Run in background	nd Profile Rep
x. m		SSH Public Key:	Wd9USpwRLkLd

FortiSIEM Secondary Node

On the Secondary FortiSIEM node, log into the FortiSIEM GUI:

- 1. Navigate to Admin > Settings > Database > Replicate (or Replication in 5.3+).
- 2. Select Enable Replication.
- 3. Click Import, and select the replicate.json file downloaded from the Primary node.
- 4. Copy the **Primary DB Password**, from Step 12 in FortiSIEM Primary Node.

If you do not have the password handy, run the following command on the Primary node's SSH session and enter the output under the **Primary DB Password** field.

```
#On the PRIMARY node
/opt/phoenix/bin/phLicenseTool -showDatabasePassword
```

5. Click Apply.

At this point, the Secondary node will display the following while the backend scripts are disabling services, etc.



Note: There will be disruption of services on both nodes, while the setup is taking place behind the scenes. While initial replication is taking place, you can view the status on the Primary node, Jobs, and Errors (Red Alert Symbol, top right of GUI) on what Step (out of 10) the process is currently at.

Jobs And Errors					□ ×
Jobs Errors Stop Job Search					Last update at 11:51:34 AM.
Start Time User	Organization Collector	Job	Status	Progress	Parameters
Apr 22 2020, 11:35:29 AM admin	Super	Replication Setting Change	Started	40%	Step 5: Run BDR script
Apr 22 2020, 11:26:35 AM	Super collector.fsm	Collector EPS Update	Done	100%	0

Backend logs will better display the current status of the replication and DR scripts being run.

Troubleshooting Disaster Recovery Setup

- Backend Logs
- Alternative Logs
- FortiSIEM Services Status on Primary and Secondary Node
- Understanding FortiSIEM Operations in DR Mode
- Verify Elasticsearch Snapshots for Data Replication

Backend Logs

On both the Primary and Secondary nodes, use the cat command to view the backend logs:

cat /opt/phoenix/config/pgMasterRep/bdrlog

Note: This process can take a while. The output below was a new installation with minimal test data and it took around 5 minutes to complete, For a live system it will take a lot longer. (It is recommended to tail -f the log).

Successful Enablement of Disaster Recovery on the Primary node

```
[root@site1 ~] # cat /opt/phoenix/config/pgMasterRep/bdrlog
bdr connection count for 10.10.2.31 is
back up pg hba.conf and postgresgl.conf
setting bdr configuration ...
inserting pg hba records ...
finished setting bdr configuration
restart postgresq19.4
ext btree gist count is 0
ext bdr count is 0
bdr nodel count is 0
please wait the bdr building ...
no primary file exist, add primary file
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
```

```
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Waiting for Secondary 10.10.2.35 to finish up synch Primary CMDB
Secondary 10.10.2.35 finished synch Primary CMDB
```

Successful Enablement of Disaster Recovery on the Secondary node

```
[root@site2 ~] # cat /opt/phoenix/config/pgMasterRep/bdrlog
slave - bdr connection count for 10.10.2.31 is
Backup unsynchable system properties from ph sys conf before replicating CMDB from Primary
     CMDB
dump file ph sys server.sql and ph sys conf.sql ...
Shutdown App Server to preparing synch CMDB from primary Stopping crond: [ OK ]
Stopping postgresql-9.4 service: [ OK ]
wait port 5432 to stop...
port 5432 stopped
join connection according cmdb buffer ... master ip = 10.10.2.31, slave ip = 10.10.2.35 bdr
     init copy: starting ...
Getting remote server identification ...
Detected 1 BDR database(s) on remote server
Updating BDR configuration on the remote node:
phoenixdb: creating replication slot ...
phoenixdb: creating node entry for local node ...
Creating base backup of the remote node...
194081/194081 kB (100%), 1/1 tablespace
Creating restore point on remote node ...
Bringing local node to the restore point ...
Transaction log reset
Initializing BDR on the local node:
phoenixdb: adding the database to BDR cluster ...
All done
please wait the connection building ...
synching CMDB from Primary, status= c
Done synching CMDB from Primary
DELETE 1
DELETE 8
DELETE 0
DELETE 58
DELETE 6
DELETE 361
import sql ph_sys_server.sql ...
COPY 1
COPY 1
Restoring non-replicable system properties
```

```
COPY 3
Stop running all quartz jobs on secondary
restart App Server ...
Starting crond: [ OK ]
ALTER ROLE
Done replication CMDB
```

