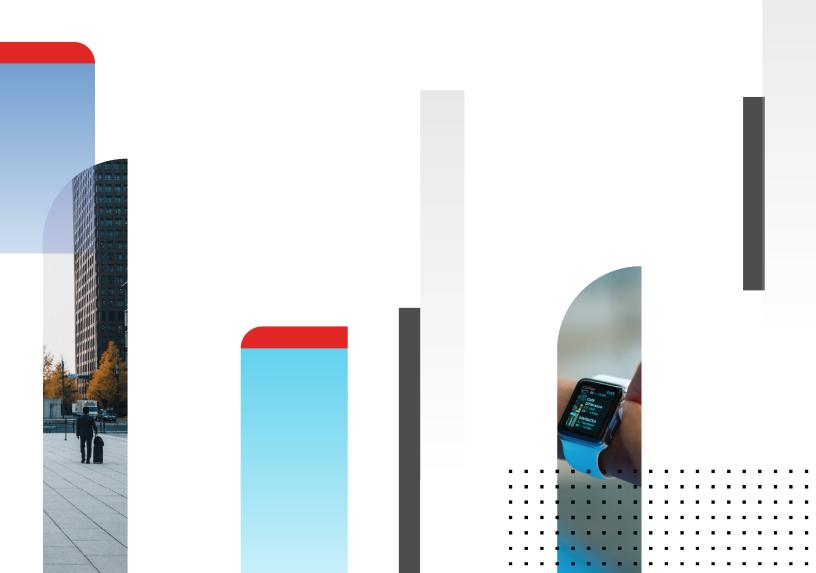
## F**E**RTINET.

# Disaster Recovery Procedures -Bi-Directional Elasticsearch

FortiSIEM 6.4.0



#### 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/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



## TABLE OF CONTENTS

Change Log	5
Disaster Recovery in Elasticsearch Deployments	6
Introduction	. 6
Understanding the FortiSIEM DR Feature	
Prerequisites for a Successful DR Implementation	9
Understanding the Requirements for DNS Names	9
Configuring Disaster Recovery - New Install	15
Basic Requirements	
Step 1. Set Up Elasticsearch for Site 1 and Site 2	16
Step 2. Enable Remote Cluster Client for Both Sites	16
Step 3. Add X-Pack's Auto Create Index for Both Sites	16
Step 4. Define Remote Clusters for Site 1	
Step 5. Define Auto-Follow Patterns in Site 1	
Step 6. Define Remote Clusters for Site 2	
Step 7. Define Auto-Follow Patterns in Site 2	
Step 8. Set Up Site 1 FortiSIEM with Elasticsearch Storage	
Step 9. Set Up Site 2 FortiSIEM with Elasticsearch Storage	
Step 10. Set Up Disaster Recovery	
Step 11. Verify Site 1 to Site 2 Event Replication	
Step 12. Verify ILM is Working for Follower Index in Site 2	
Step 13. Verify Site 2 to Site 1 Event Replication	
Step 14. Verify ILM is Working for Follower Index in Site 1	
Configuring Disaster Recovery - Existing Install	
Basic Requirements	
Step 1. Set Up Elasticsearch for Site 2	
Step 2. Enable Remote Cluster Client for Both Sites	
Step 3. Add X-Pack's Auto Create Index for Both Sites	
Step 4. Define Remote Clusters for Site 1	
Step 5. Define Auto-Follow Patterns in Site 1	
Step 6. Define Remote Clusters for Site 2	
Step 7. Define Auto-Follow Patterns in Site 2	
Step 8. Set Up Site 2 FortiSIEM with Elasticsearch Storage	
Step 9. Set Up Disaster Recovery	
Step 10. Verify Site 1 to Site 2 Event Replication	
Step 11. Verify ILM is Working for Follower Index in Site 2 Step 12. Verify Site 2 to Site 1 Event Replication	
Step 12. Verify ILM is Working for Follower Index in Site 1	
Step 14. (Optional) Copy Older Indices from Site 1 to Site 2	
Primary (Site 1) Fails, Site 2 Becomes Primary	
Step 1. Switch Site 2 Role to Primary in FortiSIEM	
Step 2. Save Elasticsearch Settings on Site 2 in FortiSIEM	
Step 3. Confirm Events are Inserted to Site 2	
•	
Step 4. Confirm Incident Index is Created and Updated to Site 2 Step 5. Confirm Lookup Index is Updated to Site 2 Site 1 is Up and Becomes Primary	36 37

Overview	
Step 1. Set Site 1 to Secondary and Confirm Data from Site 2 is Replicated to Site 1	138
Step 2. Stop Collectors from Sending Events to Site 2	38
Step 3. Switch Site 1 Role to Primary in FortiSIEM	39
Step 4. Save Elasticsearch Settings on Site 1 in FortiSIEM	39
Step 5. Verify All Event Workers are Added to Site 1	39
Step 6. Verify Events are Being Written into Site 1	39
Step 7. Confirm Incident Index is Re-Created and Updated to Site 1	40
Step 8. Confirm Lookup Index is Updated to Site 1	40
Step 9. Verify Events are Being Replicated to Site 2	41
Viewing Replication Health	42
Implementation Notes	42
Changing Index Lifecycle Management Parameters on Primary	
Circuit Breaking Exception in Elasticsearch	42
Possible Inconsistent Index State (Follower and Frozen) in Secondary	42

## Change Log

Date	Change Description
10/15/2021	Initial version of FortiSIEM - Disaster Recovery Procedures for Bi-Directional Elasticsearch for 6.3.2
12/22/2021	Initial version of FortiSIEM - Disaster Recovery Procedures for Bi-Directional Elasticsearch for 6.3.3
01/18/2022	Initial version of FortiSIEM - Disaster Recovery Procedures for Bi-Directional Elasticsearch for 6.4.0
05/23/2022	Initial version of FortiSIEM - Disaster Recovery Procedures for Bi-Directional Elasticsearch for 6.4.1
09/15/2022	Updated Prerequisites for a Successful DR Implementation section.
12/14/2022	Initial version of FortiSIEM - Disaster Recovery Procedures for Bi-Directional Elasticsearch for 6.4.2

## **Disaster Recovery in Elasticsearch Deployments**

The following sections describe how to configure and work with FortiSIEM Disaster Recovery (DR) in Elasticsearch based deployments. This is based on Elasticsearch *bi-directional* replication (see <a href="https://www.elastic.co/guide/en/elasticsearch/reference/7.12/xpack-ccr.html">https://www.elastic.co/guide/en/elasticsearch/reference/7.12/xpack-ccr.html</a>).

- Introduction
- Configuring Disaster Recovery New Install
- · Configuring Disaster Recovery Existing Install
- Primary (Site 1) Fails, Site 2 Becomes Primary
- Site 1 is Up and Becomes Primary
- Viewing Replication Health
- Implementation Notes

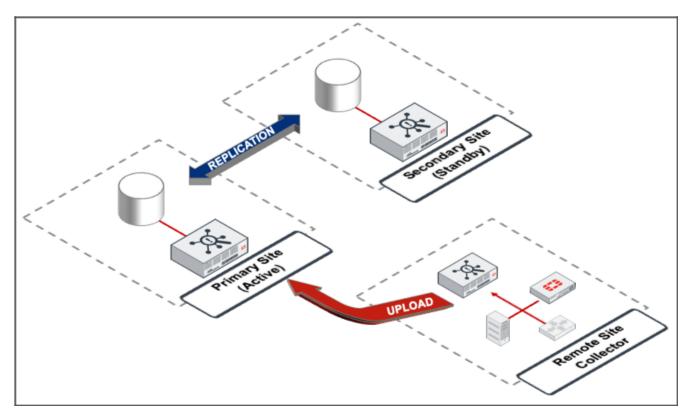
## Introduction

- 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), Site 1, and the other the Secondary (hot standby) site, Site 2. The two systems replicate the Primary sites (Site 1) databases.

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.

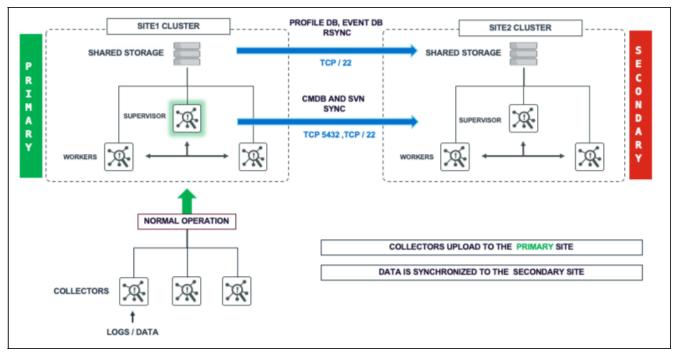


Under normal operations, if collectors are being used, these upload to Site 1, the Primary site and will buffer by design when this site is not available. If DR is set up and a disaster occurs, then these same collectors will revert to uploading to Site 2, the Secondary site, which will now be designated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

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

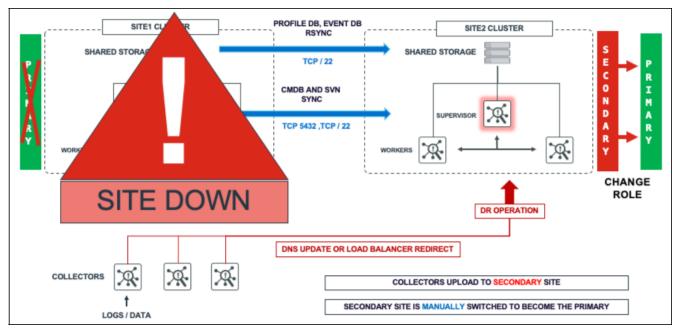
To provide DR features, FortiSIEM must have a Secondary system ready on standby to take over operations, with the following databases replicated from the Primary site:

- 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 Elasticsearch.



When disaster strikes:

- 1. The Secondary (Site 2) must become the Primary FortiSIEM.
- 2. DNS Changes must be made so that users will login 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).

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. Elasticsearch clusters should also be set up identically on 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), Elasticsearch replication (TCP/9200), 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.

