COHESITY

Integrate Splunk with Cohesity

Version 1.1

August 2025

ABSTRACT

This document guides you on integrating Splunk (Enterprise and Cloud) with Cohesity (Self-managed clusters and Cohesity Data Cloud) to enhance the security visibility, investigation, and rapid response of Cohesity events to achieve business success.

Table of Contents

Figures

Tables

General Information

Purpose and Scope

This document provides technical guidance on integrating Splunk (Enterprise and Cloud) with Cohesity (Self-managed clusters and Cohesity Data Cloud). It discusses each integration scenario in detail with elaborate steps and screenshots. It also discusses how to troubleshoot the issues if you encounter one during the integration.

Intended Audience

This document is intended for anyone willing to integrate Splunk with Cohesity. It doesn't require you to be an expert in Splunk, however, you must be versed in the basics of managing Cohesity Clusters and(or) Cohesity Data Cloud. This document assumes that:

- The reader has general knowledge of Cohesity Cluster(s) and(or) Cohesity Data Cloud and how to use it.
- The reader has basic knowledge of Splunk and what it does.
- The reader is already using a Cohesity Cluster(s) or Cohesity Data Cloud.
- The reader is already using Splunk Enterprise and(or) Splunk Cloud.

How to use this Guide

- If you are an expert in Splunk and need quick integration, refer to Quick Webhook Integration in 5 steps.
- If you are a beginner and need detailed step-by-step guidance, then refer to Integrate Cohesity with Splunk Enterprise and Integrate Cohesity with Splunk Cloud.
- If you already have set up your Cohesity and Splunk integration, and are not getting alerts and logs in Splunk, refer to Troubleshooting.
- If you already have set up your Cohesity and Splunk integration and want to know how to search for Cohesity logs in Splunk, refer to Search and Reporting.
- If you have any questions regarding the integration, refer to Frequently Asked Questions.

Cohesity and Splunk Integration

Overview

Integrating Cohesity with Splunk enables you to send alerts and audit logs from Cohesity sources to Splunk. Splunk captures and indexes these alerts and audit logs in searchable repository using which it can generate graphs, reports, alerts, dashboards, and visualizations.

- Cohesity sources can be
  - Self-managed Cohesity clusters *(On-premises and Cloud)*
  - Cohesity Data Cloud
    - DataProtect *(Self-managed Cohesity clusters - On-premises, and Cloud)*
    - DataProtect as a Service *(Cohesity SaaS)*
- Splunk can be
  - Splunk Enterprise (On-premises)
  - Splunk Cloud

Figure 1: Cohesity and Splunk Integration

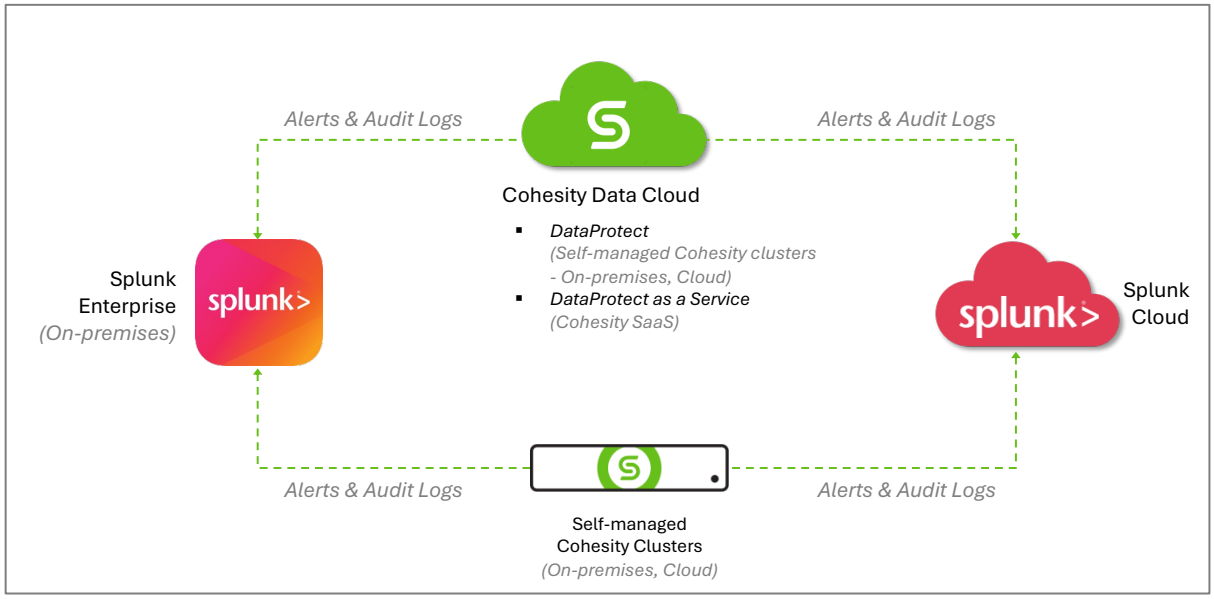


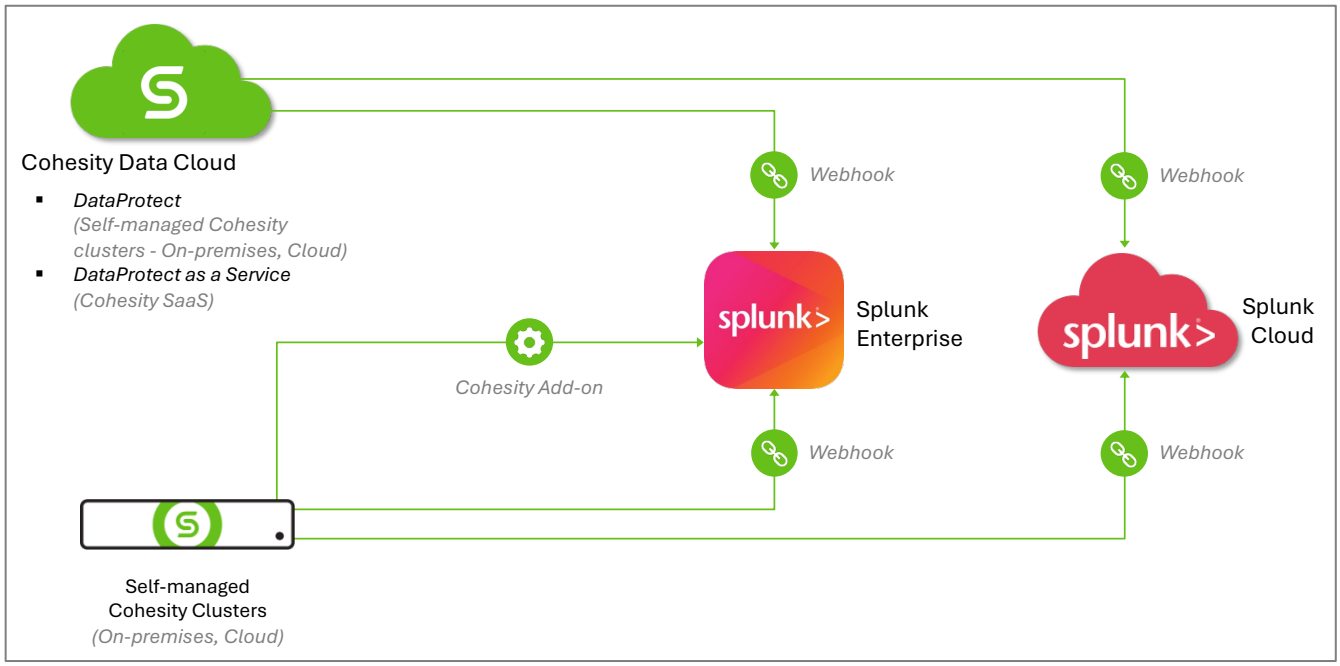
Table 1: Cohesity and Splunk Compatibility Matrix

	Splunk Enterprise	Splunk Cloud
Self-managed Cohesity Clusters	✓	✓
Cohesity Data Cloud	✓	✓

Integration Types

Cohesity can communicate with Splunk via webhook or Cohesity add-on *(uses REST APIs).*

Figure 2: Cohesity and Splunk Integration Types



1. **Webhook** – is an HTTP callback that gets triggered by an event. A webhook is configured on a source website with a destination website URL. When an event occurs on the source website, an HTTP request is made to the destination website.
   In Cohesity and Splunk integration, a webhook is configured at Cohesity side (source) with Splunk URL as the destination. So, whenever an alert or audit log is triggered at Cohesity side, it transmits the same to Splunk via this webhook.
2. **Cohesity add-on** – is a *Splunk app developed by Cohesity*, published in Splunkbase, that uses secure REST APIs to transmit alerts and audit logs from your self-managed Cohesity clusters *(On-premises/Cloud)* to Splunk enterprise *(On-premises).*

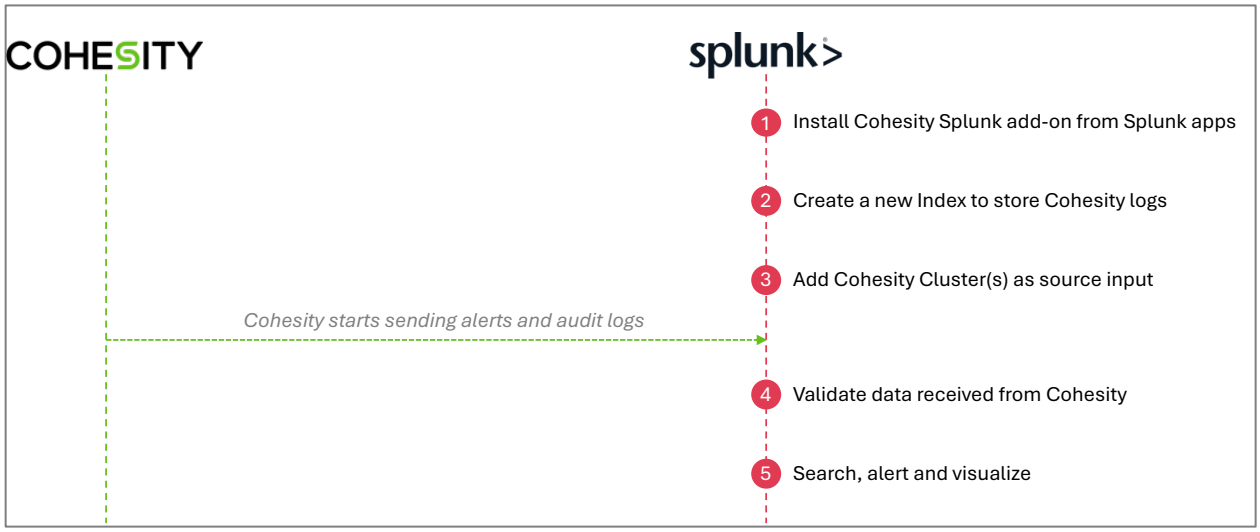
Table 2: Cohesity and Splunk Integration Matrix

		Splunk Enterprise	Splunk Cloud
Webhook Integration	Self-managed Cohesity Clusters	✓	✓
	Cohesity Data Cloud	✓	✓
Cohesity Add-on Integration	Self-managed Cohesity Clusters	✓	✗
	Cohesity Data Cloud	✗	✗

Integration Workflow

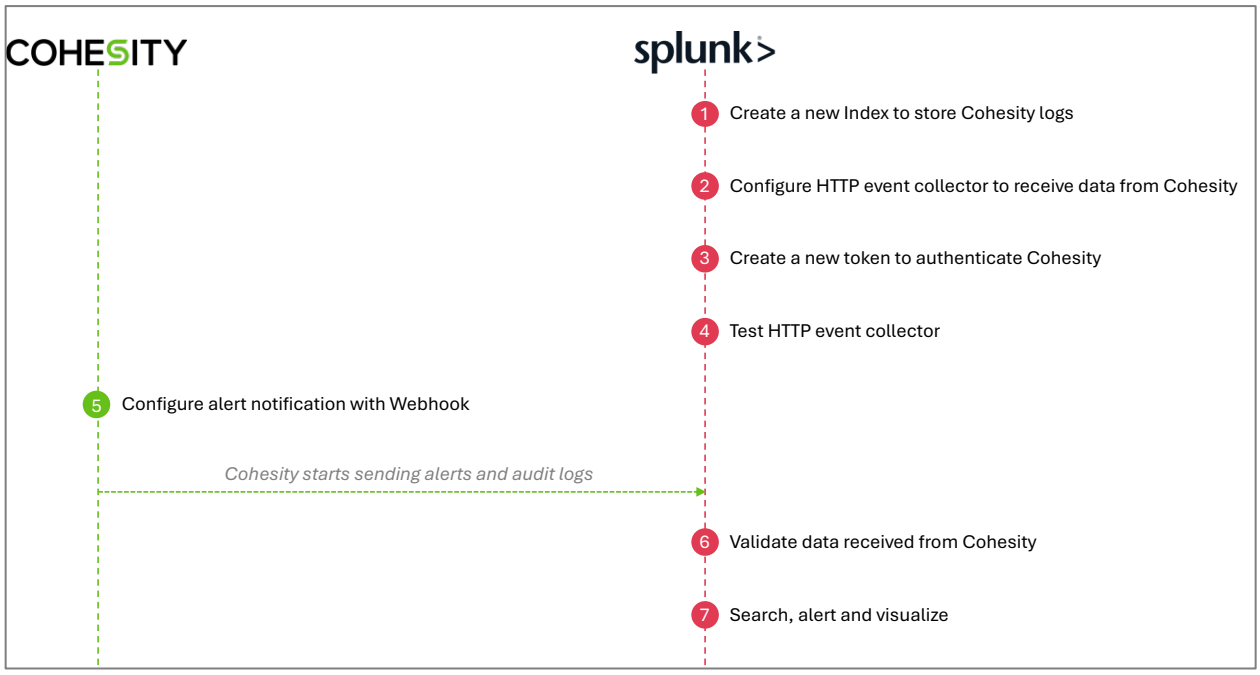
Cohesity Splunk Add-on Integration Workflow

Figure 3: Cohesity Add-on Integration Workflow



Webhook Integration Workflow

Figure 4: Webhook Integration Workflow



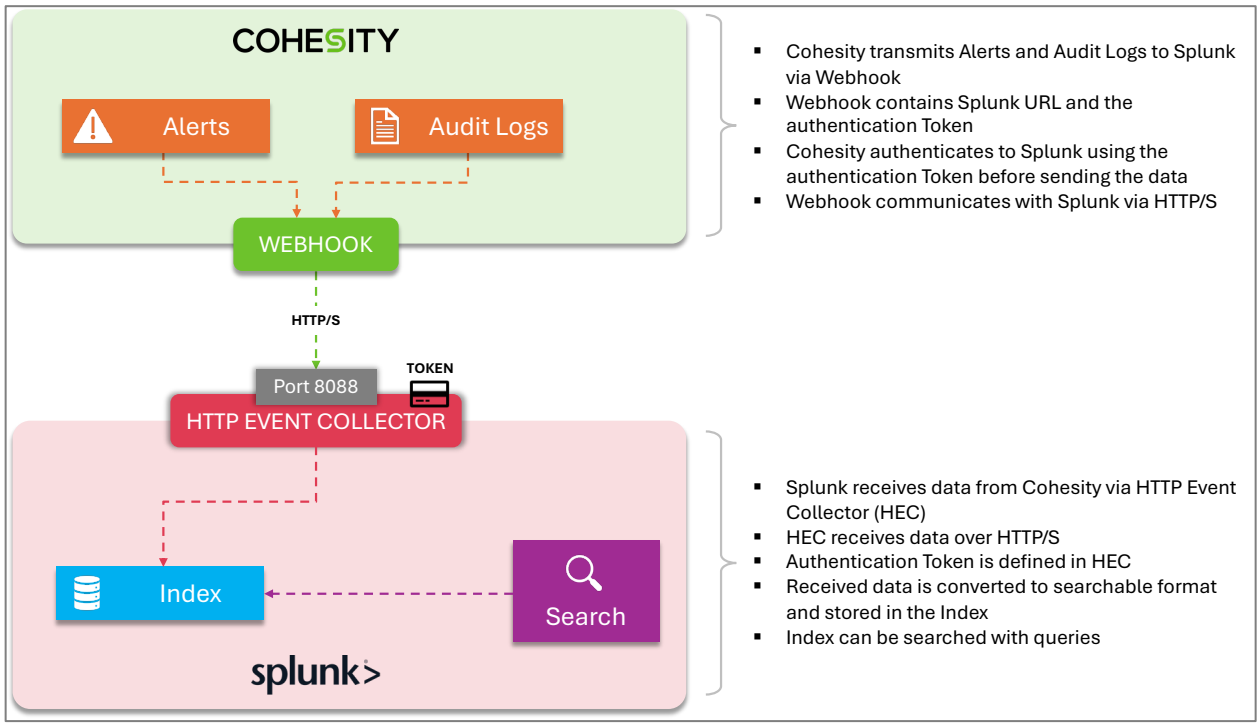
Webhook Integration Overview

A webhook integration of Cohesity with Splunk requires defining an HTTP Event Collector on the Splunk side and defining a webhook on the Cohesity side. This integration consists of the following components:

- **Index** – is a repository for data in Splunk, that receives and stores data in a searchable format. There are two types of indexes:
  - Event index – stores any type of data. It is the default index type
  - Metrics index – stores only metric data

  By default, Splunk provides three default indexes: main, internal, and audit.
- **HTTP Event Collector (HEC)** – is an endpoint that sends app events directly to Splunk platform via HTTP or HTTPS using a token-based authentication model. The clients which intend to use it must authenticate with a token before sending data. HEC receives data over HTTPS on TCP port 8088 by default
- **Webhook** – is an HTTP callback defined in Cohesity as a notification alert. The **w**ebhook configuration is the destination Splunk URL and the Authentication Token *(which is defined in Splunk HEC)*. Cohesity authenticates to Splunk using this authentication token before sending the data. Cohesity sends the data in raw format to Splunk.

Figure 5: Webhook Integration Overview



Quick Webhook Integration in 5 Steps

This is for Splunk experts who are veterans with the concepts and usage of Splunk. For novice users who are new to Splunk and need detailed steps visit Integrate Cohesity with Splunk Enterprise and Integrate Cohesity with Splunk Cloud.

1. Create a new index in Splunk to store Cohesity Logs
    a. Click **Indexes** under **Data** in **Settings**.
    b. Click **New Index** and fill in the requested details for index and **Save.**
2. Configure HTTP Event Collector in Splunk to receive Cohesity Logs
    a. Click **Data Inputs** under **Data** in **Settings**.
    b. Click **HTTP Event Collector**.
    c. Click **Global Settings** fill in the requested details and **Save**.
        i. Select **Enabled** for **All Tokens.**
        ii. Select **Default Source Type** as **_json.**
        iii. Select **Default Index** as the new index created in step 1.
        iv. By default, **SSL** is enabled with default **Port 8088**. Modify these according to your requirements.
3. Create a new token in Splunk to authenticate Cohesity.
    a. Click **Data Inputs** under **Data** in **Settings.**
    b. Click **HTTP Event Collector.**
    c. Click **New Token** and provide requested details.
        i. Choose **Select** under **Input Settings**, then choose **Select Source Type** and choose **_json.**
        ii. Select **Index** as the new index created in step 1.
        iii. Select **Default Index** as the new index created in step 1.
    d. Copy the **Token Value** of the above-created token – we will require this in the next step.
4. Configure alert notification with Webhook in Cohesity.
    a. Create alert notification

> **Self-managed Cohesity Clusters *(On-premises)*:**
> *Click on **System** > **Health** > **Settings** and **Add Alert Notification Rule***
>
> **Cohesity DataProtect *(Cohesity Data Cloud)*:**
> *Click on **System** > **Health** > **Notification** > **Create > New Alert Notification Rule***
>
> **Cohesity DataProtect as a Service *(Cohesity Data Cloud)*:**
> *Click on **Health** > **Notification** > **Create > New Alert Notification Rule***

b. Choose **Webhook** as the alert notification type and provide the Webhook **URL** and **Options** as shown below:

> **For Splunk Enterprise:**
> **URL:** https://<Your Splunk IP>:8088/services/collector/raw
> **Options:** -H “Authorization: Splunk *<HEC Token>*” -H “Content-Type: application/json”
>
> **For Splunk Cloud:**
> **URL:** https://<Your Domain>.splunkcloud.com:8088/services/collector/raw
> **Options:** -H “Authorization: Splunk *<HEC Token>*” -H “Content-Type: application/json”

5. Search for Cohesity alerts and logs in Splunk.
   a. Click **Search** and **Reporting.**
   b. In the search field, use an appropriate criterion to filter logs with.

Supported Alerts

The Cohesity integration with Splunk supports the following alerts:

Table 3: Cohesity-supported Alerts

		Alerts
Self-managed Cohesity Clusters		• Hardware Alerts • Software Alerts • Data Service Alerts • Maintenance Alerts
Cohesity Data Cloud	**DataProtect**	• Hardware Alerts • Software Alerts • Data Service Alerts • Maintenance Alerts • Security Alerts *(Data Ingest Anomaly, Threat Detection, Data Classification)*
	DataProtect as a Service	• Archival and Restore Alerts • Backup and Restore Alerts • Security Alerts *(Data Ingest Anomaly)*

Table 4: Cohesity and Splunk Alert Compatibility Matrix

		Splunk Enterprise			Splunk Cloud		
		Self-Managed Clusters	Cohesity Data Cloud		Self-Managed Clusters	Cohesity Data Cloud	
			DataProtect	DataProtect as a Service		DataProtect	DataProtect as a Service
Hardware Alerts		✓	✓	NA	✓	✓	NA
Software Alerts		✓	✓	NA	✓	✓	NA
Maintenance Alerts		✓	✓	NA	✓	✓	NA
Remote Replication Alerts		✓	✓	NA	✓	✓	NA
Backup and Restore Alerts		✓	✓	✓	✓	✓	✓
Archival and Restore Alerts		✓	✓	✓	✓	✓	✓
Security Alerts	**Data Anomaly**	✗	✓	✓	✗	✓	✓
	Threat Detection	✗	✓	✗	✗	✓	✗
	Data Classification	✗	✓	✗	✗	✓	✗

NOTE:

- For Threat Detection Alerts you require DataHawk ThreatProtection SKU in Cohesity Data Cloud.
- For Data Classification Alerts you require DataHawk DataClassification SKU in Cohesity Data Cloud.

