**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**BÁO CÁO**

**TẠO SEARCH AND REPORT,**

**TÌM HIỂU VỀ INDEX CLUSSTER,**

**SERVER CLASS, ROLES BASE OF USER**

Người thực hiện: Mai Thành Thắng

Hà Nội, 9/2019

Mục Lục

[1. Create Search and report 3](#_Toc20261375)

[1.1. Linux 3](#_Toc20261376)

[1.2. Window7 3](#_Toc20261377)

[2. Index cluster 3](#_Toc20261378)

[2.1. Các phần của index cluster: 5](#_Toc20261379)

[2.2. Cài đặt Cluster và tìm kiếm trong Cluster: 5](#_Toc20261380)

[2.3. Multisite indexer clusters: 6](#_Toc20261381)

[2.4. The basics of indexer cluster architecture: 7](#_Toc20261382)

[2.5. Deploy index cluster: 8](#_Toc20261383)

[2.6. Configure the Master 10](#_Toc20261384)

[2.7. Configure the peer 11](#_Toc20261385)

[2.8. Deploy and configure a multisite indexer cluster: 13](#_Toc20261386)

[2.8.View indexer cluster status: 16](#_Toc20261387)

[2.9. Manage the indexer cluster: 19](#_Toc20261388)

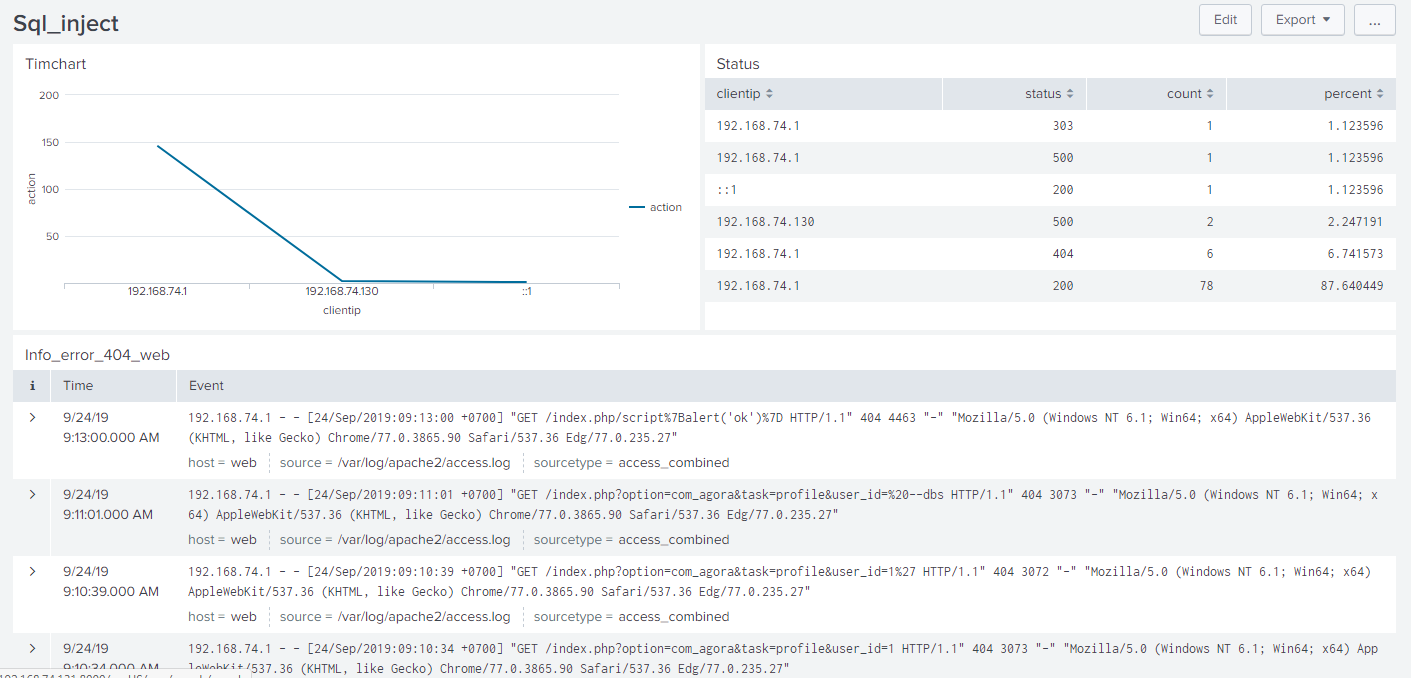
[3. Server class 19](#_Toc20261389)

[4. Roles base of user set up splunk forwarder 21](#_Toc20261390)