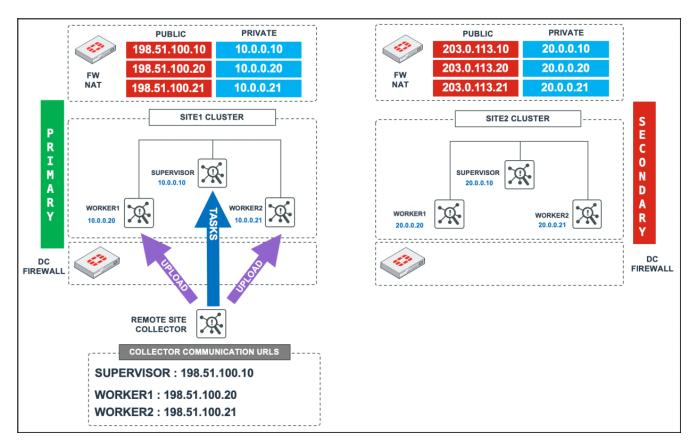
An example is shown below, where the customer has *not* followed best practice advice and used IP Addresses and not FQDNs.

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

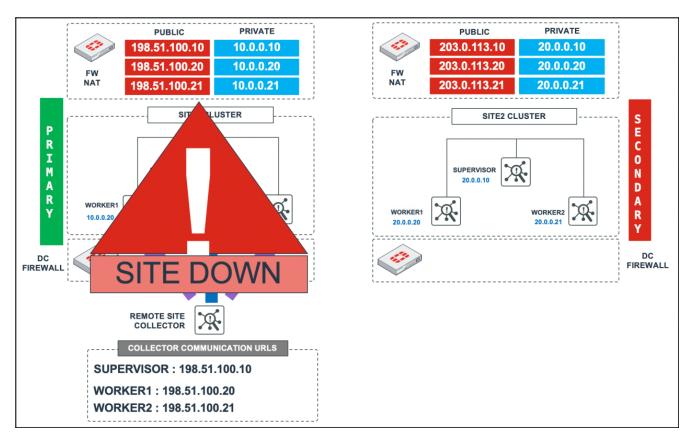
In addition to the Worker Event entries, Collectors also maintain communication with the Supervisor node, to receive jobs/tasks and report Collector health data. When Collectors register for the first time with the Supervisor node, these communication addresses are stored for this purpose.

## 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:

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

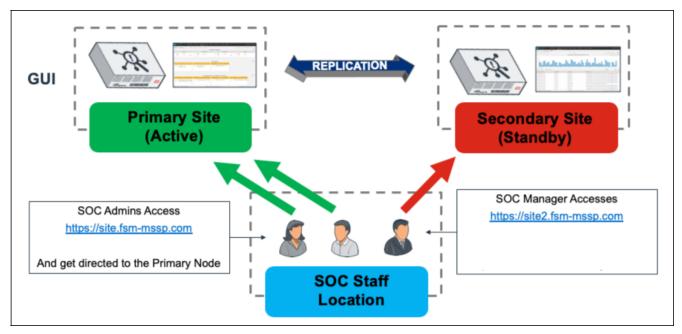
Node	DNS Record Type	Name	IP/Alias
Active Supervisor	CNAME	site.fsm-mssp.com	site1.fsm-mssp.com
Worker1 (Primary)	А	worker1.fsm-mssp.com	198.51.100.20
Worker2 (Primary)	А	worker2.fsm-mssp.com	198.51.100.21

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

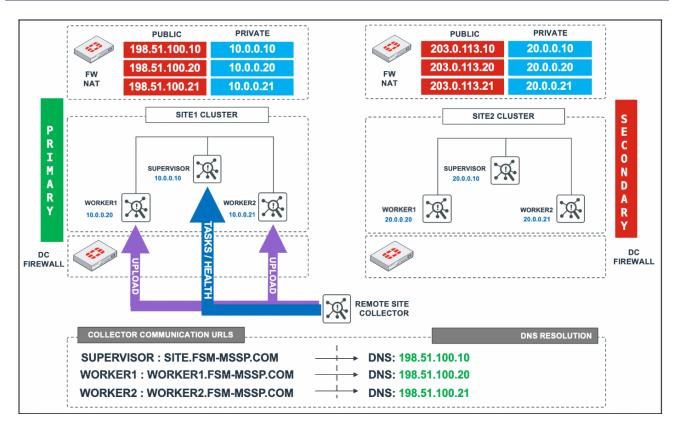
Node	DNS Record Type	Name	IP/Alias
Supervisor (Primary)	А	site1.fsm-mssp.com	10.0.0.10
Supervisor (Secondary)	A	site2.fsm-mssp.com	20.0.0.10
Active Supervisor	CNAME	site.fsm-mssp.com	site1.fsm-mssp.com

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.

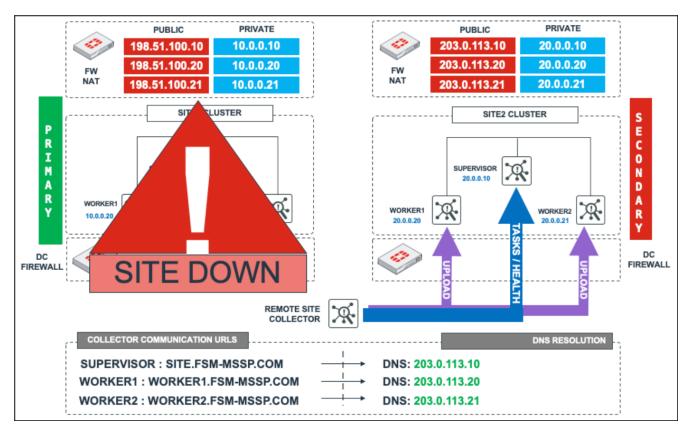


Note: Any DNS changes, are made manually in the event of a failover.

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 GUI.

#### **Performing Collector Registration**

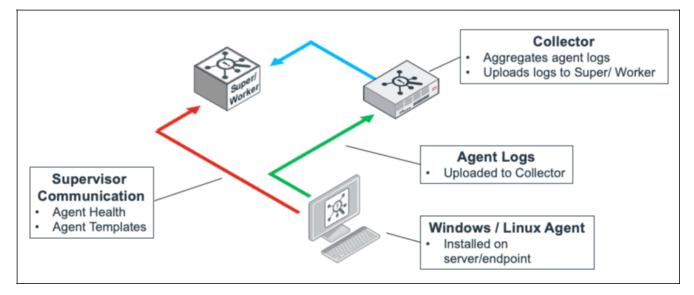
When registering Collectors, you should ignore the Supervisor-IP requirement, and instead use the CNAME for the Active Supervisor node.

```
[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 - New Install**

Ensure you have followed the Prerequisites for a Successful DR Implementation and Basic Requirements (below) prior to this configuration.

This configuration assumes a completely new FortiSIEM install. To facilitate configuration, assume that there are two Sites: Site 1 and Site 2. Initially, Site 1 is Primary and Site 2 is Secondary.

Follow all the proceeding steps to configure a **bidirectional Elasticsearch Cross-Cluster replication** (CCR) that works with FortiSIEM Disaster Recovery (DR).

#### **Basic Requirements**

Site 1 and Site 2 must have an identical setup for its Supervisor, Workers, and Elasticsearch cluster (Master, Coordinator only and Data Nodes) if the Secondary Site needs to take the workload of the Primary Site for extended periods of time. Specifically, this means for Site 1 and Site 2:

- They must have the same number of Workers.
- The Super and Workers hardware configuration must be identical.
- They must have the same number of Master node, Coordinating nodes, Hot, Warm, and Cold Data nodes.

#### Step 1. Set Up Elasticsearch for Site 1 and Site 2

Set up two separate Elasticsearch Clusters, one as Site 1 and one as Site 2. Do not add the Elasticsearch cluster to FortiSIEM yet. This will be done after cross-cluster replication (CCR) is setup.

#### Step 2. Enable Remote Cluster Client for Both Sites

Take the following steps to set up the Elasticsearch Clusters for Site 1 and Site 2.

1. Modify the elasticsearch.yml file for each node in Site 1 with:

node.remote cluster client: true

- 2. Restart each node in the cluster for Site 1.
- Modify the elasticsearch.yml file for each node in Site 2 with: node.remote cluster client: true
- 4. Restart each node in the cluster for Site 2.

#### Step 3. Add X-Pack's Auto Create Index for Both Sites

X-Pack needs its indices to be created. To create these indices to action.auto\_create\_index list, take the following steps:

1. Run the following command against the Site 1 Coordinator node.