Webhook Integration v/s Cohesity Splunk Add-on

Table 5: Webhook Integration v/s Cohesity Splunk Add-on

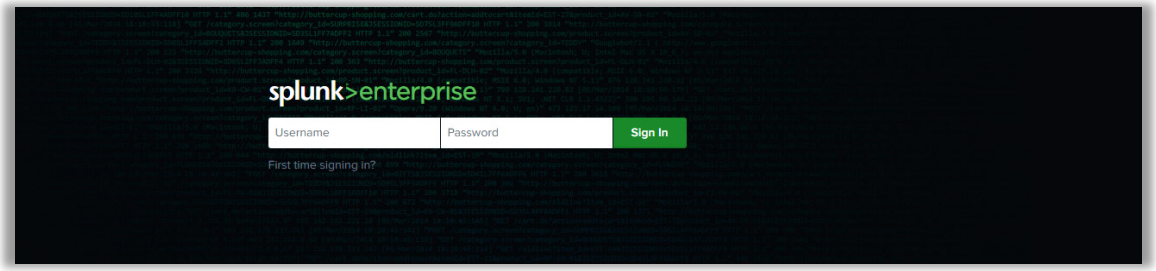
Webhook Integration	Cohesity Splunk Add-on
Uses HTTP Callbacks	Uses REST APIs
Configured at Cohesity side	Configured at Splunk side
Pushes alerts from Cohesity to Splunk	Pulls alerts from Cohesity into Splunk
Works with both Self-managed Cohesity clusters and Cohesity Data Cloud	Works only with Self-managed Cohesity clusters
Supports Security alerts	Doesn’t support Security alerts
Doesn’t require any app to be installed	Requires a Splunk app to be installed
Easy configuration and maintenance (no dependency on app)	Comparatively complex configuration and requires maintenance (App requires update upon enhancement)

Integrate Cohesity with Splunk Enterprise

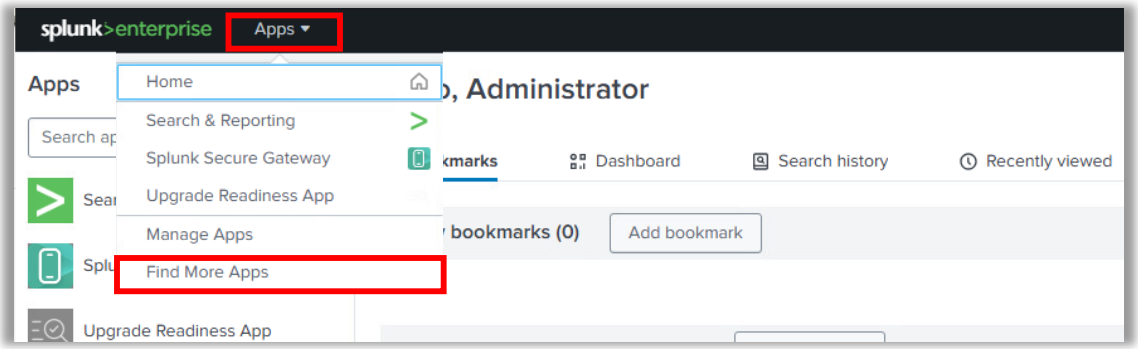
Self-managed Cohesity Clusters

Integration via Cohesity add-on

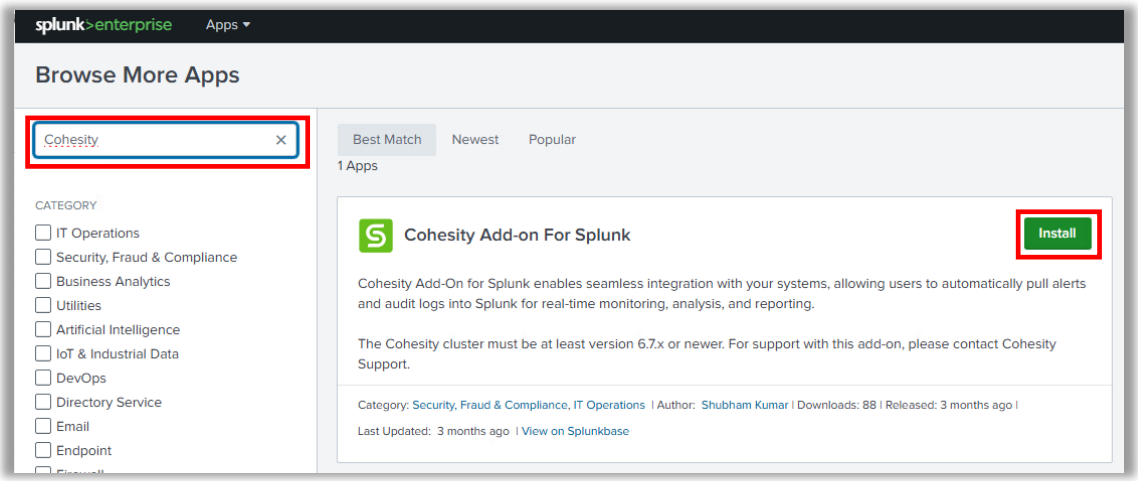
1. Install the Cohesity Splunk Add-on.
   a. Login to your Splunk Enterprise Instance.



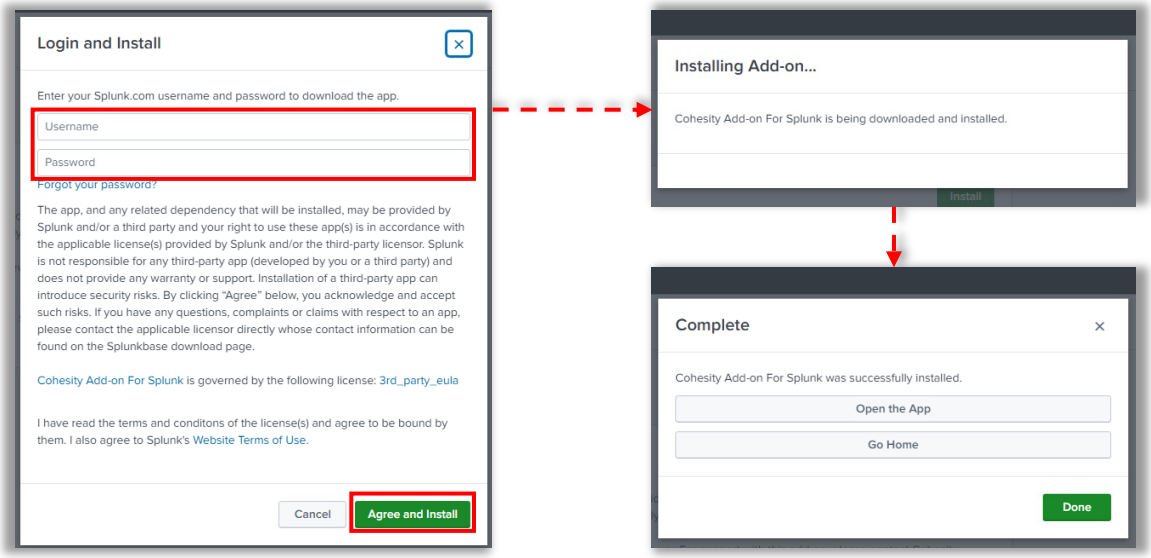
   b. Click **Find More Apps** under **Apps**.



   c. Search for **Cohesity Add-on For Splunk** and click **Install**.

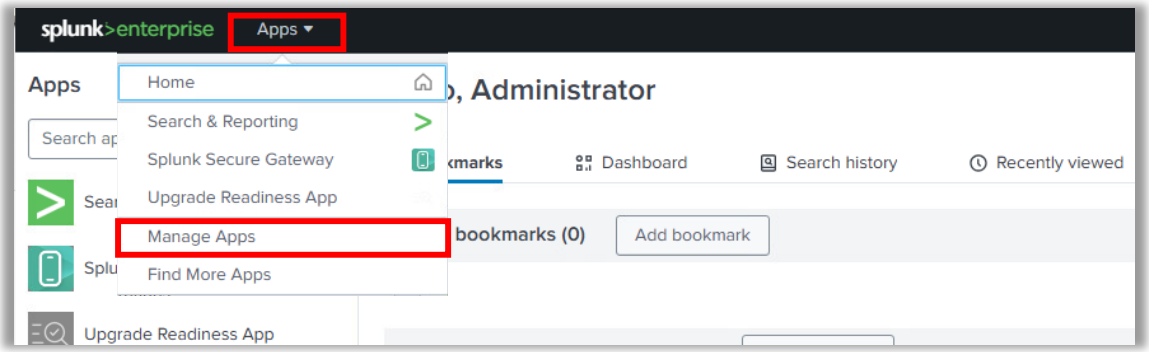


d. Enter your **Splunk credentials** and click **Agree and Install** (This installs the Cohesity Splunk Add-on on your Splunk Enterprise).

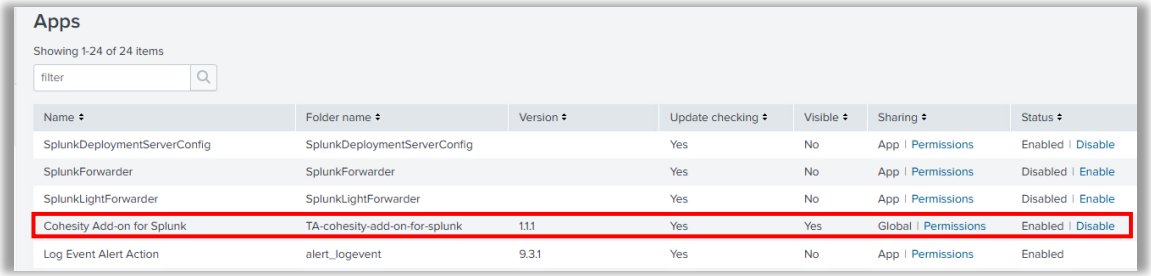


2. Verify the installed Cohesity Splunk Add-on.

a. Click **Manage Apps** under **Apps**.

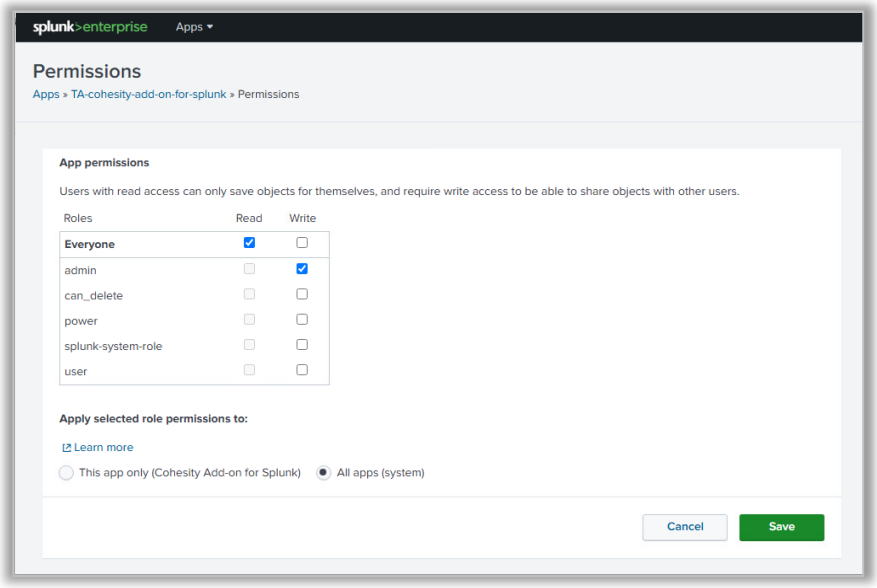


b. Verify the **Status** is **Enabled** for the app.

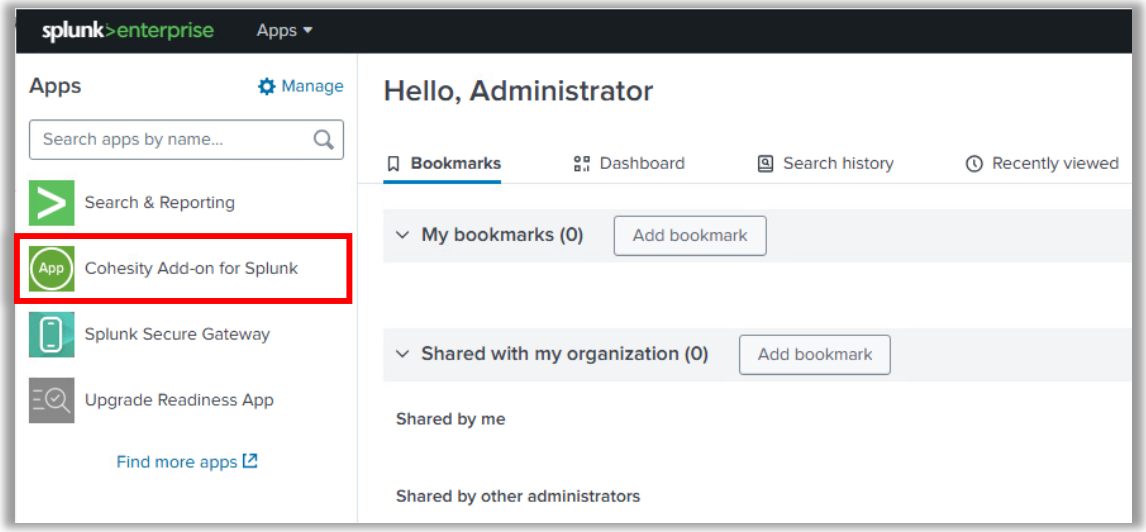


NOTE: If the status is Disabled, then manually Enable it from the Apps.

c. Click **Permissions** to modify the **App permission** if required.



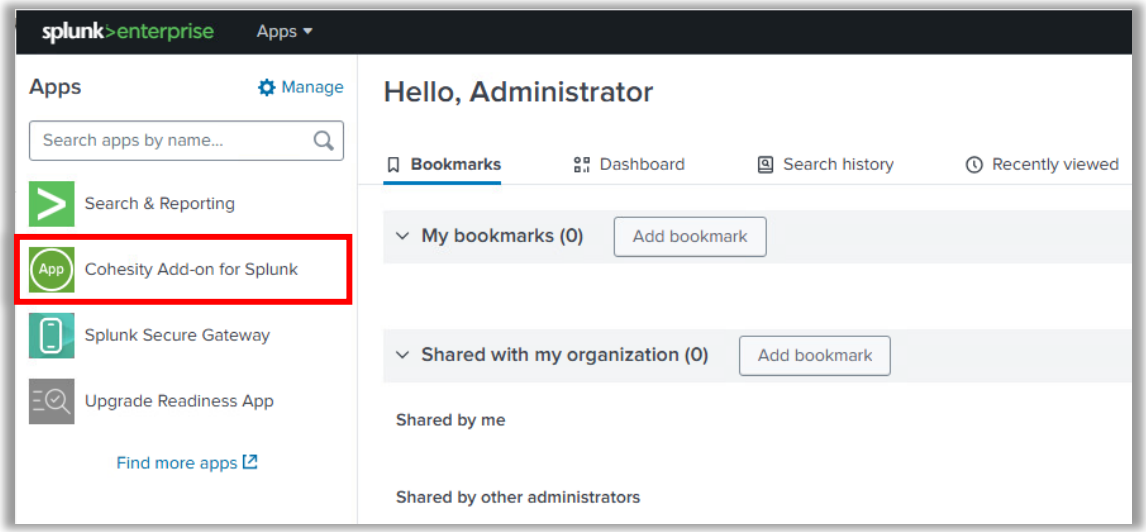
d. On the Splunk Home Page, **Cohesity Add-on for Splunk** must be available.



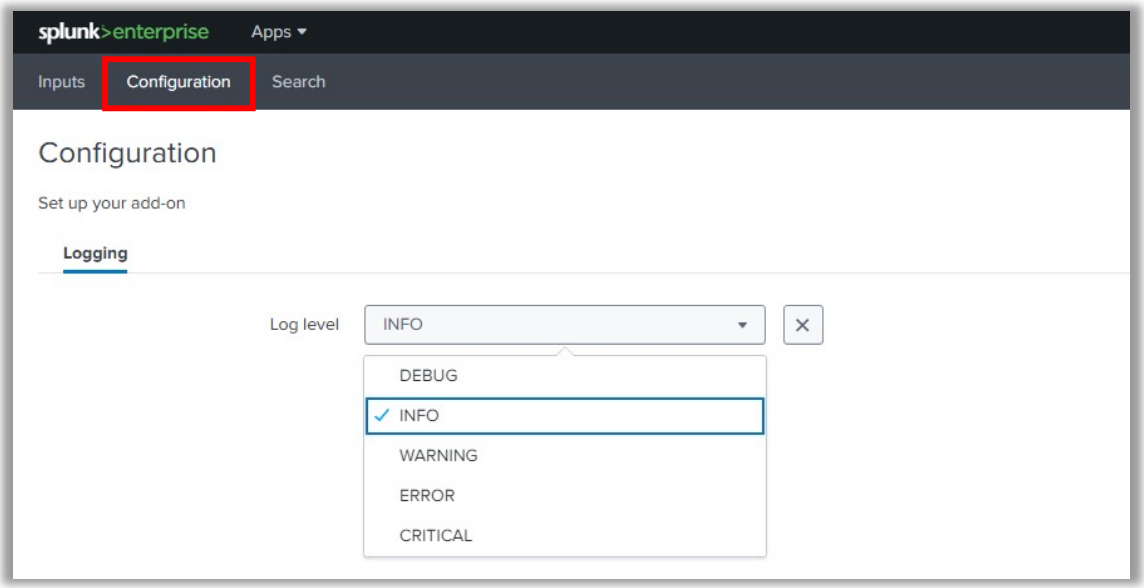
NOTE: If the add-on is not visible in the home page, then the add-on might still be getting installed. Wait for some time and then try again. If the add-on is still not visible, then the installation could have been interrupted. Try to reinstall the add-on again.

3. Configure Cohesity Splunk Add-On.

a. From Splunk Web Home console, click **Cohesity Add-on for Splunk.**



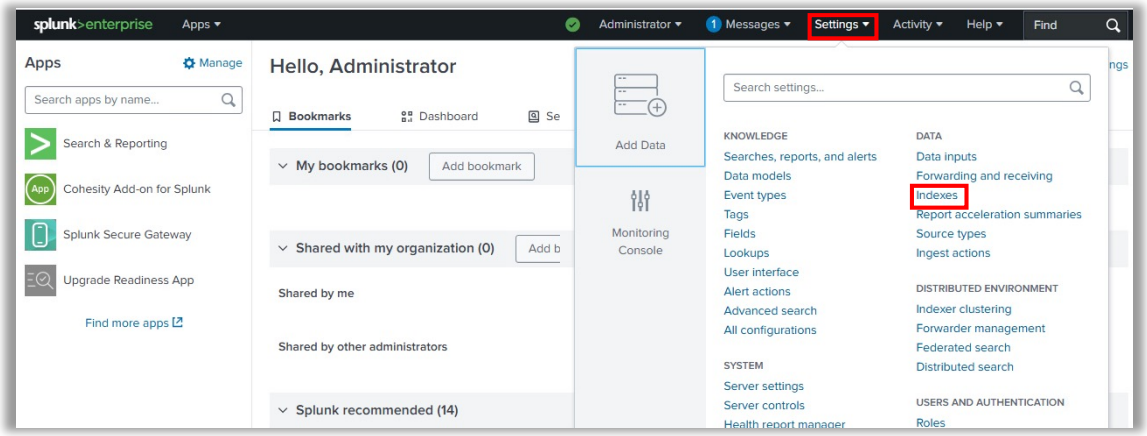
b. Click **Configuration** and set up the desired **Log Level**. By default, **Info** is selected.



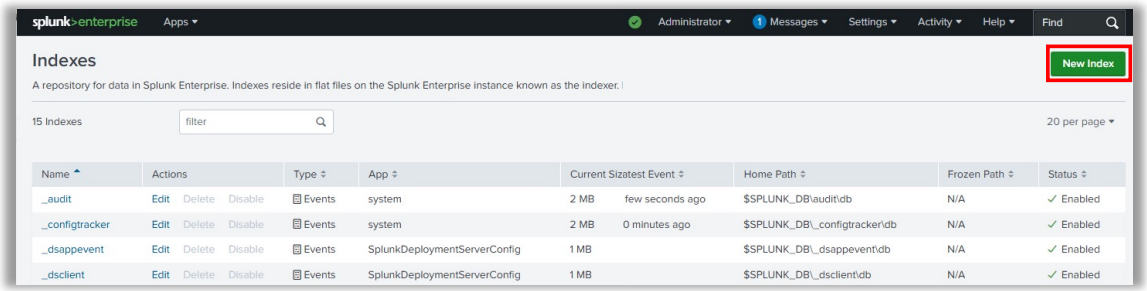
4. Create a new index to store Cohesity logs.
This is an optional however, recommended step. Create a new index to store Cohesity alerts and logs.

> **NOTE**: You can use already existing index in your Splunk instance. But it is advised to create and use a new custom index specific to Cohesity logs and alerts. This will help keep things organized and ensure easy querying and managing.

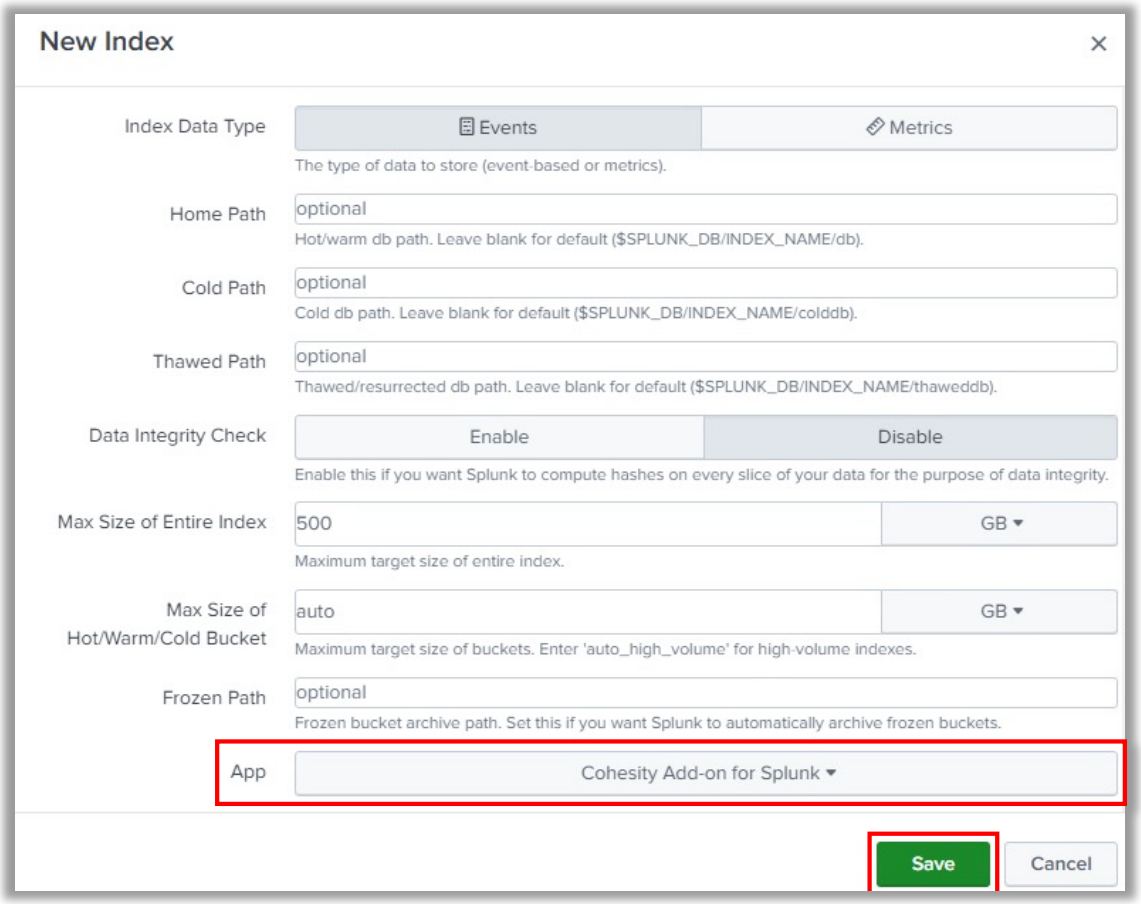
a. Click **Indexes** under **Data** in **Settings**.



b. Click **New Index** and fill in all requested details.