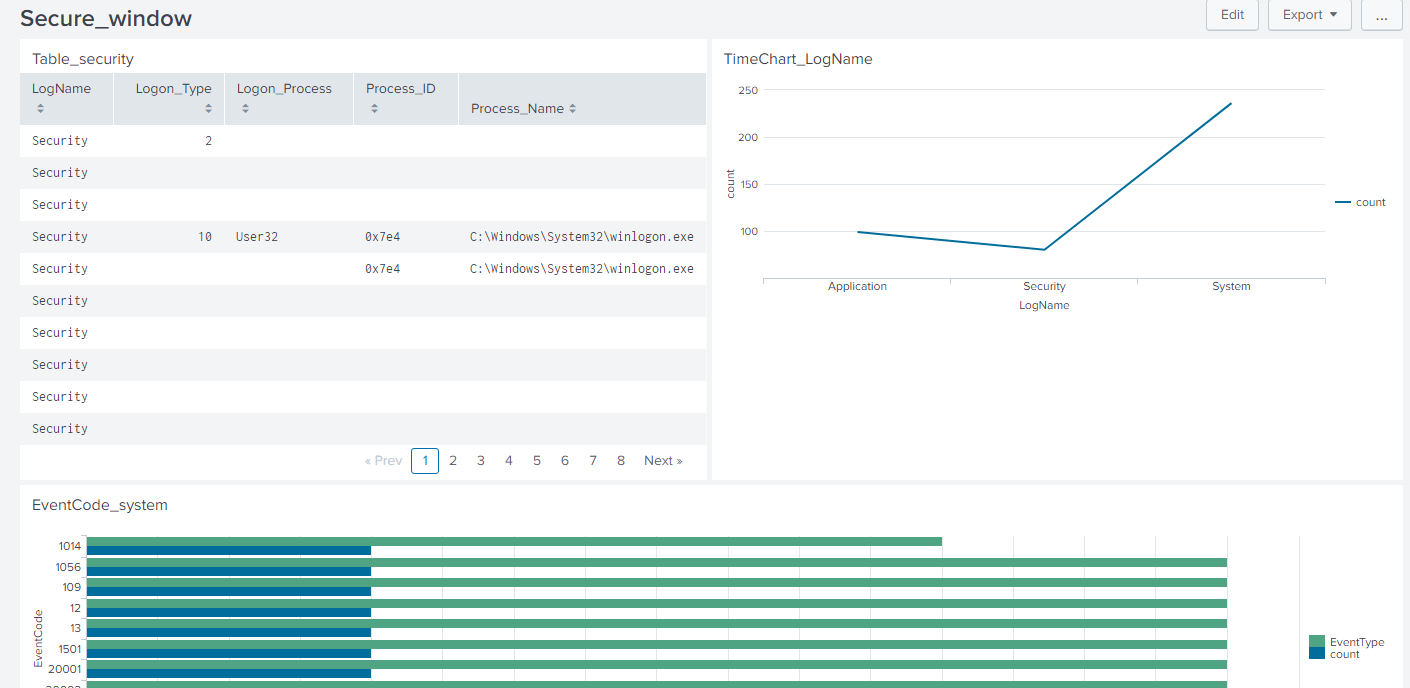
## Create Search and report

### Linux

Status 404 khi truy cập web



### Window7



## Index cluster

Index clusster là một nhóm các Splunk Enterprise indexer được cấu hình để sao chép dữ liệu của nhau, để hệ thống giữ nhiều bản sao của tất cả dữ liệu.

Quá trình này được gọi là sao chép chỉ mục hoặc phân cụm chỉ mục. Bằng cách duy trì nhiều bản sao dữ liệu giống hệt nhau, các cụm ngăn ngừa mất dữ liệu trong khi thúc đẩy tính khả dụng của dữ liệu để tìm kiếm.



* Những lợi ích chính của việc nhân rộng chỉ số là:

+ Dữ liệu sẵn có. Một bộ chỉ mục luôn có sẵn để xử lý dữ liệu đến và dữ liệu được lập chỉ mục có sẵn để tìm kiếm.

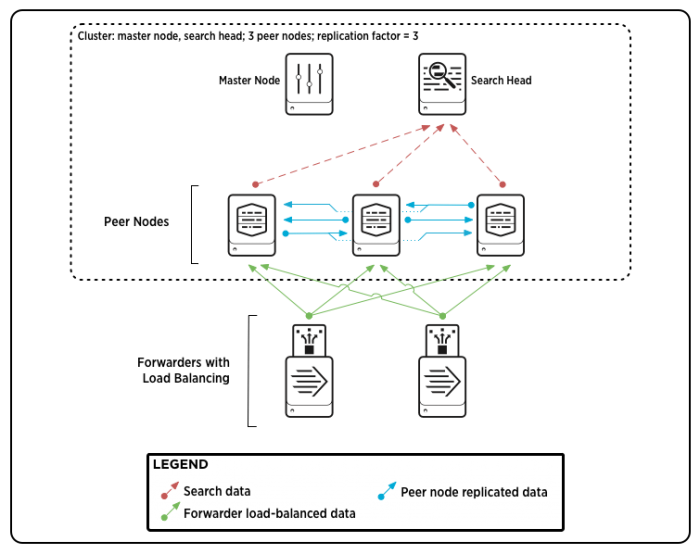
+ Dữ liệu trung thực. Bạn không bao giờ mất bất kỳ dữ liệu. Bạn sẽ đảm bảo rằng dữ liệu được gửi đến cụm chính xác là cùng một dữ liệu được lưu trữ trong cụm và sau đó tìm kiếm có thể truy cập.