Alternative Logs

It is also possible to track the DR scripts by examining the phoenix.log file. Use the grep command on both Primary and Secondary nodes to track progress.

```
grep "521-ReplicationRoleChange" /opt/phoenix/log/phoenix.log
[root@site1 log]# grep "521-ReplicationRoleChange" /opt/phoenix/log/phoenix.log 2020-04-
     15T20:04:55.143563+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=6866, [phLogDetail]=521-
     ReplicationRoleChange, Step 1.1: check command type
2020-04-15T20:04:55.143667+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp,[lineNumber]=6875,[phLogDetail]=521-
     ReplicationRoleChange, Step 1.2: check command data
2020-04-15T20:04:55.143729+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=6882, [phLogDetail]=521-
     ReplicationRoleChange, Step 2: load replication setting
2020-04-15T20:04:55.183173+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr
ocess.cpp, [lineNumber]=6897, [phLogDetail]=521-ReplicationRoleChange, Step 3: handle
     replication
role change
2020-04-15T20:04:55.183344+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp,[lineNumber]=6916,[phLogDetail]=521-
     ReplicationRoleChange, Step 3.1: handle replication role change on super
2020-04-15T20:04:55.183442+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=6919, [phLoqDetail]=521-
     ReplicationRoleChange, Step 3.2: prepare role info
2020-04-15T20:04:55.218565+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=6942, [phLogDetail]=521-
     ReplicationRoleChange, Step 3.3: update SSH keys
2020-04-15T20:04:55.265239+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr
ocess.cpp,[lineNumber]=6955,[phLogDetail]=521-ReplicationRoleChange, Step 3.4: update SSH
configurations
2020-04-15T20:04:55.312994+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=6970, [phLogDetail]=521-
     ReplicationRoleChange, Step 3.5: run database replication script
2020-04-15T20:19:39.991395+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=6992, [phLogDetail]=521-
     ReplicationRoleChange, Step 3.6: wait appsvr back
```

```
2020-04-15T20:19:40.056744+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp,[lineNumber]=7001,[phLogDetail]=521-
     ReplicationRoleChange, Step 3.7: update service and SVN password for the first time
2020-04-15T20:19:40.542801+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=7198, [phLogDetail]=521-
     ReplicationRoleChange, Step 3.7.1: get sevice user
2020-04-15T20:19:40.542861+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp,[lineNumber]=7206,[phLogDetail]=521-
     ReplicationRoleChange, Step 3.7.2: get secondary host
2020-04-15T20:19:40.543375+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp,[lineNumber]=7225,[phLogDetail]=521-
     ReplicationRoleChange, Step 3.7.3: update secondary
2020-04-15T20:19:40.670656+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr
ocess.cpp, [lineNumber]=7013, [phLogDetail]=521-ReplicationRoleChange, Step 3.8: restart
     processes
on super
2020-04-15T20:19:40.711471+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity] = PHL INFO, [procName] = phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp, [lineNumber]=7021, [phLogDetail]=521-
     ReplicationRoleChange, Step 3.9: notify processes on super
2020-04-15T20:19:40.751225+02:00 site1 phMonitorSupervisor[4874]:
[PH GENERIC INFO]: [eventSeverity]=PHL INFO, [procName]=phMonitorSupervisor,
     [fileName]=phMonitorPr ocess.cpp,[lineNumber]=7031,[phLogDetail]=521-
     ReplicationRoleChange, Step 3.10: finish role change on super
```

FortiSIEM Services Status on Primary and Secondary Node

On the Primary node, all FortiSIEM ph* services will be in an "up" state. (They will all restart, but it may take up to 3 to 5 minutes to restart.)