```
PUT /_cluster/settings?pretty
{
    "persistent": {
        "action.auto_create_index": "-fortisiem-event-*,fortisiem-*,.monitoring-*"
    }
}
```

2. Run the same command against the Site 2 Coordinator node.

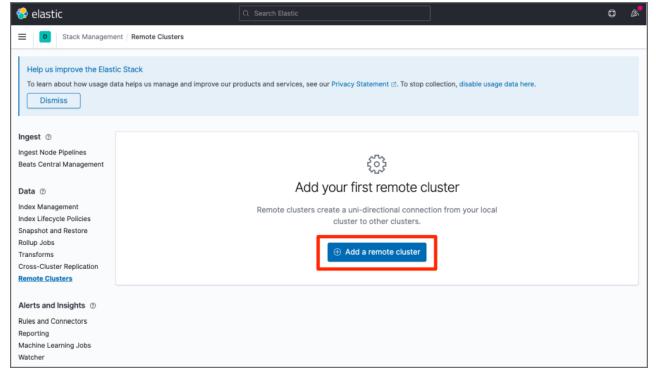
```
PUT /_cluster/settings?pretty
{
    "persistent": {
        "action.auto_create_index": "-fortisiem-event-*,fortisiem-*,.monitoring-*"
    }
}
```

#### Step 4. Define Remote Clusters for Site 1

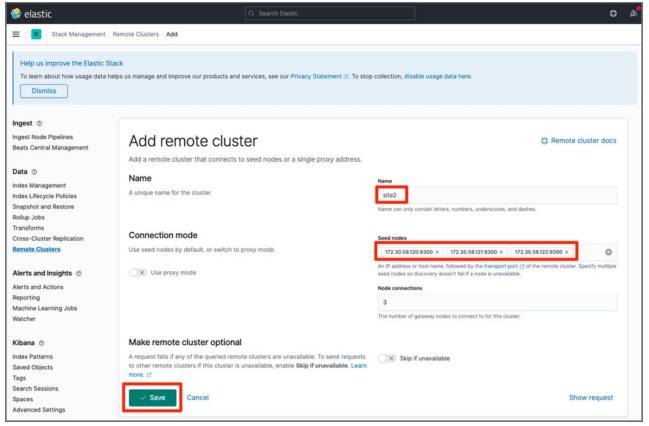
**Note**: Do not add the master dedicated node to seeds. This is because dedicated master nodes are never selected as gateway nodes. It is recommended that at least three nodes with low traffic, node.remote\_cluster\_client enabled, and transport port opened be added in the list of seed nodes, such as the coordinator node.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Remote Clusters.



3. Add Site 2's nodes as the remote servers to Site 1. After adding the Site 1's nodes, click Save.



#### Step 5. Define Auto-Follow Patterns in Site 1

Since indices are dynamically created in Site 2, you must configure auto-follow pattern in Site 1 to enable the dynamically generated indices in Site 2 to be replicated to Site 1.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.
- Define an Auto-Follow patterns for fortisiem-event-\* time-series indices. Do NOT make similar definitions for other indices. The example screenshot here shows the fortisiem-event.auto\_follow\_pattern being defined.

😔 elastic	Q Search Elastic	0
E Stack Management / C	Cross-Cluster Replicat / Add	
Help us improve the Elastic Sta To learn about how usage data hel Dismiss	ck ps us manage and improve our products and services, see our Privacy Statement &. To sto	p collection, disable usage data here.
Ingest ① Ingest Node Pipelines Beats Central Management	Add auto-follow pattern	Auto-follow pattern docs
Data ③ Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs Transforms <u>Cross-Cluster Replication</u> Remote Clusters	Name A unique name for the auto-follow pattern. Remote cluster The remote cluster to replicate leader indices from.	Name fortisiem-event_auto_follow_pattern  Remote cluster  Site2  Add remote cluster
Alerts and Insights ① Alerts and Actions Reporting Machine Learning Jobs Watcher	Leader indices One or more index patterns that identify the indices you want to replicate from the remote cluster. As new indices matching these patterns are created, they are replicated to follower indices on the local cluster. Note: Indices that already exist are not replicated.	Index patterns for tisiem-event * × Spaces and the characters \/?*<> are not allowed.
Kibana © Index Patterns Saved Objects Tags Search Sessions Spaces Advanced Settings Stack © License Management 8.0 Upgrade Assistant	Follower indices (optional) A custom prefix or suffix to apply to the names of the follower indices so you can more easily identify replicated indices. By default, a follower index has the same name as the leader index.	Prefix     Suffix       copy:
	✓ Create Cancel	Show request

The screenshot here shows that auto-follow patterns have been created for fortisiem-event-\* time-series indices.

😔 elastic		Q Searc	h Elastic				
Stack Management / Cross-Cluster Replication							
To visualize and explore data in Kibana, you must create	an index pattern to retrieve dat	a from Elasticsearch	6				
Ingest ③ Ingest Node Pipelines Beats Central Management Data ③ Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs	Cross-Cluste Follower indices Auto An auto-follow pattern rep local cluster. Q Search	o-follow patterns		er and copies them to fo	llower indices on the	Greate an auto-fo	llow pattern
Transforms Cross-Cluster Replication Remote Clusters	□ Name ↑	Status	Remote cluster	Leader patterns	Follower index prefix	Follower index suffix	Actions
Alerts and Insights ①	fortisiem- event_auto_follow_patt ern	Active	site2	fortisiem-event-*	сору-		
Alerts and Actions Reporting Watcher	Rows per page: 20 $\checkmark$						< 1 >

When completed, Elasticsearch on Site 1 is now ready for replication.

#### Step 6. Define Remote Clusters for Site 2

Since Site 2 will initiate the replication, the Site 1 nodes must be defined in Site 2 using Kibana.

**Note**: Do not add the master dedicated node to seeds. This is because dedicated master nodes are never selected as gateway nodes. It is recommended that at least three nodes with low traffic, node.remote\_cluster\_client enabled, and transport port opened be added in the list of seed nodes, such as the coordinator node.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Remote Clusters.

😔 elastic		٩	۵.
Stack Manageme	nt / Remote Clusters		
Help us improve the Elast To learn about how usage di Dismiss	c Stack Ita helps us manage and improve our products and services, see our Privacy Statement ඵ. To stop collection, disable usage data here.		
Ingest ①			
Ingest Node Pipelines Beats Central Management	502		
Data 💿	Add your first remote cluster		
Index Management Index Lifecycle Policies Snapshot and Restore	Remote clusters create a uni-directional connection from your local cluster to other clusters.		
Rollup Jobs Transforms Cross-Cluster Replication	⊕ Add a remote cluster		
Remote Clusters			
Alerts and Insights ①			
Rules and Connectors Reporting Machine Learning Jobs Watcher			

3. Add Site 1's nodes as the remote servers to Site 2. After adding the Site 1's nodes, click Save.

Ingest @			
Ingest Node Pipelines Beats Central Management	Add remote cluster		Remote cluster docs
	Add a remote cluster that connects to seed nodes or to a single proxy ad	ldress.	
Data 💿	Name	Maria	
Index Management	A unique name for the cluster.	Name	
Index Lifecycle Policies Snapshot and Restore		site1	
Rollup Jobs		Must contain only letters, numbers, underscores, and d	ashes.
Transforms	Connection mode		
Cross-Cluster Replication	Connection mode	Seed nodes	
Remote Clusters	Use seed nodes by default, or switch to proxy mode.	172.30.58.120:9300 × 172.30.58.121:9300 ×	0
		172.30.58.122:9300 ×	0
Alerts and Insights ②	<ul> <li>X Use proxy mode</li> </ul>		
		An IP address or host name, followed by the transport p	oort 🕑 of the remote cluster. Specify
Rules and Connectors		An IP address or host name, followed by the transport p multiple seed nodes so discovery doesn't fail if a node i	
Reporting			
		multiple seed nodes so discovery doesn't fail if a node is	
Reporting Machine Learning Jobs		multiple seed nodes so discovery doesn't fail if a node i Node connections	s unavailable.
Reporting Machine Learning Jobs		multiple seed nodes so discovery doesn't fail if a node i Node connections	s unavailable.
Reporting Machine Learning Jobs Watcher	Make remote cluster optional	multiple seed nodes so discovery doesn't fail if a node i Node connections	s unavailable.
Reporting Machine Learning Jobs Watcher Kibana ©	If any of the remote clusters are unavailable, the query request fails. To avoid	multiple seed nodes so discovery doesn't fail if a node i Node connections	s unavailable.
Reporting Machine Learning Jobs Watcher Kibana ① Index Patterns Saved Objects Tags	If any of the remote clusters are unavailable, the query request fails. To avoid this and continue to send requests to other clusters, enable <b>Skip if</b>	multiple seed nodes so discovery doesn't fail if a node is Node connections 3 The number of gateway nodes to connect to for this clu	s unavailable.
Reporting Machine Learning Jobs Watcher Kibana ① Index Patterns Saved Objects Tags Search Sessions	If any of the remote clusters are unavailable, the query request fails. To avoid	multiple seed nodes so discovery doesn't fail if a node is Node connections 3 The number of gateway nodes to connect to for this clu	s unavailable.
Reporting Machine Learning Jobs Watcher Kibana ① Index Patterns Saved Objects Tags Search Sessions Spaces	If any of the remote clusters are unavailable, the query request fails. To avoid this and continue to send requests to other clusters, enable <b>Skip if</b> unavailable. Learn more.	multiple seed nodes so discovery doesn't fail if a node is Node connections 3 The number of gateway nodes to connect to for this clu	s unavailable.
Reporting Machine Learning Jobs Watcher Kibana ① Index Patterns Saved Objects Tags Search Sessions	If any of the remote clusters are unavailable, the query request fails. To avoid this and continue to send requests to other clusters, enable <b>Skip if</b>	multiple seed nodes so discovery doesn't fail if a node is Node connections 3 The number of gateway nodes to connect to for this clu	s unavailable.

## Step 7. Define Auto-Follow Patterns in Site 2

Since indices are dynamically created in Site 1, you must configure auto-follow pattern in Site 2 to enable the dynamically generated indices in Site 1 to be replicated to Site 2.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.
- 3. Define Auto-Follow patterns for fortisiem-event-\* time-series indices. Do NOT make similar definitions for other indices. The example screenshot here shows the fortisiem-event.auto\_follow\_pattern being defined.

😚 elastic	Q Search Elastic	ه ۵
E Stack Management / 0	Cross-Cluster Replicat / Add	
Help us improve the Elastic Sta To learn about how usage data he Dismiss	ack Ips us manage and improve our products and services, see our Privacy Statement @. To sto	p collection, disable usage data here.
Ingest ① Ingest Node Pipelines Beats Central Management	Add auto-follow pattern	C Auto-follow pattern docs
Data ① Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs Transforms <u>Cross-Cluster Replication</u> Remote Clusters	Name A unique name for the auto-follow pattern. Remote cluster The remote cluster to replicate leader indices from.	Name fortislem-event_auto_follow_pattern  Remote cluster  Site1  Add remote cluster
Alerts and Insights ① Alerts and Actions Reporting Machine Learning Jobs Watcher	Leader indices One or more index patterns that identify the indices you want to replicate from the remote cluster. As new indices matching these patterns are created, they are replicated to follower indices on the local cluster. Note: Indices that already exist are not replicated.	Index patterns fortisiem-event.* × Spaces and the characters \/?*<>   are not allowed.