+ Phục hồi dữ liệu. Hệ thống có thể chấp nhận các chỉ mục bị giảm mà không mất dữ liệu hoặc mất quyền truy cập vào dữ liệu.

+ Phục hồi sau thảm họa. Với clusster, hệ thống của bạn có thể chịu đựng được thảm họa ảnh hưởng tới toàn bộ trung tâm dữ liệu hệ thống.

+ Tìm kiếm sự giống nhau: các đầu tìm kiếm có thể truy cập toàn bộ bộ dữ liệu thông qua các trang web cục bộ của họ, giúp giảm đáng kể lưu lượng truy cập mạng đường dài.

### 2.1. Các phần của index cluster:

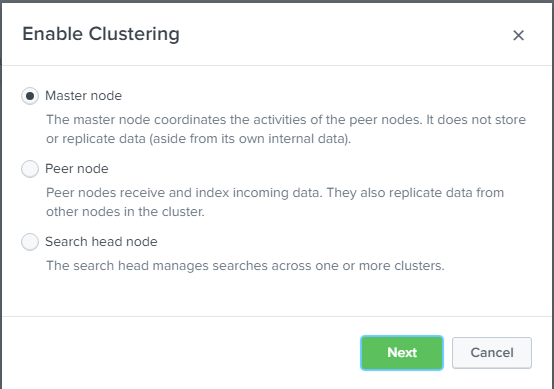


* The **master node** nút chủ quản lý clusster. Nó phối hợp các hoạt động sao chép dữ liệu của các nút ngang hàng và báo cho search head nơi tìm dữ liệu. Nó cũng giúp quản lý cấu hình của các nút ngang hàng và phối hợp các hoạt động khắc phục nếu một nút ngang hàng hỏng.
* The **peer nodes** nhận và lập chỉ mục dữ liệu đến, giống như các bộ chỉ mục không phân cụm, độc lập. Tuy nhiên, không giống như các bộ chỉ mục độc lập, các nút ngang hàng cũng sao chép dữ liệu từ các nút khác trong cụm. Một nút ngang hàng có thể lập chỉ mục dữ liệu đến của chính nó đồng thời lưu trữ các bản sao dữ liệu từ các nút khác. Cần tối thiểu ba nút ngang hàng.
* The **search head** chạy các tìm kiếm trên tập hợp các nút ngang hàng. Bạn phải sử dụng search head để quản lý các tìm kiếm trên các cụm chỉ mục.

Note: **Multisite indexer clusters** cho phép bạn duy trì các bản sao hoàn chỉnh của dữ liệu được lập chỉ mục của mình ở nhiều vị trí. Điều này cung cấp các lợi thế của tăng cường phục hồi thảm họa và tìm kiếm sự giống nhau.

### 2.2. Cài đặt Cluster và tìm kiếm trong Cluster:

- Cài đặt clusster rất dễ: Vào **Setting -> Index clustering** chọn **Enable index clustering** Chọn kiểu cluster bạn muốn dùng.



* Tìm kiếm trong cluster giống như tìm kiếm khi không có cluster. Bạn gửi tìm kiếm của bạn thông qua search head

### 2.3. Multisite indexer clusters:

- Trường hợp sử dụng:

+ Cải thiện khắc phục thảm họa

+ Tìm kiếm dữ liệu giống nhau

* Bạn có thể cấu hình multisite cluster từ  basic, single-site clusters. Khác biệt của multisite cluster:

+ Bạn có thể chỉ định một trang web cho mỗi nút.

+ Bạn có thể chỉ định các yếu tố sao chép và tìm kiếm trên cơ sở từng trang web. Nghĩa là, bạn có thể chỉ định số lượng bản sao và bản sao có thể tìm kiếm mà bạn muốn duy trì trên mỗi trang web, cùng với số lượng bạn muốn duy trì trên toàn bộ cụm.

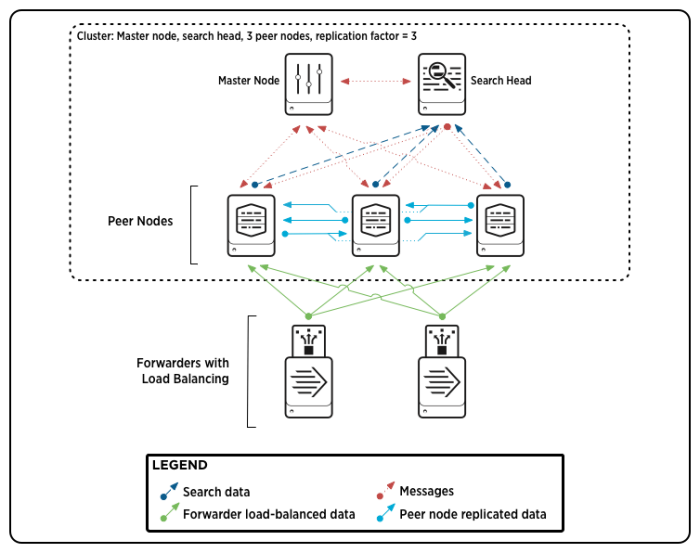
* Kiến trúc đa cluster và một cluster là như nhau. Chỉ có một số điểm khác sau:

+ Mỗi nút thuộc về một trang web được chỉ định.