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/phoeni	x/bin/phstat	us.py			Every 1.0s: /opt/phoeni	x/bin/phstat	us.py
System uptime: 18:11:0 Tasks: 25 total, 0 runn Cpu(s): 8 cores, 3.1%us Mem: 8060332k total, 76 Swap: 25165820k total,	ning, 24 slee , 0.9%sy, 0.0 28060k used,	ping, 0 stoppe 0%ni, 96.0%id, 432272k free,	d, 0 zombie 0.0%wa, 0.0%hi, 77548k buffers		System uptime: 18:11:2 Tasks: 25 total, 0 runn Cpu(s): 8 cores, 1.0%us Mem: 8060332k total, 61 Swap: 25165820k total,	ing, 9 sleep , 0.5%sy, 0. 92344k used,	ing, 0%ni 186
PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM	PROCESS	UPTIME	
phParser	01:58	ø	1837m	222m	phParser	DOWN	
phQueryMaster	00:48	õ	910m	71m	phQueryMaster	00:49	
bhRuleMaster	01:55	ø	591m	53m	phRuleMaster	DOWN	
phRuleWorker	01:55	õ	1338m	321m	phRuleWorker	DOWN	
bhQueryWorker	01:55	õ	1377m	320m	phQueryWorker	00:49	
bhDataManager	01:55	õ	1133m	67m	phDataManager	DOWN	
phDiscover	01:58	õ	423m	44m	phDiscover	DOWN	
bhReportWorker	01:55	õ	1429m	96m	phReportWorker	DOWN	
bhReportMaster	01:55	õ	496m	50m	phReportMaster	DOWN	
hlpIdentityWorker	01:55	õ	938m	50m	phIpIdentityWorker	DOWN	
hlpIdentityMaster	01:55	õ	398m	31m	phIpIdentityMaster	DOWN	
hAgentManager	01:58	ø	1504m	45m	phAgentManager	DOWN	
phCheckpoint	01:55	õ	117m	22m	phCheckpoint	DOWN	
ohPerfMonitor	01:58	õ	756m	55m	phPerfMonitor	DOWN	
hReportLoader	01:55	õ	736m	320m	phReportLoader	DOWN	
ohBeaconEventPackager	01:58	õ	1046m	57m	phBeaconEventPackager	DOWN	
phDataPurger	01:55	õ	516m	50m	phDataPurger	00:49	
phEventForwarder	01:58	õ	476m	38m	phEventForwarder	DOWN	
phMonitor	47:53	ø	1228m	582m	phMonitor	00:30	
Apache	49:04	õ	224m	6088	Apache	48:53	
Node.js-charting	48:57	õ	922m	73m	Node.js-charting	48:47	
Node.js-pm2	47:56	õ	0	114m	Node.js-pm2	48:14	
AppSvr	51:30	1	- 11170m	2907m	AppSvr	04:15	
DBSvr	52:03	ē	376m	28m	DBSvr	05:40	
Redis	51:35	õ	130m	7608	Redis	51:26	

Understanding FortiSIEM Operations in DR Mode

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

- Both the Primary and Secondary nodes GUI are available for login.
- The CMDB is set in a multi-master mode, so any changes on the Secondary are replicated over to the Primary.
- Although the CMDB can be edited from either site, it is recommended to do all edits on the Primary site.
- Analytical queries and reports can be run from either node.
- Performing Real-Time queries: You will see results only on the Primary node, as this is done in memory before storage.

Primary vs Secondary – Real-Time Search

Action - I [1] Real-time Search		🗘 Action 👻 I [1] Real-time Search	
Edit Filters and Time Range	I≣ - x Stop	Edit Filters and Time Range	🔳 👻 🗴 Stop
	*Real-time Search		*Real-time Search
4 มหายมูลัดขางารระ เอก็รด อาการระ	ແລ້ວນ ແດ້ວວ ແດ້ວວ	а - Аргия, доо 11-12-13 10-12-11 10-12-11	ແນ່ລະ ແນ່ລະ
Pause Fast forward Clear 🗭 Show Event Type 🗌 Wrap Raw Event		Pause Fast forward Clear 🗹 Show Event Type 🗌 Wrap Raw Event	
Event Receive Time Reporting IP Event Type	Raw Event Log	Event Receive Time Reporting IP Event Type	Raw Event Log
Apr 15 2020, 03:13:47 PM 10.0.0.1 FortiGate-traffic-allowed	<189>Apr 15 21:13:47 date=2016-09-13 time=15		
Apr 15 2020, 03:13:47 PM 10.0.0.1 FortiGate-traffic-allowed	<189>Apr 15 21:13:47 date=2016-09-13 time=15		
Apr 15 2020, 03:13:47 PM 10.0.0.1 FortiGate-appctrl-ips-pass	<190>Apr 15 21:13:47 date=2016-09-13 time=15		
Apr 15 2020, 03:13:47 PM 10.0.0.1 FortiGate-traffic-allowed	<189>Apr 15 21:13:47 date=2016-09-13 time=15		
Apr 15 2020, 03:13:46 PM 10.0.0.1 FortiGate-traffic-allowed	<189>Apr 15 21:13:46 date=2016-09-13 time=15		
Apr 15 2020, 03:13:46 PM 10.0.0.1 FortiGate-traffic-allowed	<189>Apr 15 21:13:46 date=2016-09-13 time=15		
Apr 15 2020, 03:13:45 PM 10.0.0.1 FortiGate-webfilter-url-firewall-allow	<189>Apr 15 21:13:45 date=2016-09-13 time=15		
Apr 15 2020, 03:13:45 PM 10.0.0.1 FortiGate-webfilter-url-firewall-allow	<189>Apr 15 21:13:45 date=2016-09-13 time=15		
Copyright © 2019 Fortinet, Inc. All rights reserved.	Organization: Super User: admin Scope: Local	Copyright © 2019 Fortinet, Inc. All rights reserved.	Organization: Super User: admin Scope: Local

• Performing Historical Queries: Bear in mind the data on the Secondary node will be slightly out of date, dependent upon how much data is being replicated, but this is ideal for running large complex queries on the Secondary without impacting the Primary's performance.