Kibana ① Index Patterns Saved Objects Tags Search Sessions Spaces Advanced Settings Stack ① License Management 8.0 Upgrade Assistant	Follower indices (optional) A custom prefix or suffix to apply to the names of the follower indices so you can more easily identify replicated indices. By default, a follower index has the same name as the leader index.	Prefix     Suffix       copy-
	Create Cancel	Show request

The screenshot here shows that auto-follow patterns have been created for fortisiem-event-\* time-series indices.

Ingest ③	Cross-Cluster Replication	
Data 🕐	Follower indices Auto-follow patterns	
ndex Management		
ndex Lifecycle Policies	An auto-follow pattern replicates leader indices from a remote cluster and copies them to follower indices on the  Oreate an auto-foll Create an auto-foll	ow patter
Snapshot and Restore	local cluster.	Contraction of the
No. II. Control of the local		
Kollup Jobs	A MALE WITH REPORT ALL	
	Q Search	
Transforms	Q. Search	
Transforms Cross-Cluster Replication	Q     Search       Name ↑     Status       Remote cluster     Leader patterns       Follower index prefix     Follower index suffix	Actio
Rollug Jobs Transforms Cross-Cluster Replication Remote Clusters Alerts and Insights ①		Actio
Transforms Cross-Cluster Replication Remote Clusters	Name ↑     Status     Remote cluster     Leader patterns     Follower index prefix     Follower index suffix       fortisiem- event_auto_follow_patt     ● Active     site1     fortisiem-event-*     copy-	

When completed, elasticsearch on Site 2 is now ready for replication.

## Step 8. Set Up Site 1 FortiSIEM with Elasticsearch Storage

Take the following steps to set up Site 1 FortiSIEM with Elasticsearch as its online storage.

- 1. Login to the FortiSIEM GUI.
- 2. Navigate to ADMIN > Setup > Storage > Online.
- 3. Select the **Elasticsearch** radio button from the three available options (Local Disk, NFS, Elasticsearch) and configure.
- 4. Click Save.

#### Step 9. Set Up Site 2 FortiSIEM with Elasticsearch Storage

Take the following steps to set up Site 2 FortiSIEM with Elasticsearch as its online storage.

- 1. Login to the FortiSIEM GUI.
- 2. Navigate to ADMIN > Setup > Storage > Online.
- 3. Select the **Elasticsearch** radio button from the three available options (Local Disk, NFS, Elasticsearch) and configure.
- 4. Click Save.

## Step 10. Set Up Disaster Recovery

See Configuring Disaster Recovery in the latest Disaster Recovery Procedures - EventDB Guide here.

## Step 11. Verify Site 1 to Site 2 Event Replication

Take the following steps to check on Elasticsearch event replication.

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.
- 3. Verify that the follower indices are created automatically.

😼 elastic		Q Search Elastic			
Stack Management Cross-Cluster	Replication				
ingest (1)					
ngest Node Pipelines	Cross-Cluster Re	olication			
Beats Central Management					
Data ®	Follower indices Auto-follow pa	tterns			
ndex Management	A follower index replicates a leader in	dex on a remote cluster			
ndex Lifecycle Policies	A follower index represees a leader in			① Create a follow	wer index
napshot and Restore	Q Search				
tollup Jobs	C Startin				
ransforms cross-Cluster Replication	Name 1	Status	Remote cluster	Leader index	Action
ransforms Cross-Cluster Replication Remote Clusters	Name ↑     copy-fortisiem-event-2021.09.20-1	Status  Active	Remote cluster	Leader index fortisiem-event-2021.09.20-1	Action
Cross-Cluster Replication					
ross-Cluster Replication emote Clusters Jerts and Insights ② Jerts and Actions	copy-fortisiem-event-2021.09.20-1 copy-fortisiem-event-2021.09.22- copy-fortisiem-event-2021.09.22- copy-fortisiem-event-2021.09.22-	Active     Active	site1	fortisiem-event-2021.09.20-1 fortisiem-event-2021.09.22-1-000	
ross-Cluster Replication emote Clusters Uerts and Insights ① letts and Actions eporting	copy-fortisiem-event-2021.09.20-1 copy-fortisiem-event-2021.09.22- 1-000001	Active	site1 site1	fortisiem-event-2021.09.20-1	
ross-Cluster Replication emote Clusters lerts and Insights ① erts and Actions	copy-fortisiem-event-2021.09.20-1 copy-fortisiem-event-2021.09.22- copy-fortisiem-event-2021.09.22- copy-fortisiem-event-2021.09.22-	Active     Active	site1 site1	fortisiem-event-2021.09.20-1 fortisiem-event-2021.09.22-1-000	

## Step 12. Verify ILM is Working for Follower Index in Site 2

To verify that index lifecycle management (ILM) is working on site 2, you will need to take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.
- 3. Under Indices, select one follower event index and under Index lifecycle management, check Lifecycle policy. It should be fsiem\_ilm\_policy.

😌 elastic	Q Search Elastic				0 4
E Stack Management / Index Manage	iment				
Ingest © Ingest Node Pipelines Beats Central Management	Index Management	Summary	ortisiem-event-2021.09.2 y Settings Mappings Stats	22-1-000001 Fellower Edit settings	
Data ⑦ Index Management Index Lifecycle Policies	Indices Data Streams Index Templates Comp Update your Elasticsearch indices individually or in bulk. Le	General	e green	Status	open
Snapshot and Restore Rollup Jobs Transforms	С) сору	Primaries Docs Count	1 at 1808748	Replicas Docs Deleted	0
Cross-Cluster Replication Remote Clusters	Name Health copy-fortisiem-event-2021.09.22-1-000 001 Follower green Follower	Stu Storage Siz		Primary Storage Size	
Alerts and Insights ① Alerts and Actions Reporting	copy-fortisiem-event-2021.09.22-3-000 01 Fotower	op Index life	1		
Watcher	copy-fortisiem-event-2021.09.20-1 e green	op Lifecycle po	olicy fsiem_ilm_policy	Current phase	new
Kibana ① Index Patterns	Rows per page: 10 $\sim$	Current act		Current action time	2021-09-22 10:00:01
Saved Objects Tags Search Sessions Spaces		Failed step		Phase definition	Show definition

## Step 13. Verify Site 2 to Site 1 Event Replication

Take the following steps to check on Elasticsearch event replication.

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.
- 3. Verify that the follower indices are created automatically.

😓 elastic		Q Search Elastic					
Stack Management Cross-Cluster	r Replication						
Ingest ①							
Ingest Node Pipelines Beats Central Management	Cross-Cluster Rep	Cross-Cluster Replication					
seats Central Management	Follower indiana Auto follower						
Data 💿	Follower indices Auto-follow pa	tterns					
ndex Management	A follower index replicates a leader in	dex on a remote cluste	ır.	⊕ Create a follo	war index		
ndex Lifecycle Policies					Her maex		
Snapshot and Restore	Q Search						
Rollup Jobs Transforms							
Cross-Cluster Replication	Name 个	Status	Remote cluster	Leader index	Actions		
Remote Clusters	copy-fortisiem-event-2021.09.20-1	Active	site1	fortisiem-event-2021.09.20-1			
Alerts and Insights ①	copy-fortisiem-event-2021.09.22- 1-000001	Active	site1	fortisiem-event-2021.09.22-1-000			
Alerts and Actions	copy-fortisiem-event-2021.09.22-	Active	site1	fortisiem-event-2021.09.22-3-000			
	3-000001	Active	site1	fortisiem-event-2021.09.22-3-000			
Reporting							
leporting Vatcher	Rows per page: 20 V				< 1 >		

## Step 14. Verify ILM is Working for Follower Index in Site 1

To verify that index lifecycle management (ILM) is working on site 1, you will need to take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.
- 3. Under Indices, select one follower event index and under Index lifecycle management, check Lifecycle policy. It should be fsiem\_ilm\_policy.

🧇 elastic	Q. Search Elastic				0
E Stack Management / Index Management					
Ingest ③ Ingest Node Pipelines Beats Central Management	Index Management	copy-fortisiem-	-event-2021.09.22-1- Mappings Stats Edit s	000001 Follower ettings	
Data 💿 Index Management	Indices Data Streams Index Templates Compone Update your Elasticsearch indices individually or in bulk. Lear	General	• green	Status	open
Index Lifecycle Policies Snapshot and Restore Rollup Jobs	Q copy	Primaries	1	Replicas	o
Transforms Cross-Cluster Replication Remote Clusters	Name Health St	Docs Count Storage Size	69728 11.4mb	Docs Deleted Primary Storage Size	
Alerts and Insights ①	001 • green op Follower copy-fortisiem-event-2021.09.22-3-000	Aliases	fortisiem-event-2021.09.22 1	-	
Alerts and Actions Reporting Watcher	001 • green op Follower	Index lifecycle mana	agement		
Kibana 💿	Copy-fortisiem-event-2021.09.20-1 e green op	Lifecycle policy Current action	fsiem_ilm_policy complete	Current phase Current action time	new 2021-09-22 09:53:10
Index Patterns Saved Objects Tags	Follower Group of Sector o	Failed step	-	Phase definition	Show definition
Search Sessions Spaces					

## **Configuring Disaster Recovery - Existing Install**

This section assumes that Elasticsearch is already running on FortiSIEM on Site 1 (Primary). Disaster Recovery needs to be set up for Site 1 and Site 2, with Site 2 to be used as Secondary.

#### **Basic Requirements**

Site 1 and Site 2 must have an identical setup for its Supervisor, Workers, and Elasticsearch cluster (Master, Coordinator only and Data Nodes) if the Secondary Site needs to take the workload of the Primary Site for extended periods of time. Specifically, this means for Site 1 and Site 2:

- They must have the same number of Workers.
- The Super and Workers hardware configuration must be identical.
- They must have the same number of Master node, Coordinating nodes, Hot, Warm, and Cold Data nodes.

#### Step 1. Set Up Elasticsearch for Site 2

Set up two separate Elasticsearch clusters, one as Site 1, and one as Site 2. Do not add the Elasticsearch cluster to FortiSIEM yet. This will be done after cross-cluster replication (CCR) is set up.

## Step 2. Enable Remote Cluster Client for Both Sites

Take the following steps to set up the Elasticsearch Cluster for Site 1 and Site 2.

- 1. Modify the elasticsearch.yml file for each node in Site 1 with:
- node.remote\_cluster\_client: true2. Restart each node in the cluster for Site 1.
- Modify the elasticsearch.yml file for each node in Site 2 with: node.remote cluster client: true
- 4. Restart each node in the cluster for Site 2.

## Step 3. Add X-Pack's Auto Create Index for Both Sites

X-Pack needs its indices to be created. To add X-Pack's Auto Create Index to action.auto\_create\_index list, take the following steps:

1. Run the following command against the Site 1 Coordinator node.