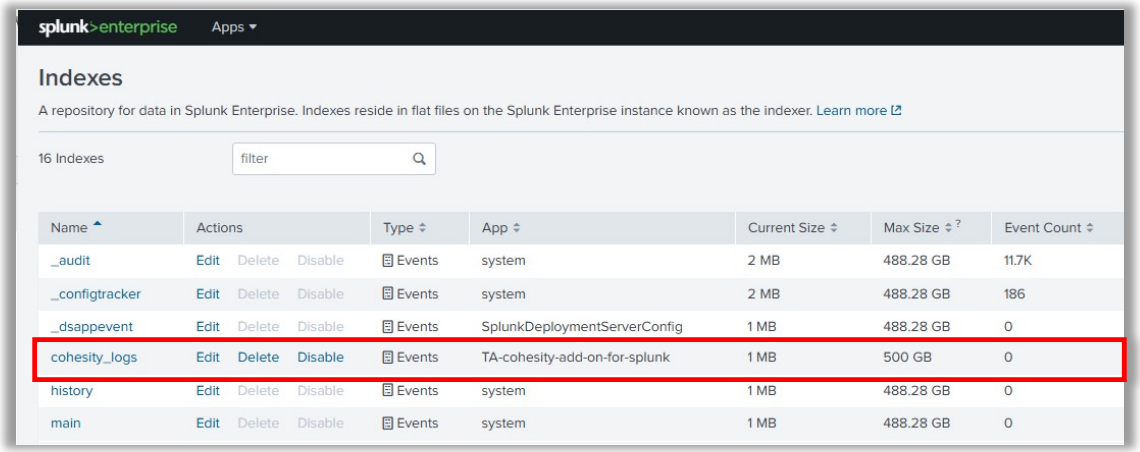


c. Select **Cohesity Add-On** for Splunk in App details. Click **Save**.



NOTE:
You can use the default **Search and Reporting** for App, but it is advised to select **Cohesity Add-On for Splunk** in App details.

d. You can see the newly created index under Indexes.



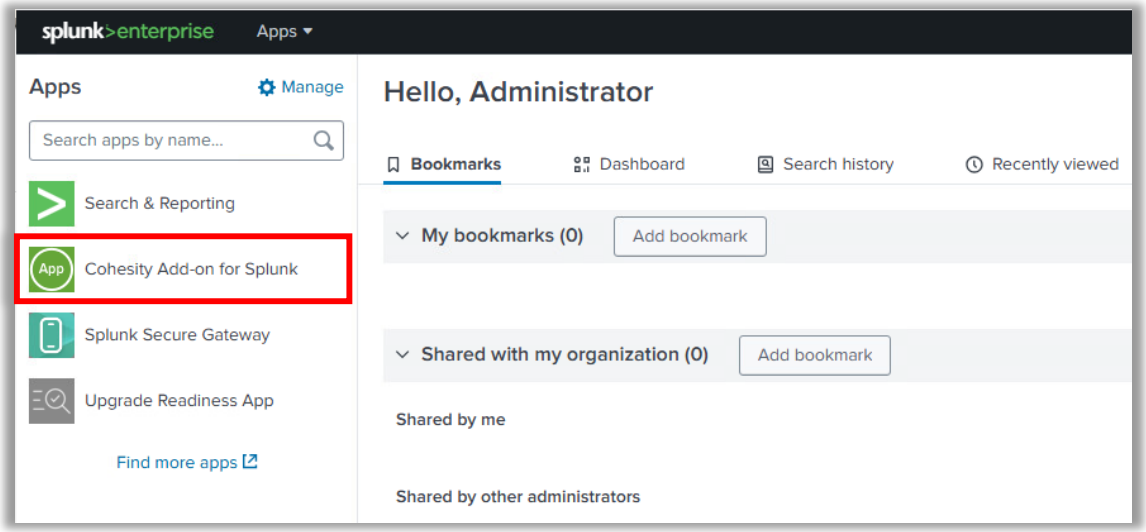
5. Add self-managed Cohesity Cluster(s) as source input.

   You must add your individual Cohesity Cluster(s) as source input in Splunk. From these Cohesity Cluster(s), Splunk ingests the alerts and logs.

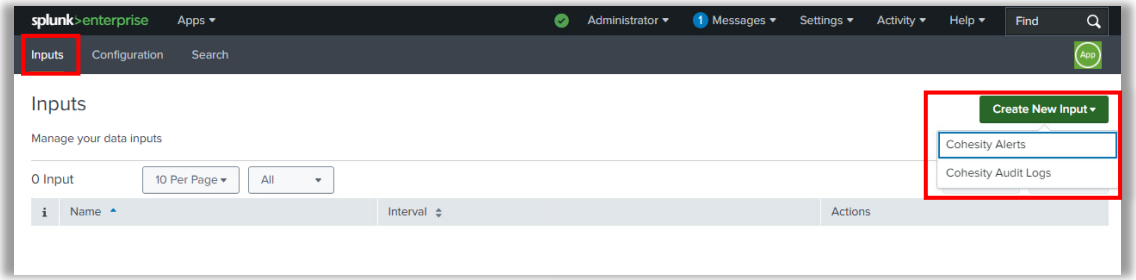
   NOTE:

   - While adding the cluster(s) as source input, you must configure whether it is intended for Cohesity Alerts or Audit Logs.
   - If you want both alerts and logs to be ingested, then you must create two inputs per cluster (one for alerts and the other for audit logs).
   - You can add multiple clusters as inputs.

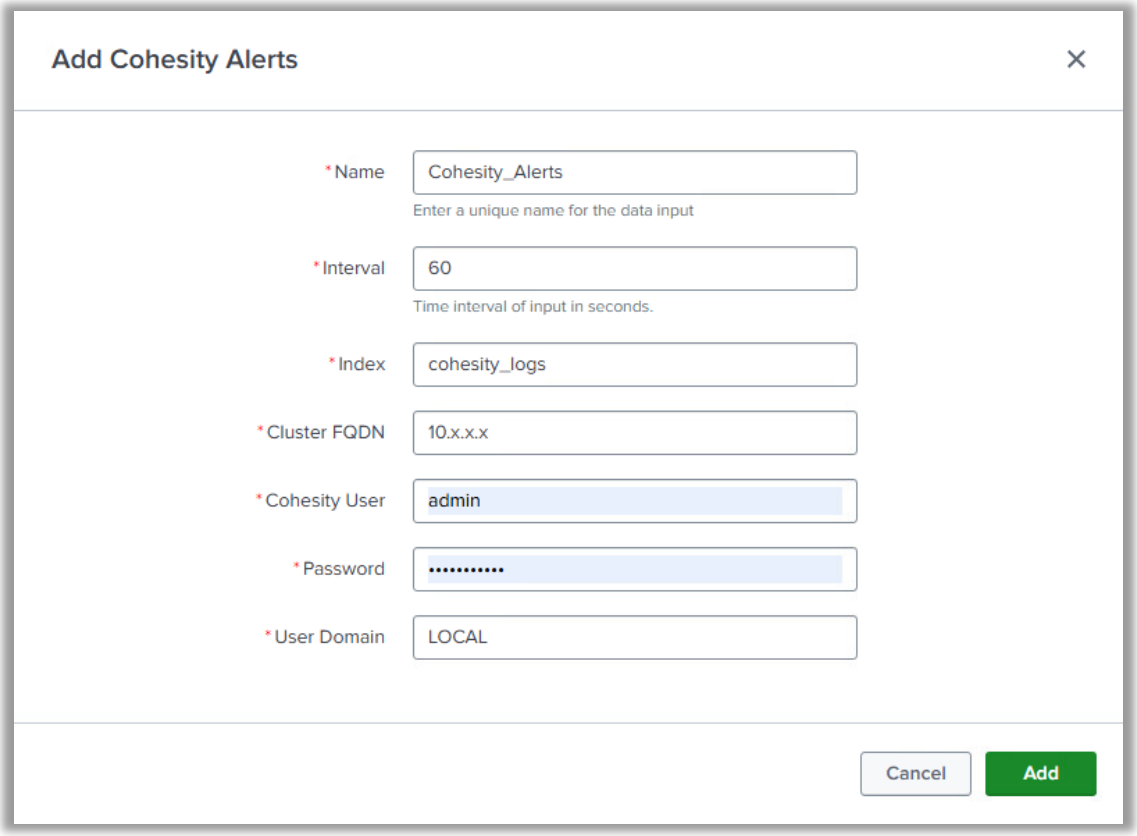
   a. From Splunk Web Home console, click **Cohesity Add-on for Splunk.**



   b. From **Inputs** Tab, click **Create New Input** and select the data to be ingested to Splunk (Alerts/Audit Logs).

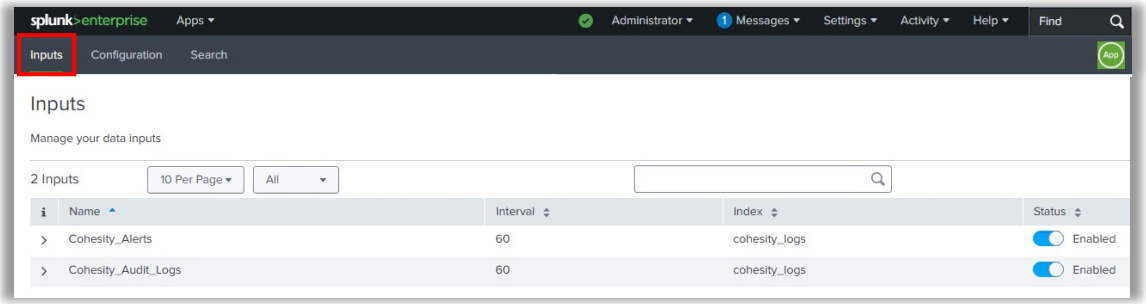


c. Provide the requested details and click **Add.**



- **Name** – A unique name for the data input
- **Interval** – Time interval of input in seconds with which the logs will be pulled from clusters
- **Index** – The Index to store the logs. By default, it takes the default index. Choose the new index we created under step 4 exclusively for Cohesity logs and alerts
- **Cluster IP/FQDN –** Enter the cluster details
- **Username –** Username of Cohesity cluster
- **Password –** Password of the cluster
- **Domain –** The domain details. The default is set to local

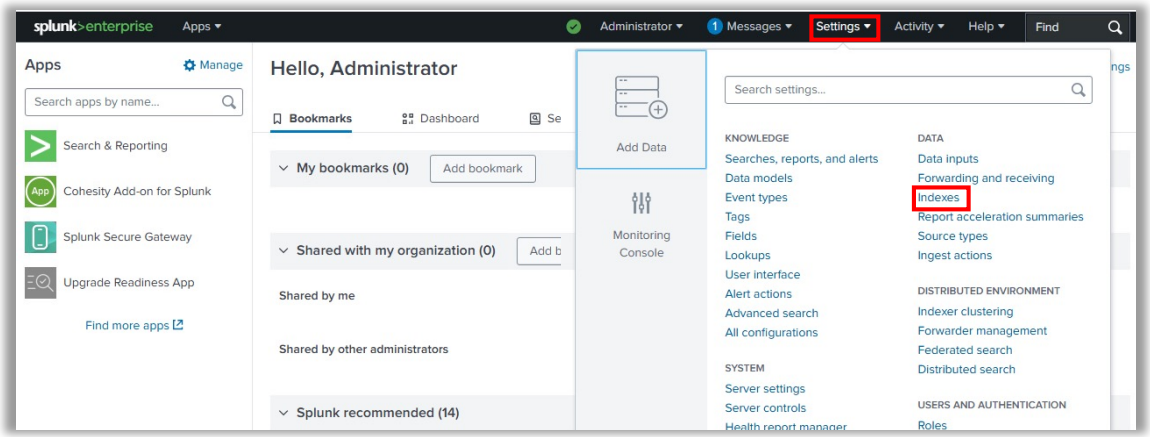
d. You can see the newly created source inputs under Inputs.



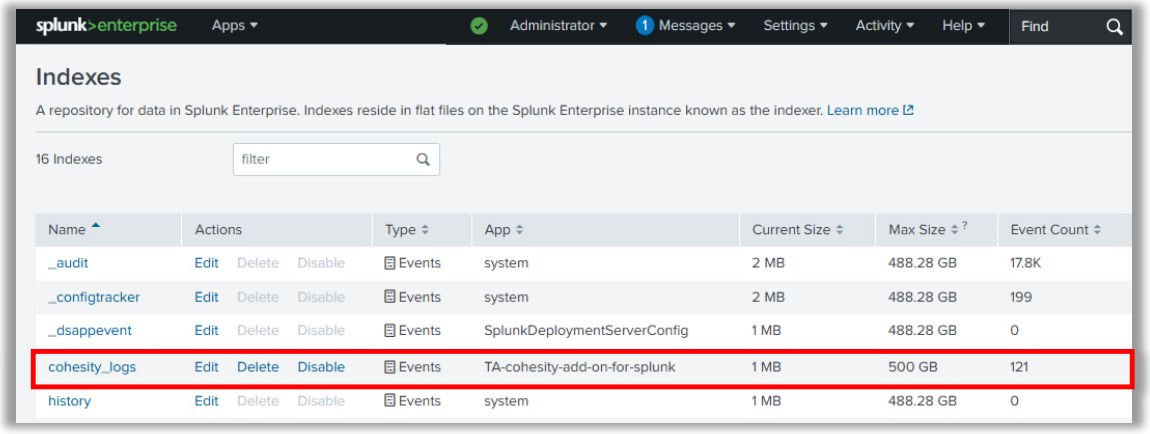
NOTE:

- Ensure the status of the input is Enabled. If it is disabled, then **Enable** it manually.

6. Validate data received from Cohesity.
   a. Click **Indexes** under **Settings**.



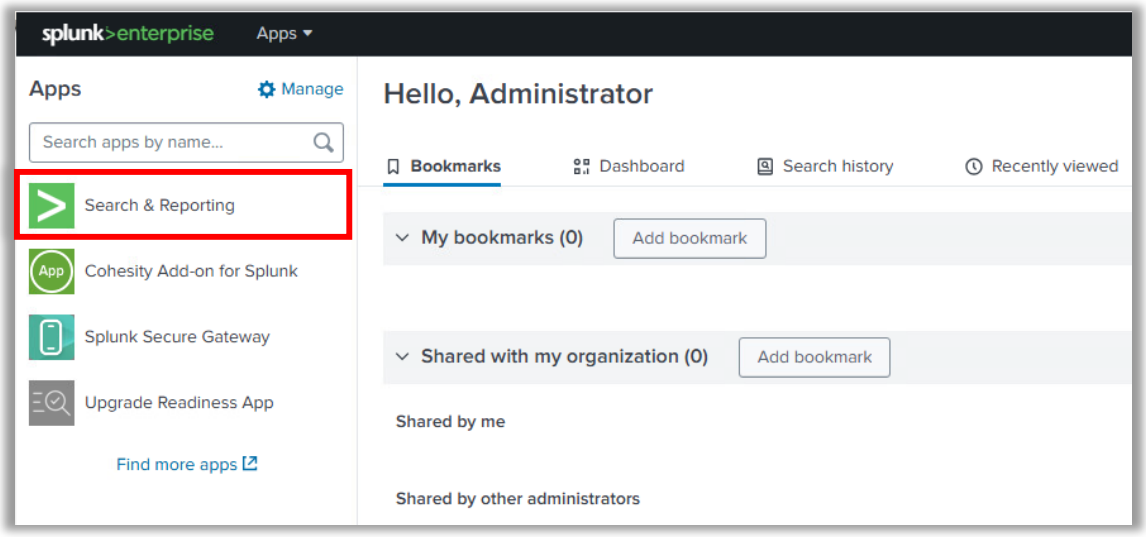
   b. Verify logs are being pushed to your index by checking the Event Count



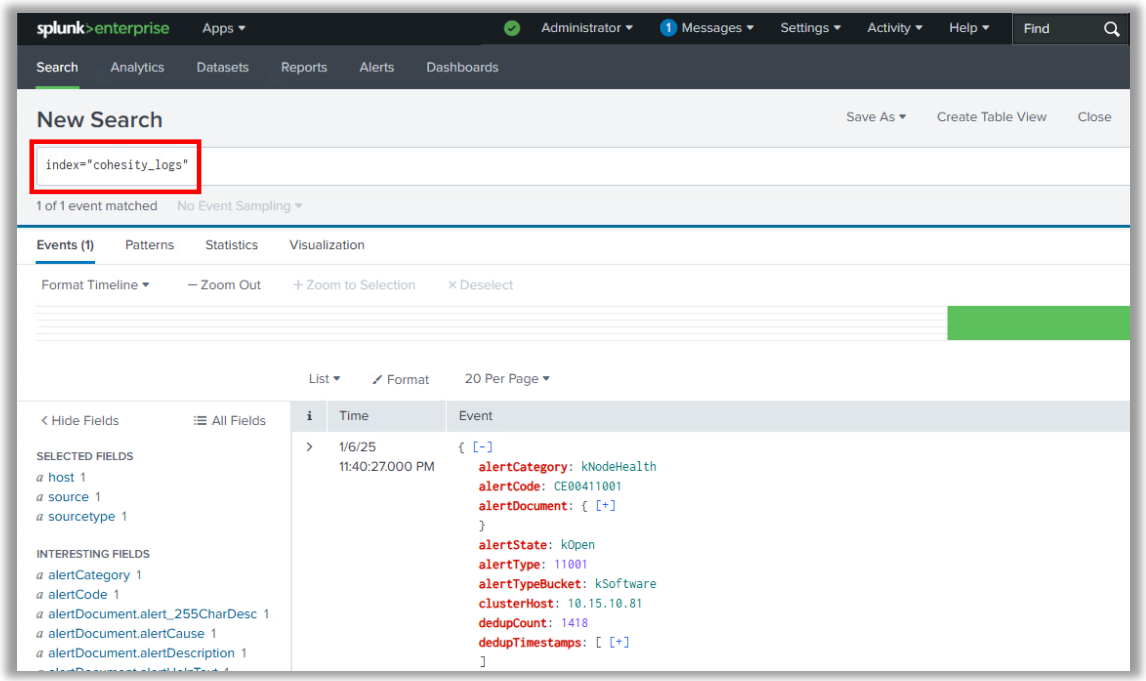
NOTE: Alerts and logs will be pulled from Cohesity to Splunk after the time-interval you have defined while creating the source input ins step 5. Wait till the time interval elapses before you see the increase in event count. If you are not seeing the events even after the time interval elapse, then there could be an issue in input configuration. Edit your input and verify the index and cluster details are proper.

7. Search, alert and visualize.

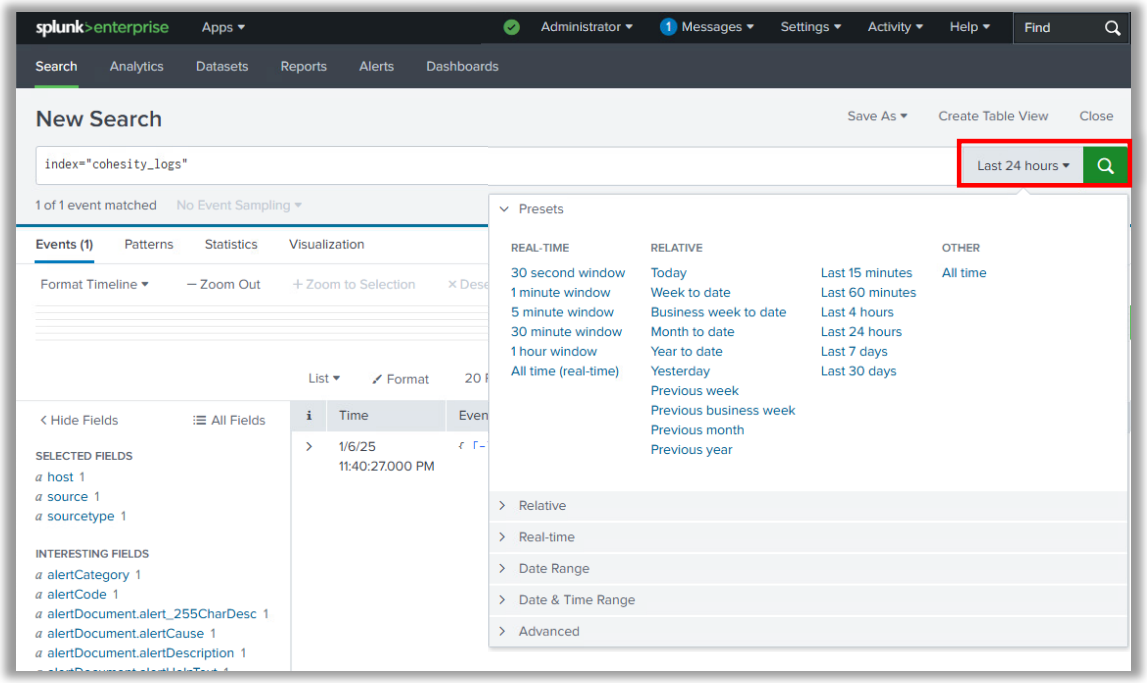
a. From Splunk Web Home console, click **Search & Reporting.**



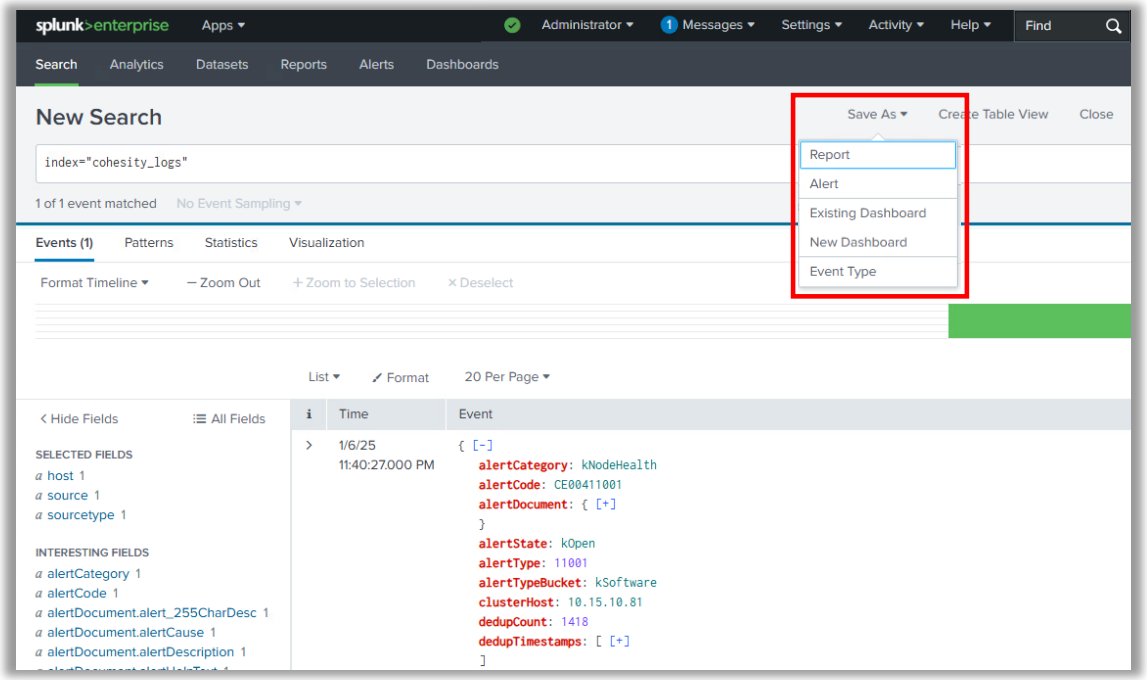
b. In **Search** field, use appropriate criteria to filter logs.



c. Filter search results based on time.



