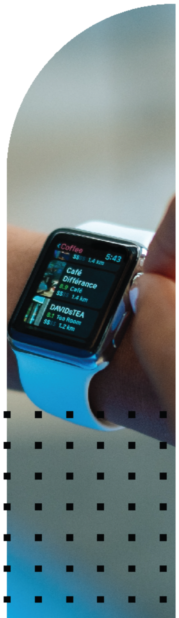
Disaster Recovery Procedures - Bi-Directional Elasticsearch

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

01/12/2023
FortiSIEM 6.4.0 Disaster Recovery Procedures - Bi-Directional Elasticsearch

TABLE OF CONTENTS

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 https://www.elastic.co/guide/en/elasticsearch/reference/7.12/xpack-ccr.html).

- 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

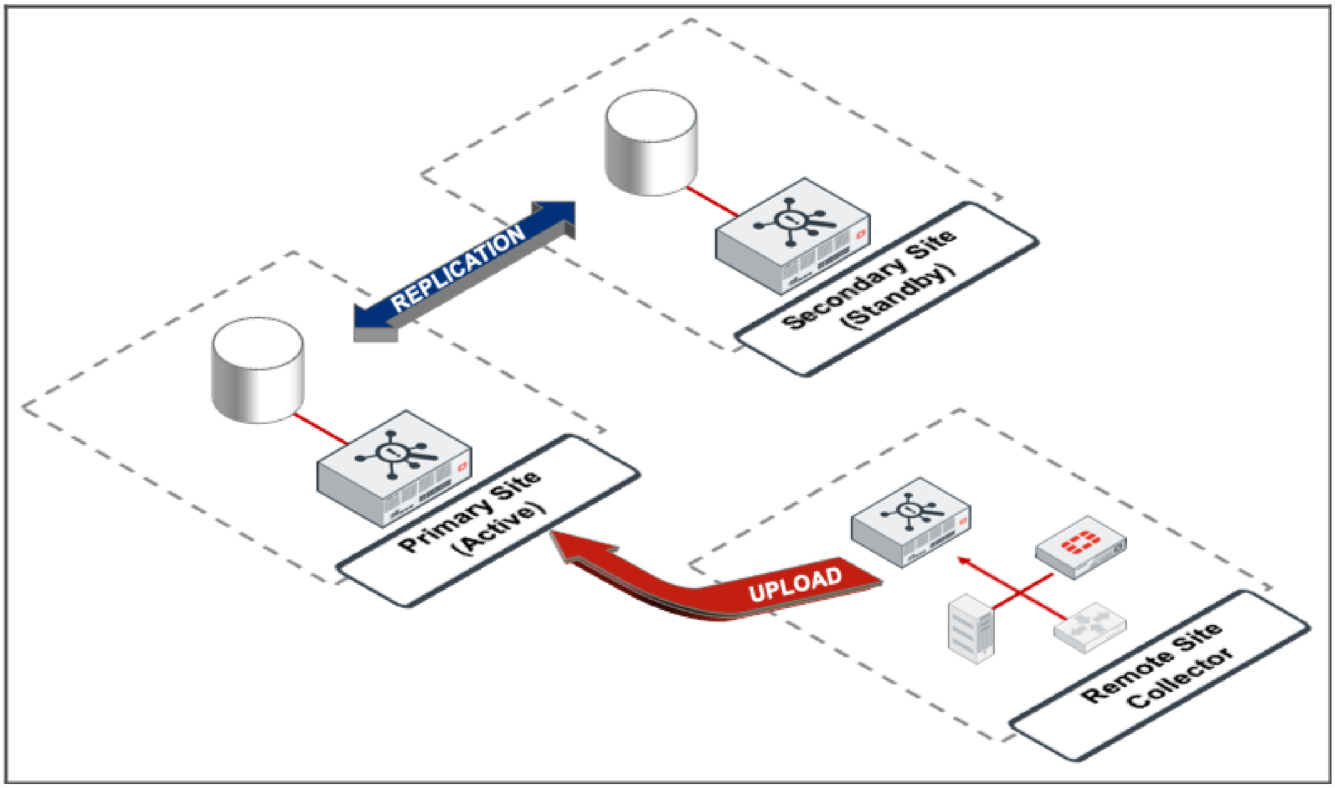
Introduction

- 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.

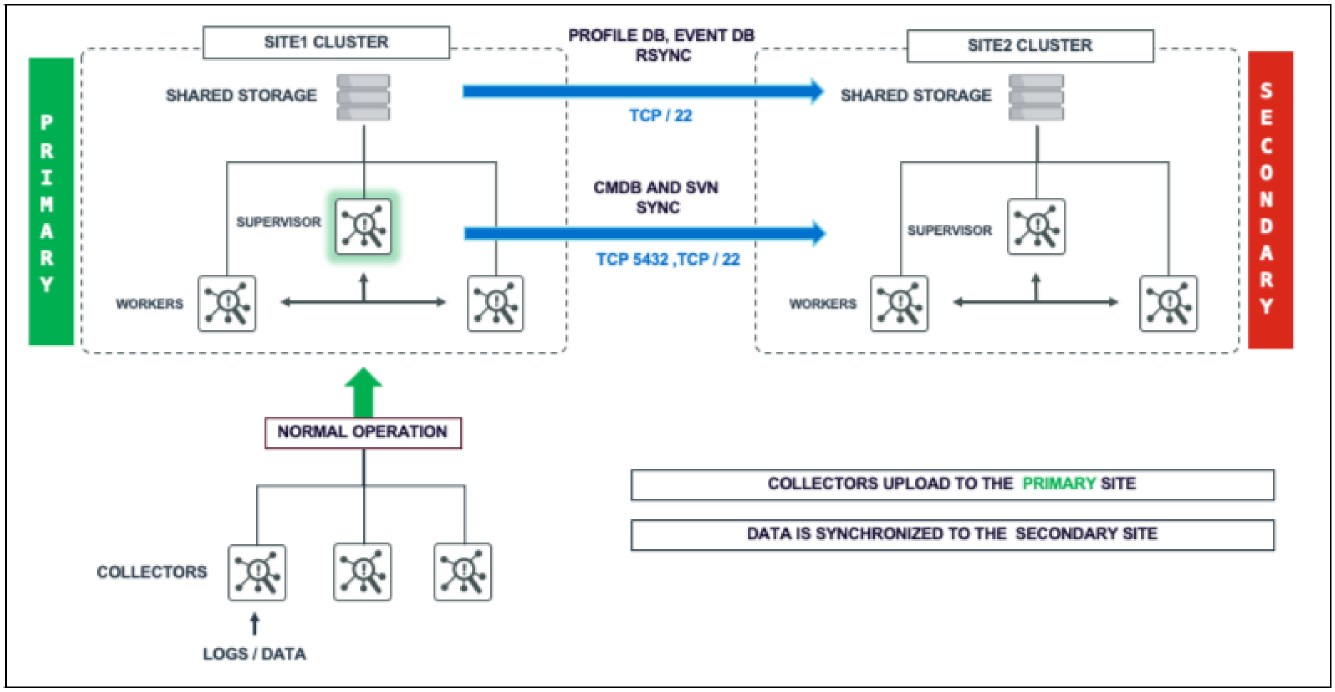


Under normal operations, if collectors are being used, these upload to Site 1, the Primary site and will buffer by design when this site is not available. If DR is set up and a disaster occurs, then these same collectors will revert to uploading to Site 2, the Secondary site, which will now be designated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

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

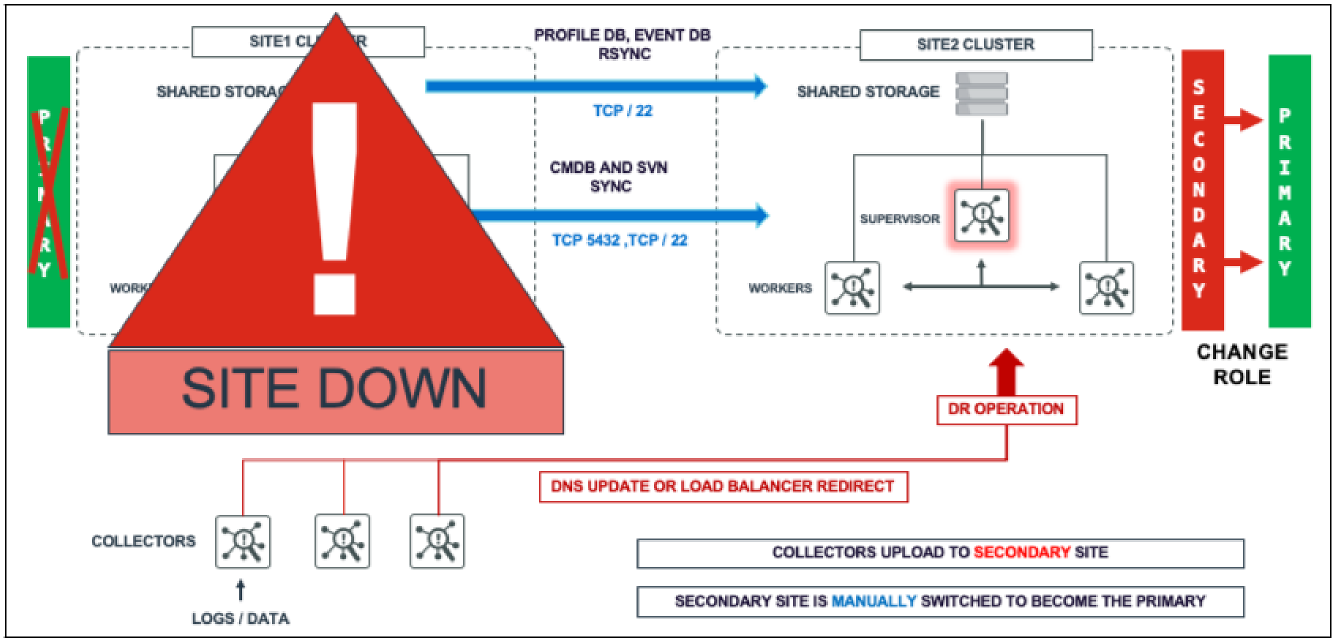
To provide DR features, FortiSIEM must have a Secondary system ready on standby to take over operations, with the following databases replicated from the Primary site:

- 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

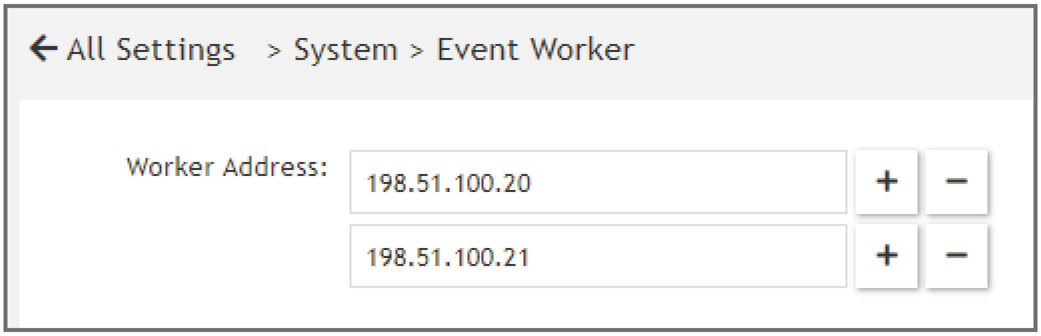
It is important to understand your FortiSIEM environment and plan ahead in terms of communications from users, agents and collectors.

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.

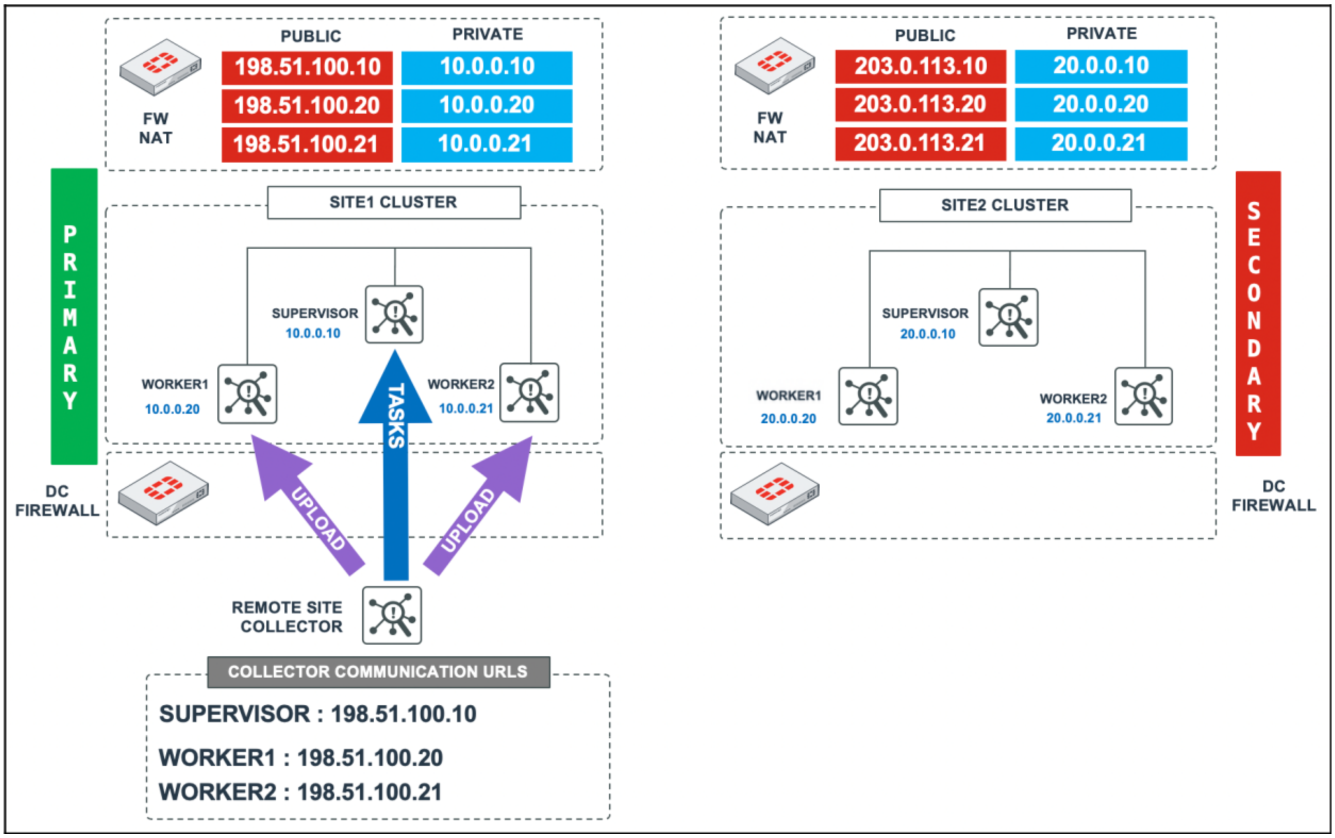


Worker Address: 198.51.100.20
198.51.100.21

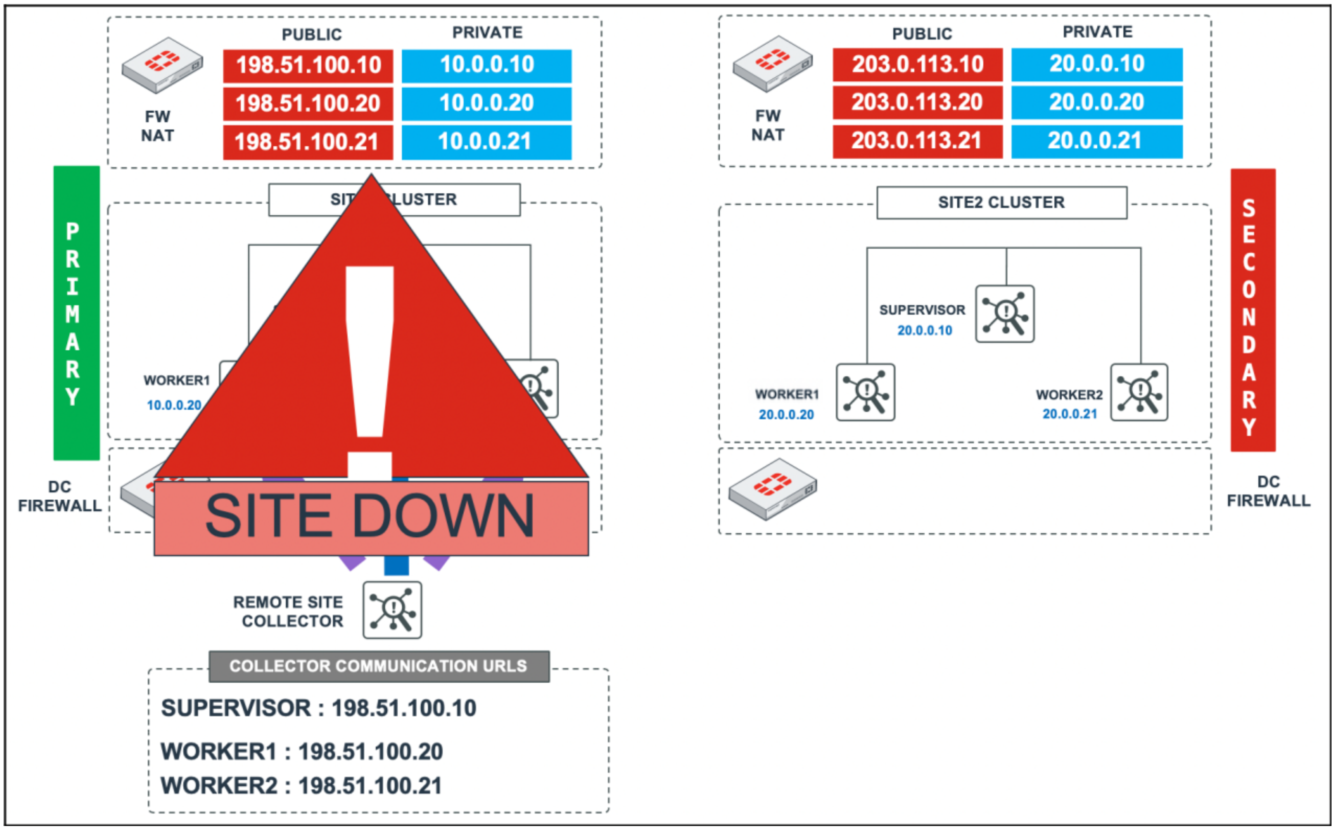
In addition to the Worker Event entries, Collectors also maintain communication with the Supervisor node, to receive jobs/tasks and report Collector health data. When Collectors register for the first time with the Supervisor node, these communication addresses are stored for this purpose.