+ Sao chép các bản sao xảy ra theo cách nhận biết trang web.

+ Serch head chỉ phân phối tìm kiếm dữ liệu trên các điểm nội bộ, bất cứ khi nào có thể.

### 2.4. The basics of indexer cluster architecture:



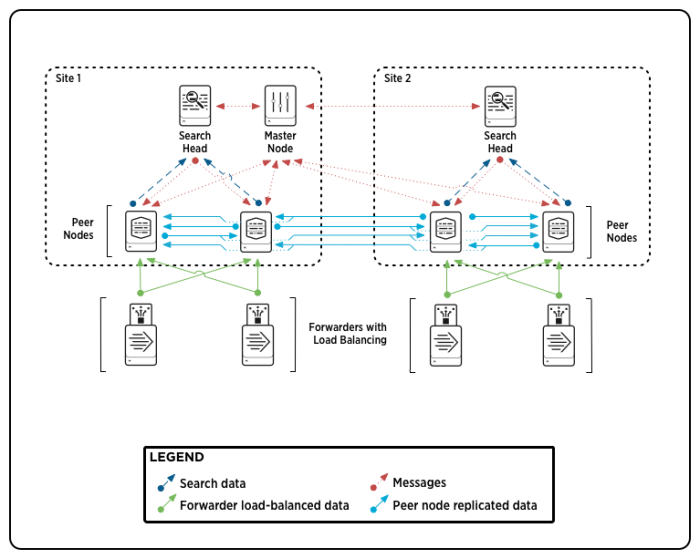
* Khái niệm quan trọng:

[**Replication factor**](https://docs.splunk.com/Splexicon:Replicationfactor). Điều này xác định số lượng bản sao dữ liệu mà cluster duy trì và do đó, xác định mức độ chịu đựng thảm họa cơ bản của cluster.

**Search factor**. Điều này xác định số lượng bản sao dữ liệu có thể tìm kiếm mà cluster duy trì và do đó, cluster có thể phục hồi khả năng tìm kiếm của nó nhanh sau khi nút ngang hàng bị hỏng.

**Buckets.** Buckets là đơn vị lưu trữ chỉ mục cơ bản. Một cluster duy trì số lượng nhân tố sao chép của mỗi Buckets

**Kiến trúc của đa cluster:**



### 2.5. Deploy index cluster:

The procedure in this topic explains how to use Splunk Web to enable a peer node. You can also enable a peer in two other ways:

* Directly edit the peer's server.conf file. See ["Configure peer nodes with server.conf"](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Configurepeerswithserverconf) for details.
* Use the CLI edit cluster-config command. See ["Configure peer nodes with the CLI"](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/ConfigurepeerswithCLI) for details.

#### 2.5.1. Enable the master:

**1.** Click **Settings** in the upper right corner of Splunk Web.

**2.** In the **Distributed environment** group, click **Indexer clustering**.

**3.** Select **Enable indexer clustering**.

**4.** Select **Master node** and click **Next**.

**5.** Lưu ý các trường khi điền:

**- Replication Factor:** Số lượng bản sao của dữ liệu thô mà bạn muốn cluster duy trì. Hệ số sao chép cao hơn bảo vệ chống mất dữ liệu nếu các nút ngang hàng lỗi. Mặc định giá trị là 3.

- **Search factor**: Số lượng bản sao dữ liệu có thể tìm kiếm mà cụm duy trì. Hệ số tìm kiếm cao hơn sẽ tăng tốc thời gian khôi phục dữ liệu bị mất tốn chi phí không gian đĩa. Phải nhỏ hơn hoặc bằng Hệ số nhân rộng.

- **Secure key:** Khóa này xác thực giao tiếp giữa chủ và các điểm và search head.

- **Cluster label**: Nhãn này cũng được sử dụng để xác định cụm này trong Bảng điều khiển giám sát.

#### 2.5.2. Peer node:

- Các bước cài đặt ban đầu giống từ 1-4.

- Bước 5: điền thông tin vào trường

**Master URI**. Nhập URI của chủ, bao gồm cả cổng quản lý của nó. Ví dụ: <https://10.152.31.202:8089>

**Peer replication port.** Đây là cổng mà ngang hàng nhận được dữ liệu sao chép được truyền phát từ các node khác. Bạn có thể chỉ định bất kỳ cổng có sẵn nào. Cổng này phải khác với cổng quản lý hoặc nhận.

**Secure key**.(tương tự như master node)

#### 2.5.3. Search head node:

- Các bước từ 1-4 giống nhau.

- Bước 5: chỉ điển 2 trường Master URI và Secure Key. Thông tin giống như trên.