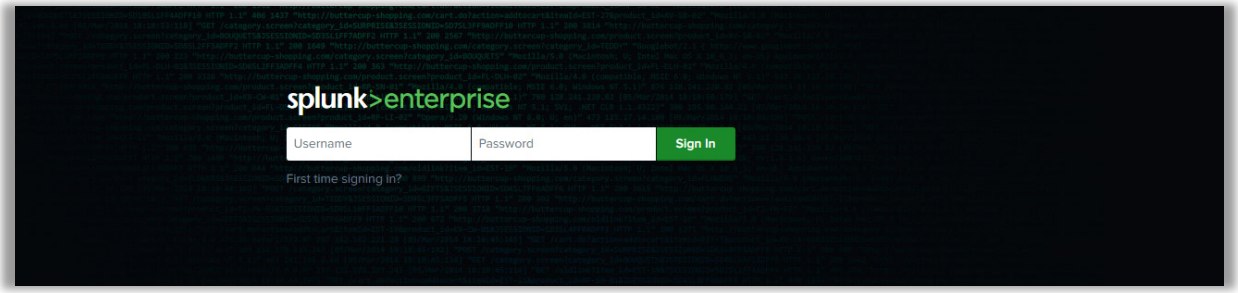
d. Alert and visualize.



NOTE: **For more details,** refer to the Search and Reporting section.

Integration via Webhook

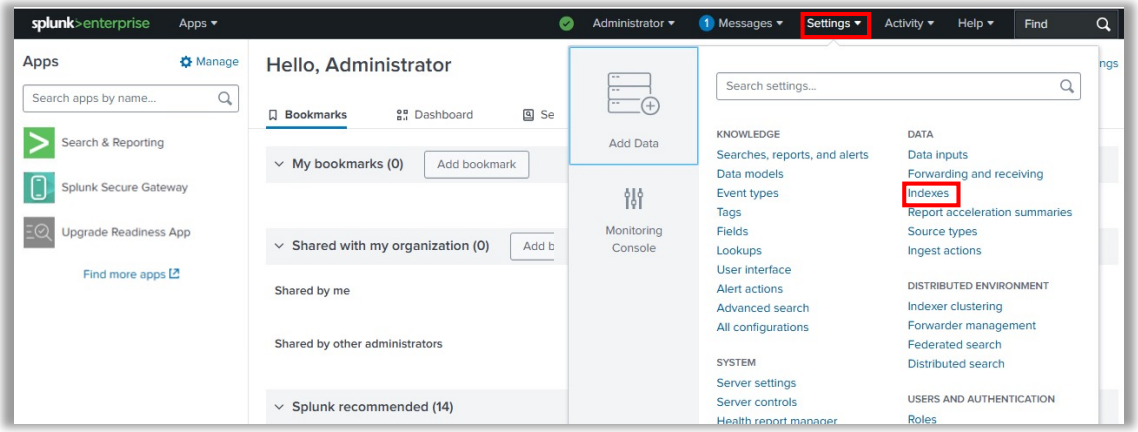
1. Login to your Splunk Enterprise Instance.



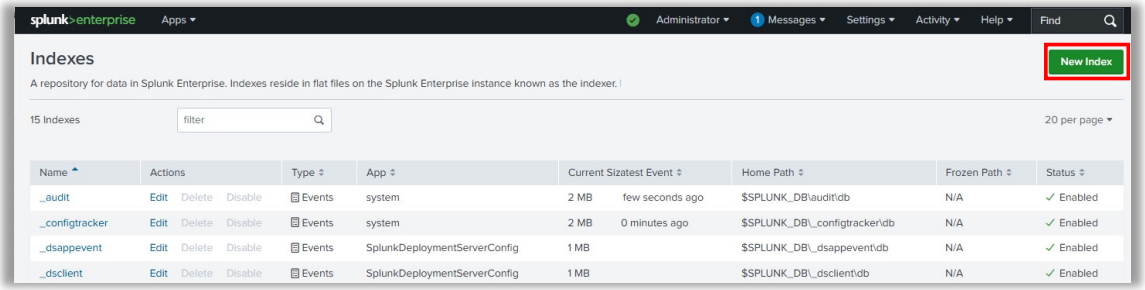
2. Create a new index to store Cohesity logs.

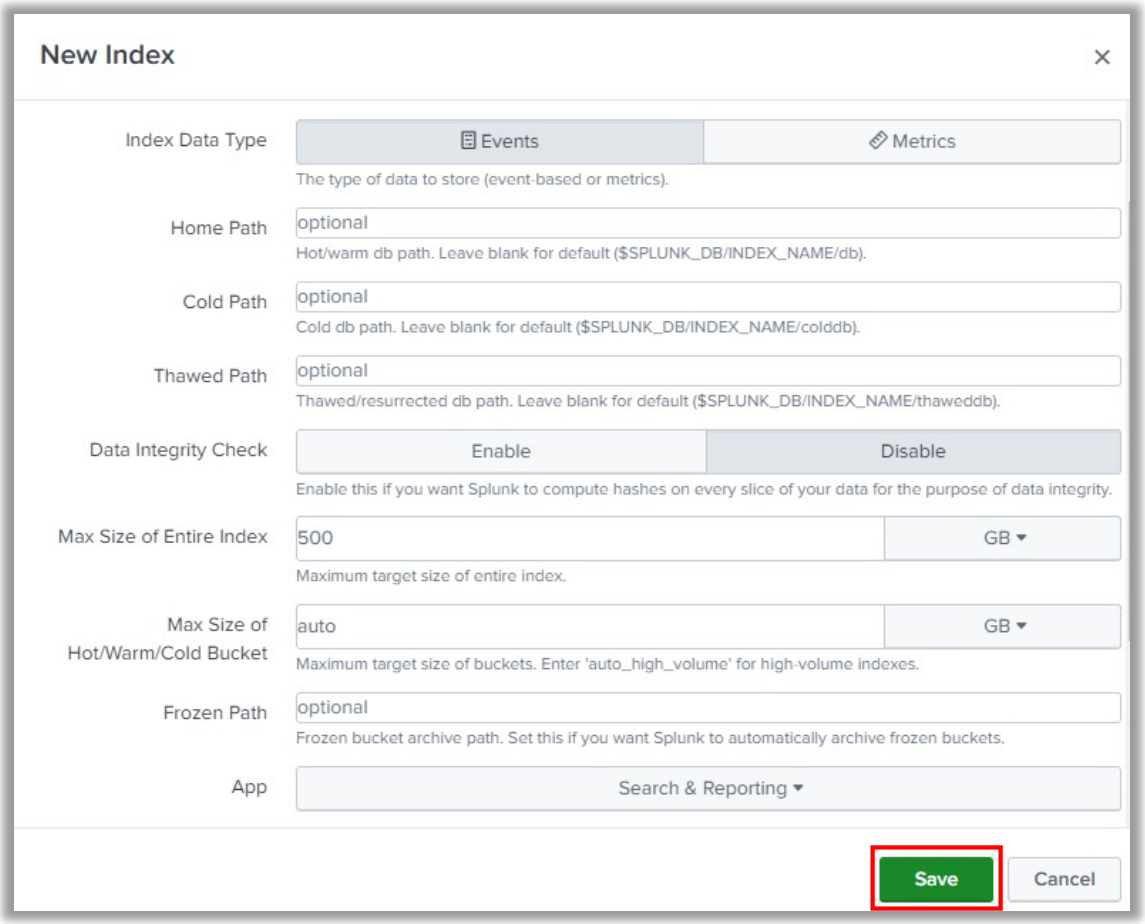
   This is an optional, however, recommended step. You can use an existing index in your Splunk instance. But it is advised to create and use a new index specific to Cohesity logs and alerts

   a. Click **Indexes** under **Data** in **Settings.**

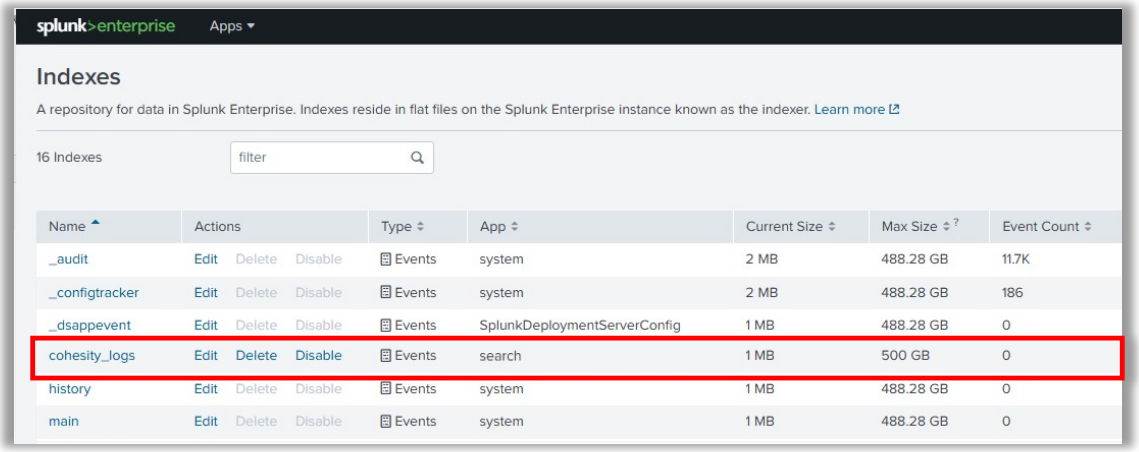


   b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save.**


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Indexes
A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer.
New Index
15 Indexes
filter
20 per page
Name
Actions
Type
App
Current Size
Earliest Event
Home Path
Frozen Path
Status
_audit
Edit Delete Disable
Events
system
2 MB
few seconds ago
$SPLUNK_DB\audit\db
N/A
Enabled
_configtracker
Edit Delete Disable
Events
system
2 MB
0 minutes ago
$SPLUNK_DB_configtracker\db
N/A
Enabled
_dsappevent
Edit Delete Disable
Events
SplunkDeploymentServerConfig
1 MB
$SPLUNK_DB_dsappevent\db
N/A
Enabled
_dsclient
Edit Delete Disable
Events
SplunkDeploymentServerConfig
1 MB
$SPLUNK_DB_dsclient\db
N/A
Enabled

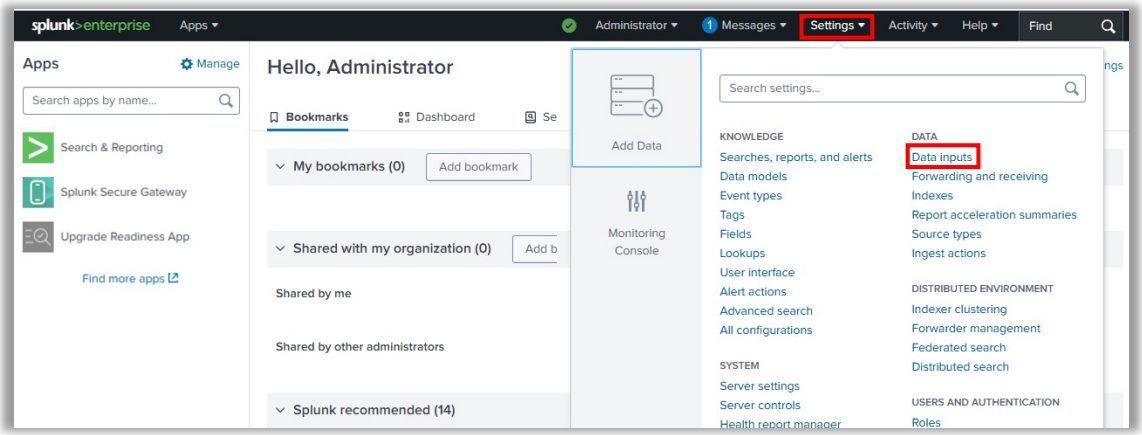

New Index
Index Data Type
Events
Metrics
The type of data to store (event-based or metrics).
Home Path
optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).
Cold Path
optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).
Thawed Path
optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).
Data Integrity Check
Enable
Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.
Max Size of Entire Index
500
GB
Maximum target size of entire index.
Max Size of Hot/Warm/Cold Bucket
auto
GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.
Frozen Path
optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.
App
Search & Reporting
Save
Cancel

c. You can see the newly created index under Indexes.

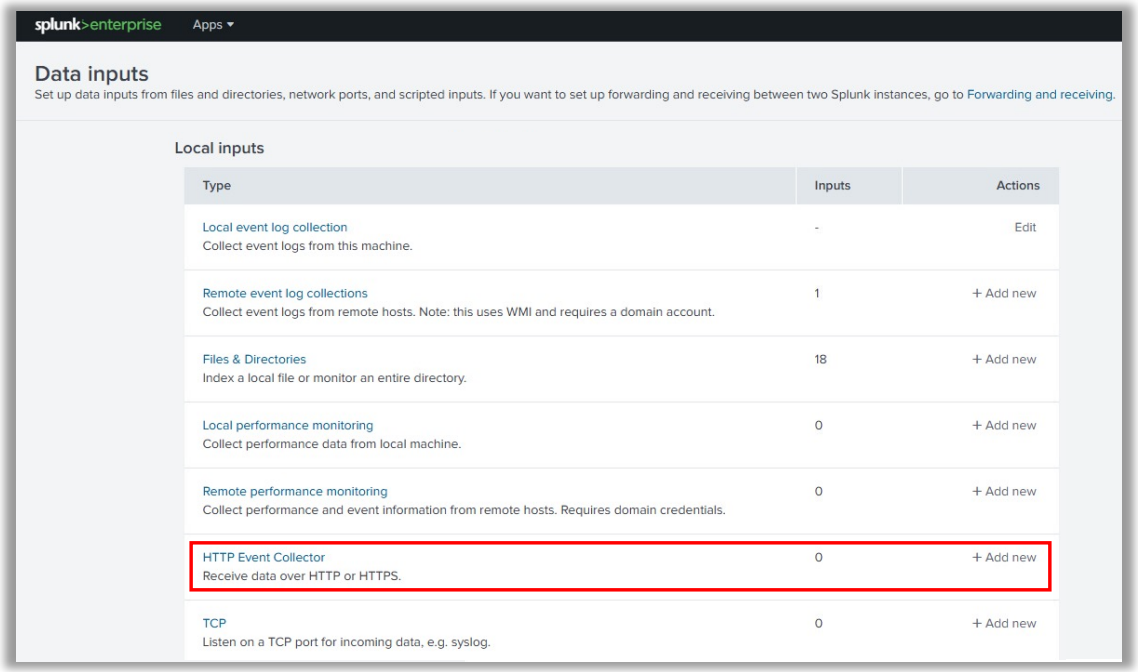


3. Configure HTTP Event Collector to receive data from Cohesity.

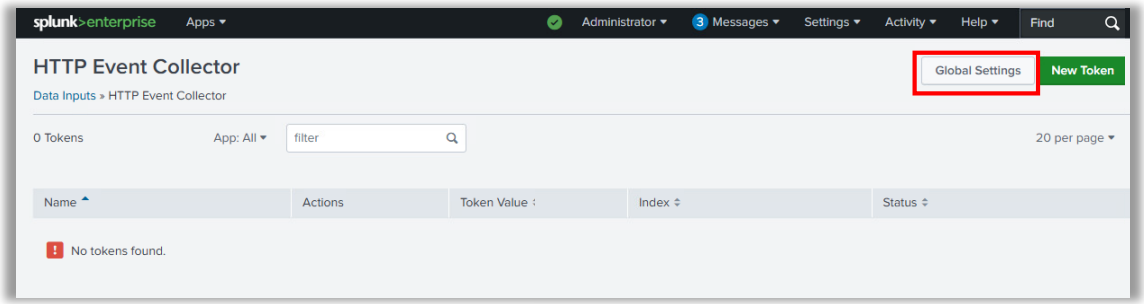
a. Click **Data Inputs** under **Data** in **Settings**.

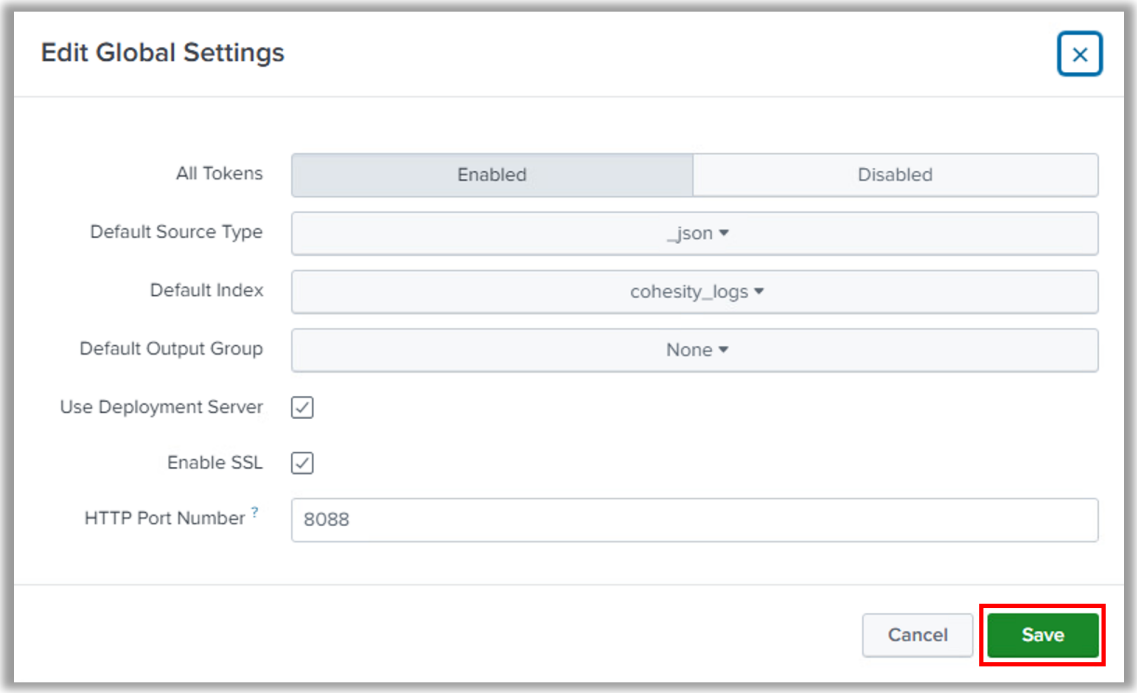


b. Click **HTTP Event Collector**.



c. Click **Global Settings** and fill in all requested details and click **Save.**





i. Select **Enabled** for **All Tokens.**

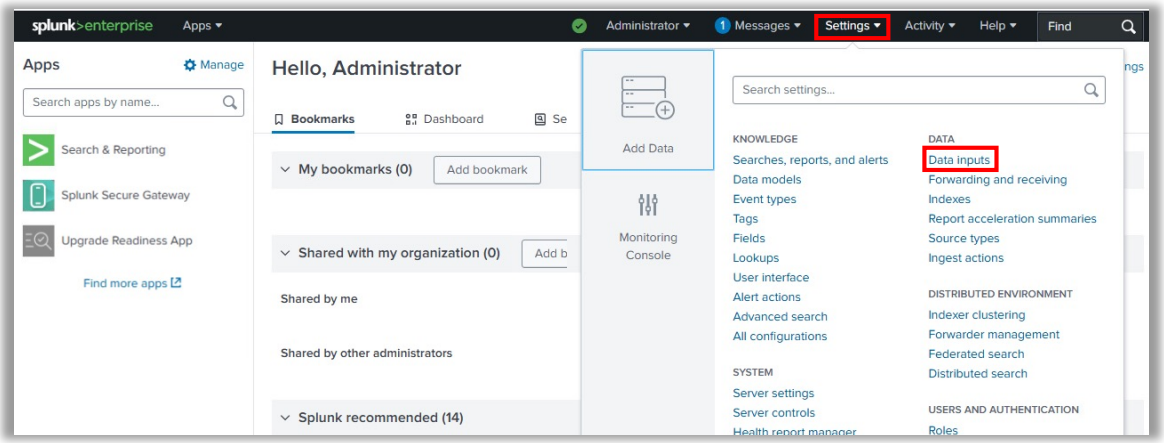
ii. Select the **Default Source Type** as **_json** (If it is not shown under the dropdown, then type _json in the search bar to bring it up).

iii. Select the **Default index** as the new index we created exclusively for Cohesity logs and alerts under step 1.

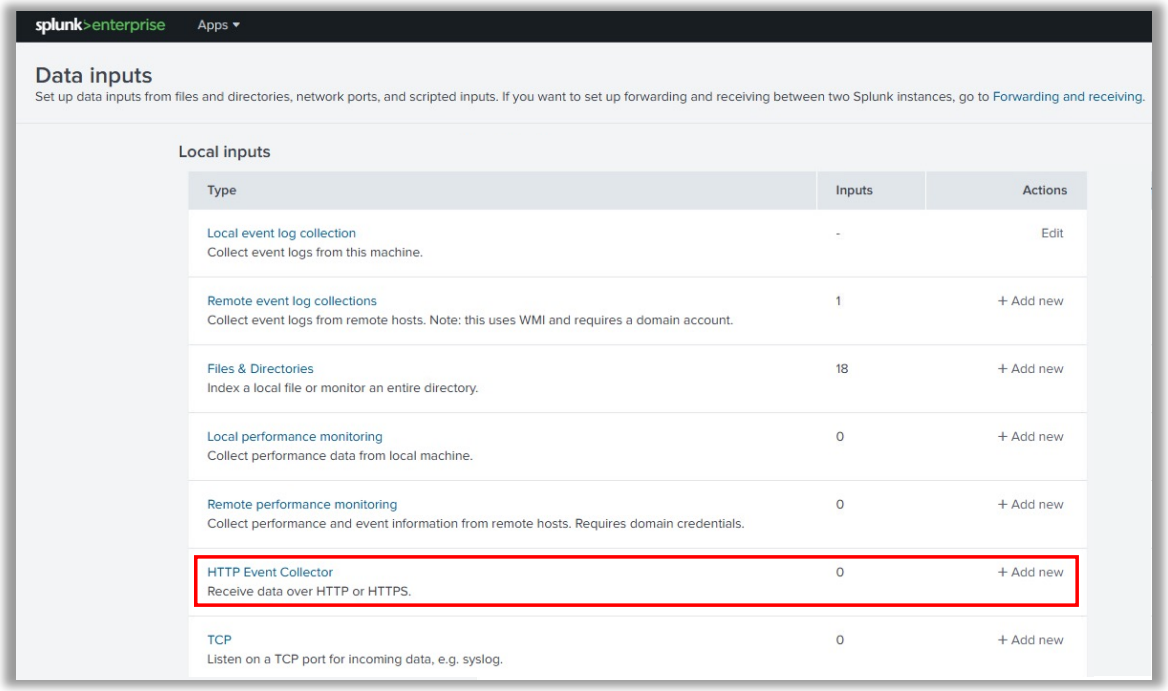
iv. By default, **SSL** is enabled with default **Port 8088**. You can disable SSL or modify the default port. A general recommendation is to enable SSL.