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.



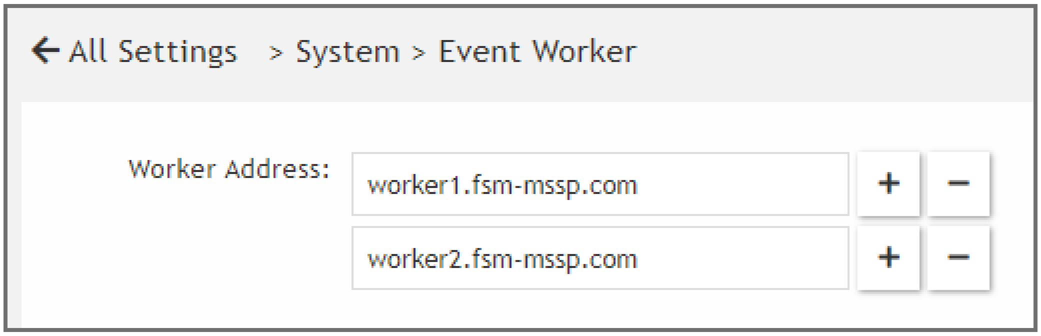
At this point, the Primary node (Site 1) is unavailable. The remote Collector nodes are essentially hard-coded (by IP) to talk to the Primary site only. Even if Site 2 (the Secondary node) is up and operational and promoted to be the Primary node, Collectors are unable to upload logs or get any tasks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



Worker Address: worker1.fsm-mssp.com

worker2.fsm-mssp.com

External DNS Example

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

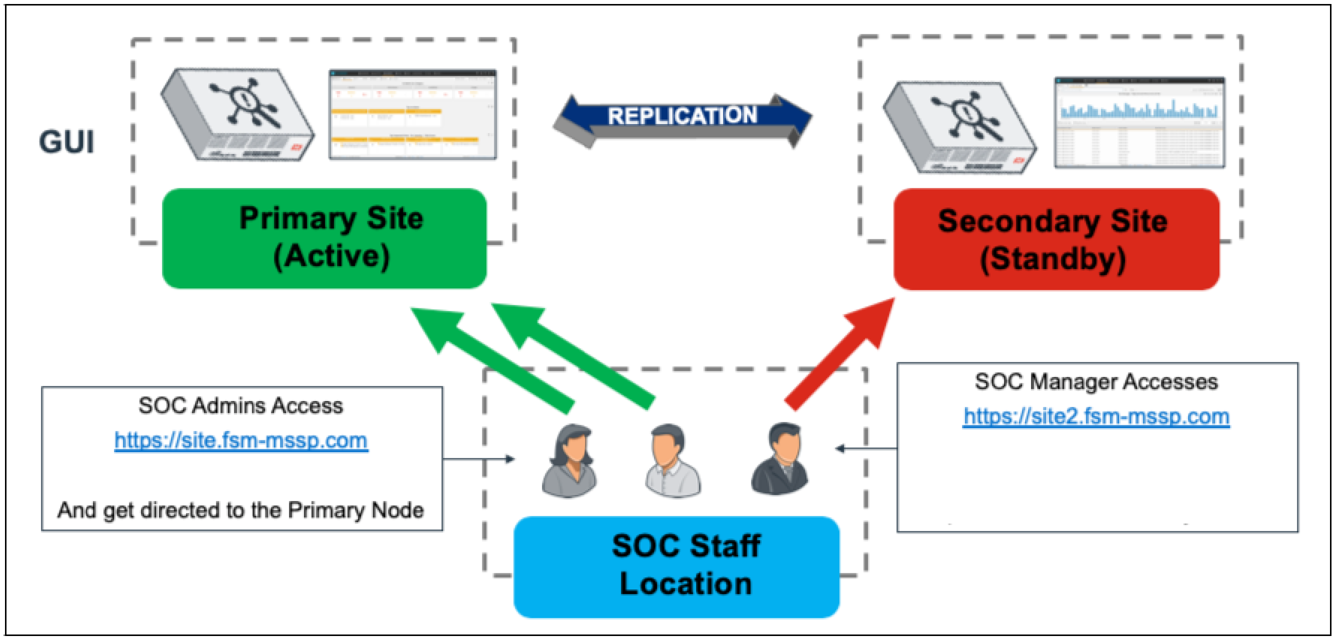
Node	DNS Record Type	Name	IP/Alias
Active Supervisor	CNAME	site.fsm-mssp.com	site1.fsm-mssp.com
Worker1 (Primary)	A	worker1.fsm-mssp.com	198.51.100.20
Worker2 (Primary)	A	worker2.fsm-mssp.com	198.51.100.21

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

Internal DNS Example

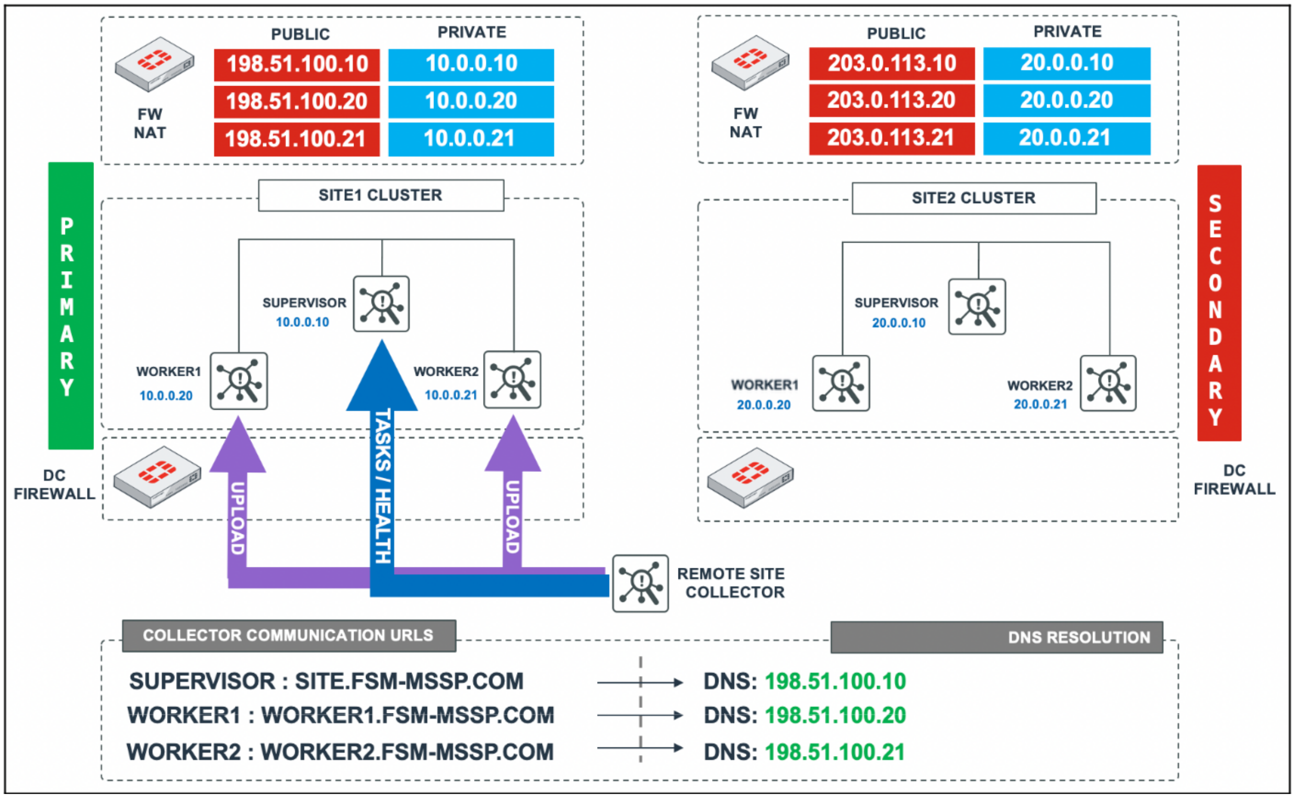
Node	DNS Record Type	Name	IP/Alias
Supervisor (Primary)	A	site1.fsm-mssp.com	10.0.0.10
Supervisor (Secondary)	A	site2.fsm-mssp.com	20.0.0.10
Active Supervisor	CNAME	site.fsm-mssp.com	site1.fsm-mssp.com

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

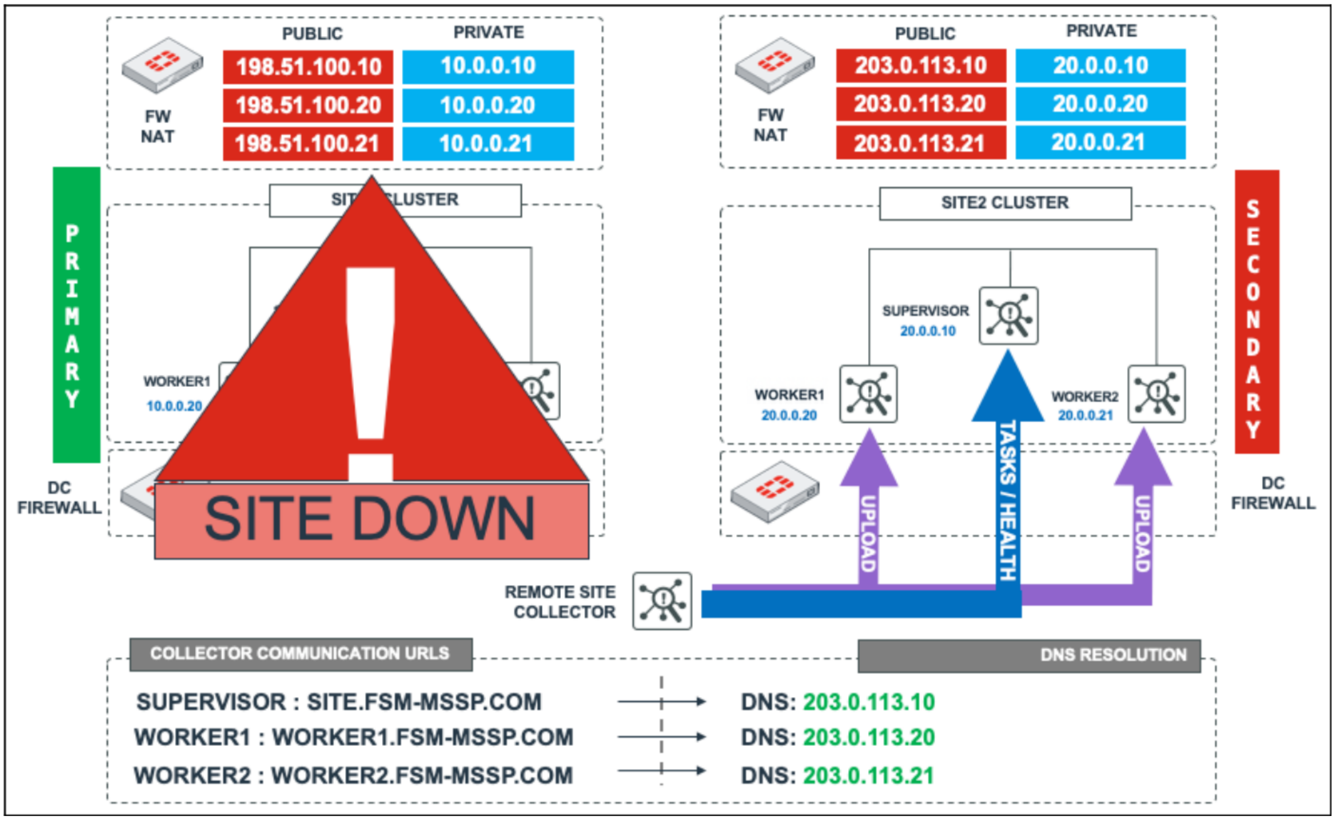


Note: Any DNS changes, are made **manually** in the event of a failover.

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



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



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

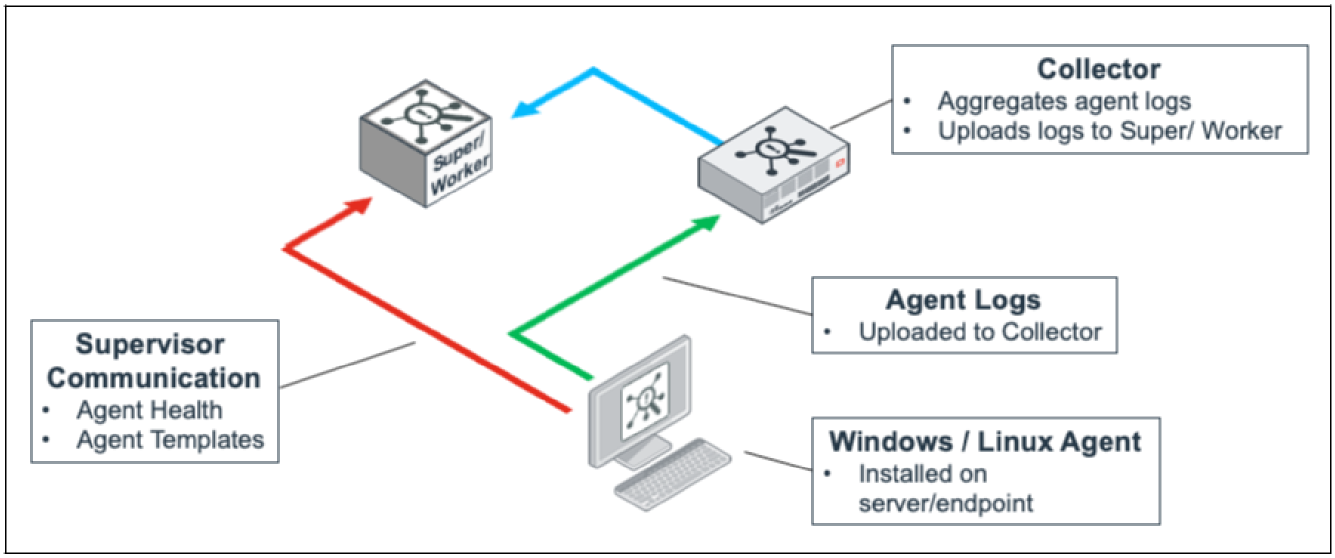
An example using `site.fsm-mssp.com` is shown below. Since Collectors always communicate with the Supervisor node, communications can be easily restored to the Primary via a simple DNS change.

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

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

Agent Communications

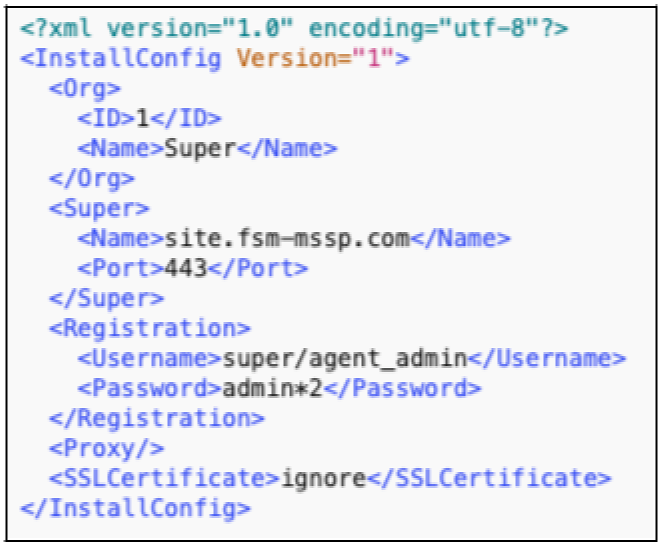
The communications for FortiSIEM Windows and Linux agents follow a similar path to the above. Agents register with the Supervisor node, and maintain this communication to receive updated templates and report health. One or more

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



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

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



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

The same concept also applies to deploying Linux agents.

Configuring Disaster Recovery - 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.
3. 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.

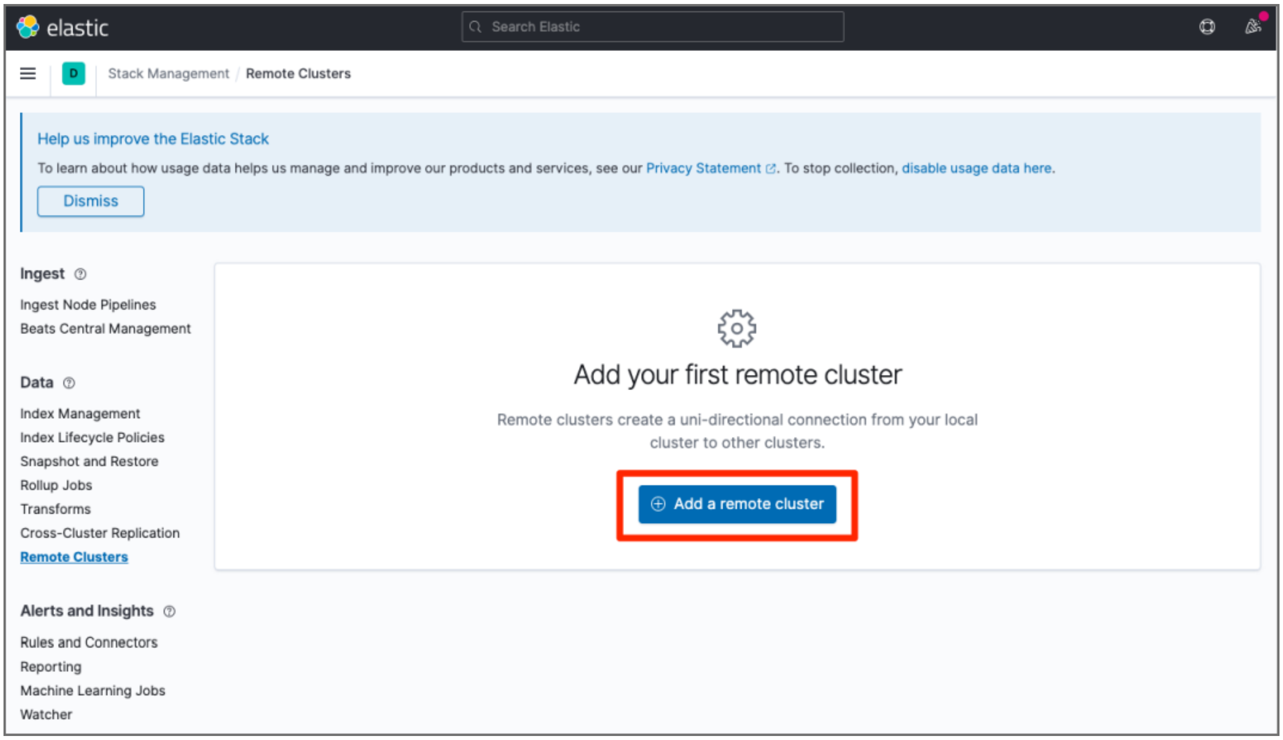
```
PUT /_cluster/settings?pretty
{
  "persistent": {
    "action.auto_create_index": "-fortisiem-event-*,fortisiem-*,.monitoring-*"
  }
}
```

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**.