### 2.6. Configure the Master

#### 2.6.1. Configure the master with the dashboard:

* In Splunk Web, click **Settings > Indexer clustering**.  
  The Master Node dashboard appears.
* Select the **Edit** button on the upper right side of the dashboard.  
  The **Edit** button presents several options:
  + **Node Type**. Change the instance's node type. **Caution:** Điều cực kỳ khó xảy ra là bạn sẽ muốn thay đổi loại nút cho các nút trong một cụm hoạt động. Hãy xem xét hậu quả cẩn thận trước khi làm.
  + **Master Node Configuration**. Change these master node settings:
    - **Replication Factor**. Change the cluster's replication factor. **Caution:** Việc tăng hệ số sao chép sau khi cụm của bạn chứa lượng dữ liệu đáng kể là không thể. Làm như vậy sẽ khởi động rất nhiều hoạt động của nhóm, điều này sẽ có ảnh hưởng xấu đến hiệu suất của cụm trong khi các bản sao của nhóm đang được tạo.
    - **Search Factor**. Change the cluster's search factor. **Caution:** Việc tăng hệ số sao chép sau khi cụm của bạn chứa lượng dữ liệu đáng kể là không thể. Làm như vậy sẽ khởi động rất nhiều hoạt động của nhóm, điều này sẽ có ảnh hưởng xấu đến hiệu suất của cụm trong khi các bản sao của nhóm đang được tìm kiếm.
    - **Security Key**. Change the security key. Chỉ thay đổi khóa bảo mật nếu bạn cũng thay đổi nó cho tất cả các nút khác trong cụm. Khóa phải giống nhau trên tất cả các phiên bản trong một cụm.
    - **Cluster Label**. Label the cluster. Thuận lợi cho làm dashboard

#### 2.6.2. Configure the master with server.conf:

[clustering]

mode = master

replication\_factor = 4

search\_factor = 3

pass4SymmKey = whatever

cluster\_label = cluster1

#### 2.6.3. [Configure the master with the CLI](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/ConfiguremasterwithCLI):

-Enable:

splunk edit cluster-config -mode master -replication\_factor 4 -search\_factor 3 -secret your\_key -cluster\_label cluster1

splunk restart

- Edit: splunk edit cluster-config command

**Note**: Trong các trường hợp hạn chế (ví dụ: để thực hiện kiểm tra hoặc giám sát cục bộ), bạn có thể tạo một indexes.conf chỉ cho một máy ngang hàng.

### 2.7. Configure the peer

#### 2.7.1. [Configure peer nodes with the dashboard](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Configurepeerswithdashboard):

**1.** Click **Settings** on the upper right side of Splunk Web.

**2.** In the **Distributed Environment** group, click **Indexer clustering**.

**3.** Select the **Edit** button on the upper right side of the dashboard.

The **Edit** button provides a number of options that affect the configuration.

**Note:** The **Edit** button is disabled for multisite clusters.

#### 2.7.2. [Configure peer nodes with server.conf](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Configurepeerswithserverconf):

[replication\_port://9887]

[clustering]

master\_uri = https://10.152.31.202:8089

mode = slave

pass4SymmKey = whatever

This example specifies that:

* the peer will use port 9887 to listen for replicated data streamed from the other peers. You can specify any available, unused port as the replication port. Do not re-use the management or receiving ports.
* the peer's cluster master resides at 10.152.31.202:8089.
* the instance is a cluster peer ("slave") node.
* the security key is "whatever".

#### 2.7.3. [Configure peer nodes with the CLI](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/ConfigurepeerswithCLI)

- Configure:

splunk edit cluster-config -mode slave -master\_uri https://10.160.31.200:8089 -replication\_port 9887 -secret your\_key

splunk restart

* Edit:

splunk edit cluster-config

#### 2.8. Configure the search head

#### 2.8.1. [Configure the search head with the dashboard](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Configuresearchheadwithdashboard):

**1.** Click **Settings** on the upper right side of Splunk Web.

**2.** In the **Distributed Environment** group, click **Indexer clustering**.

The dashboard includes a number of menu items and actions that affect the configuration.

Để xóa đầu tìm kiếm khỏi cụm chỉ mục, chọn hành động **Remove Cluster** trên hàng cho cụm đó.

#### 2.8.2. [Configure the search head with server.conf](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Configuresearchheadwithserverconf):

[clustering]

master\_uri = https://10.152.31.202:8089

mode = searchhead

pass4SymmKey = whatever

This example specifies that:

* the search head's cluster master resides at 10.152.31.202:8089.
* the instance is a cluster search head.
* the security key is "whatever".

#### 2.8.3. [Configure the search head with the CLI](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/ConfiguresearchheadwithCLI):

-Configure

splunk edit cluster-config -mode searchhead -master\_uri https://10.160.31.200:8089 -secret your\_key

splunk restart

-Edit:

You use the splunk edit cluster-config command. To change the search head configuration, you must instead use the splunk edit cluster-master command.