```
PUT /_cluster/settings?pretty
{
    "persistent": {
        "action.auto_create_index": "-fortisiem-event-*,fortisiem-*,.monitoring-*"
    }
}
```

2. Run the same command against the Site 2 Coordinator node.

```
PUT /_cluster/settings?pretty
{
    "persistent": {
        "action.auto_create_index": "-fortisiem-event-*,fortisiem-*,.monitoring-*"
    }
}
```

## Step 4. Define Remote Clusters for Site 1

**Note**: Do not add the master dedicated node to seeds. This is because dedicated master nodes are never selected as gateway nodes. It is recommended that at least three nodes with low traffic, node.remote\_cluster\_client enabled, and transport port opened be added in the list of seed nodes, such as the coordinator node.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Remote Clusters.

😔 elastic		٥	as <mark>-</mark>
E Stack Manageme	Int / Remote Clusters		
Help us improve the Elast To learn about how usage de Dismiss	ic Stack ta helps us manage and improve our products and services, see our Privacy Statement 🗷. To stop collection, disable usage data here.		
Ingest ③			
Ingest Node Pipelines Beats Central Management	ર્ટેટર		
Data ①	Add your first remote cluster		
Index Management Index Lifecycle Policies Snapshot and Restore	Remote clusters create a uni-directional connection from your local cluster to other clusters.		
Rollup Jobs Transforms Cross-Cluster Replication Remote Clusters	⊕ Add a remote cluster		
Alerts and Insights ⑦			
Rules and Connectors Reporting Machine Learning Jobs Watcher			

3. Add Site 2's nodes as the remote servers to Site 1. After adding Site 1's nodes, click Save.

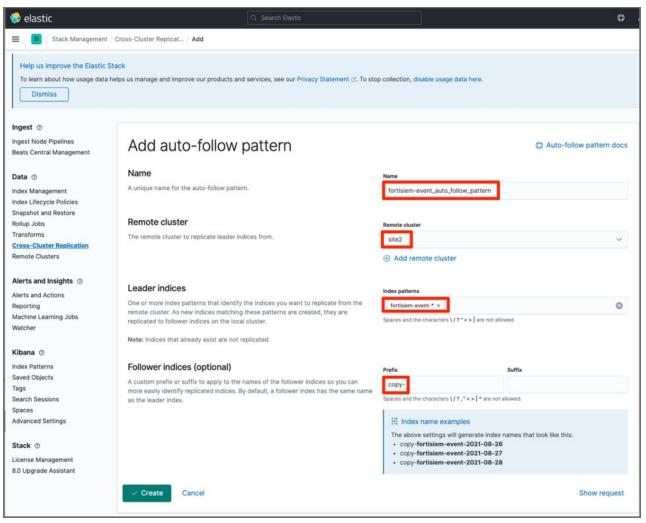
🔗 elastic	Q. Search Elastic		٥	ø
E Stack Management / Re	mote Clusters / Add			
Dismiss	k s us manage and improve our products and services, see our Privacy Statement 안. To stop	o collection, disable usage data here.		
Ingest ① Ingest Node Pipelines Beats Central Management	Add remote cluster Add a remote cluster that connects to seed nodes or a single proxy address.	C Remote cluster de	ocs	
Data ① Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs	Name A unique name for the cluster.	Name site2 Name can only contain letters, numbers, underscores, and dashes.		
Transforms Cross-Cluster Replication	Connection mode	Seed nodes		
Remote Clusters Alerts and Insights ① Alerts and Actions Reporting	Use seed nodes by default, or switch to proxy mode.	172.30.58.120:9300 ×       172.30.58.122:9300 ×       172.30.58.122:9300 ×       (f)         An IP address or host name, followed by the transport port (2) of the remote cluster. Specify mult seed nodes so discovery doesn't fail if a node is unavailable.       Node connections       3	C Itiple	
Machine Learning Jobs Watcher		The number of gateway nodes to connect to for this cluster.		
Kibana Index Patterns Saved Objects Tags	Make remote cluster optional A request fails if any of the queried remote clusters are unavailable. To send requests to other remote clusters if this cluster is unavailable, enable Skip if unavailable. Learn more. C	X Skip if unavailable		
Search Sessions Spaces Advanced Settings	Save Cancel	Show reque	est	

## Step 5. Define Auto-Follow Patterns in Site 1

Since indices are dynamically created in Site 2, you must configure auto-follow pattern in Site 1 to enable the dynamically generated indices in Site 2 to be replicated to Site 1.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.
- 3. Define Auto-Follow patterns for fortisiem-event-\* time-series indices. Do NOT make similar definitions for other indices.



The screenshot here shows that an auto-follow pattern has been created for for fortisiem-event-\* time-series indices.

🖻 elastic							
Stack Management / Cross-Cluster Re	eplication						
③ To visualize and explore data in Kibana, year and the second	ou must create an index pattern to retrieve	data from Elasticsear	ch.				
gest 💿							
gest Node Pipelines	Cross-Clus	ter Replic	ation				
eats Central Management							
ata 💿	Follower indices	uto-follow patterns					
dex Management	An auto-follow pattern	anlicates leader ind	ices from a remote clust	er and copies them to fo	lower indices on the		
dex Lifecycle Policies	local cluster.	epiloates leader ind	icea nom a remote cidat	er and copies them to to	iower indices on the	Create an auto-fo	llow pattern
apshot and Restore							
llup Jobs	Q Search						
ansforms							
ross-Cluster Replication	Name 🛧	Status	Remote cluster	Leader patterns	Follower index prefix	Follower index suffix	Actions
mote clusters	fortisiem-						
	event_auto_follow_p	att • Active	site2	fortisiem-event-*	copy-		101
erts and Insights ③			1				
rts and Actions	Rows per page: 20 😒						< 1 >
porting							
itcher							

When completed, Elasticsearch on Site 1 is now ready for replication.

## Step 6. Define Remote Clusters for Site 2

Since Site 2 will initiate the replication, the Site 1 nodes must be defined in Site 2 using Kibana.

**Note**: Do not add the master dedicated node to seeds. This is because dedicated master nodes are never selected as gateway nodes. It is recommended that at least three nodes with low traffic, node.remote\_cluster\_client enabled, and transport port opened be added in the list of seed nodes, such as the coordinator node.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Remote Clusters.

😔 elastic	Q Search Elastic	٩	æ
E D Stack Manageme	nt / Remote Clusters		
Help us improve the Elast To learn about how usage da Dismiss	ic Stack Ita helps us manage and improve our products and services, see our Privacy Statement 🗷. To stop collection, disable usage data here.		
Ingest ③			
Ingest Node Pipelines Beats Central Management	502		
Data ①	Add your first remote cluster		
Index Management Index Lifecycle Policies Snapshot and Restore	Remote clusters create a uni-directional connection from your local cluster to other clusters.		
Rollup Jobs Transforms Cross-Cluster Replication	⊕ Add a remote cluster		
Remote Clusters			
Alerts and Insights ①			
Rules and Connectors Reporting Machine Learning Jobs Watcher			

3. Add Site 1's nodes as the remote servers to Site 2. After adding the Site 1's nodes, click Save.

Ingest ③			
Ingest Node Pipelines Beats Central Management	Add remote cluster		Remote cluster docs
	Add a remote cluster that connects to seed nodes or to a single proxy ad	dress.	
Data ⑦ Index Management Index Lifecycle Policies	Name A unique name for the cluster.	Name site1	
Snapshot and Restore		Must contain only letters, numbers, underscores, and d	lashes.
Rollup Jobs			
Transforms	Connection mode		
Cross-Cluster Replication		Seed nodes	
Remote Clusters	Use seed nodes by default, or switch to proxy mode.	172.30.58.120:9300 × 172.30.58.121:9300 ×	0
Alerts and Insights ⑦	X Use proxy mode	172.30.58.122:9300 ×	Ŭ
Rules and Connectors		An IP address or host name, followed by the transport multiple seed nodes so discovery doesn't fail if a node	
Reporting			is unavaliable.
Machine Learning Jobs		Node connections	
Watcher		3	
		The number of gateway nodes to connect to for this cl	uster.
Kibana 💿			
Index Patterns	Make remote cluster optional		
Saved Objects	If any of the remote clusters are unavailable, the query request fails. To avoid	Skip if unavailable	
Tags	this and continue to send requests to other clusters, enable Skip if		
Search Sessions	unavailable. Learn more. 🖄		
Spaces Advanced Settings	✓ Save Cancel		Show request
Stack @			

## Step 7. Define Auto-Follow Patterns in Site 2

Since indices are dynamically created in Site 1, you must configure auto-follow pattern in Site 2 to enable the dynamically generated indices in Site 1 to be replicated to Site 2.

Take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.
- 3. Define Auto-Follow patterns for fortisiem-event-\* time-series indices. Do NOT make similar definitions for other indices. The example screenshot here shows the fortisiem-event.auto\_follow\_pattern being defined.

🤣 elastic						0 6
E Stack Management / C	cross-Cluster Replicat / Add					
Help us improve the Elastic Star To learn about how usage data hel Dismiss		services, see our Privacy Statement (3. To stop	o collection, dis	able usage data here.		
Ingest ① Ingest Node Pipelines Beats Central Management	Add auto-follow p	pattern			Auto-foll	low pattern docs
Data ③ Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs Transforms <u>Cross-Cluster Replication</u> Remote Clusters	Name A unique name for the auto-follow pattern Remote cluster The remote cluster to replicate leader ind		Name fortisiem-ev Remote cluster site1 (+) Add remo	vent_auto_follow_pattern		~
Alerts and Insights ① Alerts and Actions Reporting Machine Learning Jobs Watcher	Leader indices One or more index patterns that identify t remote cluster. As new indices matching i replicated to follower indices on the local Note: Indices that already exist are not re	these patterns are created, they are cluster.	Index patterns fortislem-eve Spaces and the	ent-* × characters \/?* <>   are not allow	ved.	٥
Kibana ① Index Patterns Saved Objects Tags Search Sessions Spaces Advanced Settings Stack ① License Management 8.0 Upgrade Assistant	Follower indices (optional) A custom prefix or suffix to apply to the n more easily identify replicated indices. By as the leader index.	ames of the follower indices so you can default, a follower index has the same name	H Index r The above • copy-fo • copy-fo	characters \/?, * <>   * are not al name examples settings will generate index n rtfslem-event-2021-08-26 rrfislem-event-2021-08-28		
	Create Cancel					Show request

The screenshot here shows that auto-follow patterns have been created for fortisiem-event-\* time-series indices.

Stack Management / Cross-Cluste	ter Replication	
Ingest @		
Ingest Node Pipelines	Cross-Cluster Replication	
Data 💿	Follower indices Auto-follow patterns	
Index Management		
	An auto-follow pattern replicates leader indices from a remote cluster and copies them to follower indices on the	a constant a sub-
ndex Lifecycle Policies	An auto-follow pattern replicates leader indices norm a remote cluster and copies them to follower indices on the	ow pattern
	An auto-rollow pattern replicates leader indices from a remote cluster and copies them to follower indices on the local cluster.	ow pattern
Snapshot and Restore	local cluster.	ow pattern
Snapshot and Restore Rollup Jobs Transforms		ow pattern
Snapshot and Restore Rollup Jobs Transforms Cross-Cluster Replication	local cluster.	ow pattern
Snapshot and Restore Rollup Jobs Transforms Cross-Cluster Replication	local cluster.	ow pattern Action
Index Lifecycle Policies Snapshot and Restore Rollup Jobs Transforms Cross-Cluster Replication Remote Clusters Alerts and Insights ①	Q Search	2010
Snapshot and Restore Rollup Jobs Transforms Cross-Cluster Replication Remote Clusters	Iocal cluster.     Iocal cluster.       Q. Search       Name ↑       Status       Remote cluster       Leader patterns       Follower index prefix       Follower index suffix	Action

When completed, Elasticsearch on Site 2 is now ready for replication.

## Step 8. Set Up Site 2 FortiSIEM with Elasticsearch Storage

Take the following steps to set up Site 2 FortiSIEM with Elasticsearch as its online storage.