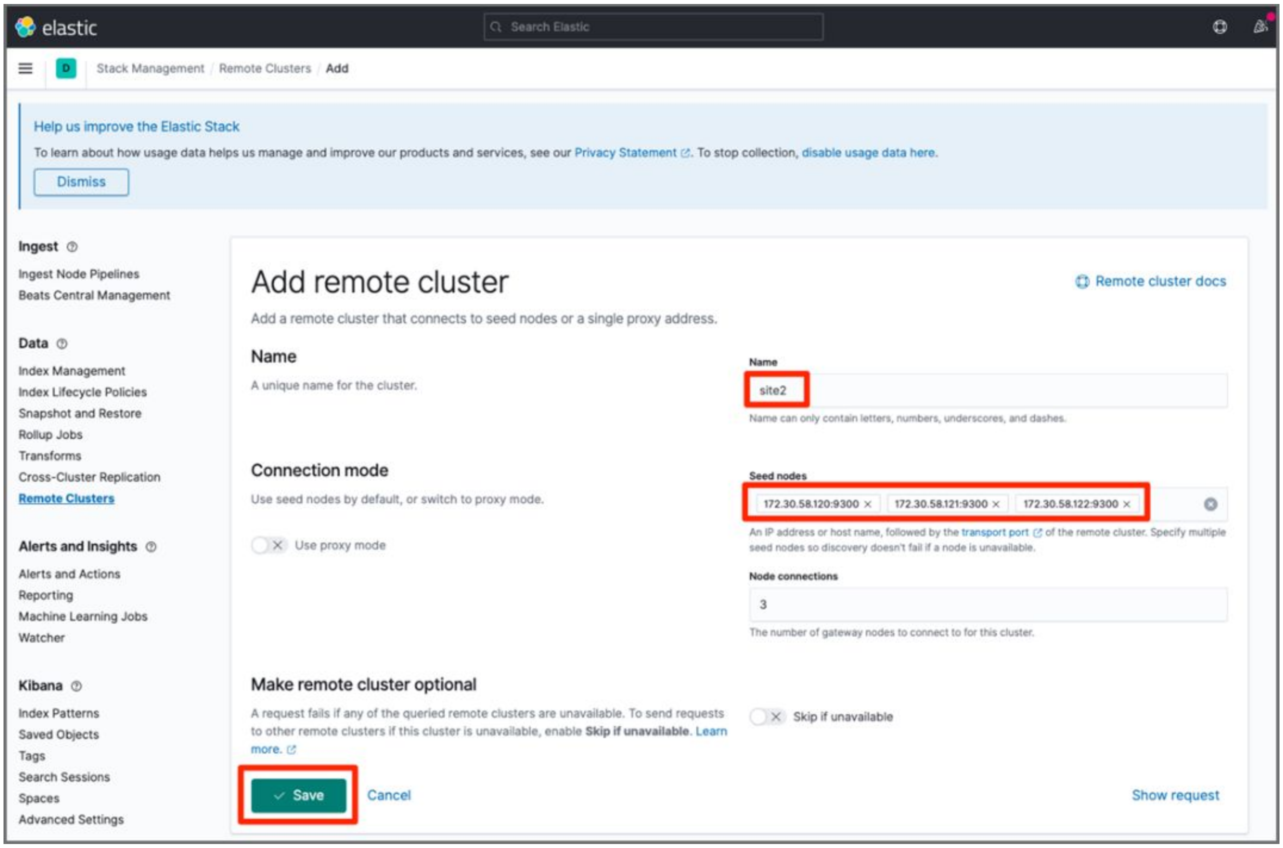
Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add your first remote cluster

Remote clusters create a uni-directional connection from your local cluster to other clusters.

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



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add remote cluster

Add a remote cluster that connects to seed nodes or a single proxy address.

Name

A unique name for the cluster.

Name: site2

Name can only contain letters, numbers, underscores, and dashes.

Connection mode

Use seed nodes by default, or switch to proxy mode.

○ Use proxy mode

Seed nodes: 172.30.58.120:9300 × 172.30.58.121:9300 × 172.30.58.122:9300 ×

An IP address or host name, followed by the transport port of the remote cluster. Specify multiple seed nodes so discovery doesn't fail if a node is unavailable.

Node connections: 3

The number of gateway nodes to connect to for this cluster.

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.

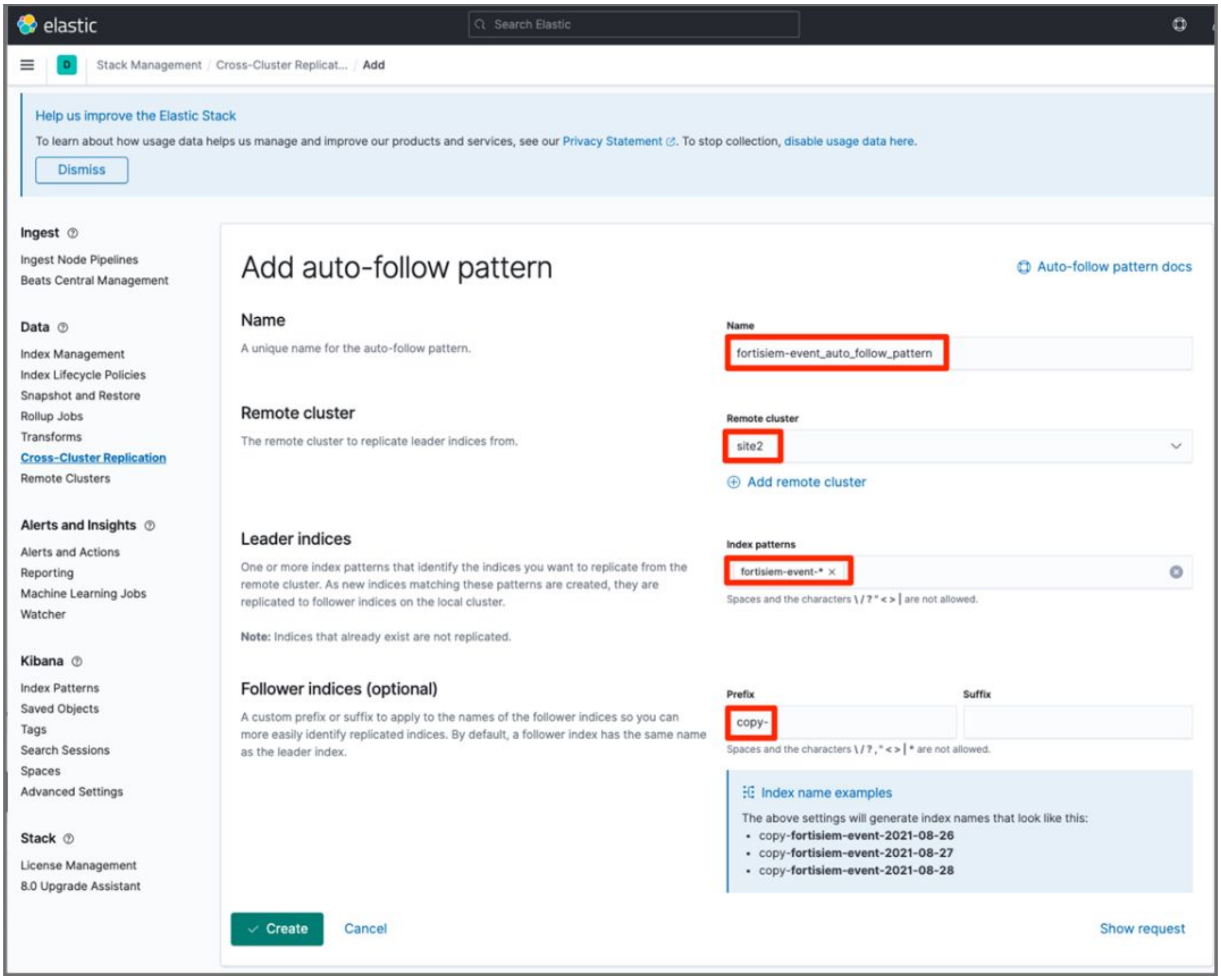
○ Skip if unavailable

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 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.



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add auto-follow pattern

Name

A unique name for the auto-follow pattern.

Name: fortisiem-event_auto_follow_pattern

Remote cluster

The remote cluster to replicate leader indices from.

Remote cluster: site2

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.

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: copy-

Suffix:

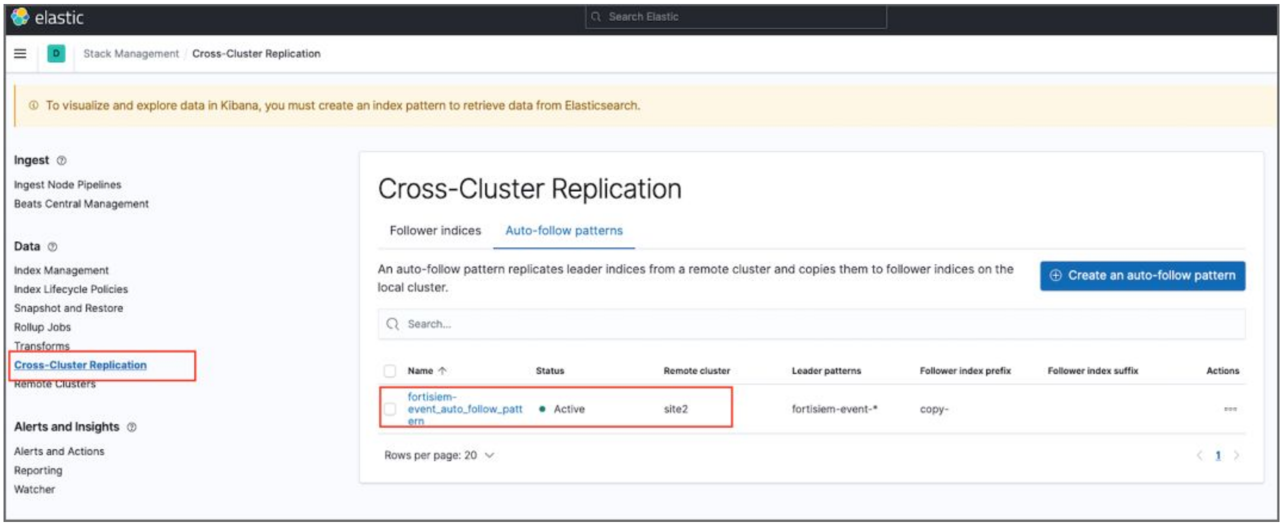
Spaces and the characters \ / ? , " < > | * are not allowed.

Index name examples

The above settings will generate index names that look like this:

- copy-**fortisiem-event-2021-08-26**
- copy-**fortisiem-event-2021-08-27**
- copy-**fortisiem-event-2021-08-28**

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



To visualize and explore data in Kibana, you must create an index pattern to retrieve data from Elasticsearch.

Cross-Cluster Replication

An auto-follow pattern replicates leader indices from a remote cluster and copies them to follower indices on the local cluster.

Name	Status	Remote cluster	Leader patterns	Follower index prefix	Follower index suffix	Actions
fortisiem-event_auto_follow_pattern	● Active	site2	fortisiem-event-*	copy-		

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

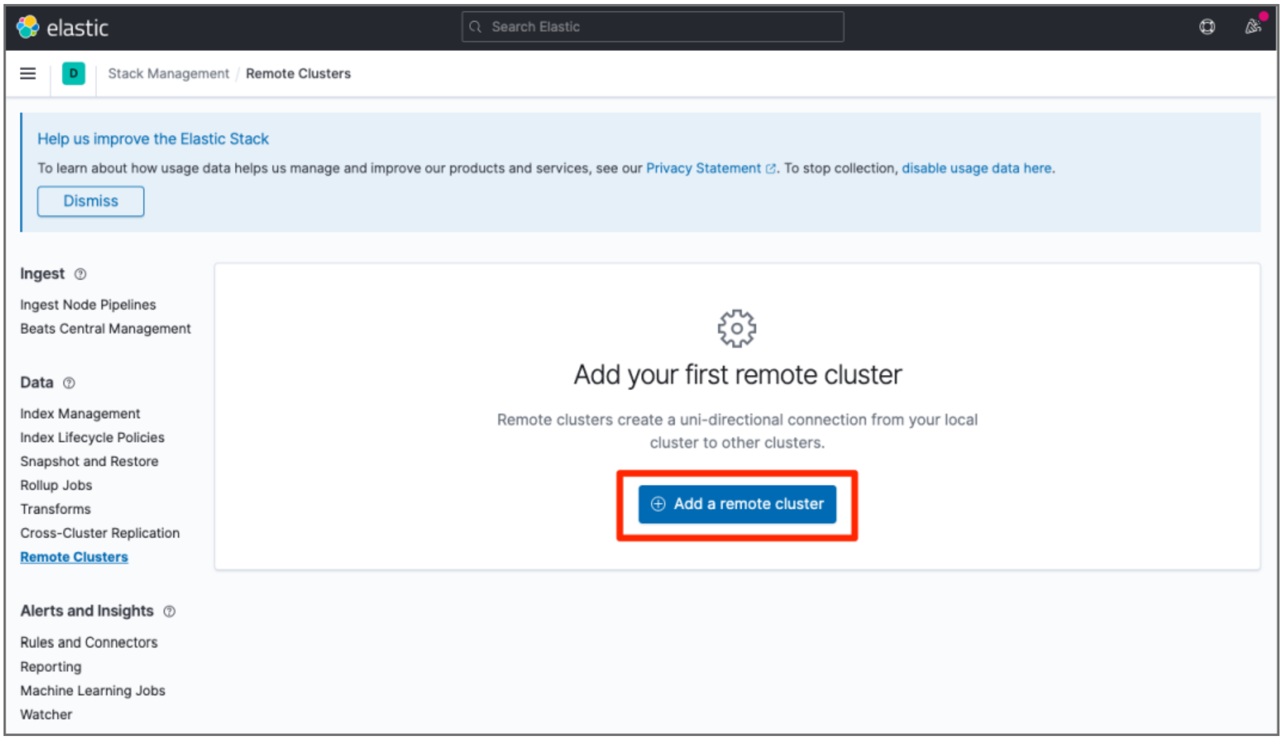
Step 6. Define Remote Clusters for Site 2

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**.



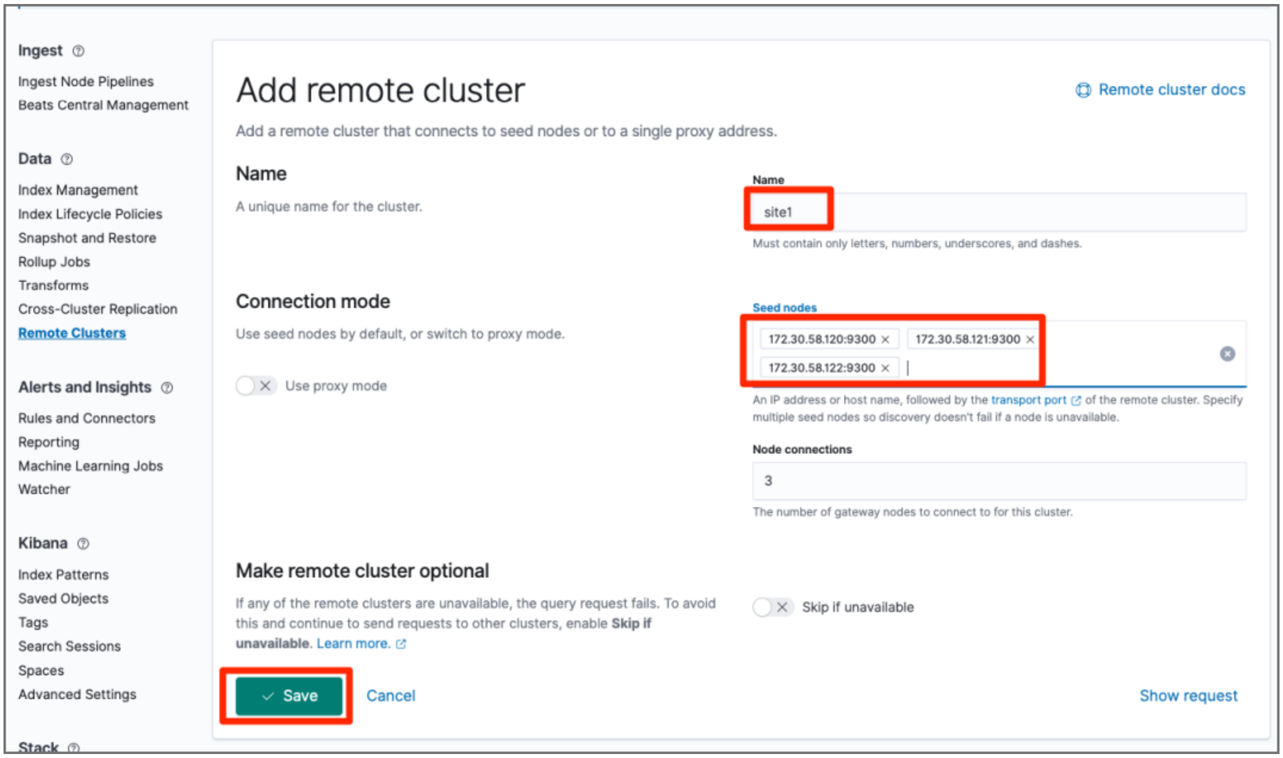
Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add your first remote cluster

Remote clusters create a uni-directional connection from your local cluster to other clusters.