#### 2.8.4. [Search across multiple indexer clusters](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Configuremulti-clustersearch):

- Trên Web :

**1.** Select the **Add cluster to be searched** button on the uppper right corner of the dashboard.

**2.** Fill out the fields in the pop-up window:

* **Master URI**. Enter the master's URI, including its management port. For example: [https://10.152.31.202:8089](https://10.152.31.202:8089/).
* **Security Key**. This is the key that authenticates communication between a cluster's master, peers, and search heads.
* **Bằng CLI**:

splunk add cluster-master <master\_uri:port>

splunk edit cluster-master <master\_uri:port>

splunk remove cluster-master <master\_uri:port>

splunk list cluster-master

* Edit server.conf

[clustering]

mode = searchhead

master\_uri = clustermaster:east, clustermaster:west

[clustermaster:east]

master\_uri=https://SplunkMaster01.example.com:8089

pass4SymmKey=someSecret

[clustermaster:west]

master\_uri=https://SplunkMaster02.example.com:8089

pass4SymmKey=anotherSecret

### 2.8. Deploy and configure a multisite indexer cluster:

#### 2.8.1. [Configure multisite indexer clusters with server.conf](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Multisiteconffile):

- Site values: Giá trị trang web xác định trang web mà một nút tồn tại. Bạn chỉ định một giá trị trang web cho mỗi nút trong một cụm nhiều trang.

- Configure the master node:

[general]

site = site1

[clustering]

mode = master

multisite = true

available\_sites = site1,site2

site\_replication\_factor = origin:2,total:3

site\_search\_factor = origin:1,total:2

pass4SymmKey = whatever

cluster\_label = cluster1

* + Configure the peer nodes:

[general]

site = site1

[replication\_port://9887]

[clustering]

master\_uri = https://10.152.31.202:8089

mode = slave

pass4SymmKey = whatever

* + Configure the search heads:

[general]

site = site1

[clustering]

multisite = true

master\_uri = https://10.152.31.202:8089

mode = searchhead

pass4SymmKey = whatever

#### 2.8.2. [Configure multisite indexer clusters with the CLI](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/MultisiteCLI):

- Site values.

**Configure the master node**

splunk edit cluster-config -mode master -multisite true -available\_sites site1,site2 -site site1 -site\_replication\_factor origin:2,total:3 -site\_search\_factor origin:1,total:2

splunk restart

**Configure the peer nodes**

splunk edit cluster-config -mode slave -site site1 -master\_uri https://10.160.31.200:8089 -replication\_port 9887 -secret your\_key

splunk restart

**Configure the search heads**

splunk edit cluster-config -mode searchhead -site site1 -master\_uri https://10.160.31.200:8089 -secret your\_key

splunk restart

**Note:** Khi bạn chỉ định tham số site , the commad tự động sets multisite=true in the search head's server.conf file. Bạn không nhất thiết phải tìm cách cài tham số multisite.

To edit the search head configuration later:

splunk edit cluster-config -mode searchhead -master\_uri https://10.160.31.200:8089

splunk restart

splunk edit cluster-master https://10.160.31.200:8089 -site site1

**Important:** The splunk edit cluster-master command always takes the current master URI:port

#### 2.8.3. [Configure the site replication factor](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Sitereplicationfactor) and site search factor:

[clustering]

mode = master

multisite=true

available\_sites=site1,site2

site\_replication\_factor = origin:2,total:3

site\_search\_factor = origin:1,total:2

#### 2.8.4. [Migrate an indexer cluster from single-site to multisite](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Migratetomultisite):

**Configure the master to convert existing buckets to multisite:**

[clustering]

mode = master

constrain\_singlesite\_buckets = false

**Thực hiện di chuyển nhiều trang**

**1.**Configure the master node for multisite and restart it.

splunk edit cluster-config -mode master -multisite true -available\_sites site1,site2 -site site1 -site\_replication\_factor origin:2,total:3 -site\_search\_factor origin:1,total:2

splunk restart

**2.** Set maintenance mode on the master:

splunk enable maintenance-mode

**3.** Configure the existing peer nodes for multisite.

splunk edit cluster-config -site site1

**4.** If you want to add new peers to the cluster:

splunk edit cluster-config -mode slave -site site1 -master\_uri https://10.160.31.200:8089 -replication\_port 9887

splunk restart

**5.** Configure the search heads for multisite

splunk edit cluster-master https://10.160.31.200:8089 -site site1

**6.** If you want to add new search heads to the cluster

splunk edit cluster-config -mode searchhead -site site1 -master\_uri https://10.160.31.200:8089

splunk restart

**7.** Disable maintenance mode on the master:

splunk disable maintenance-mode

Để xác nhận rằng chủ đã rời khỏi chế độ bảo trì,run splunk show maintenance-mode.

8. Nếu bạn đang sử dụng indexer discovery để kết nối các nhà chuyển tiếp với các nút ngang hàng, bạn phải chỉ định một trang web cho mỗi giao nhận

### 2.8.View indexer cluster status:

#### 2.8.1. [View the master dashboard](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster) :

1. Click **Settings** on the upper right side of Splunk Web.
2. In the **Distributed Environment** group, click **Indexer clustering**.