Primary vs Secondary – Historical Search (Last 10 Minutes)

users, load average: 0.30, 0.49, 0.33 15 stopped, 0 zombie , 98.6%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st 7988k free, 84284k buffers 0k free, 1905052k cached

VIRT_MEM

910m

1366m

516m

999m 224m 923m

11046r 374m

0000000

RES_MEM

68m

317m

50m

27m 6088 74m

> 28m 7612

♦ Action • I [1] Raw Mer	isage 🖸				Action • I [1] Raw B	lessage				
B . Edit Filters and Time F	tange				Edit Filters and Time	e Range			🖩 🖌 Q. Run	
			Raw Message - Last 10 Minutes					*5	Raw Message - Last 10 Minutes	
12 10- 8- 4- 2- 0 Apr 1389, 2000 14:53	14.52	ućsa reše	ida ida	1407	12 10 6 4 2 - 2 - 4 4 120, 200 H 5 1	1452	1453	1 14:54	1455	1456 1457
Show Event Type					Show Event Type				for the second se	Anna Rossent Lana
Event Receive Time	Reporting IP	Event Type	Event Name	Raw Event Log	Event Receive Time Apr 15 2020, 02:54:21 PM	Reporting IP	Event Type Win-Security-4634		Event Name Windows logoff	Raw Event Log 2020-04-15T18:48:08
Apr 15 2020, 02:54:21 PM	10.10.2.30	Win-Security-4634	Windows logoff	2020-04-15T18:48:08Z D		10.10.2.30				
Apr 15 2020, 02:54:21 PM	10.10.2.30	Win-Security-4624	Windows logon success	2020-04-15T18:48:08Z D	Apr 15 2020, 02:54:21 PM	10.10.2.30	Win-Security-4624		Windows logon success	2020-04-15T18:48:08
Apr 15 2020, 02:54:21 PM	10.10.2.30	Win-Security-4672	Windows administrator equivalent successful logon	2020-04-15T18:48:08Z D	Apr 15 2020, 02:54:21 PM	10.10.2.30	Win-Security-4672		Windows administrator equivalent successful logon	2020-04-15T18:48:08
Apr 15 2020, 02:53:20 PM	10.10.2.30	Win-Security-4634	Windows logoff	2020-04-15T18:47:08Z D	Apr 15 2020, 02:53:20 PM	10.10.2.30	Win-Security-4634		Windows logoff	2020-04-15T18:47:08
Apr 15 2020, 02:53:20 PM	10.10.2.30	Win-Security-4624	Windows logon success	2020-04-15T18:47:08Z DI	Apr 15 2020, 02:53:20 PM	10.10.2.30	Win-Security-4624		Windows logon success	2020-04-15T18:47:08
Apr 15 2020, 02:53:20 PM	10.10.2.30	Win-Security-4672	Windows administrator equivalent successful logon	2020-04-15T18:47:08Z D	Apr 15 2020, 02:53:20 PM	10.10.2.30	Win-Security-4672		Windows administrator equivalent successful logon	2020-04-15T18:47:08
Apr 15 2020, 02:52:19 PM	10.10.2.30	Win-Security-4634	Windows logoff	2020-04-15T18:46:08Z D	Apr 15 2020, 02:52:19 PM	10.10.2.30	Win-Security-4672		Windows administrator equivalent successful logon	2020-04-15T18:46:08
Copyright O 2019 Fortinet, Inc. All ri	ights reserved.	Inter President MAX	Organization: Super User: admin Scope: Loc		Copyright O 2019 Fortinet, Inc. Al	I rights reserved.			Organization: Super User: admin	Icope: Local

• Any notifications or scheduled report deliveries are performed on the Primary node only. (Since most of the required ph* processes are down on the Secondary).

DR Change When the Primary site is Unavailable

It is important to note that it is a manual process to promote the Secondary node to be the Primary.

As soon as the Primary node is unavailable (that is, down/unavailable), any collector nodes will start to buffer their uploads, as the Worker Upload addresses they deliver to will be unavailable.

On the Secondary FortiSIEM node, log into the GUI:

- 1. Navigate to Admin > Settings > Database > Replicate (or Replication in 5.3+).
- 2. Change the Role selector for the Secondary node to be Primary.