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



Add remote cluster

Add a remote cluster that connects to seed nodes or to a single proxy address.

Name

A unique name for the cluster.

Name: site1

Must contain only letters, numbers, underscores, and dashes.

Connection mode

Use seed nodes by default, or switch to proxy mode.

○ Use proxy mode

Seed nodes: 172.30.58.120:9300 172.30.58.121:9300 172.30.58.122:9300

An IP address or host name, followed by the transport port of the remote cluster. Specify multiple seed nodes so discovery doesn't fail if a node is unavailable.

Node connections: 3

The number of gateway nodes to connect to for this cluster.

Make remote cluster optional

If any of the remote clusters are unavailable, the query request fails. To avoid this and continue to send requests to other clusters, enable **Skip if unavailable.** Learn more.

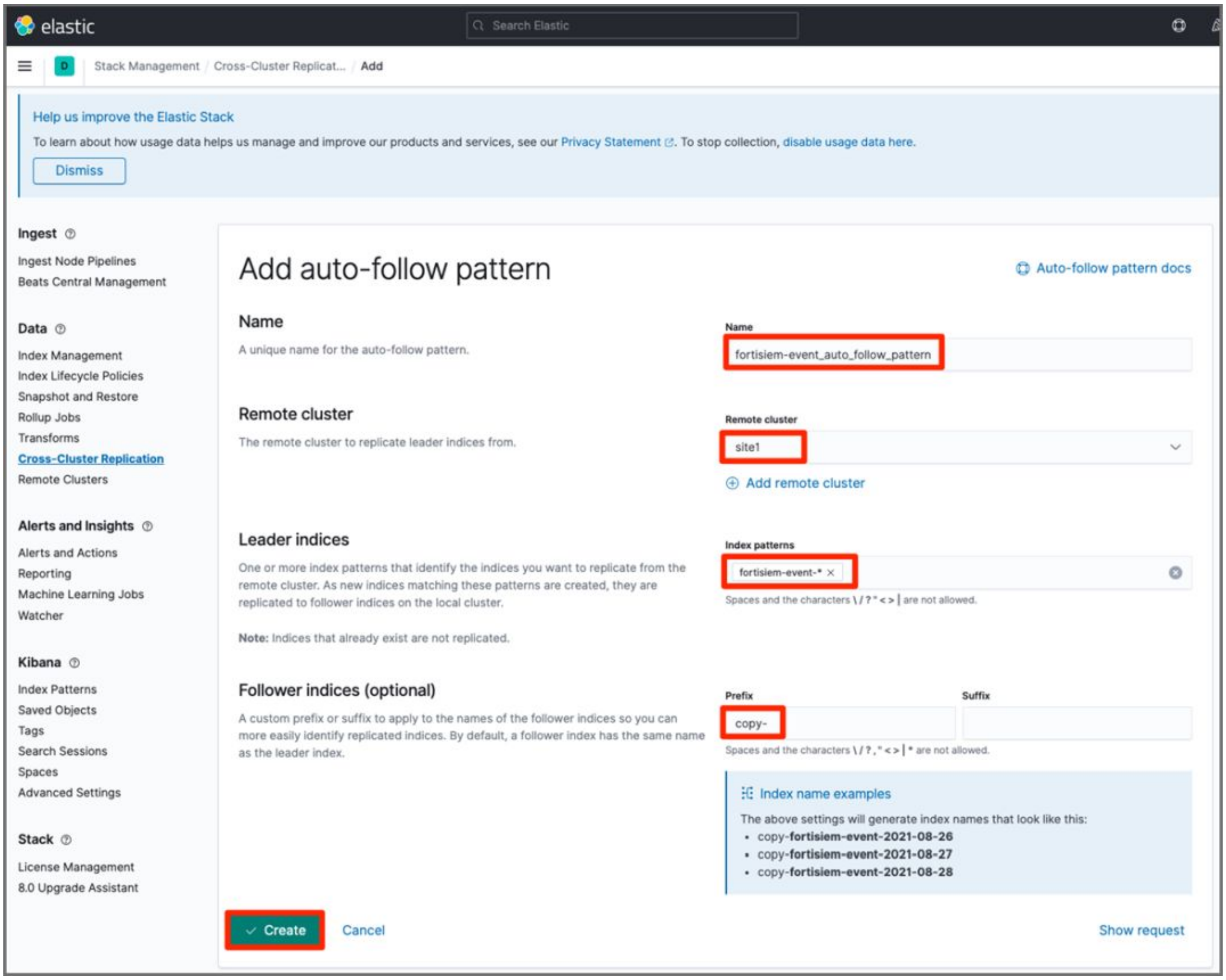
○ Skip if unavailable

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.



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add auto-follow pattern

Name

A unique name for the auto-follow pattern.

Name: fortisiem-event_auto_follow_pattern

Remote cluster

The remote cluster to replicate leader indices from.

Remote cluster: site1

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.

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: copy-

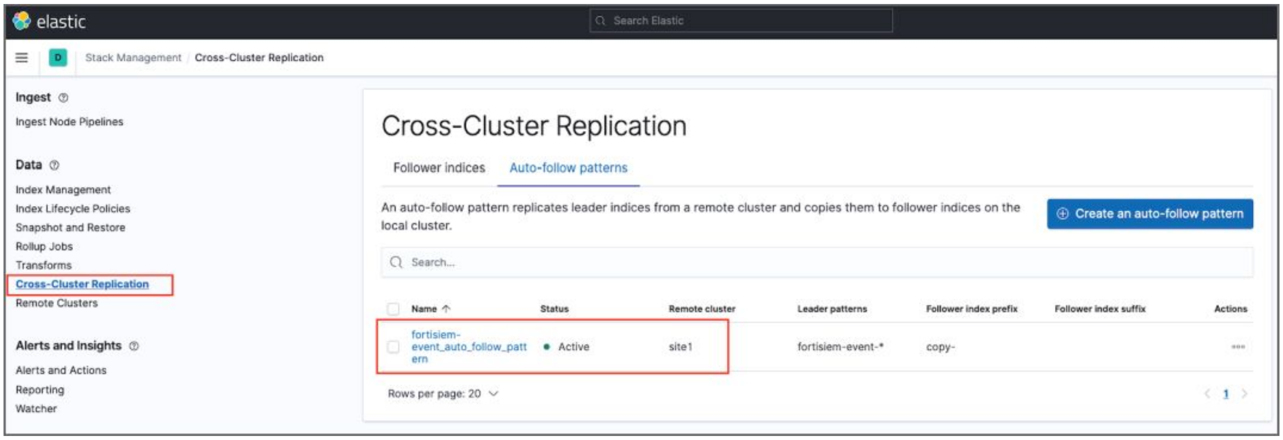
Suffix:

Spaces and the characters \ / ? , " < > | * are not allowed.

The above settings will generate index names that look like this:

- copy-**fortisiem-event-2021-08-26**
- copy-**fortisiem-event-2021-08-27**
- copy-**fortisiem-event-2021-08-28**

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



Cross-Cluster Replication

An auto-follow pattern replicates leader indices from a remote cluster and copies them to follower indices on the local cluster.

Name	Status	Remote cluster	Leader patterns	Follower index prefix	Follower index suffix	Actions
fortisiem-event_auto_follow_pattern	● 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**.

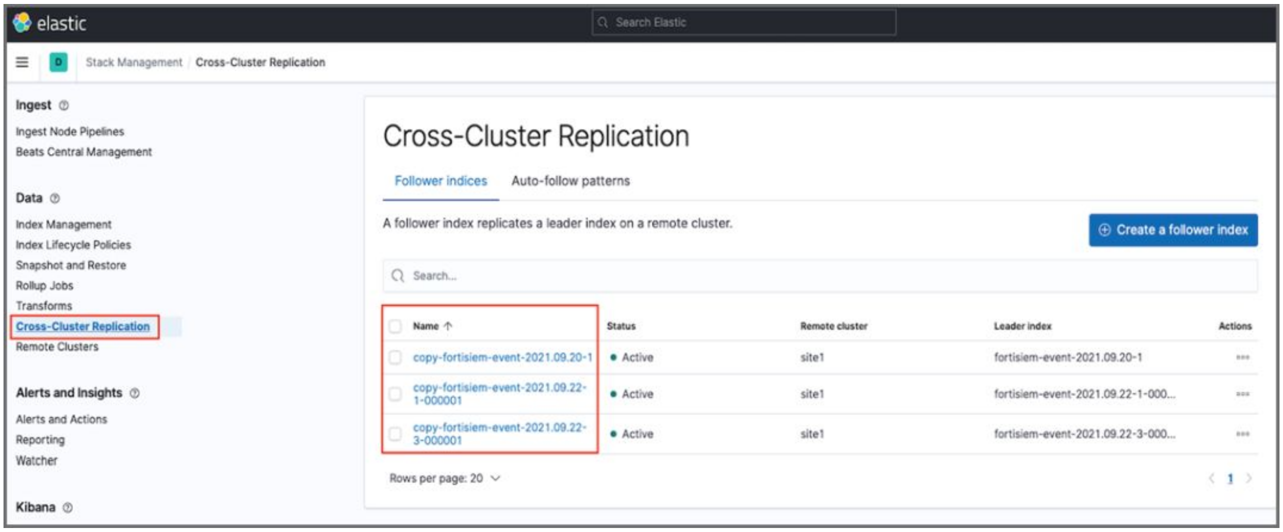
Step 10. Set Up Disaster Recovery

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.



Cross-Cluster Replication

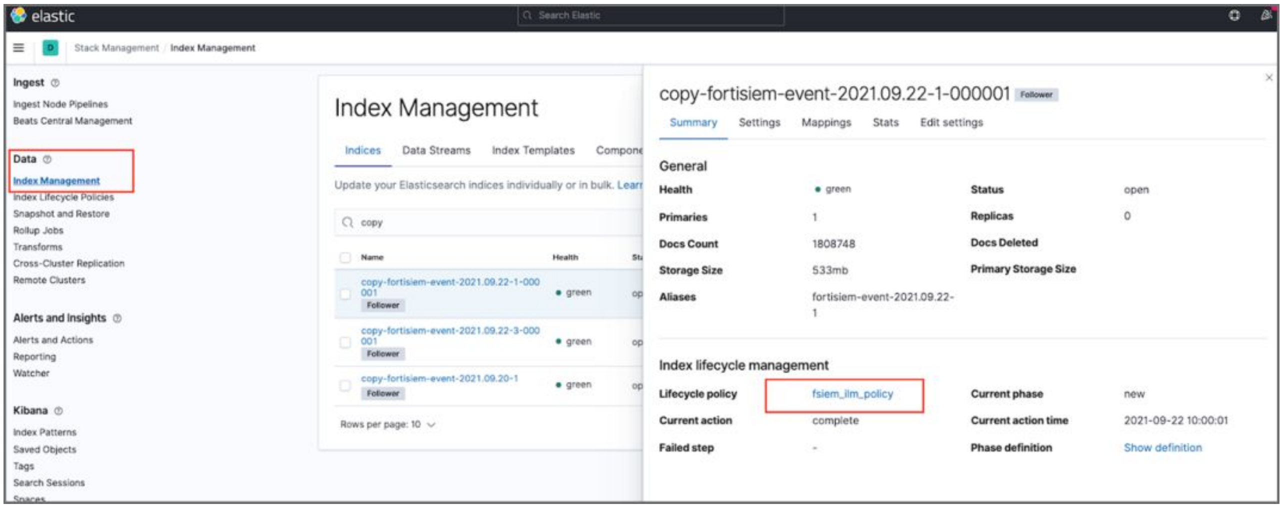
A follower index replicates a leader index on a remote cluster.

Name ↑	Status	Remote cluster	Leader index	Actions
copy-fortisiem-event-2021.09.20-1	● Active	site1	fortisiem-event-2021.09.20-1	•••
copy-fortisiem-event-2021.09.22-1-000001	● Active	site1	fortisiem-event-2021.09.22-1-000...	•••
copy-fortisiem-event-2021.09.22-3-000001	● Active	site1	fortisiem-event-2021.09.22-3-000...	•••

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**.



Update your Elasticsearch indices individually or in bulk. Learn

copy

Name	Health	St
copy-fortisiem-event-2021.09.22-1-000001 Follower	● green	op
copy-fortisiem-event-2021.09.22-3-000001 Follower	● green	op
copy-fortisiem-event-2021.09.20-1 Follower	● green	op

Rows per page: 10

copy-fortisiem-event-2021.09.22-1-000001 Follower

General

Health	● green	Status	open
Primaries	1	Replicas	0
Docs Count	1808748	Docs Deleted	
Storage Size	533mb	Primary Storage Size	
Aliases	fortisiem-event-2021.09.22-1		

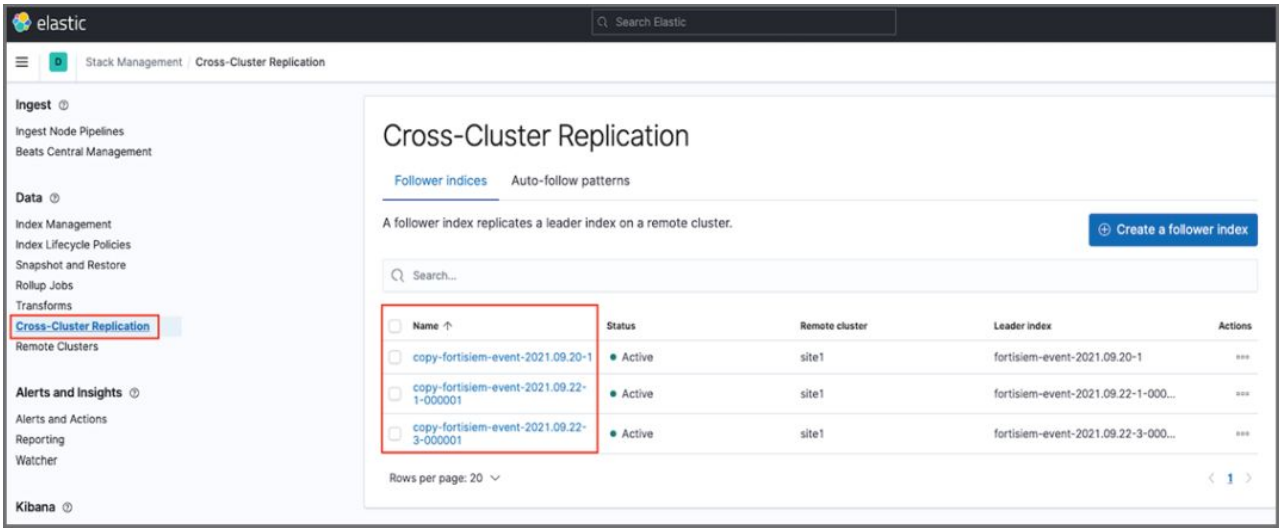
Index lifecycle management

Lifecycle policy	fsiem_ilm_policy	Current phase	new
Current action	complete	Current action time	2021-09-22 10:00:01
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.



A follower index replicates a leader index on a remote cluster.

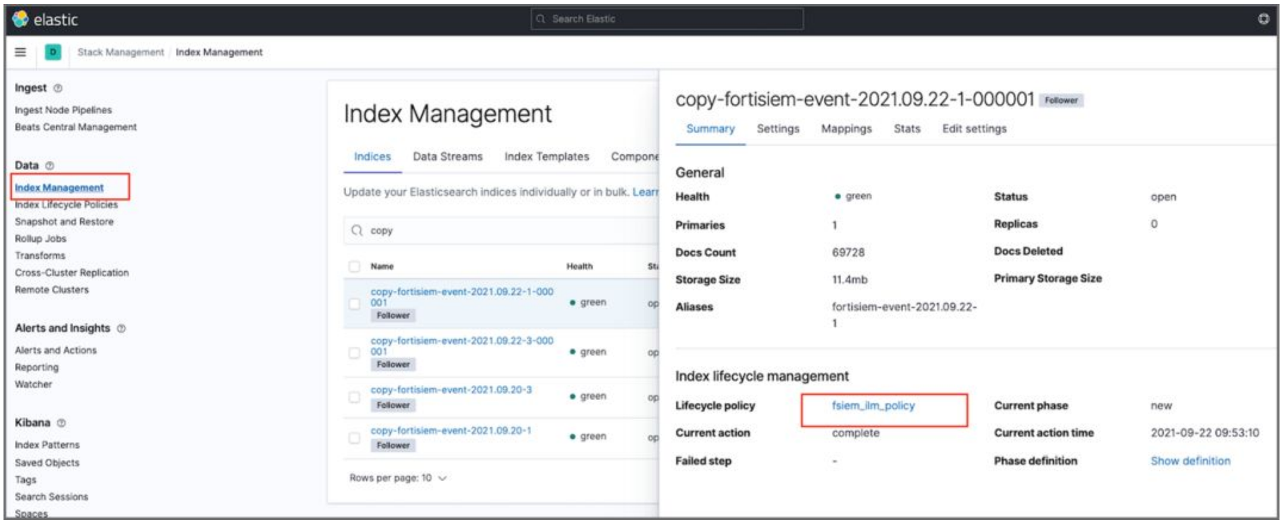
Name ↑	Status	Remote cluster	Leader index	Actions
copy-fortisiem-event-2021.09.20-1	● Active	site1	fortisiem-event-2021.09.20-1	•••
copy-fortisiem-event-2021.09.22-1-000001	● Active	site1	fortisiem-event-2021.09.22-1-000...	•••
copy-fortisiem-event-2021.09.22-3-000001	● Active	site1	fortisiem-event-2021.09.22-3-000...	•••

Rows per page: 20

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**.