Hiển thị lên cho chúng ta thấy được bảng điều khiển Master Node có những trường sau:

* [**Cluster overview**](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster#Cluster_overview)
* [**Peers tab**](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster#Peers_tab)
* [**Indexes tab**](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster#Indexes_tab)
* [**Search Heads tab**](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster#Search_heads_tab)

##### *2.8.1.1.* [*Cluster overview*](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster#Cluster_overview)*:*

Tổng quan về cụm tóm tắt thông tin của cluster của bạn:

* Liệu dữ liệu của cụm có thể tìm kiếm đầy đủ hay không; nghĩa là, liệu tất cả các nhóm trong cụm có một bản sao chính hay không.
* Liệu các yếu tố tìm kiếm và nhân rộng đã được đáp ứng.
* Có bao nhiêu peer có thể tìm kiếm.
* Có bao nhiêu chỉ mục có thể tìm kiếm.

**Tùy thuộc vào thông tin của cluster hiện tại bạn đang thấy hệ thống sẽ trả về những cảnh báo:**

* Một số dữ liệu không thể tìm kiếm được.
* Yếu tố nhân rộng không được đáp ứng.
* Yếu tố tìm kiếm không được đáp ứng.

**Ở phía trên bên phải của bảng điều khiển, có ba nút:**

* **Edit.** For information on this button.
* **More Info.** This button provides details on the master node configuration:
  + **Name**. The master's serverName, as specified in the master's $SPLUNK\_HOME/etc/system/local/server.conf file.
  + **Replication Factor**.
  + **Search Factor**.
  + **Generation ID.**
* **Documentation.**

##### *2.8.1.2. Peers tab:*

* **Peer Name.** The peer's serverName, as specified in the peer's $SPLUNK\_HOME/etc/system/local/server.conf file.
* **Fully searchable.** This column indicates whether the peer currently has a complete set of primaries and is fully searchable.
* **Site.** (For multisite only.) This column displays the site value for each peer.
* **Status.** The peer's status.
* **Buckets.** The number of buckets for which the peer has copies.

Để có thêm thông tin cho bất kỳ peer nào, nhấp vào mũi tên bên trái của tên peer:

* **Location.** The peer's IP address and port number.
* **Last Heartbeat.** The time of the last heartbeat the master received from the peer.
* **Replication port.** The port on which the peer receives replicated data from other peers.
* **Base generation ID.** The peer's base generation ID, which is equivalent to the cluster's generation ID at the moment that the peer last joined the cluster.
* **GUID.** The peer's GUID

##### *2.8.1.3.* [*Indexes tab*](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster#Indexes_tab)

* **Index Name.** The name of the index.
* **Fully searchable.** Là chỉ số đầy đủ có thể tìm kiếm? Nói cách khác, nó có ít nhất một bản sao có thể tìm kiếm của mỗi nhóm không? Nếu thậm chí một nhóm trong chỉ mục không có bản sao có thể tìm kiếm, trường này sẽ báo cáo chỉ mục là không thể tìm kiếm.
* **Searchable Data Copies.** The number of complete searchable copies of the index that the cluster has.
* **Replicated Data Copies.** The number of copies of the index that the cluster has. Each copy must be complete, with no buckets missing.
* **Buckets.** The number of buckets in the index. This number does not include replicated bucket copies.
* **Cumulative Raw Data Size.** The size of the index's raw data, excluding hot buckets. This number does not included replicated copies of the raw data.

##### *2.8.1.4.* [*Search Heads tab*](http://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howtomonitoracluster#Search_heads_tab)

* **Search head name.** The search head's serverName, as specified in its $SPLUNK\_HOME/etc/system/local/server.conf file.
* **Site.** (For multisite only.) This column displays the site value for each search head.
* **Status.** Is the search head up or down? The master decides that a search head is down if the search head does not poll the master for generation information within a period twice the length of the generation\_poll\_interval. That attribute is configurable in server.conf.

#### 2.8.2. [View the peer dashboard](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Viewthepeerdashboard)

**1.** Click **Settings** on the upper right side of Splunk Web.

**2.** In the **Distributed Environment** group, click **Indexer clustering**.

You can only view this dashboard on an instance that has been enabled as a peer.

Bảng điều khiển cung cấp thông tin về trạng thái:

* **Name**. The peer's serverName, as specified in its $SPLUNK\_HOME/etc/system/local/server.conf file.
* **Replication port.** The port on which the peer receives replicated data from other peers.
* **Master location.** The master node's IP address and port number.
* **Base Generation ID.** The peer's base generation ID, which is equivalent to the cluster's [**generation ID**](https://docs.splunk.com/Splexicon:GenerationID) at the moment that the peer last joined the cluster.

#### 2.8.3. [View the search head dashboard](https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Viewthesearchheaddashboard)

Bảng điều khiển này cung cấp thông tin chi tiết về trạng thái của đầu tìm kiếm trong cụm chỉ mục

To access the dashboard:

**1.** Click **Settings** on the upper right side of Splunk Web.

**2.** In the **Distributed Environment** group, click **Indexer clustering**.

Bạn có thể xem dash board bằng cách  enabled as a cluster search head.

Bảng điều khiển liệt kê master nodes for all clusters the search head nó cho ta thấy được trạng thái của mỗi cluster.