← All Settings	s > Dat	abase > Replication			
🗹 Enable	Replic	ation			
Host Info				Host Info	
	Role:	Primary	¢	Role:	Primary Secondary
	Host:	site1.fsm-mssp.com		Host:	site2.fsm-mssp.com
	IP:	10.10.2.31		IP:	10.10.2.35
	UUID:	56		UUID:	
				Primary DB Password:	•••••
🗹 CMDB Re	plicatio	n		CMDB Replicatio	n

3. Notice how the original Primary Role has now switched to Secondary, and the **PrimaryDB** Password field moves across to the left.

← All Settings > Database > Replication								
🗹 Enable Replic	cation							
Host Info			Host Info					
Role:	Secondary	¢	Role:	Primary	¢			
Host:	site1.fsm-mssp.com		Host:	site2.fsm-mssp.com				
IP:	10.10.2.31		IP:	10.10.2.35				
UUID:	54-0000 1000 4040 4040 400 4040		UUID:	56				
Primary DB Password:								
CMDB Replicatio	n		🗹 CMDB Replicatio	n				

This field must be input again, but it can be obtained from an SSH session to the Secondary now, as it now has the same database as the Primary. Run the following command and paste the output into the **Primary DB Password** field.

#On the SECONDARY node /opt/phoenix/bin/phLicenseTool -showDatabasePassword

- 4. Click Apply.
- 5. Click Yes to the warning, Are you sure you want to switch Roles?.



At this time, the following will appear in the GUI and it will seem to disconnect and the DR scripts will be run in the background.

		×	
	Error		
	503 Service Temporarily Unavailable		
	Service Temporarily Unavailable The server is temporarily unable to service your		ion
	problems. Please time or capacity		ION
EA7	Apache Server at 10.10.2.35 Port 443		чAВ
	· · · · · · · · · · · · · · · · · · ·		.h/io

After a short period of time, all the backend processes will start and the GUI will return to the login page.

If you run a Real-Time search you will probably find no data is still being received. This is because a DNS change is now required for the shared DNS addresses for the Supervisor node and the Worker upload settings, as in this example case:

DNS Address	Old Value	New Value
site.fsm-mssp.com	CNAME -> site1.fsm-mssp.com	CNAME -> site2.fsm-mssp.com
worker1.fsm-mssp.com	198.51.100.20	203.0.113.20
worker2.fsm-mssp.com	198.51.100.21	203.0.113.21

Change the DNS addresses and data will start to flow in normally.

Note: When the original Primary is recovered and powered back on, it will detect this and take on the Secondary role automatically.

Change-Over Where Both Systems are Operational

Operationally, there may be a need to perform a DR change over while both nodes are actually up and running.

Again, to note, this is a manual process of promoting the Secondary node to be the Primary.

On the Primary FortiSIEM node, log into the GUI:

- 1. Navigate to Admin > Settings > Database > Replicate (or Replication in 5.3+).
- 2. Change the Role selector for the Primary node to be Secondary.
- 3. Populate the Primary DB Password field. Run the following command on either the Primary or Secondary node via SSH: #On the PRIMARY or SECONDARY node /opt/phoenix/bin/phLicenseTool --showDatabasePassword
- 4. Click Apply, and respond Yes to the warning, "Are you sure you want to switch Roles?". Note: The extra steps below are very important. You will have a cluster which thinks it has two Primary nodes if you do not follow the two steps below.
- 5. Switch to the Secondary node GUI, and navigate to Admin > Settings > Database > Replicate (or Replication in 5.3+).
- 6. Change the Roles (unless the CMDB sync has already updated).
- 7. Click Apply.

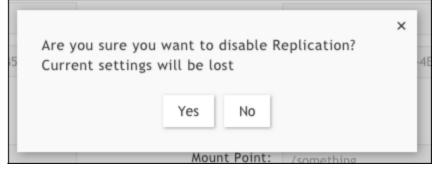
Remember to change the DNS addresses after the migration.

Turning Off the Disaster Recovery Feature

There are cases where the DR Replication feature needs to be disabled, such as performing upgrades.

On the Primary FortiSIEM node, log into the GUI:

- 1. Navigate to Admin > Settings > Database > Replicate (or Replication in 5.3+).
- 2. Deselect the Enable Replication check box.
- 3. Respond Yes to the warning regarding disabling the Replication.



- 4. Click Apply.
- 5. Wait for the response Replicate settings applied.

Since the database is shared, this only needs to be performed on one node.

But, due to a bug in 5.2.8, it can only be re-enabled from the opposite node, Secondary in this case.





Copyright© (Undefined variable: FortinetVariables.Copyright Year) Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGate® 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 is 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.