Name	Health	St
copy-fortisiem-event-2021.09.22-1-000001 Follower	● green	op
copy-fortisiem-event-2021.09.22-3-000001 Follower	● green	op
copy-fortisiem-event-2021.09.20-3 Follower	● green	op
copy-fortisiem-event-2021.09.20-1 Follower	● green	op

copy-fortisiem-event-2021.09.22-1-000001 Follower

General

Health	● green	Status	open
Primaries	1	Replicas	0
Docs Count	69728	Docs Deleted	
Storage Size	11.4mb	Primary Storage Size	
Aliases	fortisiem-event-2021.09.22-1		

Index lifecycle management

Lifecycle policy	fsiem_ilm_policy	Current phase	new
Current action	complete	Current action time	2021-09-22 09:53:10
Failed step	-	Phase definition	Show definition

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: true`
2. Restart each node in the cluster for Site 1.
3. 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.

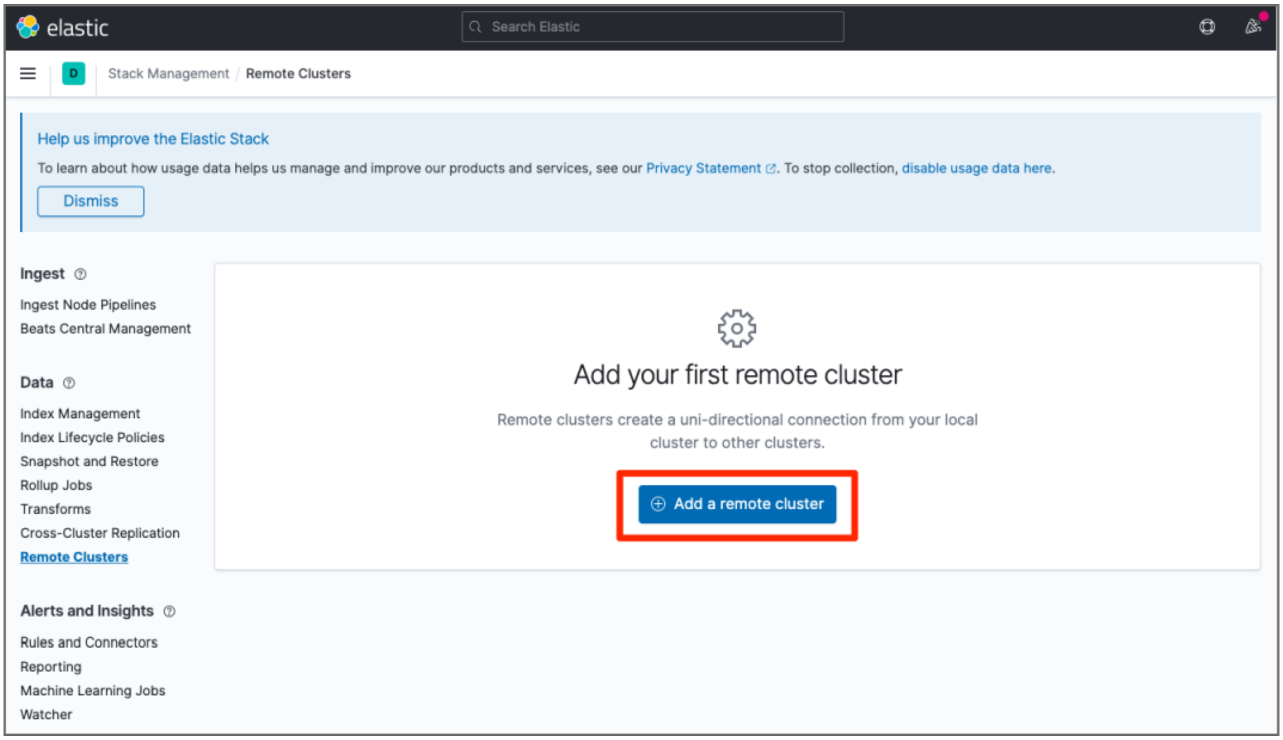
```
PUT /_cluster/settings?pretty
{
  "persistent": {
    "action.auto_create_index": "-fortisiem-event-*,fortisiem-*,.monitoring-*"
  }
}
```

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**.



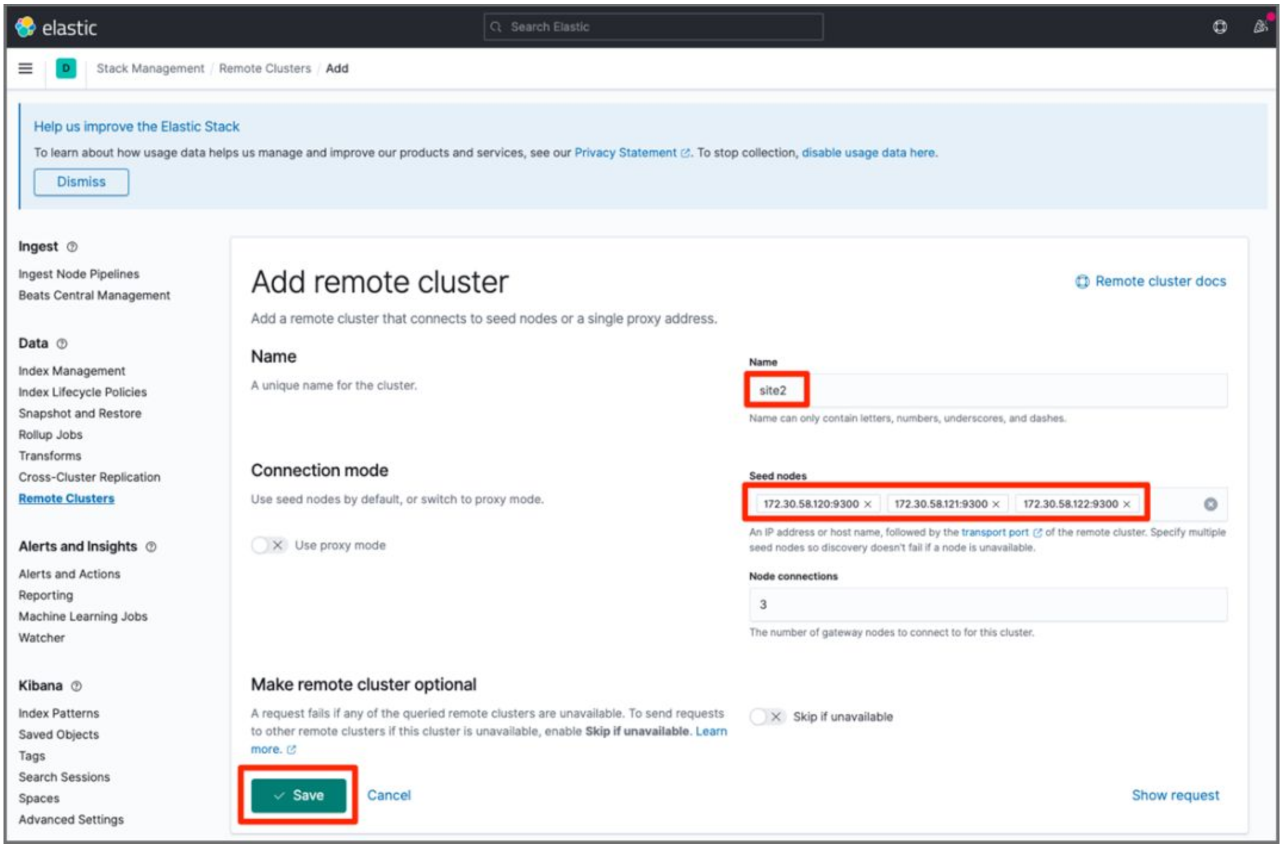
Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add your first remote cluster

Remote clusters create a uni-directional connection from your local cluster to other clusters.

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



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add remote cluster

Add a remote cluster that connects to seed nodes or a single proxy address.

Name

A unique name for the cluster.

Name: site2

Name can only contain letters, numbers, underscores, and dashes.

Connection mode

Use seed nodes by default, or switch to proxy mode.

○ Use proxy mode

Seed nodes: 172.30.58.120:9300 × 172.30.58.121:9300 × 172.30.58.122:9300 ×

An IP address or host name, followed by the transport port of the remote cluster. Specify multiple seed nodes so discovery doesn't fail if a node is unavailable.

Node connections: 3

The number of gateway nodes to connect to for this cluster.

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.

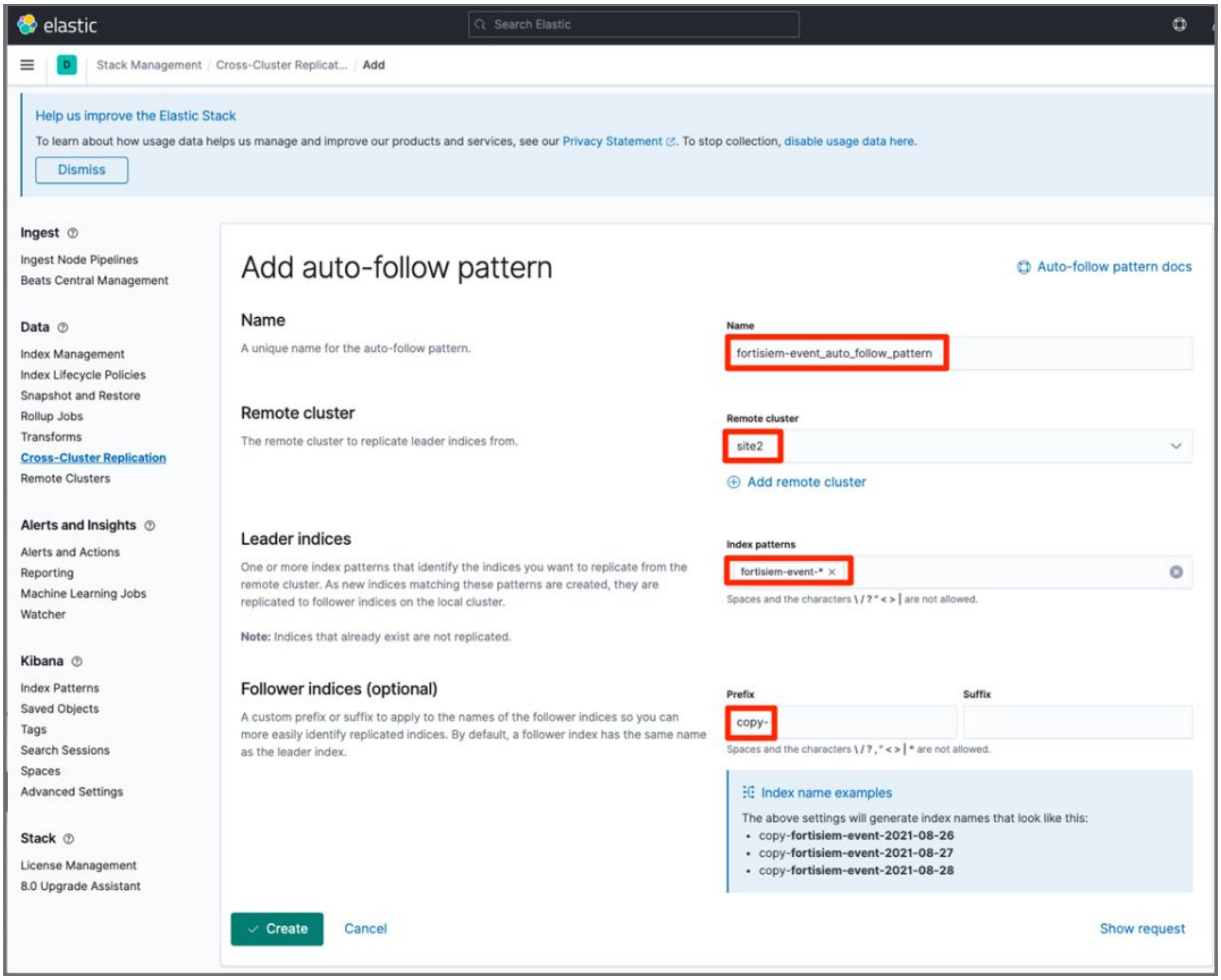
○ Skip if unavailable

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.



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add auto-follow pattern

Name

A unique name for the auto-follow pattern.

Name: fortisiem-event_auto_follow_pattern

Remote cluster

The remote cluster to replicate leader indices from.

Remote cluster: site2

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.

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: copy-

Suffix:

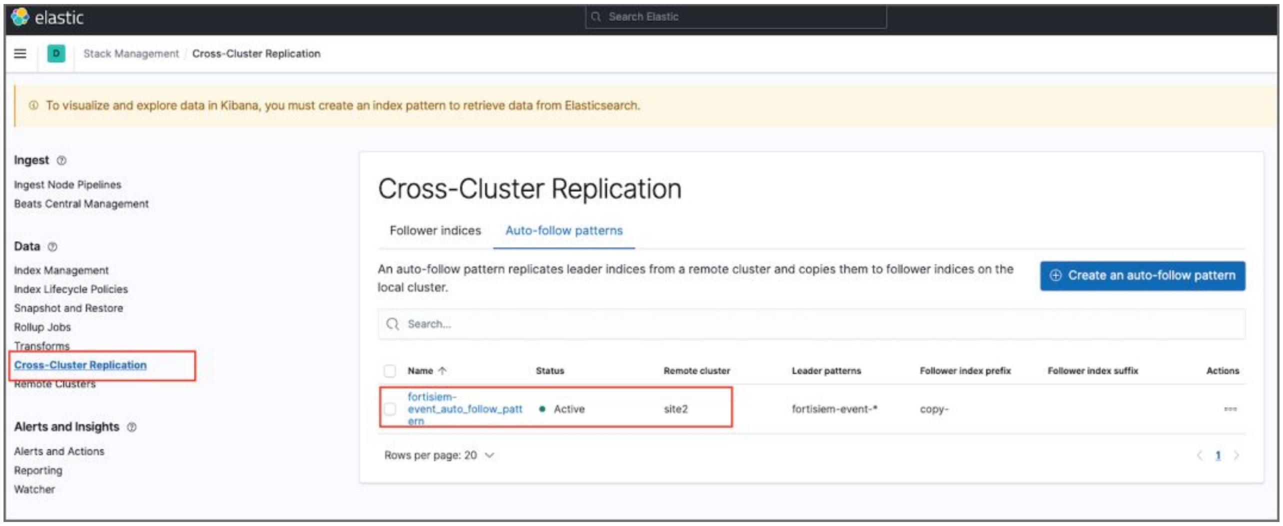
Spaces and the characters \ / ? , " < > | * are not allowed.

Index name examples

The above settings will generate index names that look like this:

- copy-**fortisiem-event-2021-08-26**
- copy-**fortisiem-event-2021-08-27**
- copy-**fortisiem-event-2021-08-28**

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



To visualize and explore data in Kibana, you must create an index pattern to retrieve data from Elasticsearch.

Cross-Cluster Replication

An auto-follow pattern replicates leader indices from a remote cluster and copies them to follower indices on the local cluster.

Name ↑	Status	Remote cluster	Leader patterns	Follower index prefix	Follower index suffix	Actions
fortisiem-event_auto_follow_pattern	● Active	site2	fortisiem-event-*	copy-		•••

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

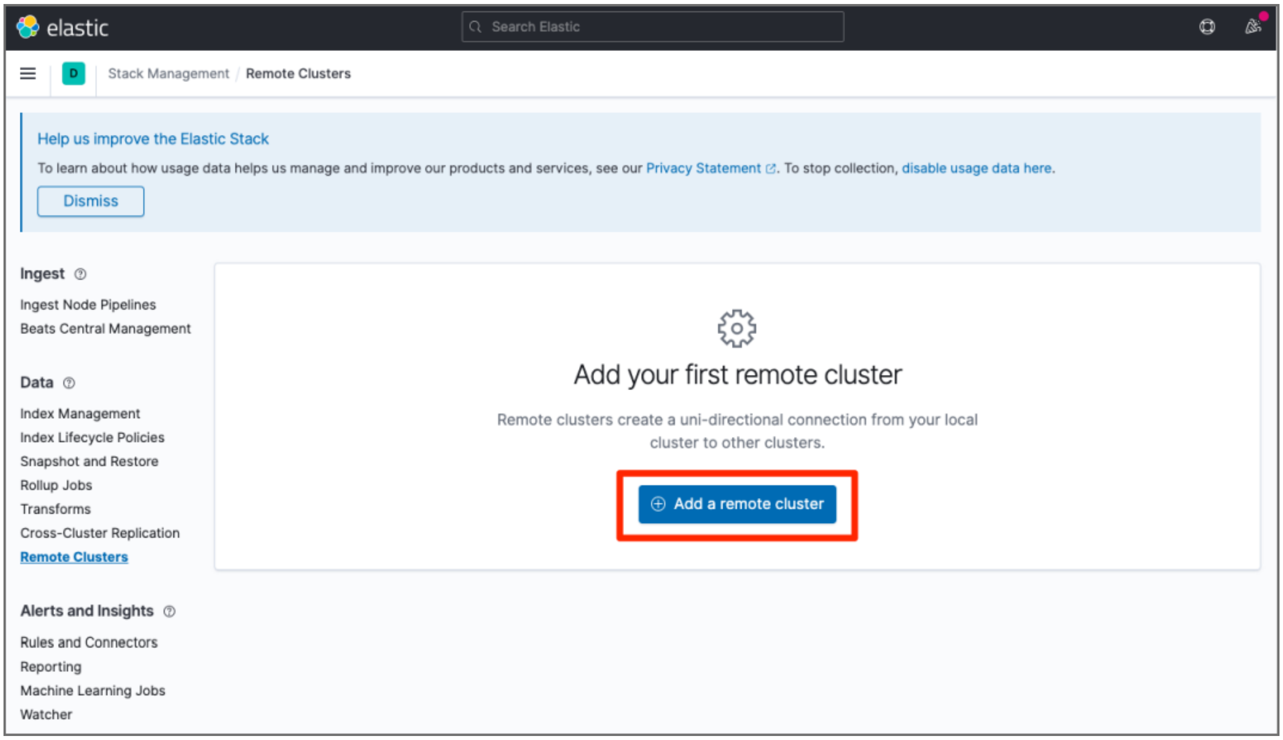
Step 6. Define Remote Clusters for Site 2

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**.