4. Create a new token to authenticate Cohesity.

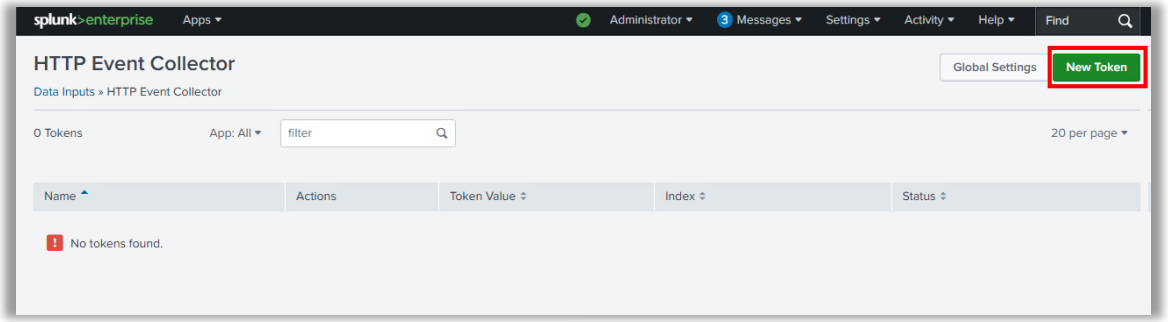
   a. Click **Data Inputs** under **Data** in **Settings**.



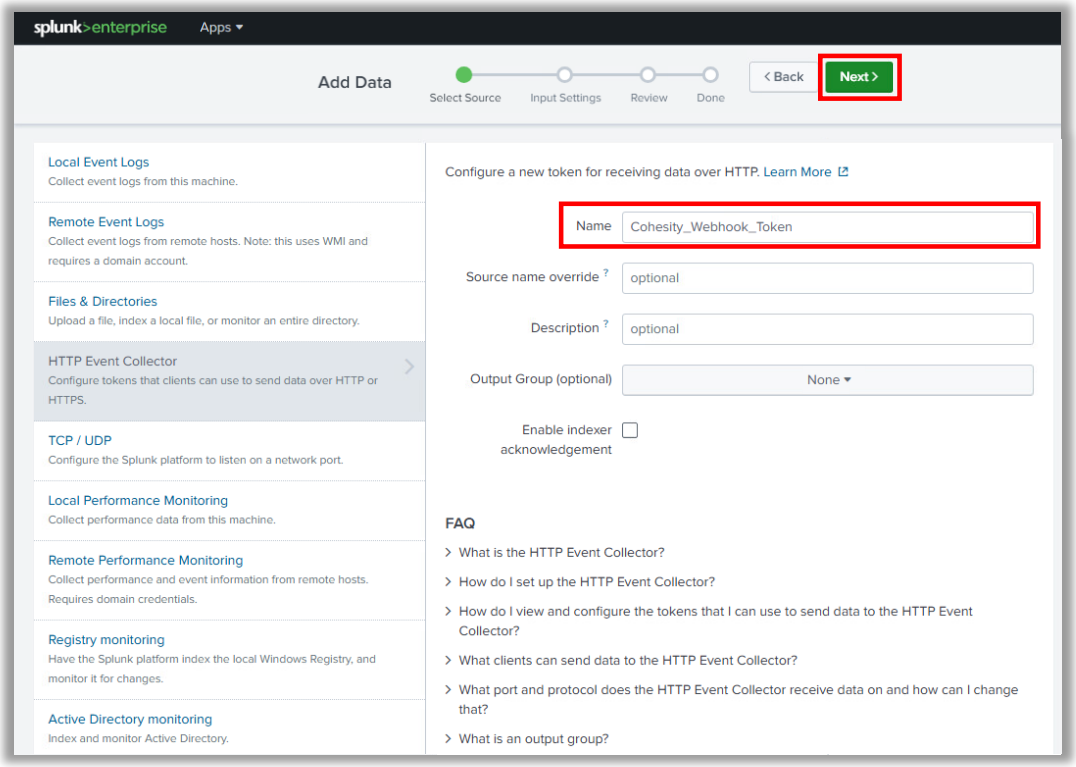
b. Click **HTTP Event Collector**.



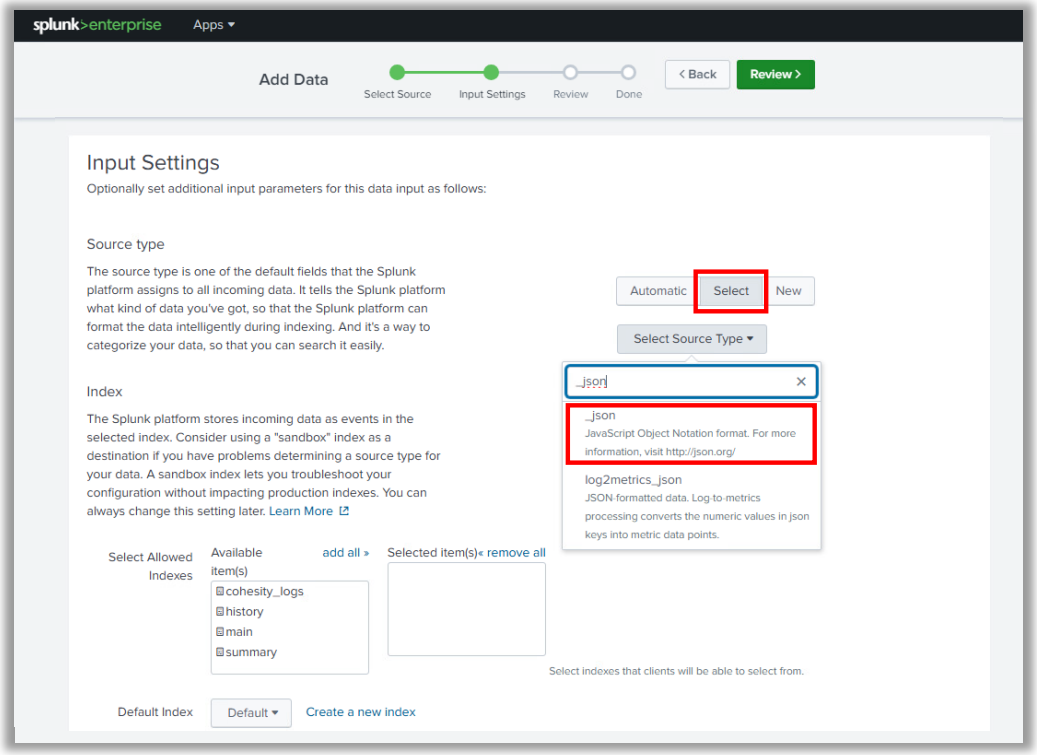
c. Click **New Token**.



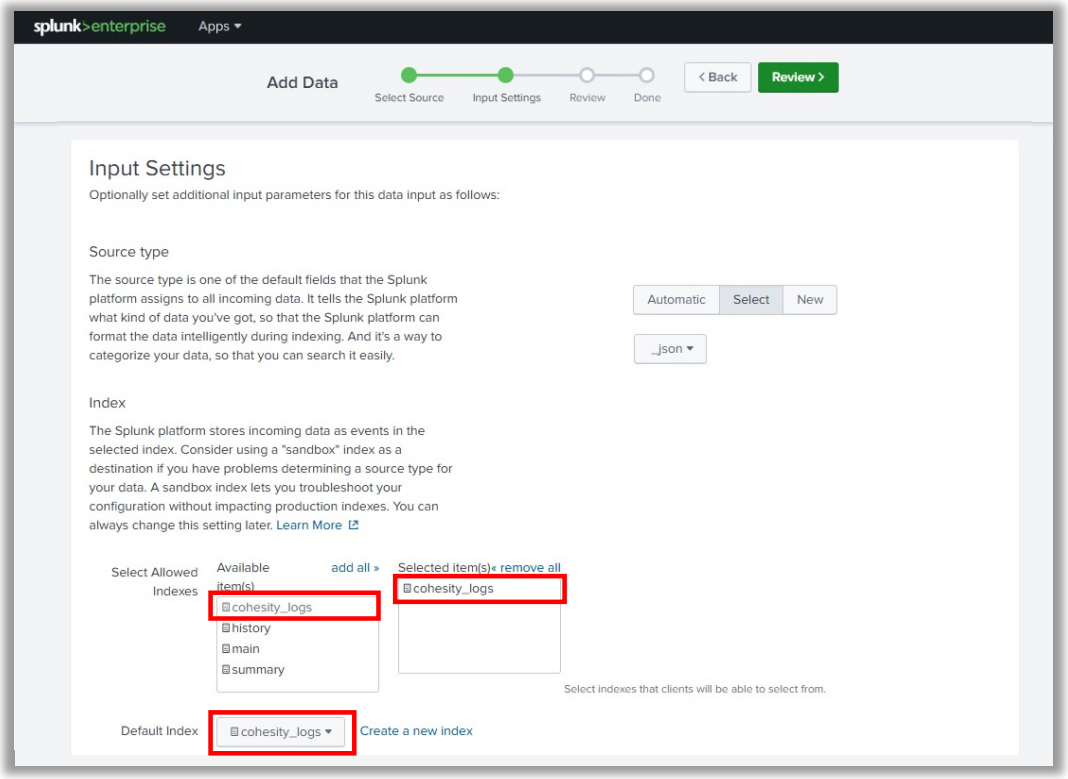
d. Provide a unique **Name** for your token and click **Next.**



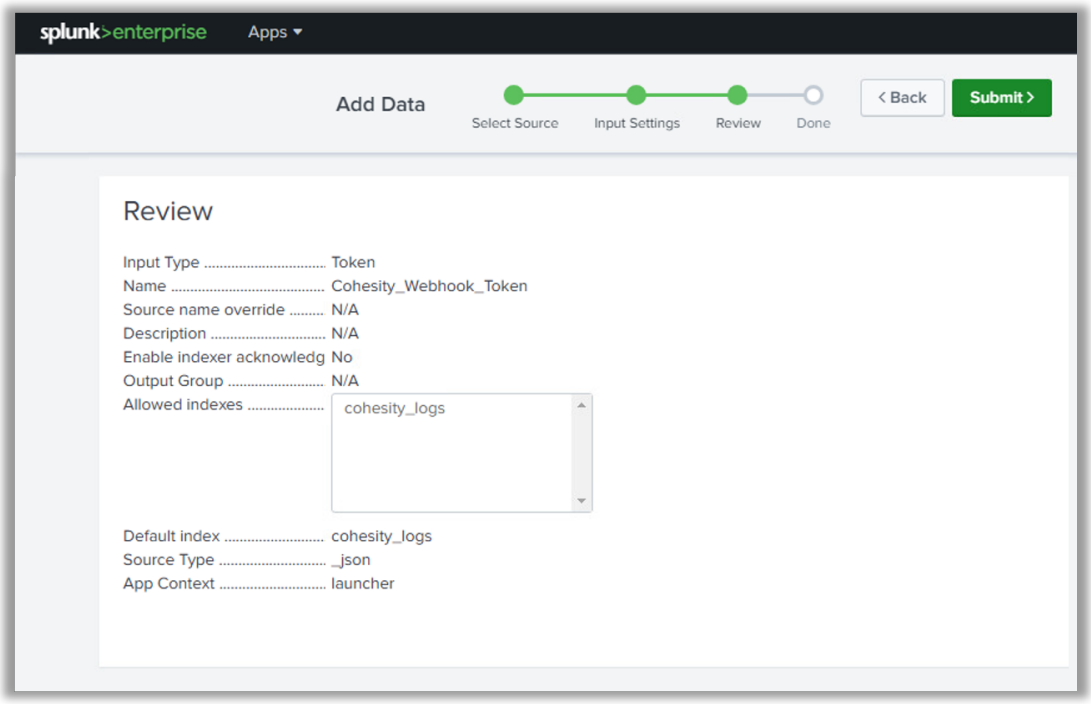
e. Under **Input Settings**, For **Source Type**, choose **Select** and then click **Select Source Type.** Select **_json** from the dropdown. If it is not shown under the dropdown, then type **_json** in search bar to bring it up.



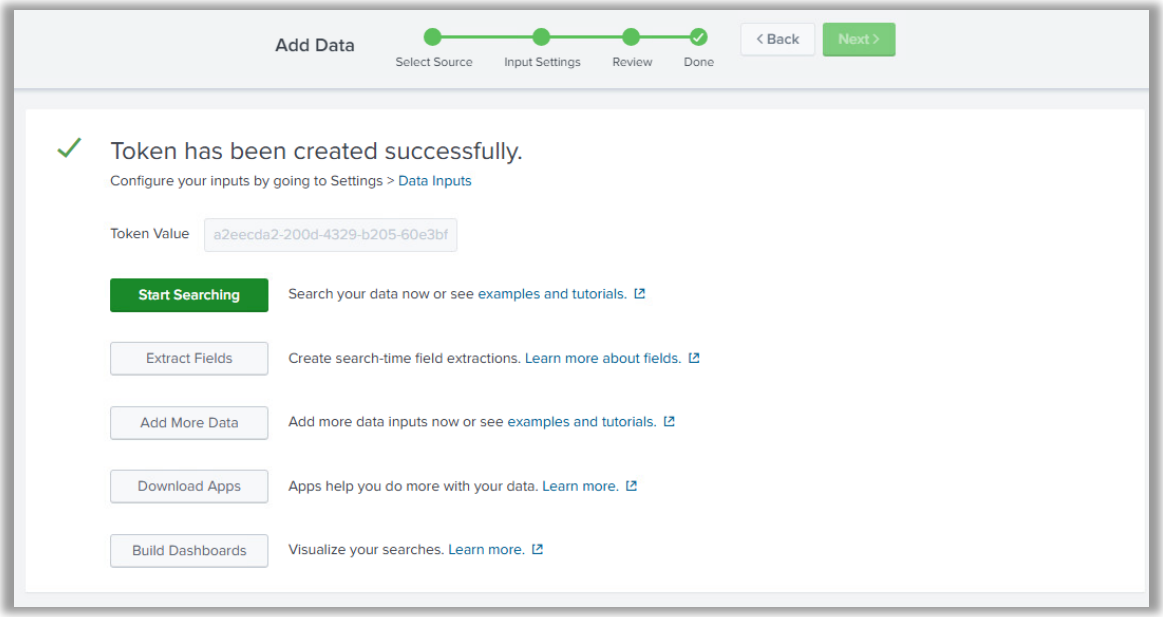
f. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.



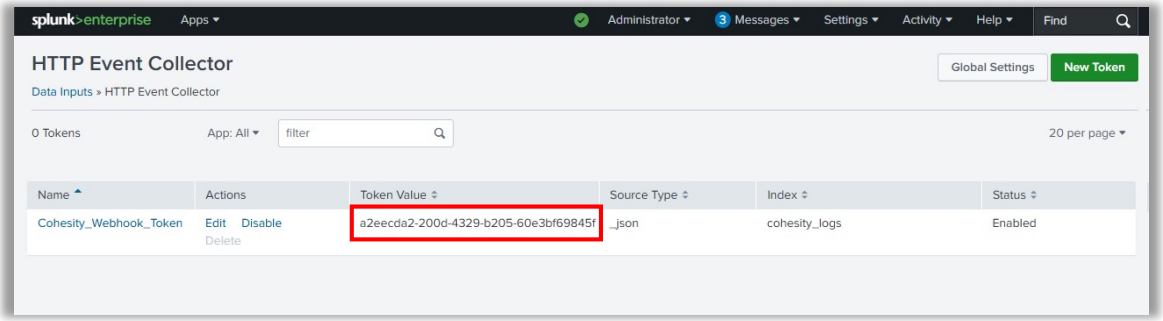
g. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.



h. Click **Submit** to successfully create the token.



i. Once the Token is created, go back to **HTTP Event Collector Page** and verify the Token created. Copy the **Token Value** (Which we will need while configuring the Webhook on Cohesity side)



5. Check HEC endpoint is accessible.

a. Open the URL below in a browser.

```
https://<your_splunk_ip>:8088/services/collector/health
```

b. If you get the below json response, then your HEC endpoint is accessible and properly configured.

```
{"text":"HEC is healthy","code":17}
```

c. If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Revisit previous steps to configure the HEC properly.

6. Test the HTTP Event Collector on any system.

   a. Test the HTTP Event Collector using a curl request from cmd prompt / terminal on any system as shown below:

```
curl -k "https://<your Splunk IP>:8088/services/collector/raw" \
     -H "Authorization: Splunk <HEC Token>" \
     -H "Content-Type: application/json" \
     -d '{"alert": "Test Alert", "alertId": "0000"}'
```

   - Your Splunk IP – is the IP address of the system where your Splunk Enterprise is running.
   - HEC Token – is the Token Value of the HTTP Event Collector Token you created in the previous step.

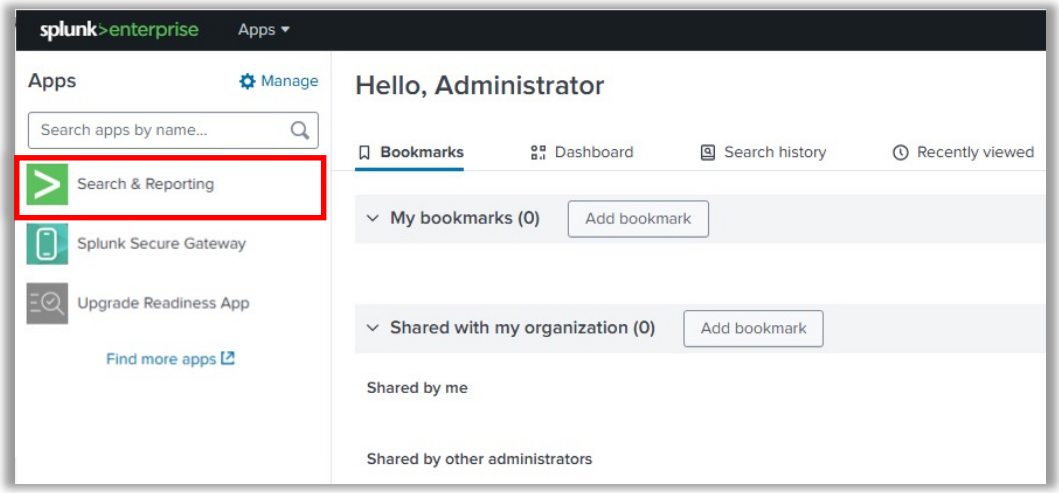
     Once the curl command executes successfully, it must return the message *{"text": "Success", "code": "0"}* as shown below:

   NOTE:

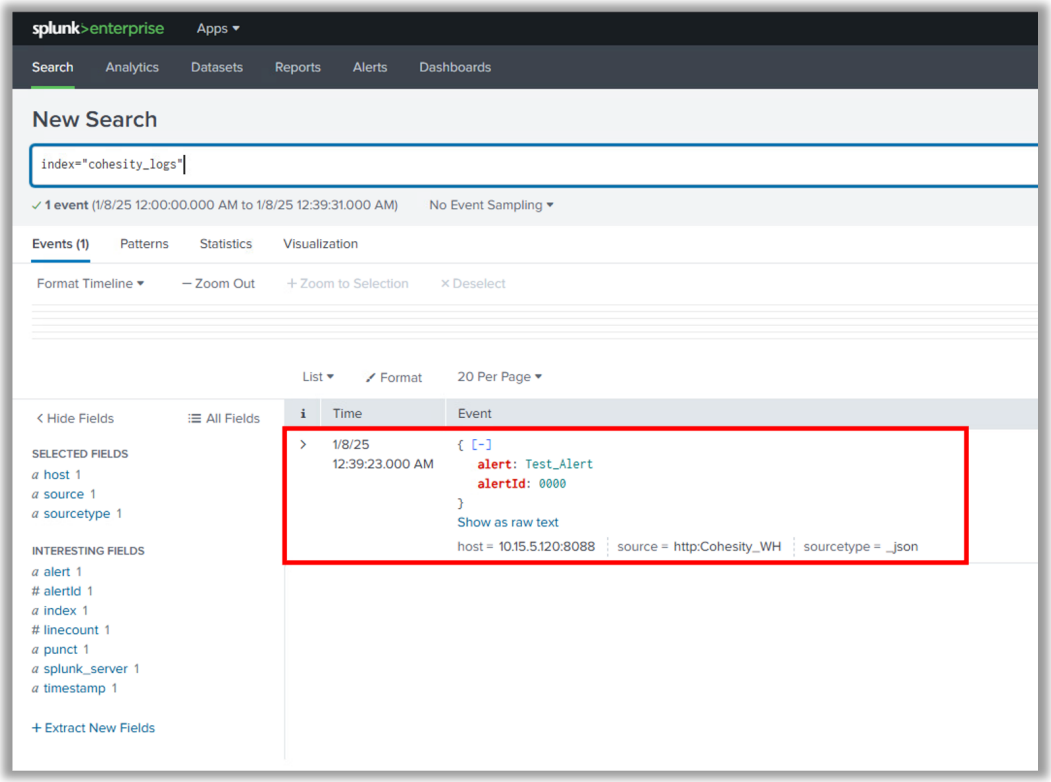
   - If you are not receiving the message *{"text": "Success", "code": "0"}* or receiving some other message, then there is some issue with the HTTP Event Collector configuration.
   - Revisit steps 2 & 3 for proper configuration.
   - Visit Troubleshooting for more details.

   b. Verify the data is successfully received on Splunk.

      i. From Splunk Web Home console, click Search & Reporting.



ii. Run search query to filter logs. You must see the event sent by curl command in Splunk.