Để biết thêm thông tin master node and its cluster  nhấp vào mũi tên ở bên trái của mỗi hàng

Bạn có thể lấy thông tin khi click vào More info ở góc trên bên phải của bảng điều khiển:

**Name**. The search head's serverName, as specified in its $SPLUNK\_HOME/etc/system/local/server.conf file.

Xem thông tin về các search peers

**1.** On the search head, click **Settings** in the upper right corner of Splunk Web.

**2.** In the **Distributed environment** section, click **Distributed search**.

**3.** Click **Search peers** to view the set of search peers.

Note: Không sử dụng trang Tìm kiếm phân tán trong Splunk Web để thay đổi cấu hình đầu tìm kiếm của bạn hoặc để thêm các peer.

### 2.9. Manage the indexer cluster:

Sử dụng chế độ bảo trì

Khởi động lại toàn bộ cụm chỉ mục hoặc một nút ngang hàng

Sử dụng khởi động lại

Cân bằng lại cụm chỉ mục

Loại bỏ các bản sao xô dư thừa khỏi cụm chỉ mục

Đặt một người ngang hàng

Xóa một đồng đẳng khỏi danh sách của chủ

## Server class

**Set up server class on GUI:**

1. From the Apps tab in Forwarder Management, in the "sendtoindexer" listing under "Actions", click **Edit**. Splunk Enterprise loads the "Edit app: sendtoindexer" page.
2. Click "+" under "Server Classes."
3. In the pop-up that appears, click **New Server Class**.
4. In the "New Server Class" dialog box that pops up, enter "Universal Forwarders".
5. Click **Save**. Splunk Enterprise saves the class and loads the information page for the server class you just created.  
   **Note:** When you first create a server class, the page says you have not added any apps or clients yet. This is okay.
6. Click **Add apps**. The "Edit Apps" page loads.
7. Locate and click the "sendtoindexer" app in the "Unselected Apps" pane on the left. The app moves to the "Selected Apps" pane on the right.
8. Click **Save**. The configuration saves and the server class information page reappears.

**Create Server class by CLI:**

* Cài đặt splunk forwarder trên mỗi server .
* Cấu hình deployment-client: (Đặt máy chủ triển khai để cập nhật thăm dò)

./splunk set deploy-poll 192.168.74.131:8089

./splunk restart

* Cấu hình app:

cd /opt/splunk/etc/deployment-apps/

mkdir linuxfile

cd linuxfile

mkdir localweb1 localweb2

cd /opt/splunk/etc/system/local/

nano serverclass.conf

[serverClass:Linux:app:linuxfile]

restartSplunkWeb = 0

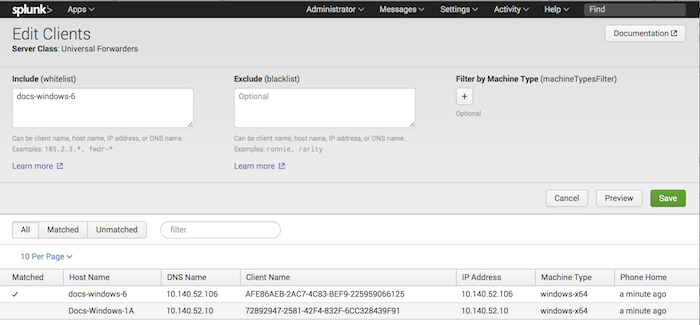
restartSplunkd = 0

stateOnClient = enabled

[serverClass:Linux]

whitelist.0 = web

**Tiếp theo là cấu hình nhận các forwarder từ agent cài forwarder. Kiểm tra kỹ xem splunk forwarder đã chạy chưa? Làm như bước sau:**

1. Log into the Splunk indexer you set up previously.
2. In the system bar, click **Settings > Forwarder Management**
3. Click the **Clients** tab. You should see the universal forwarder you installed in the previous step. If you don't, confirm that the forwarder service is active and that its configuration points to this deployment server.
4. Click the **Server Classes** tab.
5. In the server class you created earlier ("Universal Forwarders"), click **Edit**.
6. In the pop-up that appears, click **Edit Clients**. The "Edit clients" page loads.  
   [](https://docs.splunk.com/File:Exch_31_basicsetup_servclasseditclients.png)  
   This page lists all clients that have connected to the deployment server. Those clients appear on the page below the **Include**, **Exclude**, and **Filter by Machine Type** controls at the top.
7. In the **Include (whitelist)** field at the top of the page, type in the host name of the deployment client.
8. Click **Preview**. The list updates to show you which clients match the string you entered in the "Include (whitelist)" field.
9. If the results look acceptable, click **Save**. The Forwarder Management page reappears and the deployment server deploys the "send to indexer" app to the deployment client.

## Roles base of user set up splunk forwarder

Quyền hạn của user được admin set trong policy của hệ thống. Nó sẽ là quyền được đọc thông tin cấu hình trong splunk forwarder. Họ có thể được xem biết được những sự kiện nào trên máy mình được forward tới splunk server.

**Phần 1: cấu hình trên thiết bị**

**Phần 2: Cấu hình splunk**

**Phần 3: build dashboard, report**