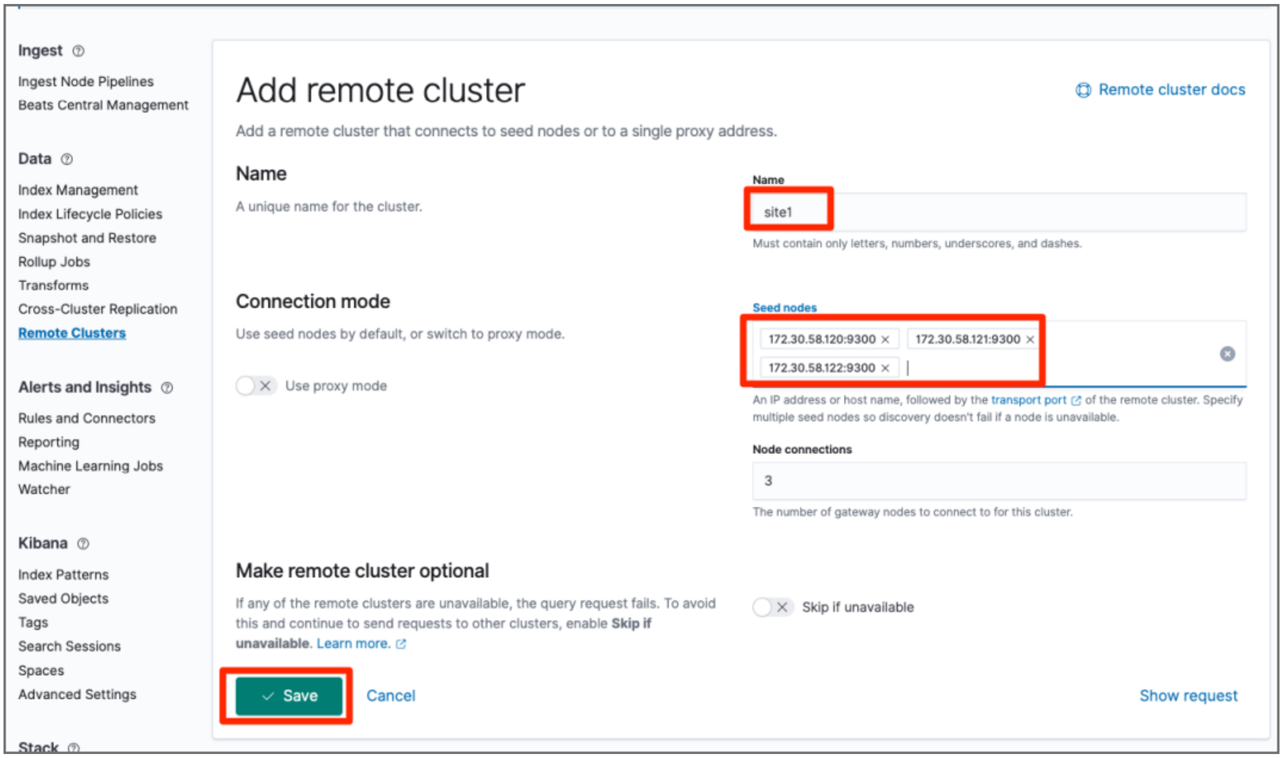
Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add your first remote cluster

Remote clusters create a uni-directional connection from your local cluster to other clusters.

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



Add remote cluster

Add a remote cluster that connects to seed nodes or to a single proxy address.

Name

A unique name for the cluster.

Name: site1

Must contain only letters, numbers, underscores, and dashes.

Connection mode

Use seed nodes by default, or switch to proxy mode.

☒ Use proxy mode

Seed nodes: 172.30.58.120:9300 × 172.30.58.121:9300 × 172.30.58.122:9300 ×

An IP address or host name, followed by the transport port of the remote cluster. Specify multiple seed nodes so discovery doesn't fail if a node is unavailable.

Node connections: 3

The number of gateway nodes to connect to for this cluster.

Make remote cluster optional

If any of the remote clusters are unavailable, the query request fails. To avoid this and continue to send requests to other clusters, enable **Skip if unavailable.** Learn more.

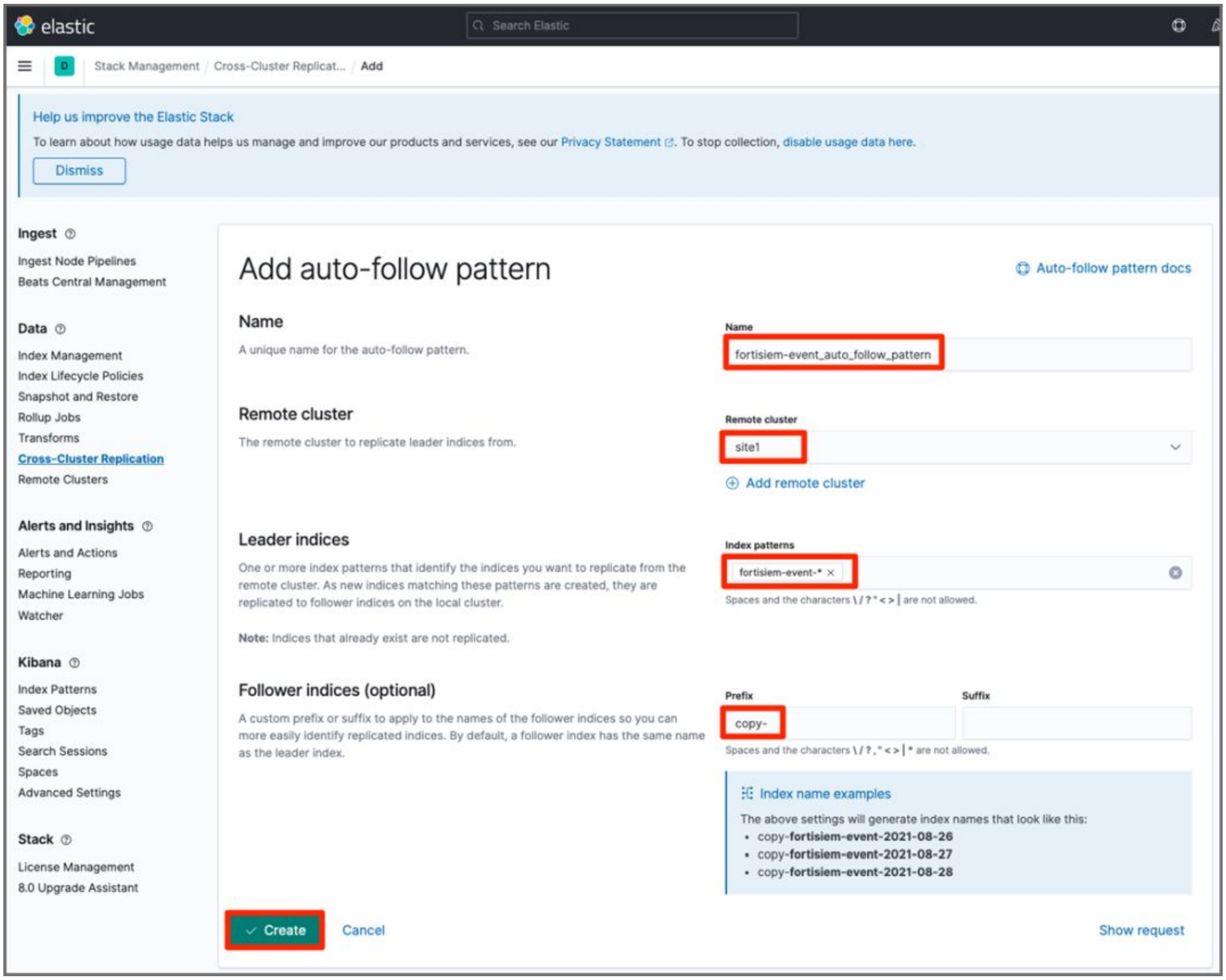
☒ Skip if unavailable

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.



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Add auto-follow pattern

Name

A unique name for the auto-follow pattern.

Name: fortisiem-event_auto_follow_pattern

Remote cluster

The remote cluster to replicate leader indices from.

Remote cluster: site1

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.

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: copy-

Suffix:

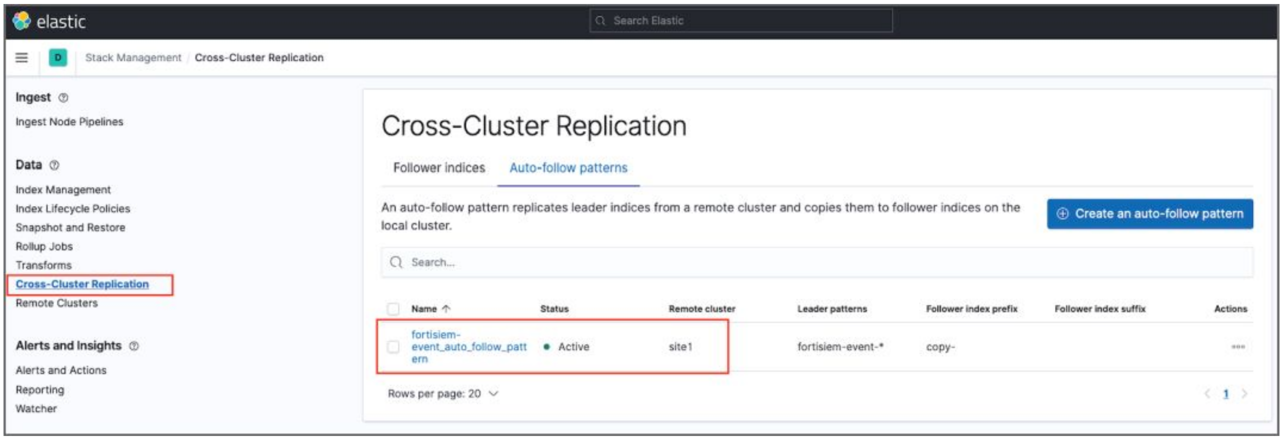
Spaces and the characters \ / ? , " < > | * are not allowed.

Index name examples

The above settings will generate index names that look like this:

- copy-**fortisiem-event-2021-08-26**
- copy-**fortisiem-event-2021-08-27**
- copy-**fortisiem-event-2021-08-28**

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



Cross-Cluster Replication

An auto-follow pattern replicates leader indices from a remote cluster and copies them to follower indices on the local cluster.

Name	Status	Remote cluster	Leader patterns	Follower index prefix	Follower index suffix	Actions
fortisiem-event_auto_follow_pattern	● Active	site1	fortisiem-event-*	copy-		•••

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

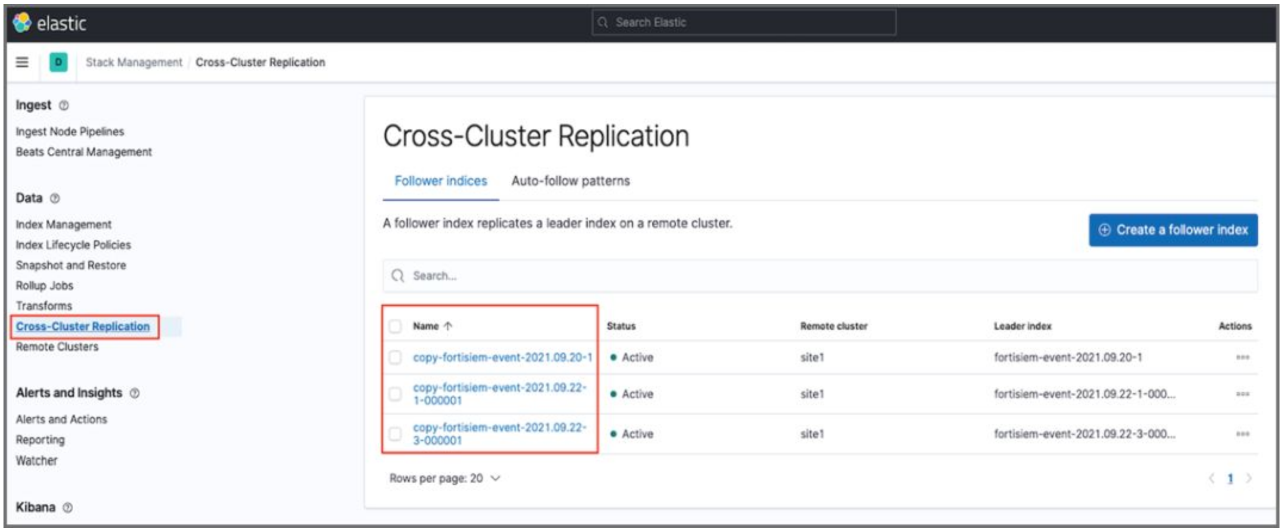
See **Configuring Disaster Recovery** in the latest *Disaster Recovery Procedures - EventDB* Guide here.

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.



Cross-Cluster Replication

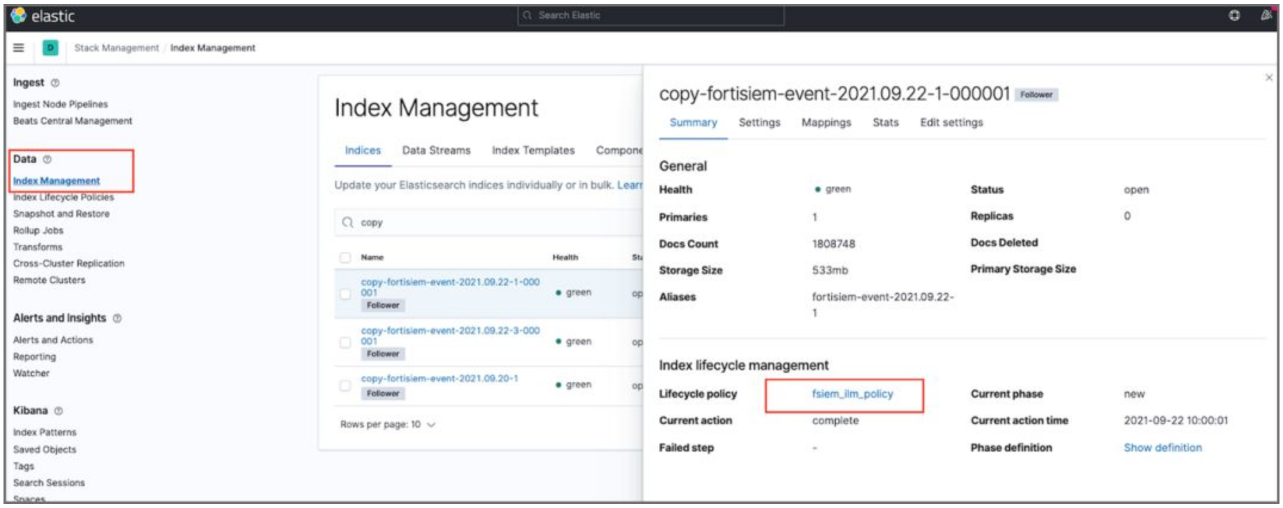
A follower index replicates a leader index on a remote cluster.

Name	Status	Remote cluster	Leader index	Actions
copy-fortisiem-event-2021.09.20-1	● Active	site1	fortisiem-event-2021.09.20-1	•••
copy-fortisiem-event-2021.09.22-1-000001	● Active	site1	fortisiem-event-2021.09.22-1-000...	•••
copy-fortisiem-event-2021.09.22-3-000001	● Active	site1	fortisiem-event-2021.09.22-3-000...	•••

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**.



Index Management

Update your Elasticsearch indices individually or in bulk. Learn

Name	Health	St
copy-fortisiem-event-2021.09.22-1-000001 Follower	● green	op
copy-fortisiem-event-2021.09.22-3-000001 Follower	● green	op
copy-fortisiem-event-2021.09.20-1 Follower	● green	op

copy-fortisiem-event-2021.09.22-1-000001 Follower

General

Health	● green	Status	open
Primaries	1	Replicas	0
Docs Count	1808748	Docs Deleted	
Storage Size	533mb	Primary Storage Size	
Aliases	fortisiem-event-2021.09.22-1		

Index lifecycle management

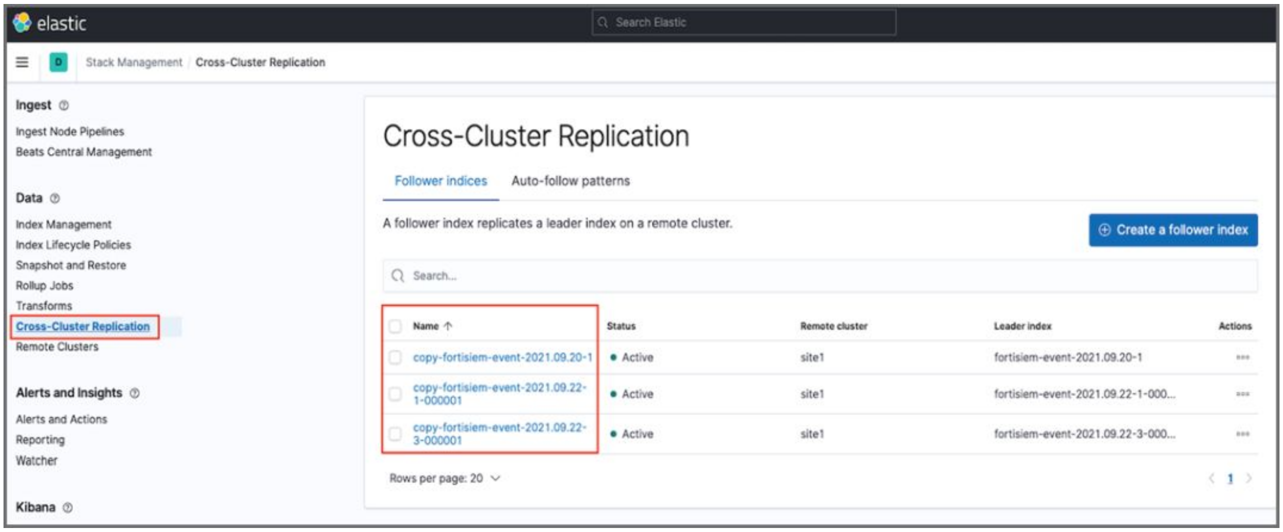
Lifecycle policy	fsiem_ilm_policy	Current phase	new
Current action	complete	Current action time	2021-09-22 10:00:01
Failed step	-	Phase definition	Show definition

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.