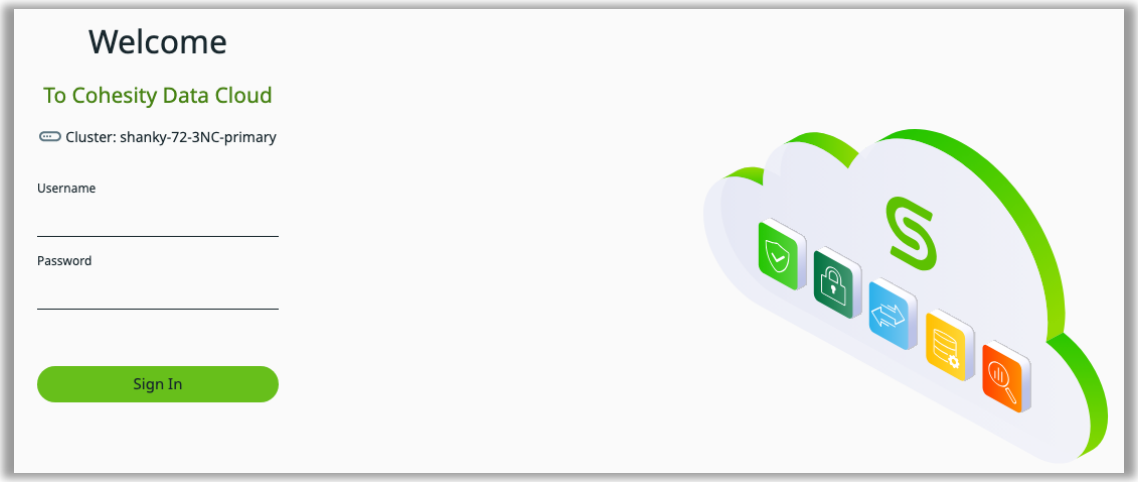


NOTE:

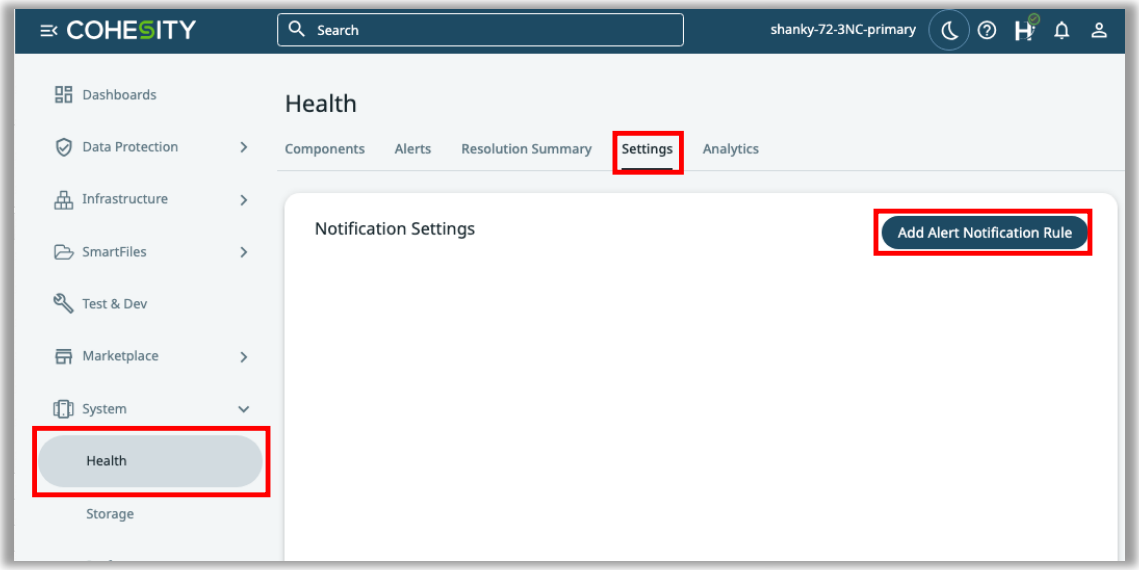
- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

7. Configure alert notification with webhook On Cohesity Cluster.

   a. Login to your Cohesity Cluster from Cluster UI.



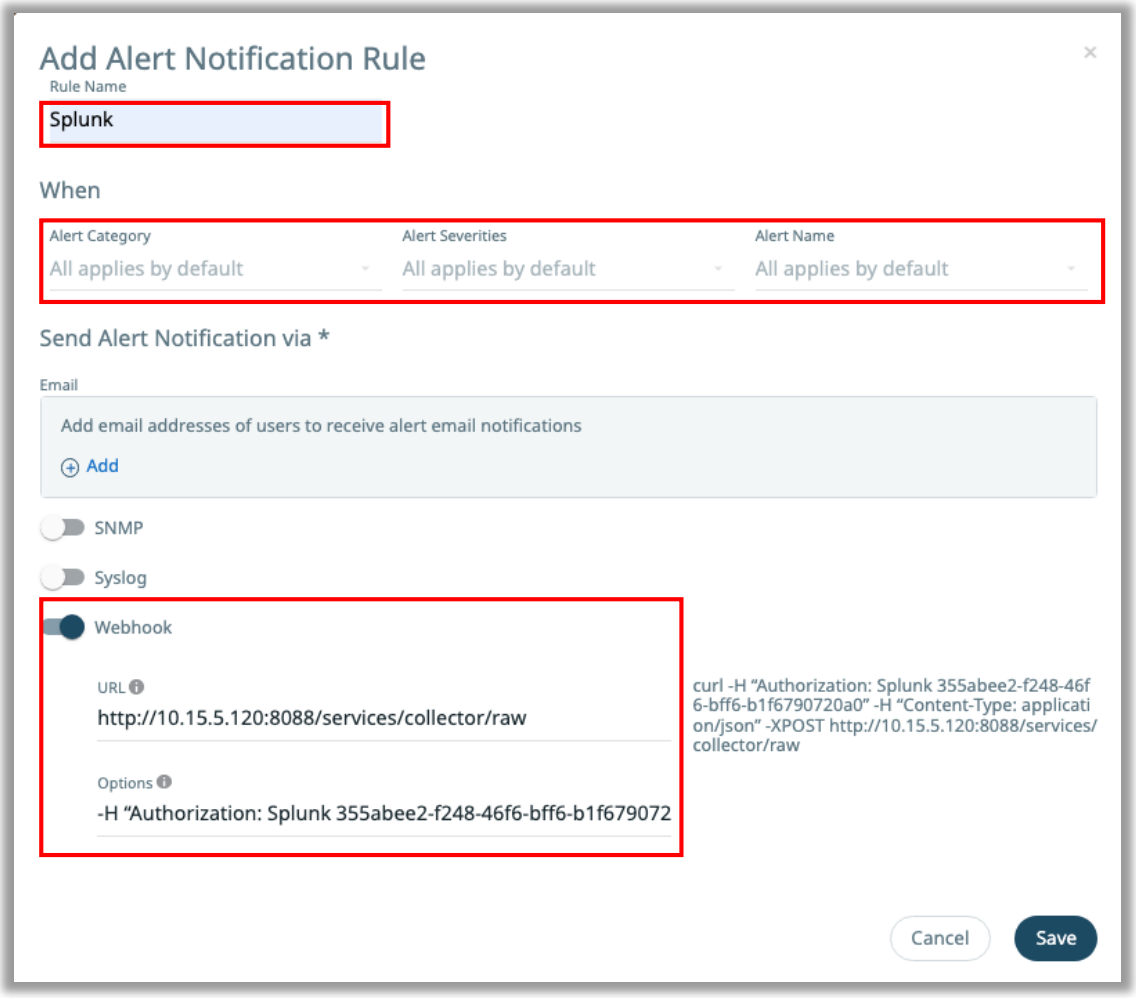
b. Click **System** > **Health** > **Settings** and then **Add Alert Notification Rule.**



c. Provide the **Rule Name**, choose required **Alert Category**, **Alert Severities** and **Alert Name**, choose **Webhook** as alert notification type and provide the Webhook **URL** and **Options** as below:

URL:
https://<Your Splunk IP>:8088/services/collector/raw

Options:
-H “Authorization: Splunk *<HEC Token>*” -H “Content-Type: application/json”

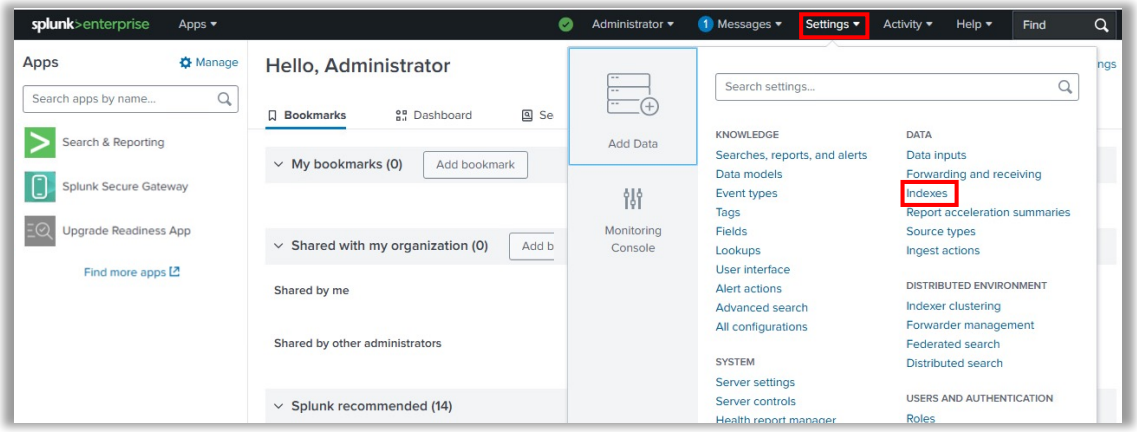


NOTE:

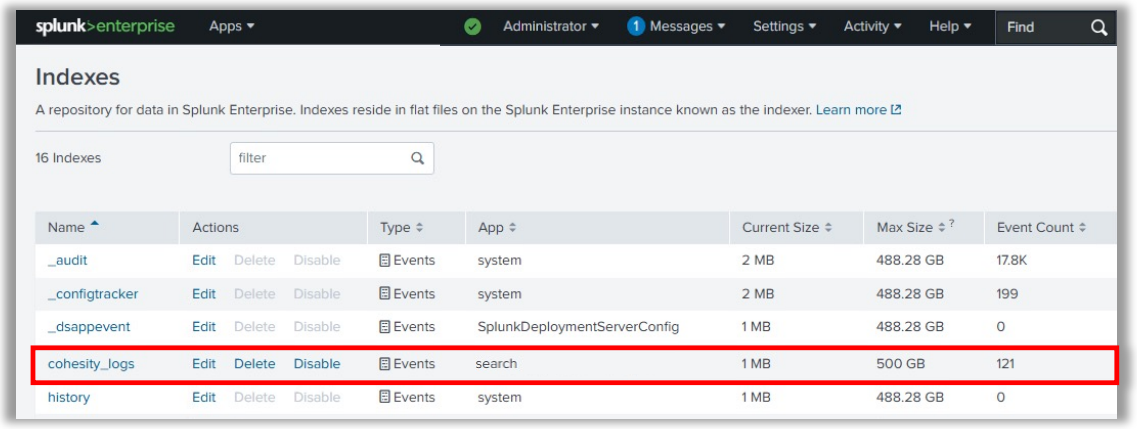
- Use Alert Category, Alert Severities or Alert Name to filter out the selective alerts you want to send to Splunk.
- If you do not select any value for Alert Category, Alert Severities or Alert Name, then all the alerts generated by Cohesity will be sent to Splunk.
- You can see the corresponding curl command framed on the Cluster UI based on your entered URL and Options for Webhook. You can test that curl command on cmd prompt / terminal of any system.
- Revisit step 5 to know more details.

8. Validate data received from Cohesity on Splunk Enterprise.

   a. Click under **Indexes Settings**.



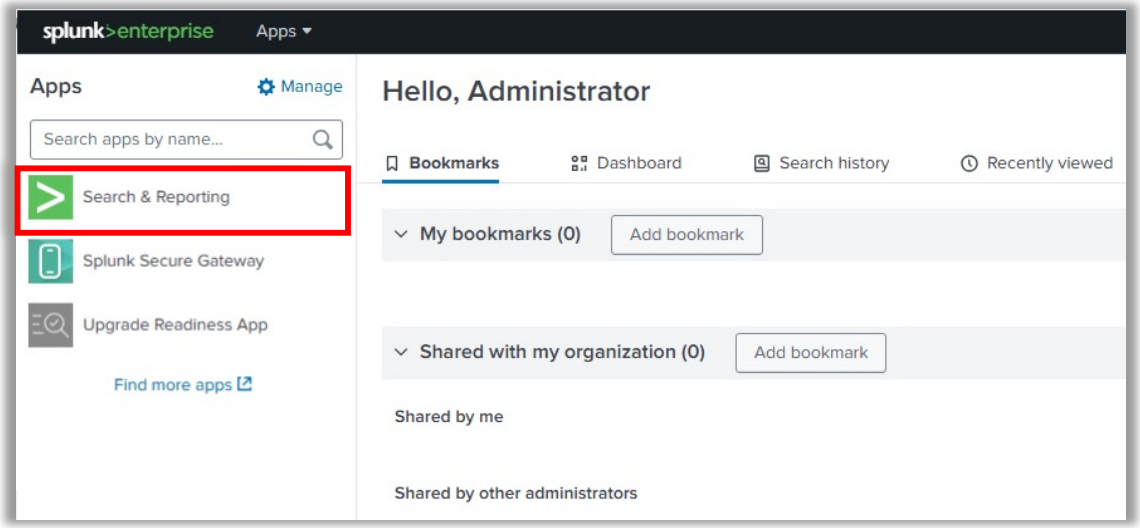
   b. Verify logs are being pushed to your index by checking the Event Count.



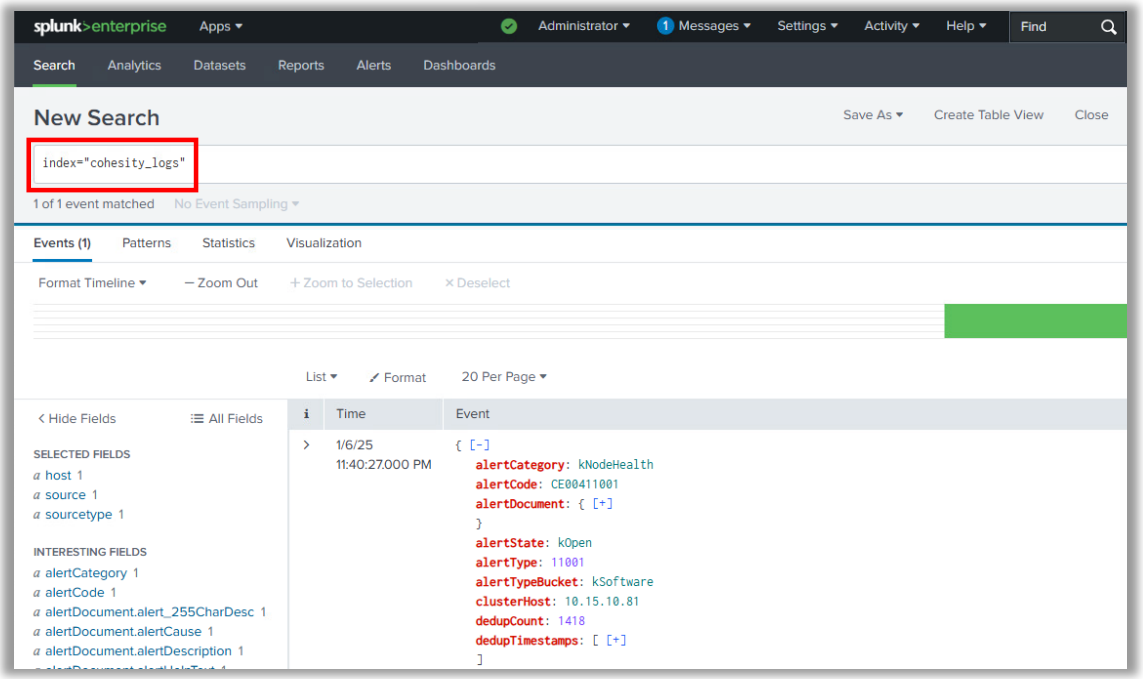
NOTE: Alerts and logs will be pushed from Cohesity to Splunk in real time. However, it is not immediate. Sometimes it takes more time for the data to be transmitted to Splunk. If you are not seeing the events after significant amount of time, then there could be an issue in HEC configuration. Edit your HEC to fix the issue.

9. Search, alert, and visualize.

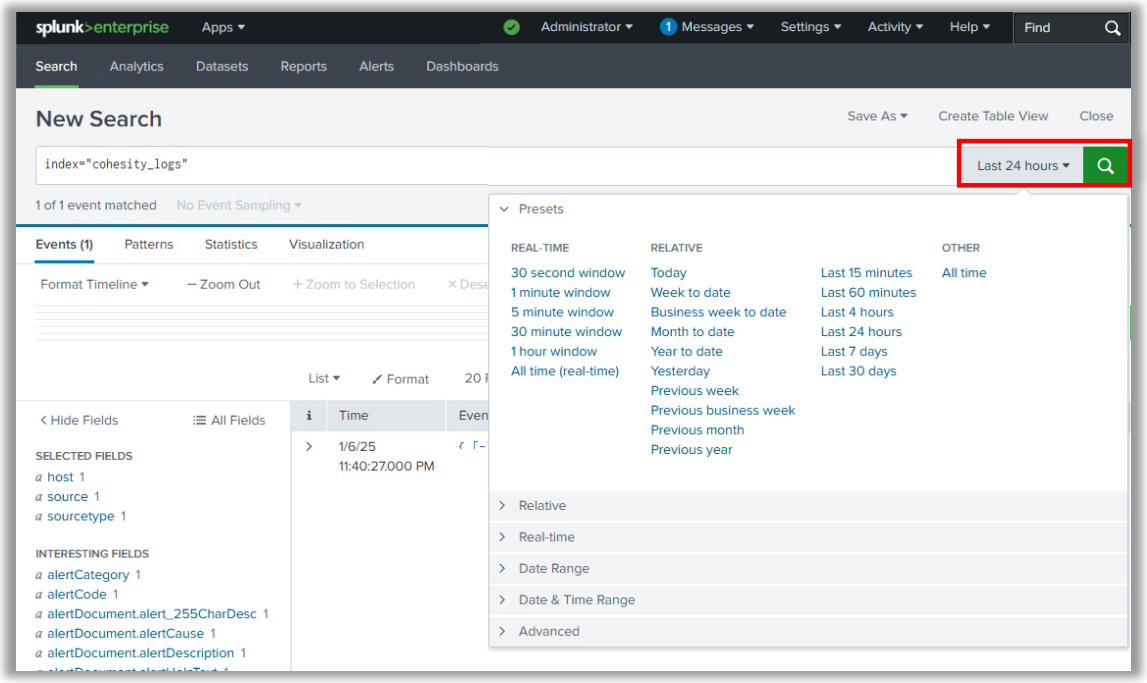
   a. From Splunk Web Home console, click Search & Reporting.



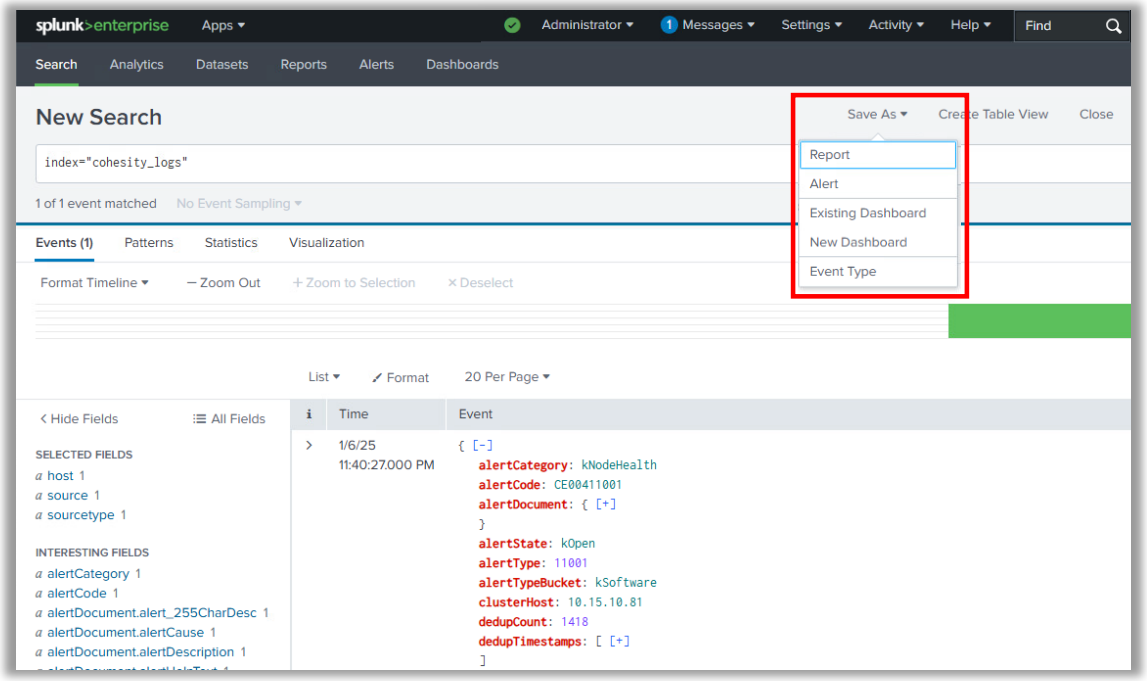
   b. Run search query to filter logs.



c. Filter search results based on time.



d. Alert and visualize.

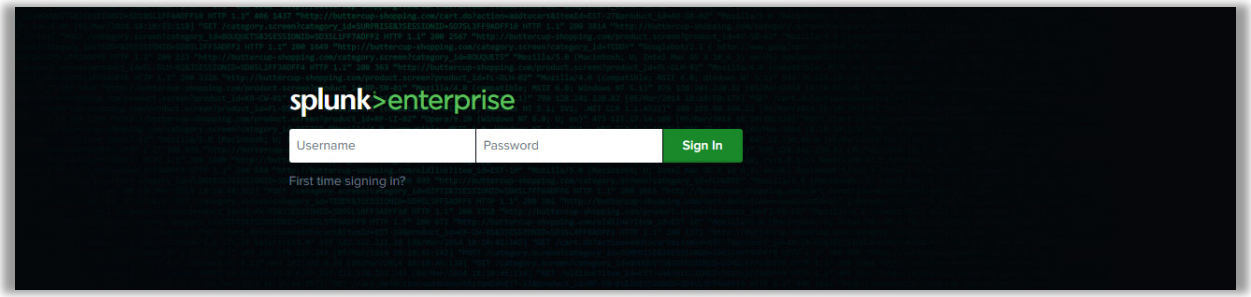


NOTE: For more details, refer to the Search and Reporting section.