- 1. Login to the FortiSIEM GUI.
- 2. Navigate to ADMIN > Setup > Storage > Online.
- 3. Select the **Elasticsearch** radio button from the three available options (Local Disk, NFS, Elasticsearch) and configure.
- 4. Click Save.

#### Step 9. Set Up Disaster Recovery

See Configuring Disaster Recovery in the latest Disaster Recovery Procedures - EventDB Guide here.

## Step 10. Verify Site 1 to Site 2 Event Replication

Take the following steps to check on Elasticsearch event replication.

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.

3. Verify that the follower indices are created automatically.

윶 elastic		ର୍ Search Elastic			
Stack Management Cross-Cluster	Replication				
ngest ()					
ngest Node Pipelines	Cross-Cluster Rep	olication			
Beats Central Management					
Data ®	Follower indices Auto-follow pa	tterns			
ndex Management	A follower index replicates a leader in	dex on a remote cluste	r.		
ndex Lifecycle Policies				Create a follo	wer index
napshot and Restore	Q Search				
Rollup Jobs Transforms	C. GROWNIN				
ransforms Cross-Cluster Replication	Name 1	Status	Remote cluster	Leader index	Actions
temote Clusters	copy-fortisiem-event-2021.09.20-1	Active	site1	fortisiem-event-2021.09.20-1	
lerts and Insights ①	C copy-fortisiem-event-2021.09.22-	Active	site1	fortisiem-event-2021.09.22-1-000	
lerts and Actions	copy-fortisiem-event-2021.09.22-				
eporting	3-000001	<ul> <li>Active</li> </ul>	site1	fortisiem-event-2021.09.22-3-000	
Vatcher	Rows per page: 20 ~				< 1 )

#### Step 11. Verify ILM is Working for Follower Index in Site 2

To verify that index lifecycle management (ILM) is working on site 2, you will need to take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.
- 3. Under Indices, select one follower event index and under Index lifecycle management, check Lifecycle policy. It should be fsiem\_ilm\_policy.

😔 elastic	C. Search Elastic				0
E Stack Management / Index Manage	ment				
ngest ⑦ ngest Node Pipelines Gentral Management	Index Management	Summary Settin	n-event-2021.09.22 gs Mappings Stats E	-1-000001 Fellower	
Data 🗇	Indices Data Streams Index Templates Component	General			
ndex Management ndex Lifecycle Policies	Update your Elasticsearch indices individually or in bulk. Lean		• green	Status	open
inapshot and Restore	Q copy	Primaries	1	Replicas	0
ollup Jobs ansforms		Docs Count	1808748	Docs Deleted	
ross-Cluster Replication	Name Health St	Charles Class	533mb	Primary Storage Size	
emote Clusters	copy-fortisiem-event-2021.09.22-1-000 001 • green op Fotower	Storage Size	fortisiem-event-2021.0		
lerts and insights 💿			1		
ilerts and Actions leporting	copy-fortisiem-event-2021.09.22-3-000 001 • green op Fotower				
Vatcher	copy-fortisiem-event-2021.09.20-1 e green or	Index lifecycle ma	fsiem_ilm_policy	Current phase	new
libana 🔿		Current action	complete	Current action time	2021-09-22 10:00:01
dex Patterns	Rows per page: 10 🗸		compiete		
aved Objects		Failed step		Phase definition	Show definition
igs					
earch Sessions naces					

#### Step 12. Verify Site 2 to Site 1 Event Replication

Take the following steps to check on Elasticsearch event replication.

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.

3. Verify that the follower indices are created automatically.

🔗 elastic		Q Search Elastic					
Stack Management / Cross-Cluster	Replication						
ingest 🔿							
ngest Node Pipelines	Cross-Cluster Reg	Cross-Cluster Replication					
Beats Central Management							
Data ®	Follower indices Auto-follow pa	iterns					
ndex Management	A follower index replicates a leader in	iex on a remote cluste	r.				
ndex Lifecycle Policies				Create a follo	wer index		
napshot and Restore	Q Search						
Rollup Jobs	et morene						
Transforms Cross-Cluster Replication	Name 🛧	Status	Remote cluster	Leader index	Actions		
temote Clusters	copy-fortisiem-event-2021.09.20-1	Active	site1	fortisiem-event-2021.09.20-1			
lerts and insights 💿	Copy-fortisiem-event-2021.09.22- 1-000001	Active	site1	fortisiem-event-2021.09.22-1-000			
lerts and Actions	copy-fortisiem-event-2021.09.22-	Active	site1	fortisiem-event-2021.09.22-3-000			
eporting	3-000001	<ul> <li>Active</li> </ul>	site1	fortisiem-event-2021.09.22*3-000			
latcher	Rows per page: 20 🗸				< 1 >		
bana 🔿							

## Step 13. Verify ILM is Working for Follower Index in Site 1

To verify that index lifecycle management (ILM) is working on site 1, you will need to take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.
- 3. Under Indices, select one follower event index and under Index lifecycle management, check Lifecycle policy. It should be fsiem\_ilm\_policy.

😌 elastic	Q. Search Elastic				
E Stack Management Index Manage	ment				
Ingest @ Ingest Node Pipelines Beats Central Management	Index Management	Summary Settin	n-event-2021.09.22- Igs Mappings Stats Ed	1-000001 Follower It settings	
Data ① Index Management Index Lifecycle Policies Snapshot and Restore	Indices Data Streams Index Templates Compon Update your Elasticsearch indices individually or in bulk. Lean	General Health Primaries	• green	Status Replicas	open 0
Rollup Jobs Transforms Cross-Cluster Replication	Name Health St	Docs Count Storage Size	69728 11.4mb	Docs Deleted Primary Storage Size	
Remote Clusters Alerts and Insights ①	copy-fortisiem-event-2021.09.22-1-000 Patower copy-fortisiem-event-2021.09.22-3-000	Aliases	fortisiem-event-2021.09 1	22-	
Alerts and Actions Reporting Watcher	Copy-fortisiem-event-2021.09.20-3	Index lifecycle ma	nagement		
Kibana ©	Follower op	Lifecycle policy	fsiem_ilm_policy	Current phase	new
index Patterns Saved Objects	copy-fortisiem-event-2021.09.20-1 green op Fotower	Current action Failed step	complete	Current action time Phase definition	2021-09-22 09:53:10 Show definition
Tags Search Sessions	Rows per page; 10 $$	10000000000000			
Spaces					

## Step 14. (Optional) Copy Older Indices from Site 1 to Site 2

Elasticsearch only replicates events after it has been configured. Use Elasticsearch API to copy all *older* indices to Site 2 by taking the following steps.

- 1. Use Kibana to copy older fortisiem-event-\* indices to Site 2.
- 2. Login to Kibana.
- 3. Navigate to Kibana Home > Stack Management > Cross-Cluster Replication > Follower indices.
- 4. In Add follower index, take the following steps:
  - a. Provide the Leader index.
  - b. Provide the Follower index.
  - c. Click Create.

Stack Management / Cross-Cluster Replicat / Add			
Ingest ③ Ingest Node Pipelines Beats Central Management	Add follower index		Follower index docs
Data ⊙ index Management Index Lifecycle Policies Snapshot and Restore	Remote cluster The cluster that contains the index to replicate.	Remote cluster newsite1  Add remote cluster	~
Rollup Jobs Transforms <u>Cross-Cluster Replication</u> Remote Clusters	Leader index The index on the remote cluster to replicate to the follower index. Nete: The leader index must already exist.	teader index fortisiem-event-202110.02-3-000001 Spaces and the characters \ / 7, * < > * are not allowed.	
Alerts and Insights ① Alerts and Actions Reporting Watcher	Follower index A unique name for your index.	Follower index Copy-fortisiem-event-202110.02-3-000001 Spaces and the characters \/7,* <>  * are not allowed.	
Kibana (*) Index Patterns Saved Objects Tags Search Sessions Spaces Advanced Settings	Advanced settings (optional) Advanced settings control the rate of replication. You can customize these settings or use the default values.		
Stack ① License Management 8.0 Upgrade Assistant	✓ Create Cancel		Show request

## Primary (Site 1) Fails, Site 2 Becomes Primary

If Site 1 fails, its Workers no longer function, and events are buffered at the Collectors, which are ready to push these events to Site 2. You must now prepare Elasticsearch on Site 2 to be ready for insertion.

#### Step 1. Switch Site 2 Role to Primary in FortiSIEM

See Switching Primary and Secondary Roles in the latest Disaster Recovery Procedures - EventDB Guide here.

#### Step 2. Save Elasticsearch Settings on Site 2 in FortiSIEM

After the Site 2 Role has been switched to Primary, take the following steps:

**Note**: If you have a custom event template on Site 1, you will need to upload the same custom event template to Site 2 first before proceeding with these instructions.

- 1. Login to the Site 2 FortiSIEM GUI.
- 2. Navigate to ADMIN > Setup > Storage Online.
- 3. Click Test to test the settings.
- 4. Click Save to save the online settings.

FortiSIEM	🙆 DASHBOARD 🖿 ANALYTICS 🌲 INCIDENTS 🗃 CASES 🛢 CMDB 🔛 RESOURCES 🖽 TASKS 🔆 ADMIN 🔞 🛕 💷 🚨 🤇
🗢 Setup	Storage > Online •         Organizations         Credentials         Discovery         Pull Events         Monitor Performance         STM         Maintenance         Windows Agent
Device Support	O Local Disk
Health	O NFS
I License	URL: http://172.30.58.128 + -
🕫 Settings	Port: 9200 0
	ES Service Type: () Native O Amazon O Elastic Cloud
	User Name: (Optional)
	Password: (Optional)
	Confirm Password: (Optional)
	Shard Allocation: O Fixed O Dynamic
	Starting Shards: 1 0
	Replicas: 0 0
	Per Org Index 🖌
	Event Attribute O Default O Custom 10attributes.csv Select
	Test Save Cancel

#### Step 3. Confirm Events are Inserted to Site 2

At this point, Collectors should be communicating to the Site 2 Supervisor, and would get a set of Site 2 Event (Upload) Workers. Since Site 2 Workers are connected to the Site 2 Elasticsearch Cluster, events are now stored in the Site 2 Elasticsearch. You can verify this by running queries from the Site 2 Supervisor's **ANALYTICS** page.

#### Step 4. Confirm Incident Index is Created and Updated to Site 2

To verify that the Incident index in Elasticsearch Site 2 has be created and updated, take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.

3. Find the incident index, and compare the Incident counts between Elasticsearch Site 1 and Elasticsearch Site 2.

😌 elastic						
E Stack Management / Index Manager	nent				4	
Ingest @ Ingest Node Pipelines Beats Central Management	Index Management	ompone	fortisiem-incid	lent-2021.09 <sub>ps Mappings Stats</sub>	Edit settings	
Data ① Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs	Update your Elasticsearch indices individually or in bu		General Health Primaries	• green 5	Status Replicas Docs Deleted	open 0
Transforms Cross-Cluster Replication Remote Clusters	Name Health     fortisiem-incident-2021.09     e green Rows per page: 10 ~	su	Docs Count Storage Size Aliases	63 1mb none	Docs Deleted Primary Storage Size	
Alerts and Actions Reporting Watcher						
Kibana © Index Patterns Swed Objects Tags Search Sessions Spaces Advanced Settings						
Stack @ License Management 8.0 Upgrade Assistant						in Mana

#### Step 5. Confirm Lookup Index is Updated to Site 2

To verify that the fortisiem-lookups index in Elasticsearch Site2 has be updated, take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.
- **3.** Find the fortisiem-lookup index, and compare the document counts between Elasticsearch Site 1 and Elasticsearch Site 2.

😔 elastic		C. Search Elastic					9
Stack Management / Index Manage	ment				_		
Ingest ⊙ Ingest Node Pipelines Beats Central Management Data ⊙	Index Manageme	Nt Templates Compone		okups-v2 tings Mappings	Stats Ed	lit settings	
Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs	Update your Elasticsearch indices ind Q. tookup	dividually or in bulk. Lear	General Health Primaries	• green		Status Replicas	open 0
Transforms Cross-Cluster Replication Remote Clusters	Name fortisiem-cmdb-lookups-v2	Health St • green op	Docs Count Storage Size Aliases	5316 14.6mb none		Docs Deleted Primary Storage Size	•
Alerts and Insights @ Alerts and Actions Reporting Watcher	C fortislem-lookups-v2 Rows per page: 10 ∨	• green op	Alleges	1010			
Kibana © Index Patterns Saved Objects Tags Sarch Sessions Spaces Advanced Settings							
Stack ① License Management 8.0 Upgrade Assistant							~ M

## Site 1 is Up and Becomes Primary

#### **Overview**

If Site 1 comes back up, you can set it to become Primary by following these general steps:

- 1. Set Site 1 to Secondary and confirm data from Site 2 is replicated to Site 1.
- 2. Stop Collectors from sending events to Site 2.
- 3. Switch Site 1 Role to Primary in FortiSIEM.

#### 4. Miscellaneous:

- Save Elasticsearch Settings on Site 1 in FortiSIEM
- Verify All Event Workers are Added to Site 1
- Verify Events are Being Written into Site 1
- Confirm Incident Index is Re-Created and Updated to Site 1
- Confirm Lookup Index is Updated to Site 1
- Verify Events are being Replicated to Site 2

## Step 1. Set Site 1 to Secondary and Confirm Data from Site 2 is Replicated to Site 1

The Site 1 CMDB must sync up with the Site 2 CMDB, since new devices, rules, reports, etc. may exist in Site 2. Hence Site 1 needs to be Secondary first.

- 1. Set Site 1 to Secondary in FortiSIEM by taking the following steps:
  - **a.** Login to the Site 2 FortiSIEM GUI.
  - **b.** Navigate to **ADMIN > License > Nodes**.
  - c. Verify that there is a Secondary Node entry for Site 1, and it shows Inactive under Replication status.
  - d. With Site 1 selected, click Edit, and double check that the information is correct.
  - e. Click Save.

At this point, Site 1 is now Secondary.

- 2. Make sure all information is correct by taking the following steps:
  - a. Login to the Site 1 GUI, and check the new devices, rules, and reports, ensuring that they are updated.
  - b. Compare the data on Site 1 and Site 2. All indices, and document numbers should be identical.

#### Step 2. Stop Collectors from Sending Events to Site 2

After following step 1, you will need to stop the Collectors from sending events to Site 2. To do this, take the following steps:

- 1. Login to the Site 2 GUI.
- 2. Navigate to ADMIN > Settings > System > Event Worker.
- 3. Remove all the Event Workers.
- 4. Click Save.

Collectors will now start buffering events.

## Step 3. Switch Site 1 Role to Primary in FortiSIEM

See Switching Primary and Secondary Roles in the latest Disaster Recovery Procedures - EventDB Guide here.

#### Step 4. Save Elasticsearch Settings on Site 1 in FortiSIEM

Save the Site 1 Elasticsearch settings by taking the following steps.

**Note**: If you have a custom event template in Site 2, you must upload the same custom event template in Site 1 first before proceeding with these instructions.

- 1. Login to FortiSIEM Site 1 GUI.
- 2. Navigate to ADMIN > Setup > Storage > Online.
- 3. Click **Test** to verify your settings.
- 4. Click Save.

#### Step 5. Verify All Event Workers are Added to Site 1

Verify that all event workers are added to Site 1 by taking the following steps.

- 1. Login to FortiSIEM Site 1 GUI.
- 2. Navigate to ADMIN > Settings > System > Event Worker.
- 3. Verify all event workers are added to the Event Worker list.

All Collectors will now send events to Site 1.

#### Step 6. Verify Events are Being Written into Site 1

Verify that events are being written into Site 1 by taking the following steps.

- 1. Login to FortiSIEM Site 1 GUI.
- 2. Navigate to ANALYTICS.

3. Run some queries and make sure events are coming in.

Actions 👻 🗄 [1] Rat	w Messages								
😂 🗸 Edit Filters and Tim	e Range		® • I≣ • Q Run			Indica	tor Chart for COUNT(M	tched Events) 🕶	lin. v
			Raw Messages	- Last 10 Minutes			1	im 1h 1d 7d 30	30d 12
20000 - 15000 - 5000 - 0 - Aug 119, 21	21 11:37	9 Vilay	1120 1121	via	120	1124	11/23	11/26	
Show Event Type	Wrap Raw Events						₩ ≪ 1/3	138 62,754	> н
Event Receive Time	Reporting IP	Event Name		Raw Event Log					
Aug 11 2021, 11:25:45 AM	172.30.58.60	Successful SSH lo	gon	<86>Aug 11 11:25:45 sp5860 :	sshd[60378]: Accepted publickey	for admin from 172.30.58	.62 port 50014 ssh2: RSA !	HA256:IZITqq9TK	(Ym3
Aug 11 2021, 11:25:45 AM	172.30.58.60	SSH session starte	ed	<86>Aug 11 11:25:45 sp5860	sshd[60378]: pam_unix(sshd:ses	ion): session opened for u	ser admin by (uid=0)		
Aug 11 2021, 11:25:44 AM	172.30.58.60	Successful SSH lo	gon	<86>Aug 11 11:25:44 sp5860	sshd[60209]: Accepted publicke	for admin from 172.30.58	.62 port 49998 ssh2: RSA !	HA256:IZITqq9TK	{Ym3
Aug 11 2021, 11:25:44 AM	172.30.58.60	Generic_Unix_ssh	d_Generic	<86>Aug 11 11:25:44 sp5860 :	sshd[60214]: Received disconner	t from 172.30.58.62 port	19998:11: disconnected by	user	
Aug 11 2021, 11:25:44 AM	172.30.58.60	Generic_Unix_ssh	d_Generic	<86>Aug 11 11:25:44 sp5860	sshd[60214]: Disconnected from	user admin 172.30.58.62 p	ort 49998		
Aug 11 2021, 11:25:41 AM	172.30.58.60	Successful SSH lo	gon	<86>Aug 11 11:25:41 sp5860 :	sshd[60037]: Accepted publicke	for admin from 172.30.58	.62 port 49964 ssh2: RSA !	HA256:IZITqq9TK	{Ym3
Aug 11 2021, 11:25:41 AM	172.30.58.60	SSH session starte	ed.	<86>Aug 11 11:25:41 sp5860	sshd[60035]: pam_unix(sshd:ses	ion): session opened for u	ser admin by (uid=0)		
Aug 11 2021, 11:25:41 AM	172.30.58.60	SSH session starte	ed	<86>Aug 11 11:25:41 sp5860 :	sshd[60037]: pam_unix(sshd:ses	ion): session opened for u	ser admin by (uid=0)		
Aug 11 2021, 11:25:36 AM	172.30.56.212	System uptime fo	r a device	[PH_DEV_MON_SYS_UPTIME]:	[eventSeverity]=PHL_INFO,[fileN	ame]=phPerfJob.cpp,[line	Number]=1129,[hostName]	-cuiping-win2016	à,[ha
			c debug message		phMonitorSupervisor[53839]: Per				

## Step 7. Confirm Incident Index is Re-Created and Updated to Site 1

To verify that the Incident index in Elasticsearch Site1 has be created and updated, take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.
- 3. Find the incident index, and compare the Incident counts between Elasticsearch Site 1 and Elasticsearch Site 2.

😵 elastic			
E Stack Management / Index Mana	igement.		
Ingest @ Ingest Node Pipelines Beats Central Management	Index Management	fortisiem-incident-2021.09 Summary Settings Mappings Stats	Edit settings
Data © Index Management Index Lifecycle Policies Snapshot and Restore Rolwa Jobs Transforms Cross-Cluster Replication Remote Clusters Alerts and Insights ©	Indices Data Streams Index Templates Compone Update your Elasticsearch indices individually or in bulk. Learn Q incide Name Health Sta fortisiem-incident-2021.09 • green op Rows per page: 10 ~	General Health • green Primaries 5 Docs Count 63 Storage Size 1mb Aliases none	Status open Replicas 0 Docs Deleted Primary Storage Size
Alerts and Actions Reporting Watcher Kibana © Index Patterns Swed Objects Tags			
Search Sessions Socies Advanced Settings Stack © License Management 8.0 Upgrade Assistant			∽ Manag

## Step 8. Confirm Lookup Index is Updated to Site 1

To verify that the fortisiem-lookups index in Elasticsearch Site1 has be updated, take the following steps:

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Index Management.
- **3.** Find the fortisiem-lookup index, and compare the document counts between Elasticsearch Site 1 and Elasticsearch Site 2.

😔 elastic	Q: Search Elestic		0
Stack Management / Index Manage	ment		
Ingest © Ingest Node Pipelines Boats Central Management Data ©	Index Management		Stats Edit settings
Index Management Index Lifecycle Policies Snapshot and Restore Rollup Jobs	Update your Elasticsearch indices individually or in bulk. Lear	General Health • green Primaries 1	Status open Replicas O
Transforms Cross-Cluster Replication Remote Clusters	Name Health St fortisiem-cmdb-lookups-v2 eigreen on	Docs Count 5316 Storage Size 14.6mb Aliases none	Docs Deleted Primary Storage Size
Alerts and Insights ① Alerts and Actions Reporting Watcher	☐ fortisilem-tookups-v2		
Kibana ① Index Patterns Saved Objects Tags Search Sessions Spaces Advanced Settings			
Stack © License Management 8.0 Upgrade Assistant			in Man

#### Step 9. Verify Events are Being Replicated to Site 2

Take the following steps to check on Elasticsearch event replication.

- 1. Login to Kibana.
- 2. Navigate to Kibana Home > Analytics section > Discover > Cross-Cluster Replication.
- 3. Verify that the follower indices are created automatically.

😽 elastic									
Stack Management / Cross-Cluster R	Replication								
Ingest ①									
Ingest Node Pipelines	Cross-Cluster Re	Cross-Cluster Replication							
Data 🕐	Follower indices Auto-follow	Follower indices Auto-follow patterns							
ndex Management									
ndex Lifecycle Policies	A follower index replicates a leader index on a remote cluster.								
Snapshot and Restore					ner moex				
Snapshot and Restore Rollup Jobs	O Search				Her muck				
Snapshot and Restore Rollup Jobs Transforms	Q Search				Well Index				
Snapshot and Restore Rollup Jobs Transforms Cross-Cluster Replication		1							
inapshot and Restore Rollup Jobs Iransforms 2ross-Cluster Replication	Q. Search Name ↑	Status	Remote cluster	Leader index	Actions				
inapshot and Restore lollup Jobs ransforms ross-Cluater Replication lemote Clusters		1	Remote cluster site1						
inapshot and Restore kollup Jobs iransforms pross-Cluster Replication Remote Clusters Nerts and Insights ① Vierts and Actions	Name ↑ fortisiem-event-2021.08.10-1-	Status		Leader index	Actions				
Snapshot and Restore Rollup Jobs Transforms Remote Clusters Alerts and Insights ① Alerts and Actions Reporting	Name ↑           fortisiem-event-2021.08.10-1-           oocooo1	Status • Active • Active	site1	Leader index fortisiem-event-2021.08.10-1-000 fortisiem-event-2021.08.10-3-000	Actions 				
inapshot and Restore lollup Jobs ransforms erross-Cluster Replication lemote Clusters Verts and Insights ① Juerts and Actions	Name ↑           fortisiem-event-2021,08.10-1-           o00001           fortisiem-event-2021,08.10-3-	Status Active	site1	Leader Index fortisiem-event-2021.08.10-1-000	Actions				

## **Viewing Replication Health**

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

## **Implementation Notes**

#### **Changing Index Lifecycle Management Parameters on Primary**

When replication is occurring, if you change the Index Lifecycle Management (ILM) age or hot/warm/cold thresholds on Primary, you will need to restart phDataPurger on Secondary. The restart is necessary to enable phDataPurger on Secondary to read the new changes.

#### Circuit\_Breaking\_Exception in Elasticsearch

Enabling Cross-Cluster Replication (CCR) may affect the heap memory usage of Elasticsearch. If you encounter a request circuit\_breaking\_exception in Elasticsearch, please try the following solutions to fix the issue:

1. 1. Increase "indices.breaker.request.limit" from its default 60% to 85%. It can be hard coded in elasticsearch.yml or configured dynamically with the command below:

```
curl -X PUT "<Site 1's coordinator ip>:9200/_cluster/settings?pretty" -H 'Content-Type:
application/json' -d'
{
   "persistent" : {
    "indices.breaker.request.limit": "85%"
   }
}
curl -X PUT "<Site 2's coordinator ip>:9200/_cluster/settings?pretty" -H 'Content-Type:
application/json' -d'
{
   "persistent" : {
    "indices.breaker.request.limit": "85%"
   }
}
```

2. Increase Elasticsearch heap size in jvm.options in data nodes, then restart all data nodes.

Circuit Breaker Settings Reference: https://www.elastic.co/guide/en/elasticsearch/reference/7.12/circuit-breaker.html

#### Possible Inconsistent Index State (Follower and Frozen) in Secondary

If Site 1 has cold nodes and Disaster Recovery is enabled, then the Secondary Site 2 may have indices in Follower and Frozen state. This will cause Elasticsearch to throw the following exception: "background management of retention lease

failed while following". An index that is frozen cannot be written into and therefore cannot be in Follower state. Also, the index will likely be in Closed state and hence cannot be queried.

ngest Node Pipelines Beats Central Management	Index Management				Index Management docs				
Data 💿	Indices Data Streams Ind	lex Templates Co	mponent Temp	lates					
ndex Management ndex Lifecycle Policies	Update your Elasticsearch indices	Update your Elasticsearch indices individually or in bulk. Learn more. $\ensuremath{\mathcal{C}}$				X Include rollup indices			
Snapshot and Restore Rollup Jobs	Manage index V Q copy-fortisiem-event-2021.10.09-2004-000001				Lifecycle status $$ Lifecycle phase $$				
Transforms Cross-Cluster Replication	Vame Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream	
Remote Clusters	copy-fortisiem-event-2021.10.09 000001 Frozen Folkower	9-2004- • green	closed	1	0				
Alerts and Insights ①									
	Rows per page: 10 V							< 1 >	

To solve this problem, the user needs to take the following two steps using Kibana.

1. Unfollow the index.

Stack Management / Cross-Cluster Replication						
Ingest © Ingest Node Pipelines Beats Central Management	Cross-Cluster	Replication				
Data ① Index Management	A follower index replicates a leader index on a remote cluster.					
Index Lifecycle Policies Snapshot and Restore Rollup Jobs	Manage follower index $ \sim $	FOLLOWER INDEX OPTIONS	21.10.09-2004-000001		0	
Transforms Cross-Cluster Replication	Name 1	Resume replication	Remote cluster	Leader index	Actions	
Remote Clusters	copy-fortisiem-event-2021. 2004-000001		newsite1	fortisiem-event-2021.10.09-2004		
Alerts and Insights ⑦ Alerts and Actions	Rows per page: 20 $ \smallsetminus $	D Unfollow leader index			< 1 >	
Reporting Watcher						

#### 2. Open the index.

Ingest ① Ingest Node Pipelines Beats Central Management	Index Mar	Index Management						Index Management docs			
Data ① Index Management Index Lifecycle Policies	Update your Elasticse	reams Index Templates	Component Temp		()×	Include rollup in	ndices 🔿 🗙	Include hidden indices			
Snapshot and Restore Rollup Jobs	Manage index $  imes $	INDEX OPTIONS	39-2004-00000	0	Lifecycle statu	s ~ Lifecycle	phase $\checkmark$	C Reload indices			
Transforms Cross-Cluster Replication	Name	Show index settings	Status	Primaries	Replicas	Docs count	Storage size	e Data stream			
Remote Clusters Alerts and Insights ③	Copy-fortisiem-ev 000001 Frozen	Show index mapping Edit index settings	closed	1	0						
Alerts and Actions	Rows per page: 10 $\sim$	Open index						< 1 >			
Reporting Watcher		Delete index Add lifecycle policy									
Kibana 💿		Add inecycle policy	_								



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.