Cross-Cluster Replication

A follower index replicates a leader index on a remote cluster.

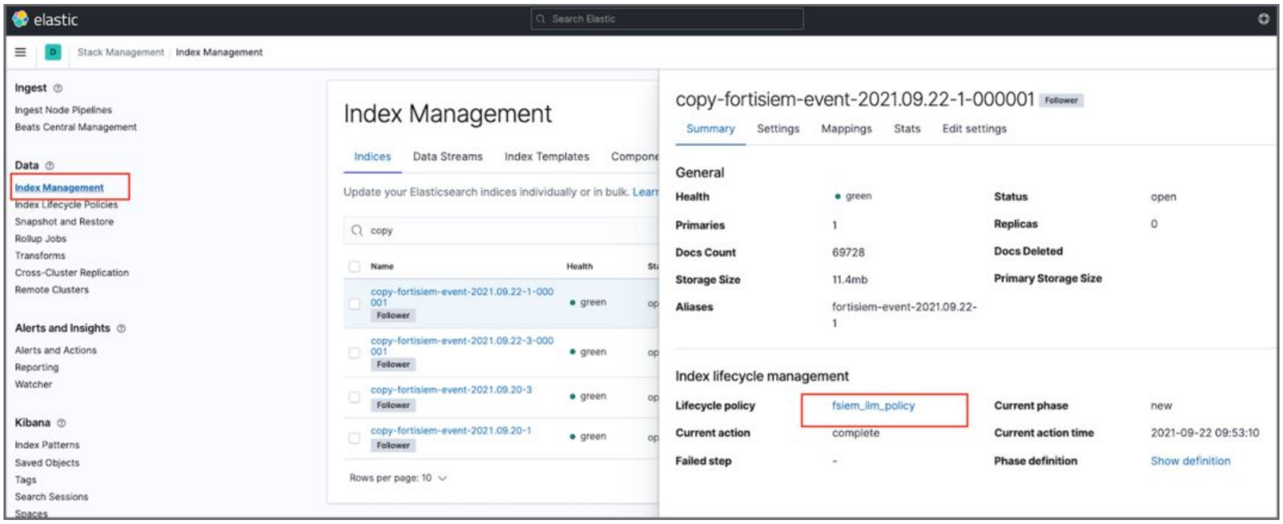
Name ↑	Status	Remote cluster	Leader index	Actions
copy-fortisiem-event-2021.09.20-1	● Active	site1	fortisiem-event-2021.09.20-1	•••
copy-fortisiem-event-2021.09.22-1-000001	● Active	site1	fortisiem-event-2021.09.22-1-000...	•••
copy-fortisiem-event-2021.09.22-3-000001	● Active	site1	fortisiem-event-2021.09.22-3-000...	•••

Rows per page: 20

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**.



Index Management

Update your Elasticsearch indices individually or in bulk. Learr

copy

Name	Health	St
copy-fortisiem-event-2021.09.22-1-000001 Follower	● green	op
copy-fortisiem-event-2021.09.22-3-000001 Follower	● green	op
copy-fortisiem-event-2021.09.20-3 Follower	● green	op
copy-fortisiem-event-2021.09.20-1 Follower	● green	op

Rows per page: 10

copy-fortisiem-event-2021.09.22-1-000001 Follower

General

Health	● green	Status	open
Primaries	1	Replicas	0
Docs Count	69728	Docs Deleted	
Storage Size	11.4mb	Primary Storage Size	
Aliases	fortisiem-event-2021.09.22-1		

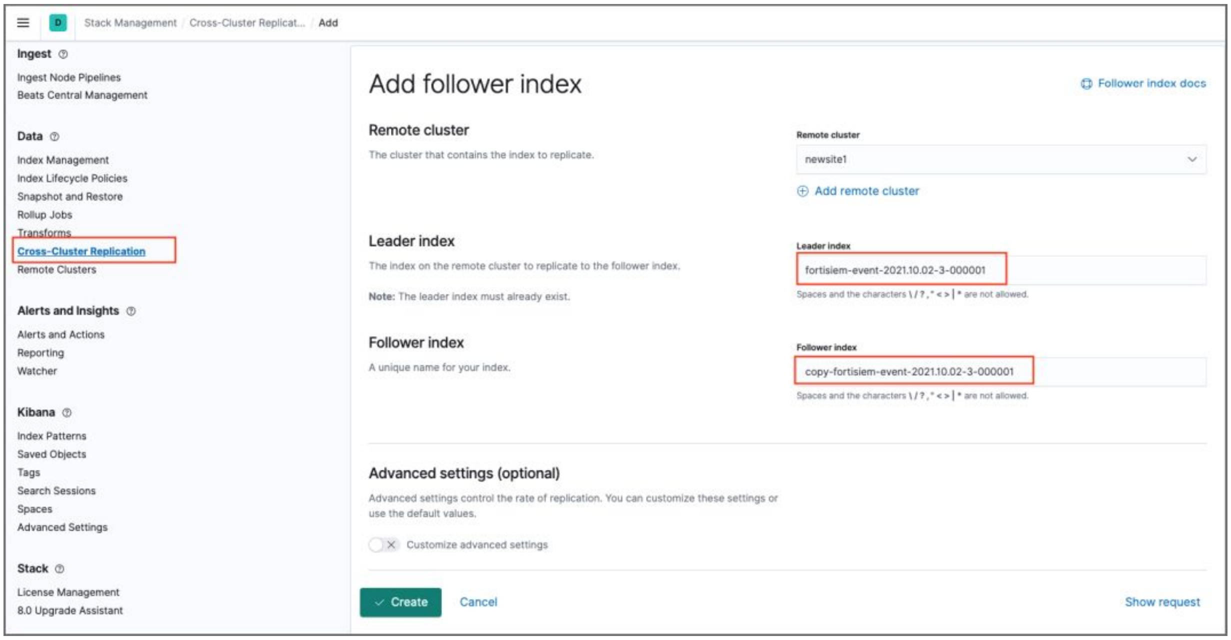
Index lifecycle management

Lifecycle policy	fsiem_ilm_policy	Current phase	new
Current action	complete	Current action time	2021-09-22 09:53:10
Failed step	-	Phase definition	Show definition

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**.



Add follower index

Remote cluster

The cluster that contains the index to replicate.

Remote cluster: newsite1

Leader index

The index on the remote cluster to replicate to the follower index.

Note: The leader index must already exist.

Leader index: fortisiem-event-2021.10.02-3-000001

Spaces and the characters \ / ? , " < > | * are not allowed.

Follower index

A unique name for your index.

Follower index: copy-fortisiem-event-2021.10.02-3-000001

Spaces and the characters \ / ? , " < > | * are not allowed.

Advanced settings (optional)

Advanced settings control the rate of replication. You can customize these settings or use the default values.

○ Customize advanced settings

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

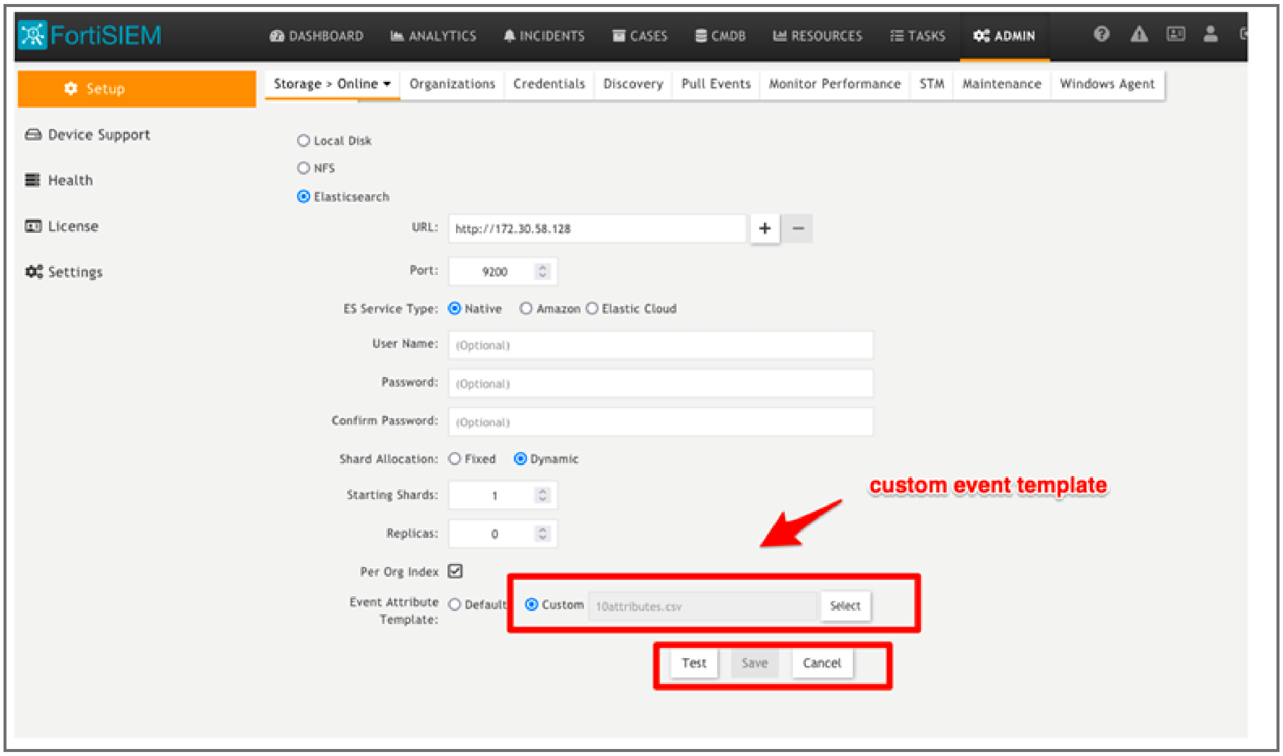
See **Switching Primary and Secondary Roles** in the latest *Disaster Recovery Procedures - EventDB* Guide here.

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.



○ Local Disk
○ NFS
● Elasticsearch

URL: http://172.30.58.128

Port: 9200

ES Service Type: ● Native ○ Amazon ○ Elastic Cloud

User Name: (Optional)

Password: (Optional)

Confirm Password: (Optional)

Shard Allocation: ○ Fixed ● Dynamic

Starting Shards: 1

Replicas: 0

Per Org Index ☑

Event Attribute Template: ○ Default ● Custom 10attributes.csv

Step 3. Confirm Events are Inserted to Site 2

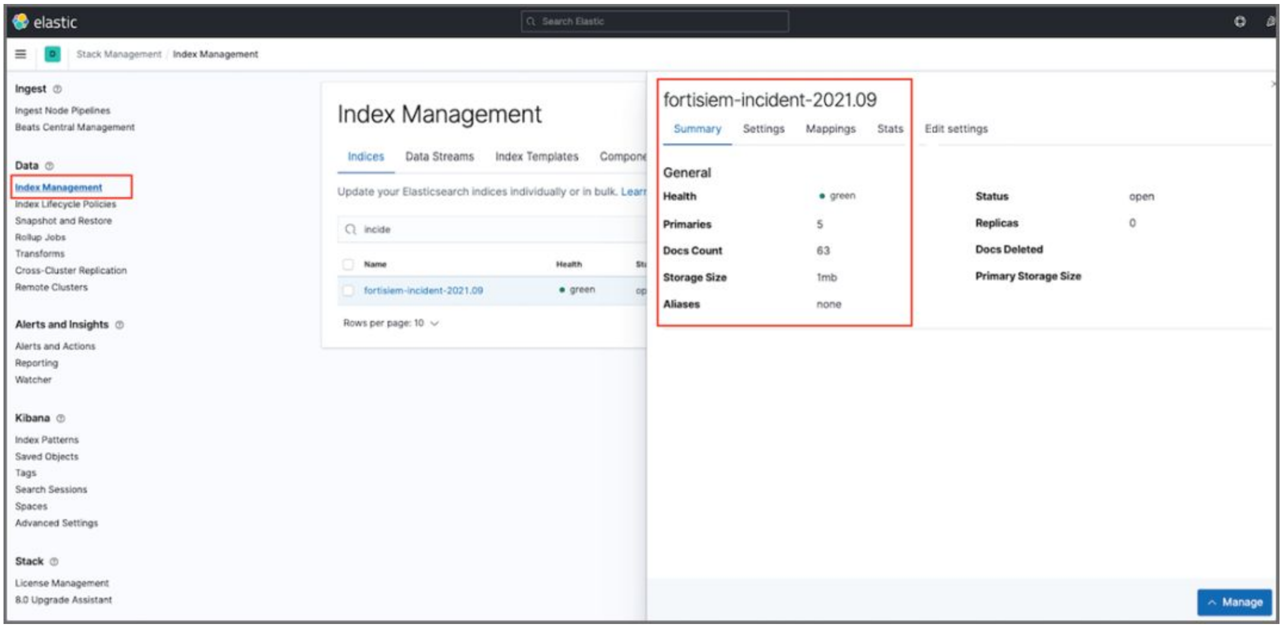
At this point, Collectors should be communicating to the Site 2 Supervisor, and would get a set of Site 2 Event (Upload) Workers. Since Site 2 Workers are connected to the Site 2 Elasticsearch Cluster, events are now stored in the Site 2 Elasticsearch. You can verify this by running queries from the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



fortisiem-incident-2021.09 ● green

fortisiem-incident-2021.09

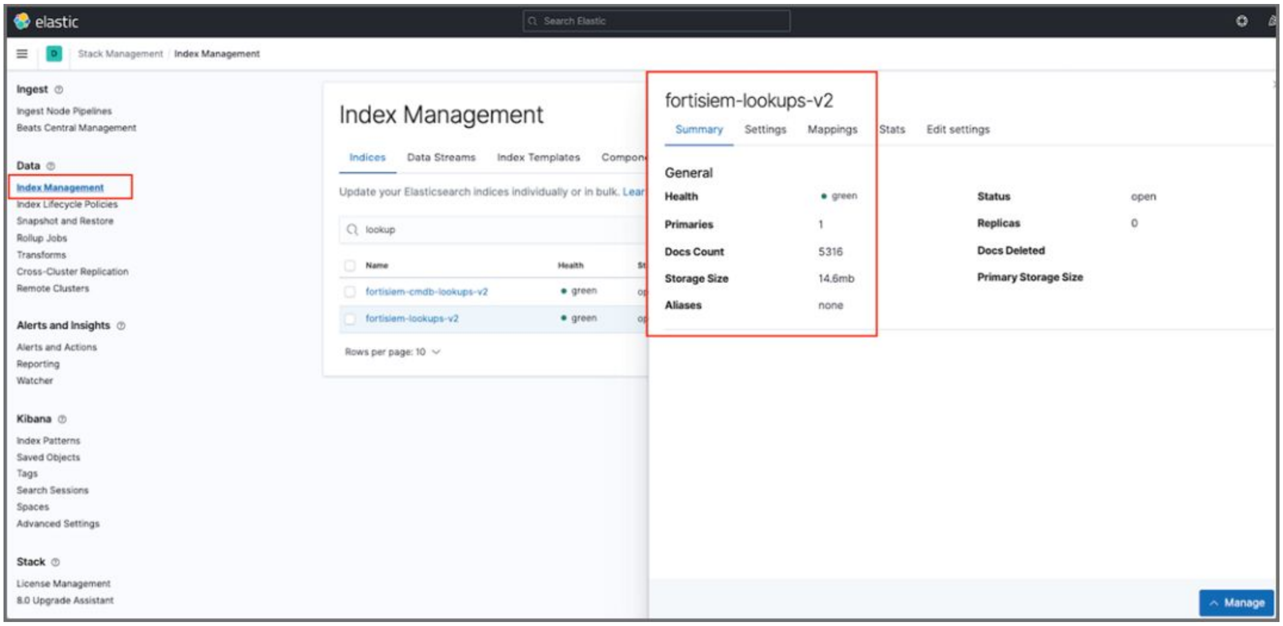
General

Health	● green	Status	open
Primaries	5	Replicas	0
Docs Count	63	Docs Deleted	
Storage Size	1mb	Primary Storage Size	
Aliases	none		

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.



fortisiem-cmdb-lookups-v2 ● green
fortisiem-lookups-v2 ● green

fortisiem-lookups-v2

General

Health	● green	Status	open
Primaries	1	Replicas	0
Docs Count	5316	Docs Deleted	
Storage Size	14.6mb	Primary Storage Size	
Aliases	none		

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.