Cohesity Data Cloud

DataProtect [Self-managed clusters managed from Cohesity Data Cloud]

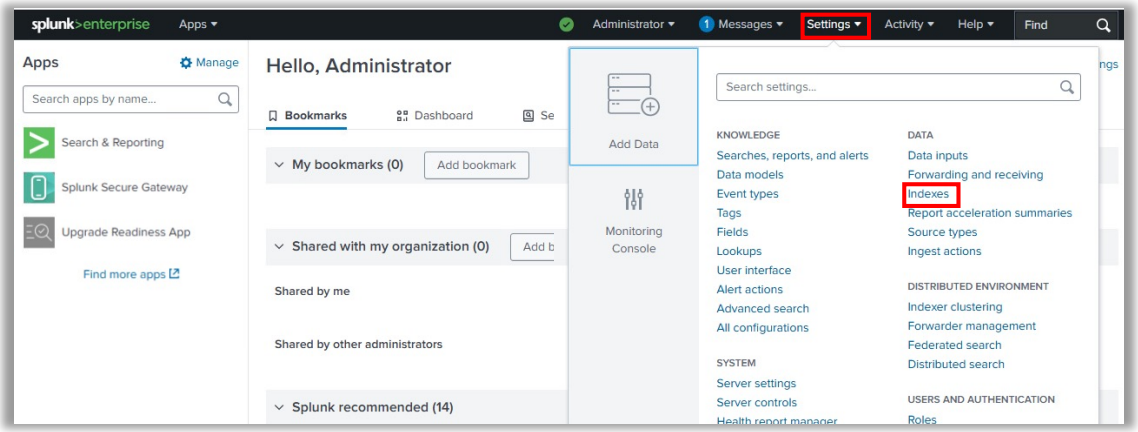
1. Login to your Splunk Enterprise Instance.



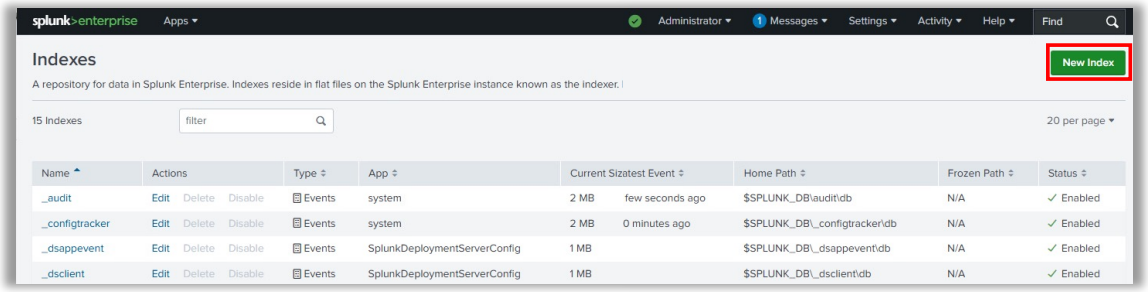
2. Create a new index to store Cohesity logs.

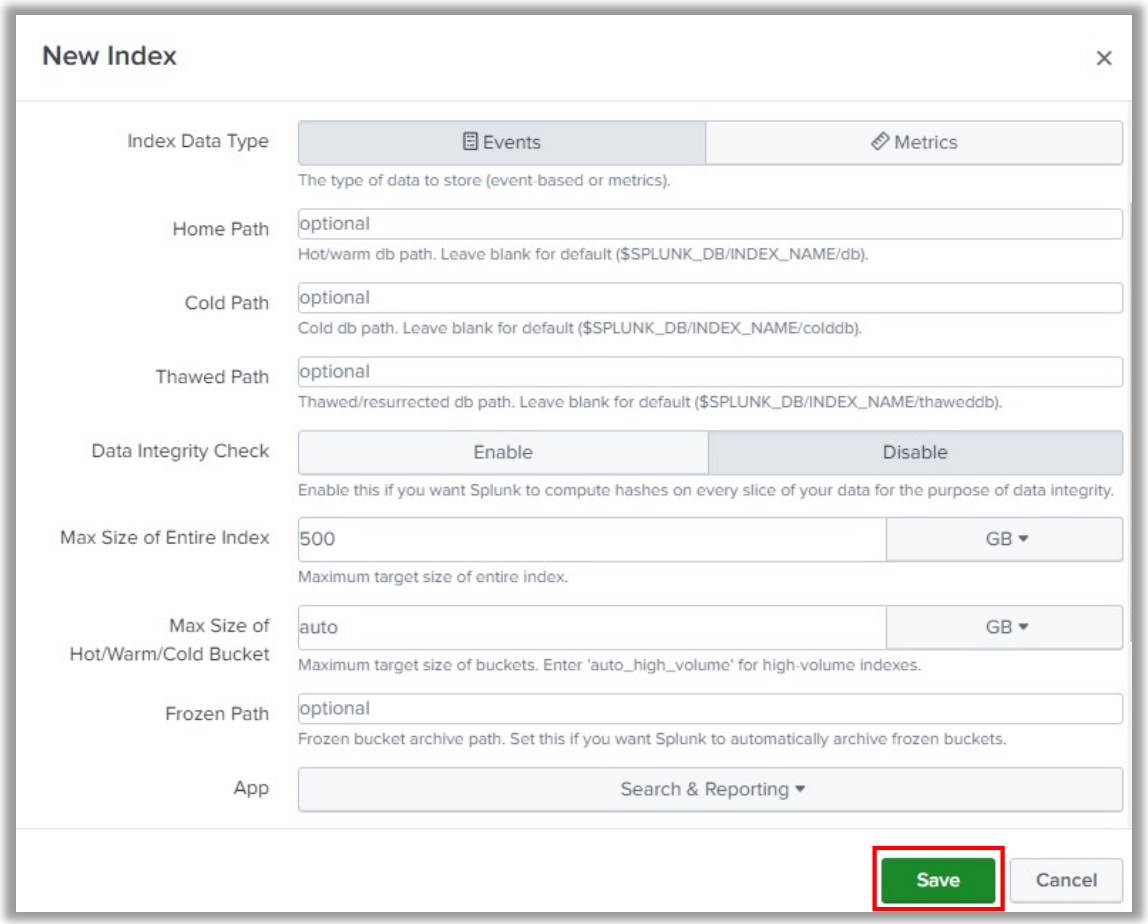
   This is an optional, however, recommended step. You can use an already existing index in your Splunk instance. But it is advised to create and use a new index specific to Cohesity logs and alerts

   a. Click **Indexes** under **Data** in **Settings**.

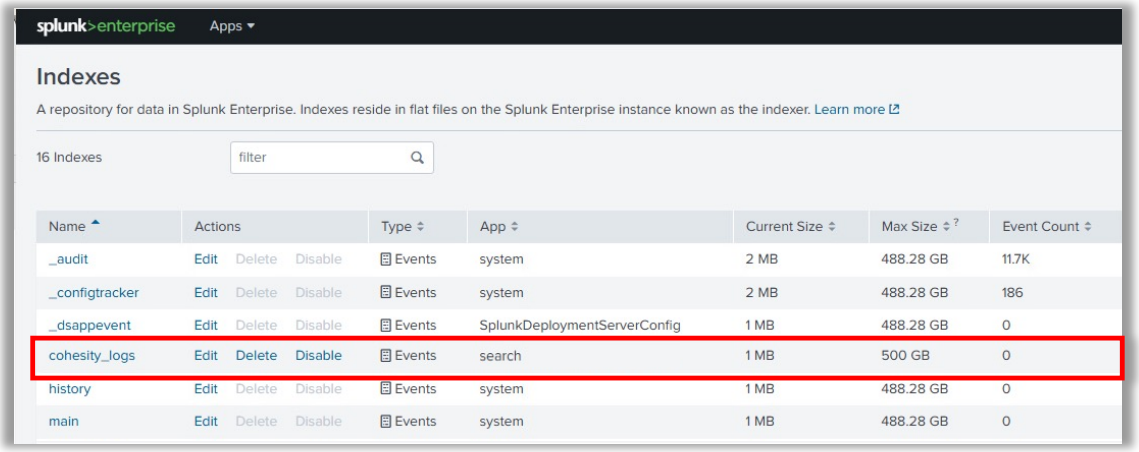


b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save.**



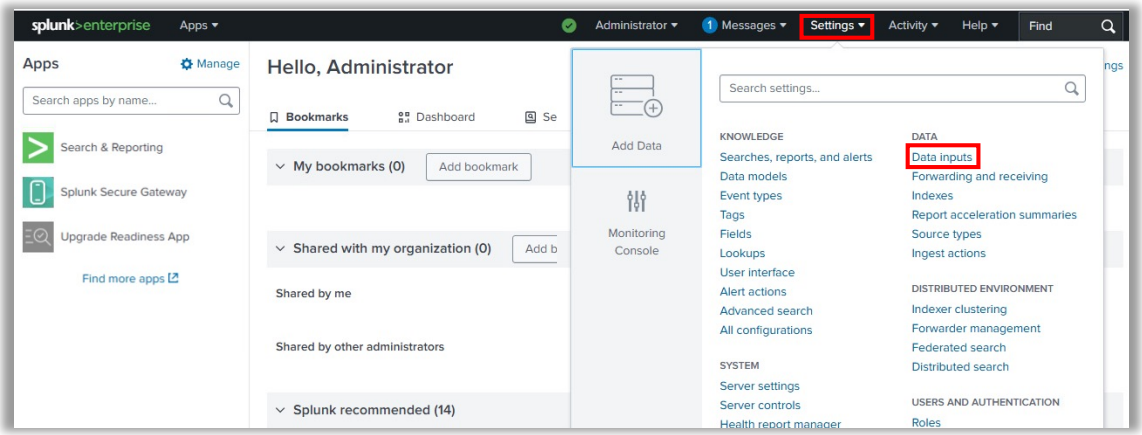


c. You can see the newly created index under Indexes.

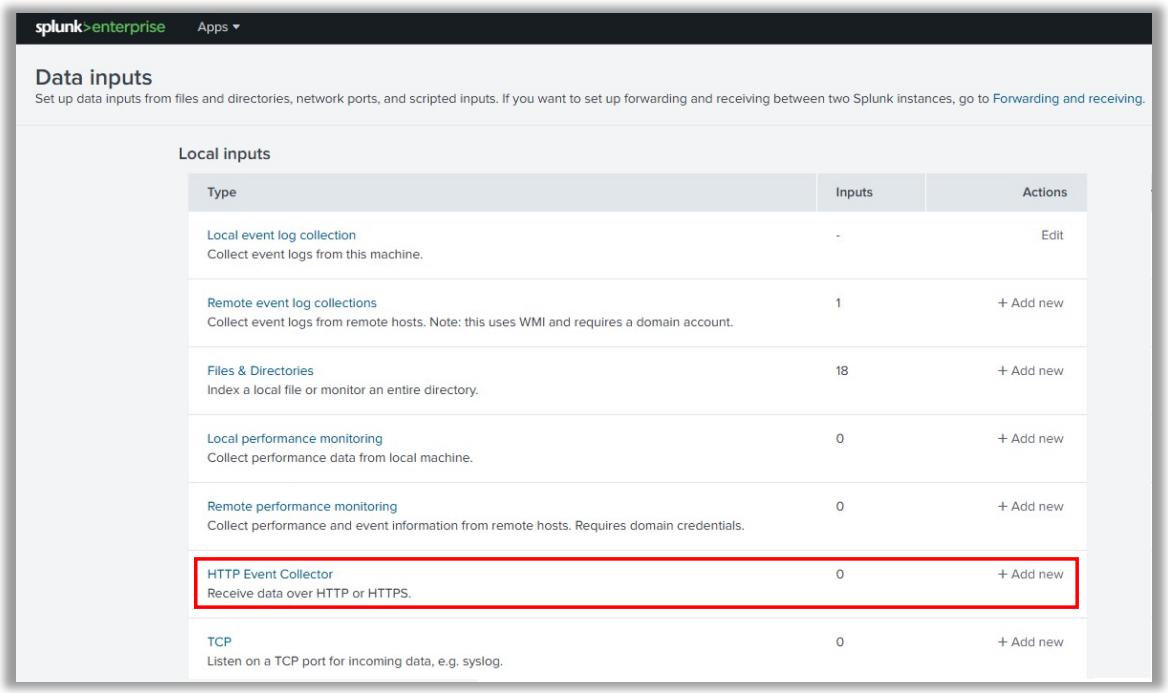


3. Configure HTTP Event Collector to receive data from Cohesity.

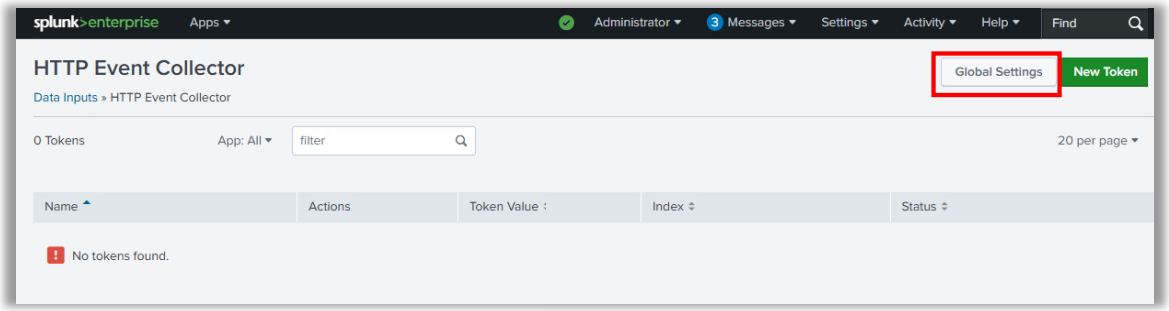
a. Click **Data Inputs** under **Data** in **Settings**.

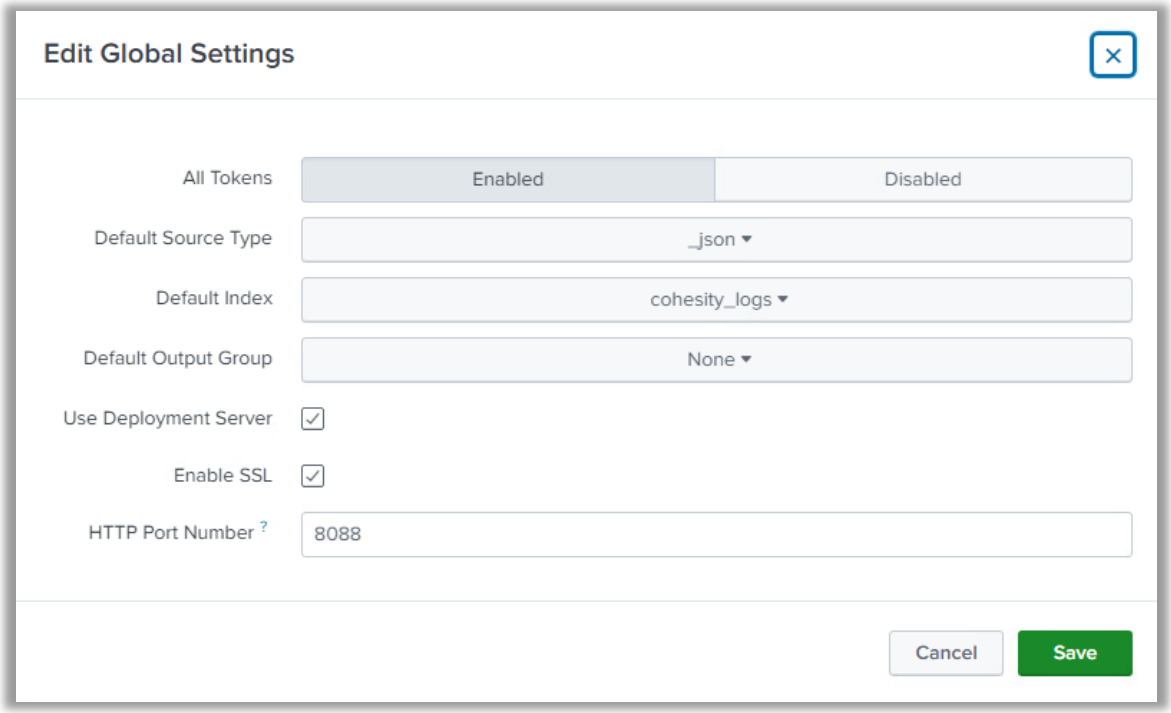


b. Click **HTTP Event Collector**.



c. Click **Global Settings** and fill in all requested details and click **Save.**

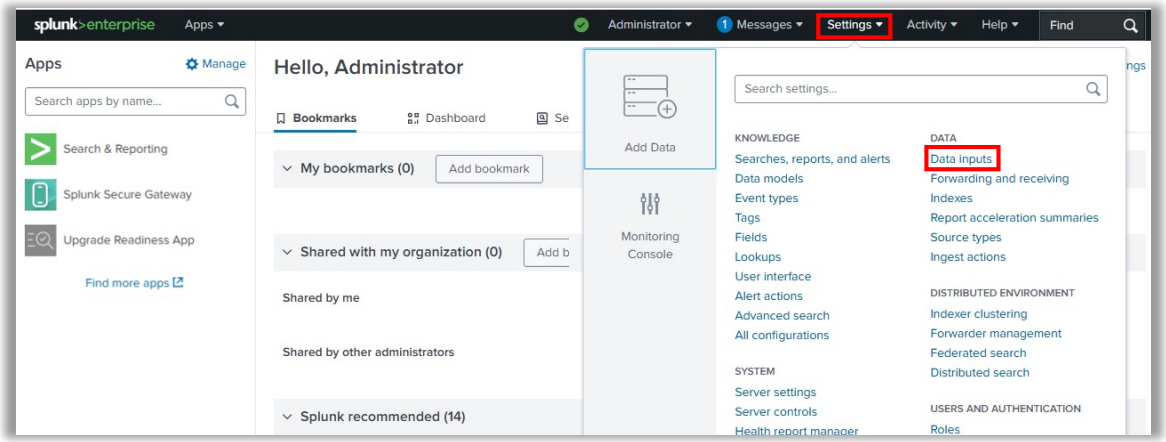




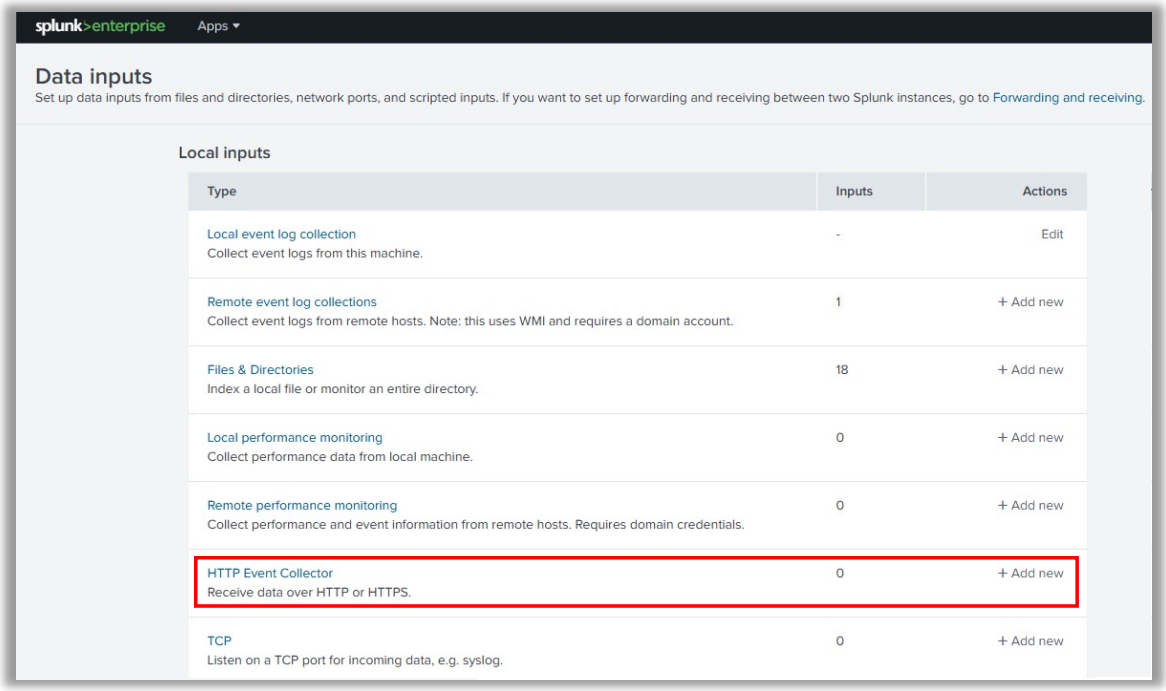
- Select **Enabled** for **All Tokens.**
- Select the **Default Source Type** as **_json** (If it is not shown under the dropdown, then type _json in the search bar to bring it up).
- Select the **Default index** as the new index we created exclusively for Cohesity logs and alerts under step 1.
- By default, **SSL** is enabled with default **Port 8088**. You can disable SSL or modify the default port. The general recommendation is to enable SSL.

4. Create a new token to authenticate Cohesity.

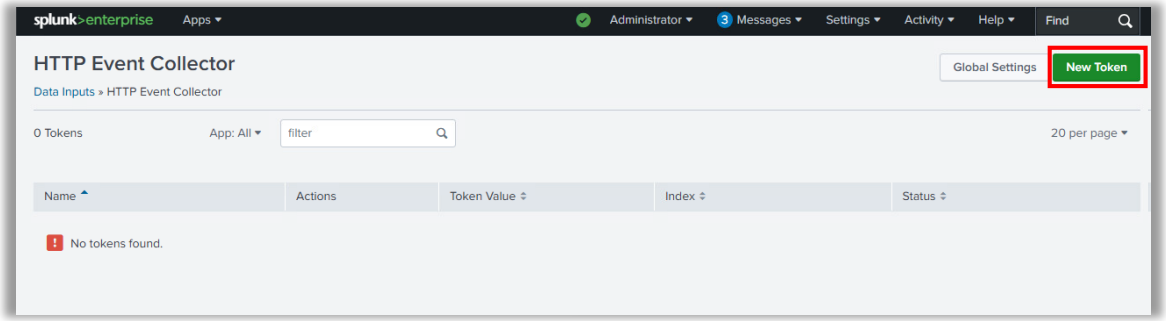
d. Click **Data Inputs** under **Data** in **Settings.**



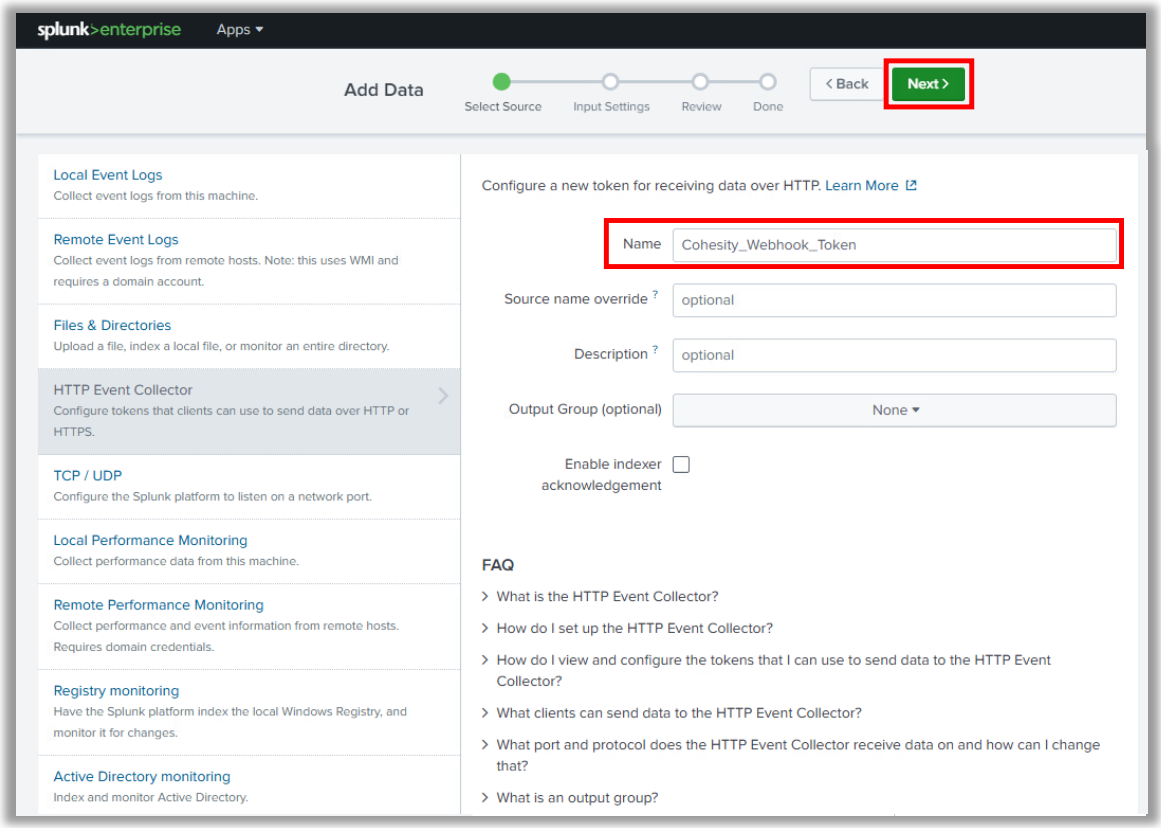
e. Click **HTTP Event Collector**.