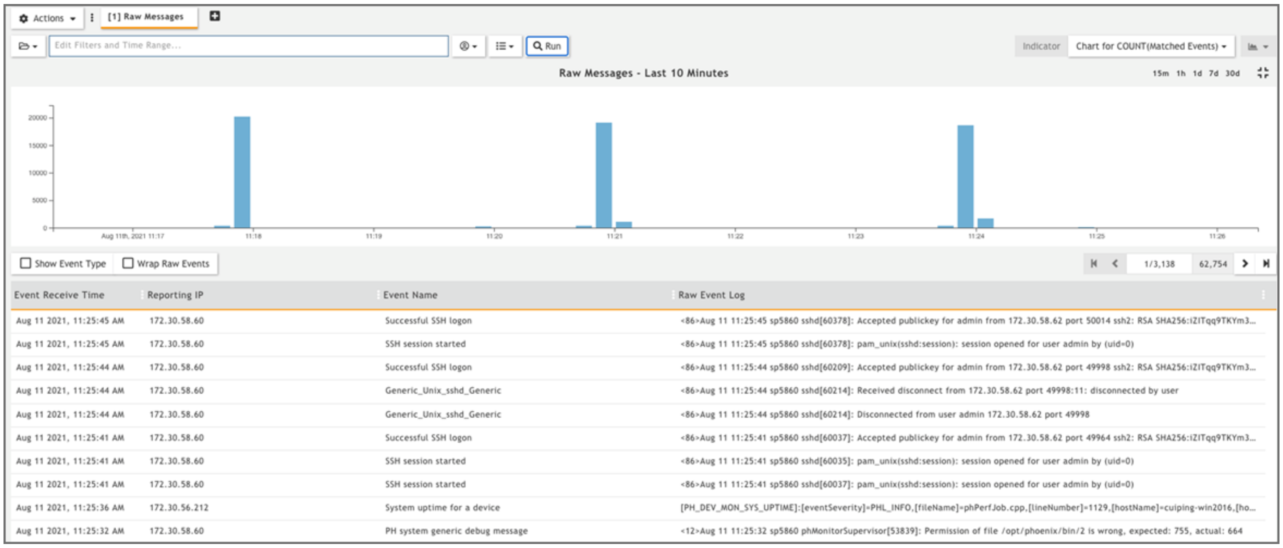
All Collectors will now send events to Site 1.

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.

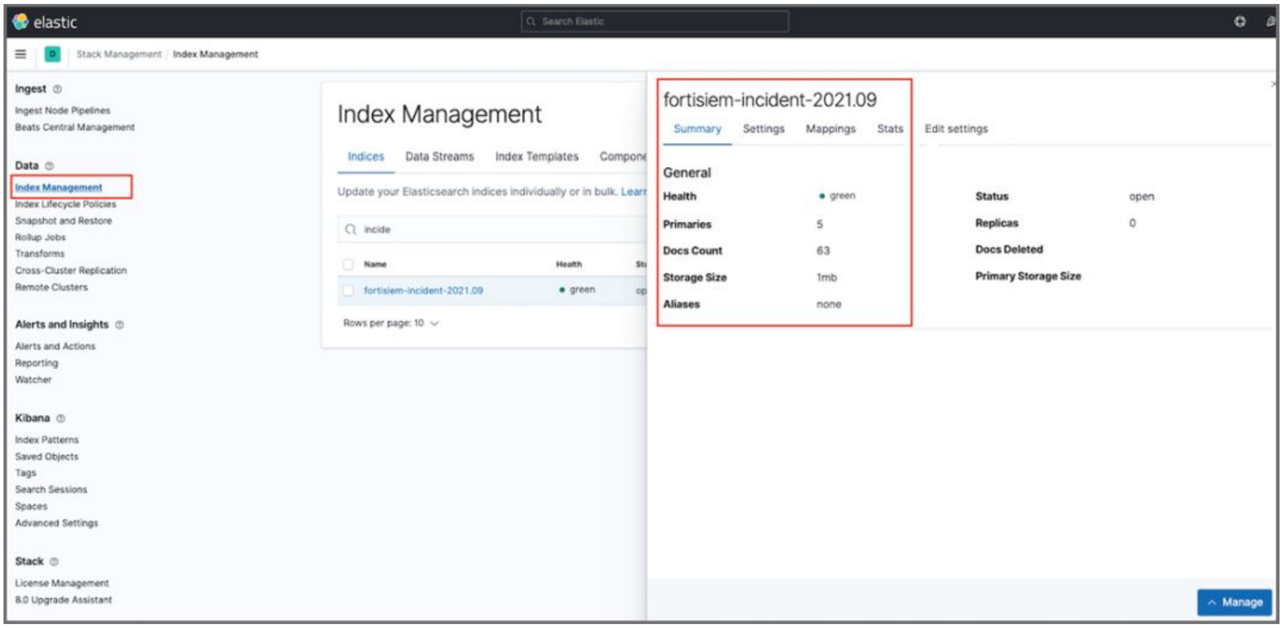


Event Receive Time	Reporting IP	Event Name	Raw Event Log
Aug 11 2021, 11:25:45 AM	172.30.58.60	Successful SSH logon	<86>Aug 11 11:25:45 sp5860 sshd[60378]: Accepted publickey for admin from 172.30.58.62 port 50014 ssh2: RSA SHA256:iZITqq9TKYm3...
Aug 11 2021, 11:25:45 AM	172.30.58.60	SSH session started	<86>Aug 11 11:25:45 sp5860 sshd[60378]: pam_unix(sshd:session): session opened for user admin by (uid=0)
Aug 11 2021, 11:25:44 AM	172.30.58.60	Successful SSH logon	<86>Aug 11 11:25:44 sp5860 sshd[60209]: Accepted publickey for admin from 172.30.58.62 port 49998 ssh2: RSA SHA256:iZITqq9TKYm3...
Aug 11 2021, 11:25:44 AM	172.30.58.60	Generic_Unix_sshd_Generic	<86>Aug 11 11:25:44 sp5860 sshd[60214]: Received disconnect from 172.30.58.62 port 49998:11: disconnected by user
Aug 11 2021, 11:25:44 AM	172.30.58.60	Generic_Unix_sshd_Generic	<86>Aug 11 11:25:44 sp5860 sshd[60214]: Disconnected from user admin 172.30.58.62 port 49998
Aug 11 2021, 11:25:41 AM	172.30.58.60	Successful SSH logon	<86>Aug 11 11:25:41 sp5860 sshd[60037]: Accepted publickey for admin from 172.30.58.62 port 49964 ssh2: RSA SHA256:iZITqq9TKYm3...
Aug 11 2021, 11:25:41 AM	172.30.58.60	SSH session started	<86>Aug 11 11:25:41 sp5860 sshd[60035]: pam_unix(sshd:session): session opened for user admin by (uid=0)
Aug 11 2021, 11:25:41 AM	172.30.58.60	SSH session started	<86>Aug 11 11:25:41 sp5860 sshd[60037]: pam_unix(sshd:session): session opened for user admin by (uid=0)
Aug 11 2021, 11:25:36 AM	172.30.56.212	System uptime for a device	[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=1129,[hostName]=cuiping-win2016,[ho...
Aug 11 2021, 11:25:32 AM	172.30.58.60	PH system generic debug message	<12>Aug 11 11:25:32 sp5860 phMonitorSupervisor[53839]: Permission of file /opt/phoenix/bin/2 is wrong, expected: 755, actual: 664

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.



fortisiem-incident-2021.09

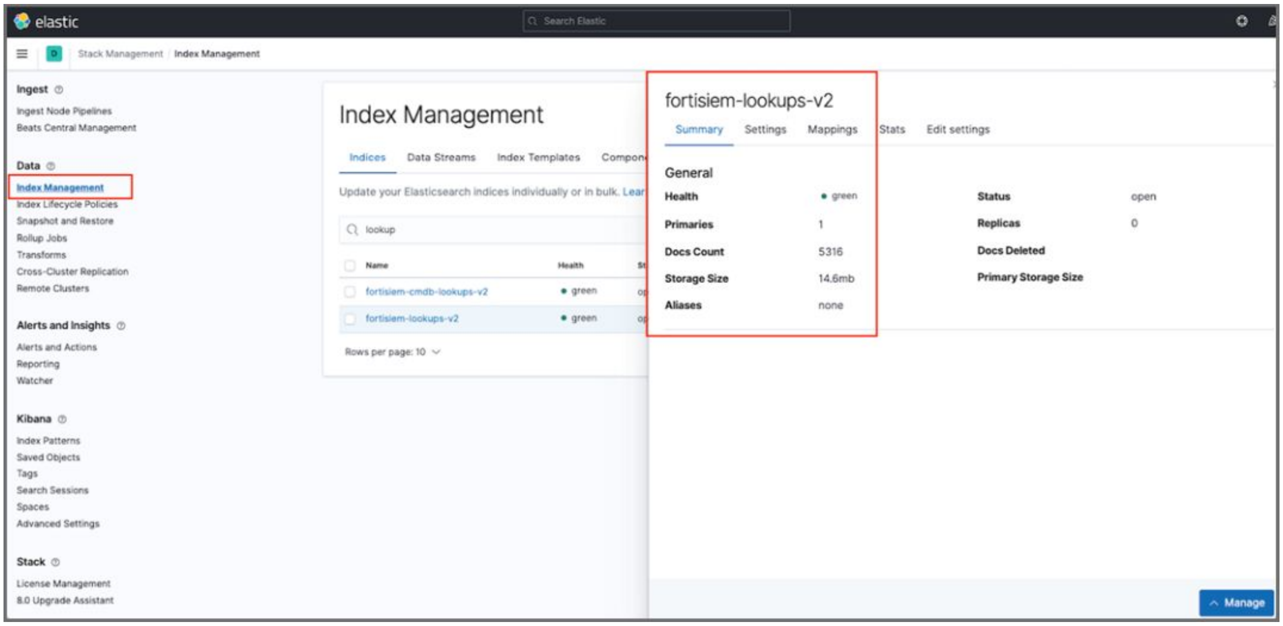
General

Health	● green	Status	open
Primaries	5	Replicas	0
Docs Count	63	Docs Deleted	
Storage Size	1mb	Primary Storage Size	
Aliases	none		

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.



Update your Elasticsearch indices individually or in bulk. Lear

lookup

	Name	Health
□	fortisiem-cmdb-lookups-v2	● green
□	fortisiem-lookups-v2	● green

Rows per page: 10

fortisiem-lookups-v2

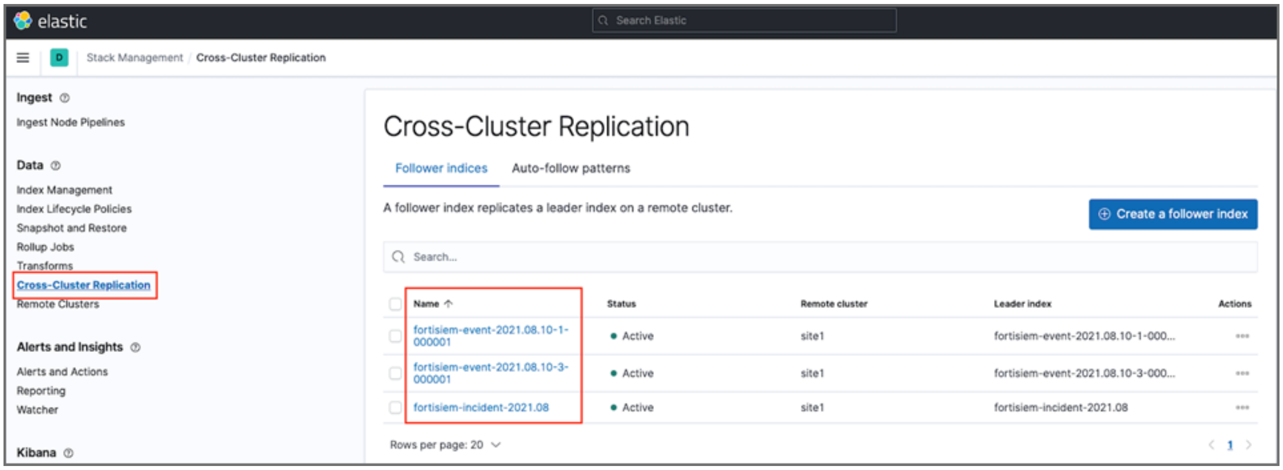
General

Health	● green	Status	open
Primaries	1	Replicas	0
Docs Count	5316	Docs Deleted	
Storage Size	14.6mb	Primary Storage Size	
Aliases	none		

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.



A follower index replicates a leader index on a remote cluster.

Search...

	Name ↑	Status	Remote cluster	Leader index	Actions
□	fortisiem-event-2021.08.10-1-000001	● Active	site1	fortisiem-event-2021.08.10-1-000...	•••
□	fortisiem-event-2021.08.10-3-000001	● Active	site1	fortisiem-event-2021.08.10-3-000...	•••
□	fortisiem-incident-2021.08	● Active	site1	fortisiem-incident-2021.08	•••

Rows per page: 20

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:

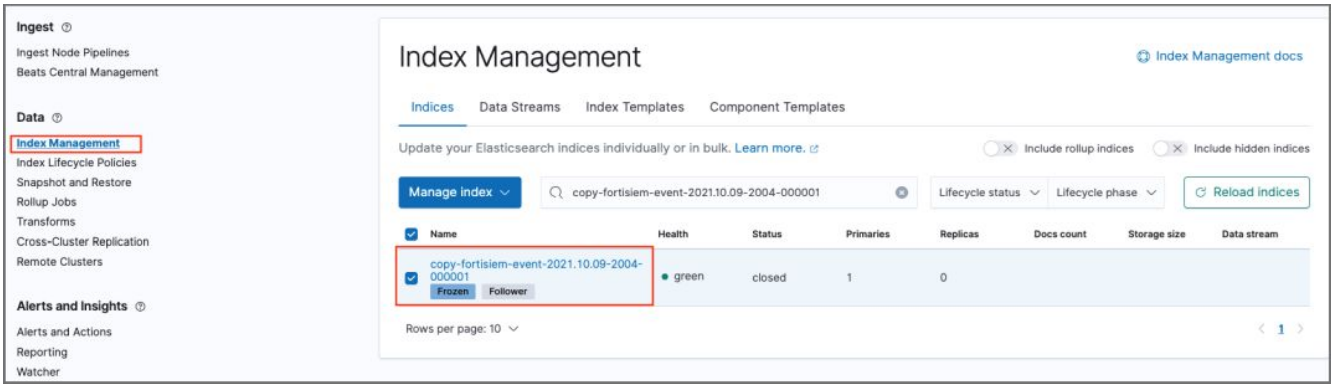
   ```
   curl -X PUT "<Site 1's coordinator ip>:9200/_cluster/settings?pretty" -H 'Content-Type:
   application/json' -d'
   {
     "persistent" : {
       "indices.breaker.request.limit": "85%"
     }
   }
   '

   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.



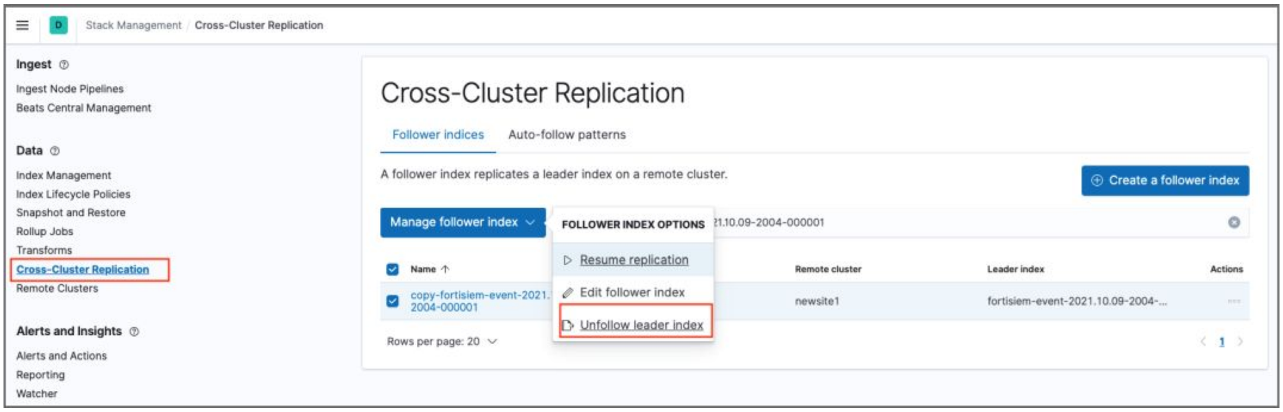
Update your Elasticsearch indices individually or in bulk. Learn more.

Search: copy-fortisiem-event-2021.10.09-2004-000001

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
copy-fortisiem-event-2021.10.09-2004-000001 Frozen Follower	● green	closed	1	0			

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

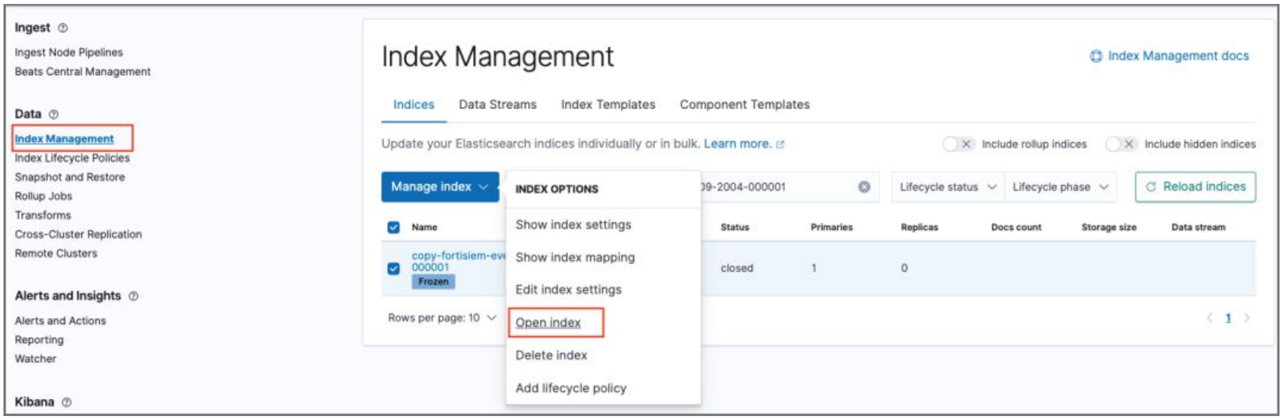
1. Unfollow the index.



A follower index replicates a leader index on a remote cluster.

Name	Remote cluster	Leader index	Actions
copy-fortisiem-event-2021.10.09-2004-000001	newsite1	fortisiem-event-2021.10.09-2004-...	···

2. Open the index.



Update your Elasticsearch indices individually or in bulk. Learn more.

Name	Status	Primaries	Replicas	Docs count	Storage size	Data stream
copy-fortisiem-ev 000001 Frozen	closed	1	0			

FORTINET®

www.fortinet.com