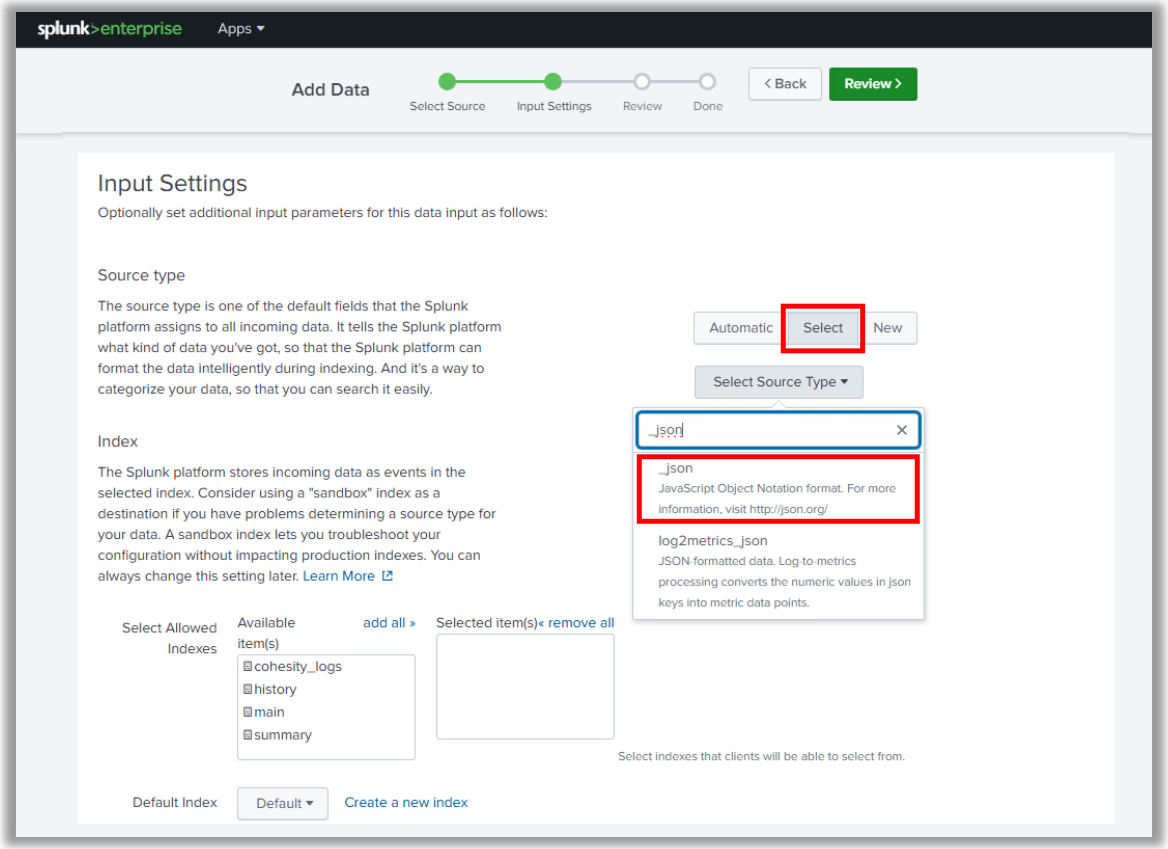
f. Click **New Token**.



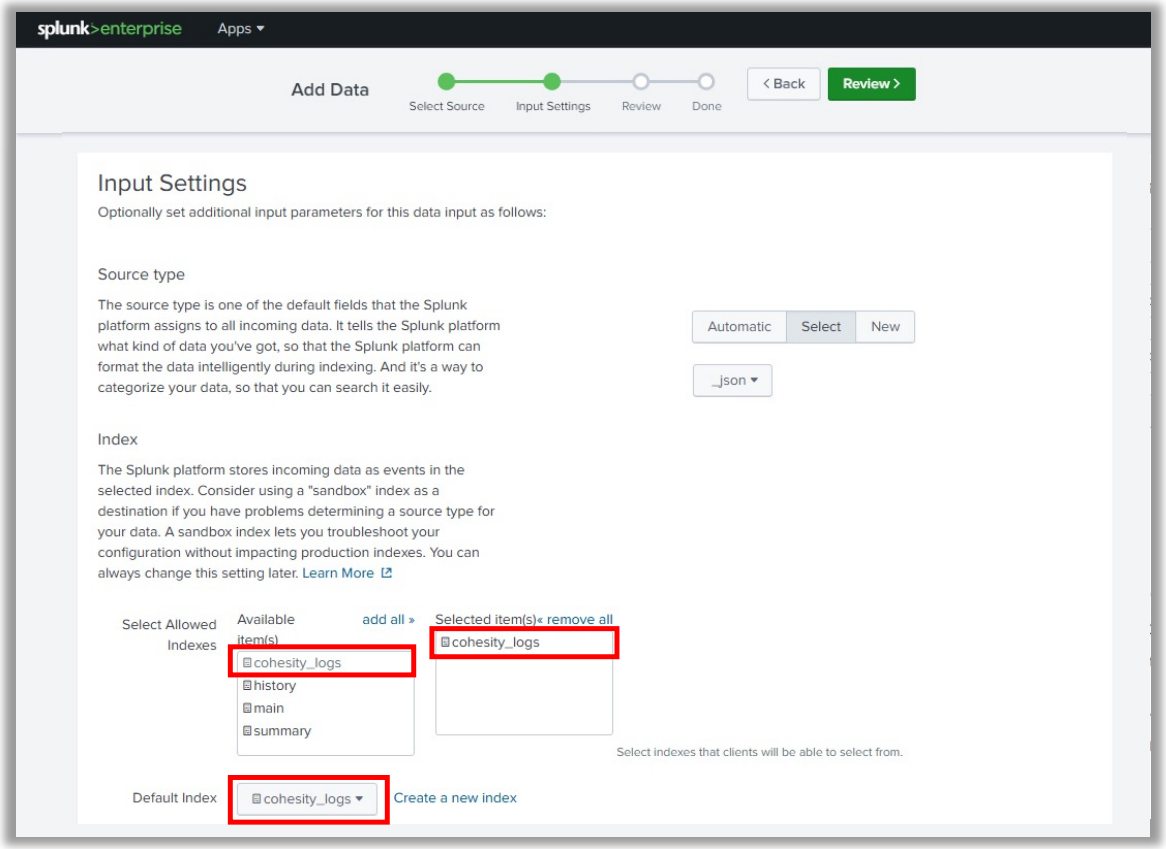
g. Provide a unique **Name** for your token and click **Next.**



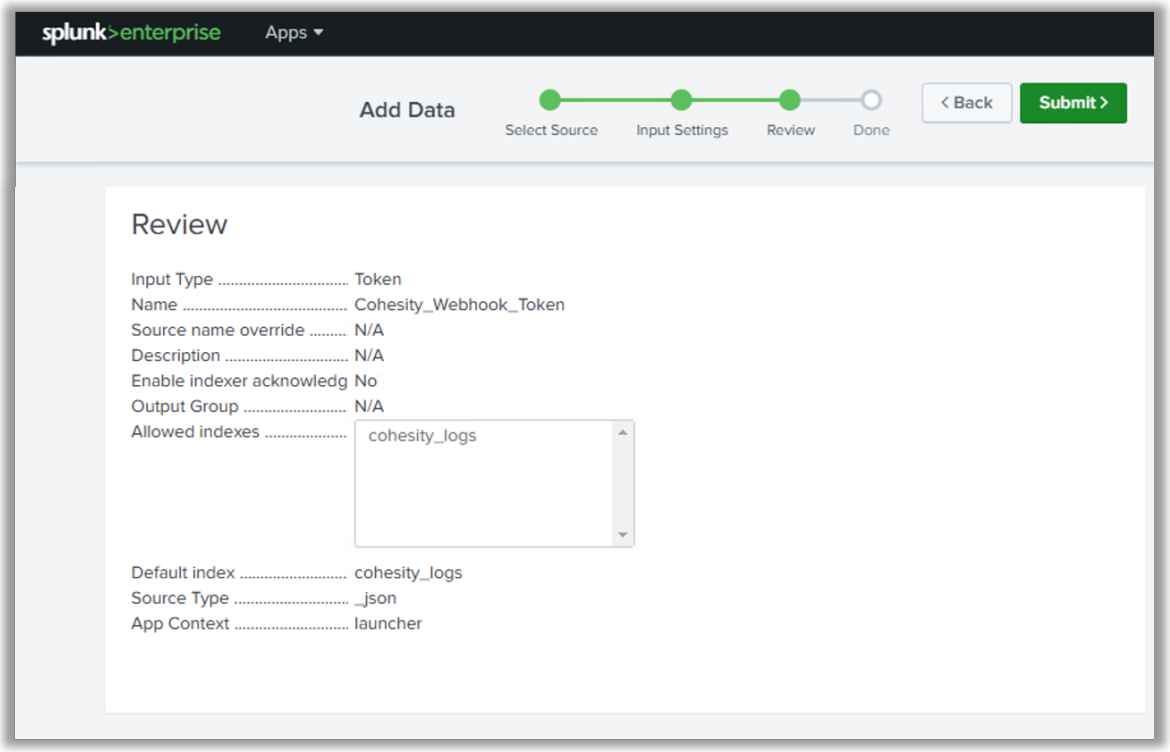
h. Under **Input Settings**, For **Source Type**, choose **Select** and then click **Select Source Type**, Select **_json** from the dropdown. If it is not shown under the dropdown, then type **_json** in search bar to bring it up.



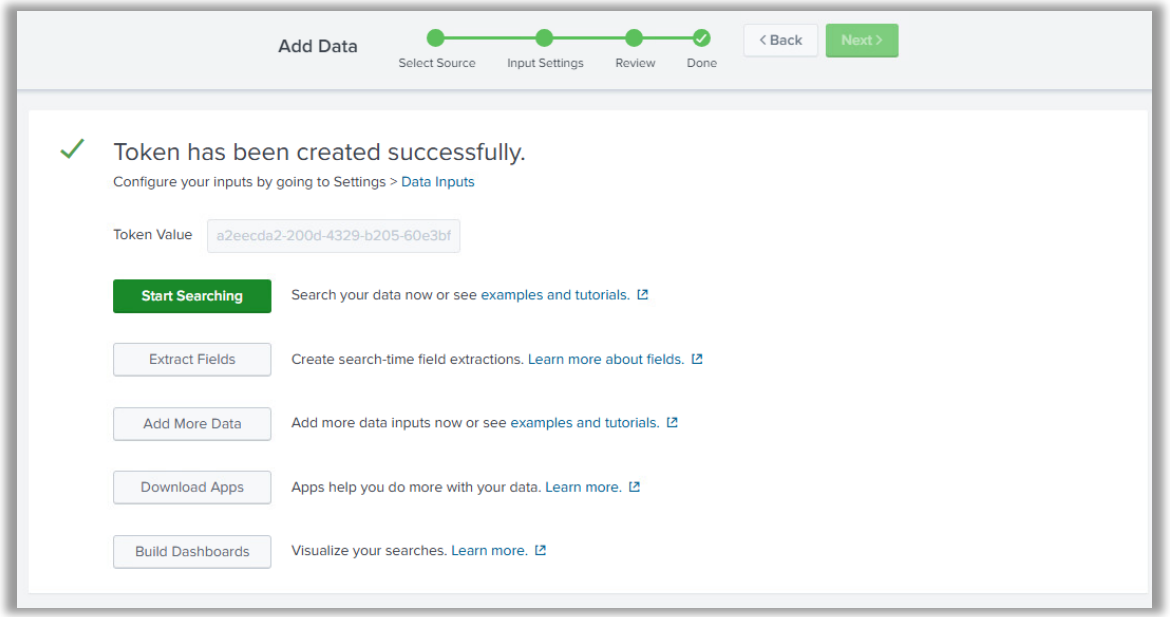
i. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.



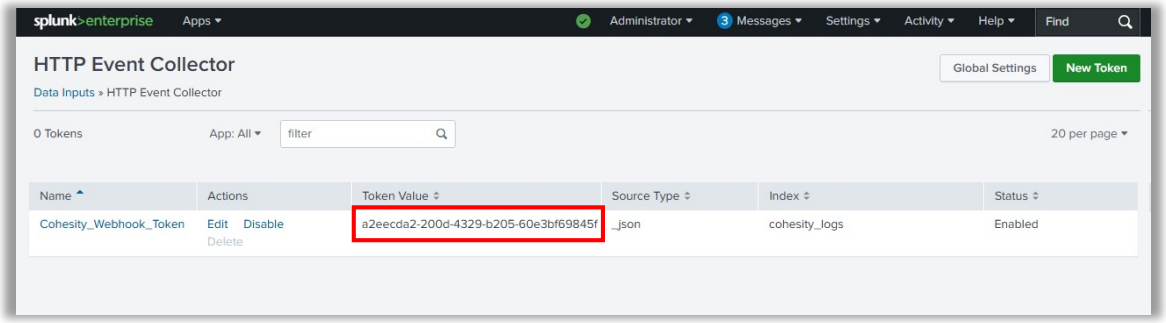
j. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.



k. Click **Submit** to successfully create the token.



l. Once the Token is created, go back to **HTTP Event Collector Page** and verify the Token created. Copy the **Token Value** (Which we will need while configuring the Webhook on Cohesity side).



5. Check HEC endpoint is accessible.

   a. Open the below URL in a browser.

   ```
   https://<your_splunk_ip>:8088/services/collector/health
   ```

   b. If you get the below json response, then your HEC endpoint is accessible and properly configured.

   ```
   {"text":"HEC is healthy","code":17}
   ```

   c. If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Revisit previous steps to configure the HEC properly

6. Test HTTP Event Collector on any system.

   a. Test the HTTP Event Collector using a curl request from cmd prompt / terminal on any system as shown below.

   ```
   curl -k "https://<your Splunk IP>:8088/services/collector/raw" \
        -H "Authorization: Splunk <HEC Token>" \
        -H "Content-Type: application/json" \
        -d '{"alert": "Test Alert", "alertId": "0000"}'
   ```

   - Your Splunk IP – is the IP address of the system where your Splunk Enterprise is running.
   - HEC Token – is the Token Value of the HTTP Event Collector Token you created in previous step

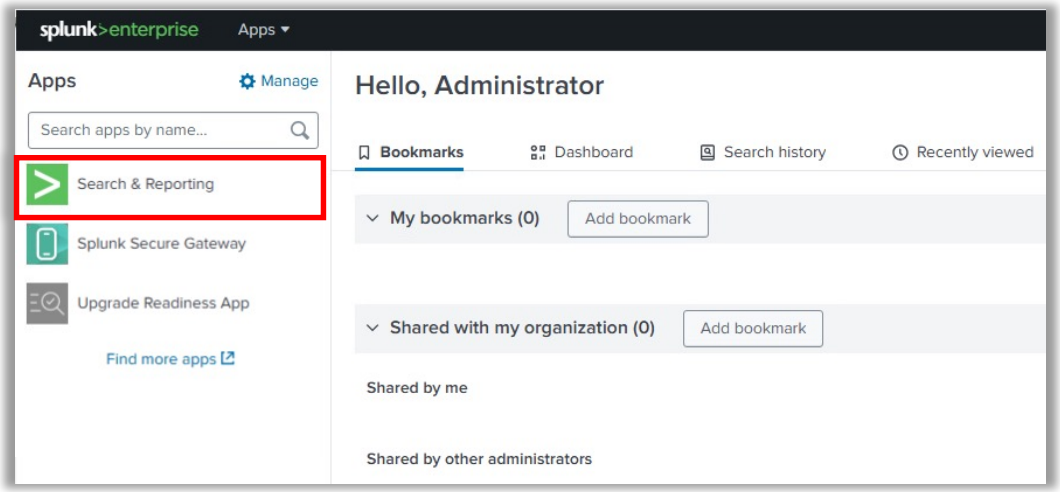
   Once the curl command executes successfully, it must return the message *{"text": "Success", "code": "0"}* as shown below:

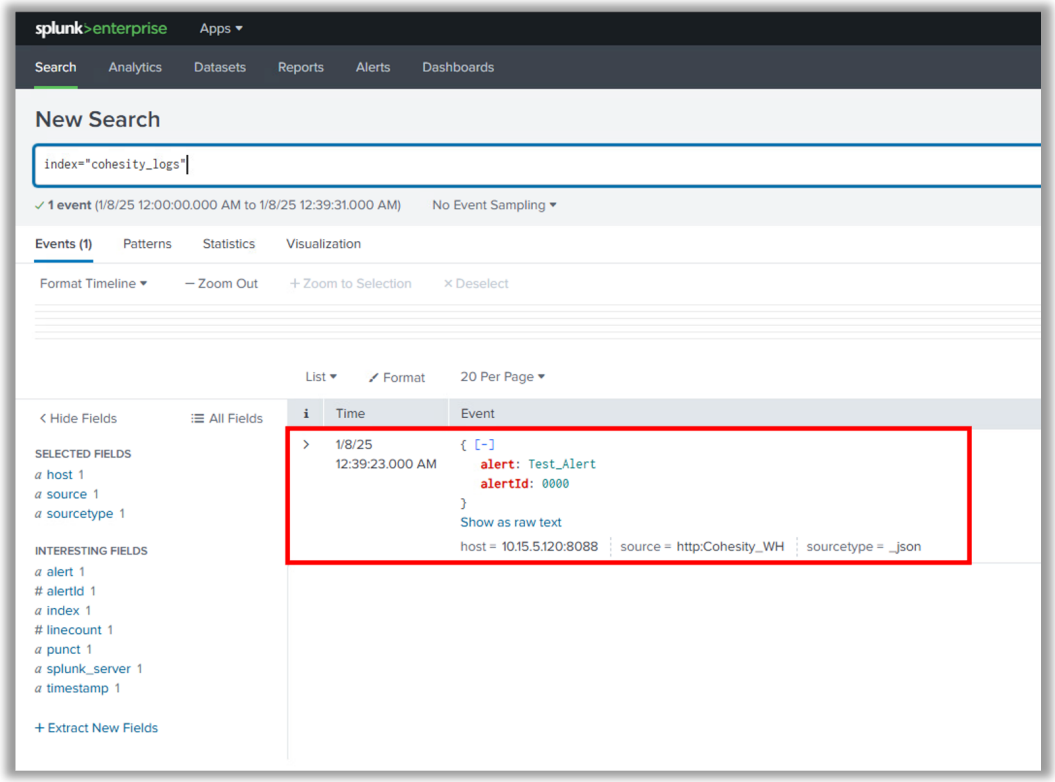
   - If you are not receiving the message *{"text": "Success", "code": "0"}* or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
   - Visit Troubleshooting for more details.

b. Verify the data is successfully received on Splunk.

i. From Splunk Web Home console, click Search & Reporting.

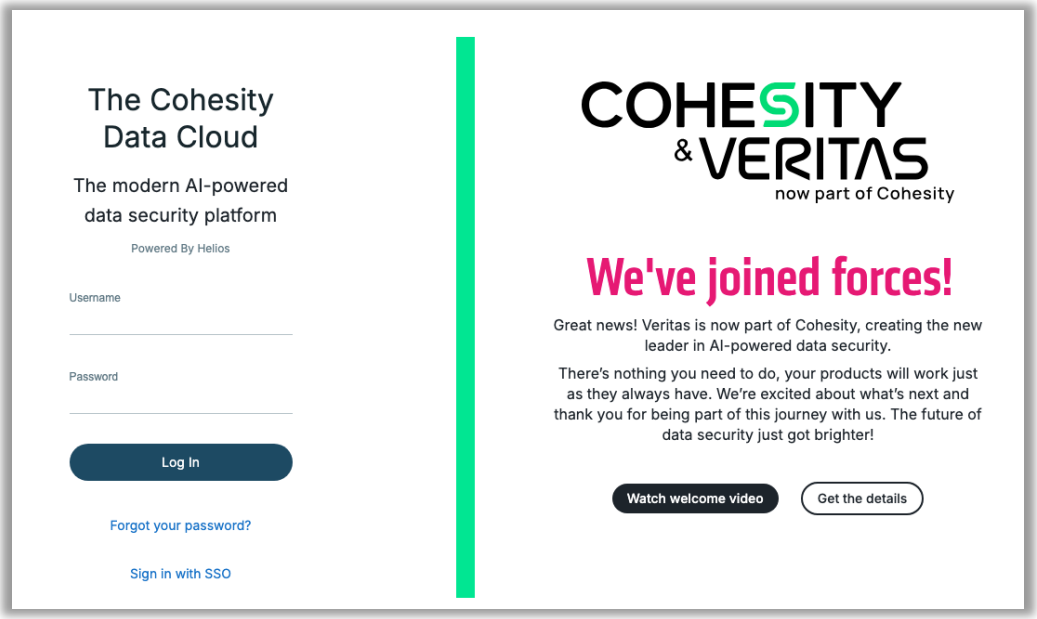


ii. Run search query to filter logs. You must see the event sent by curl command in Splunk.

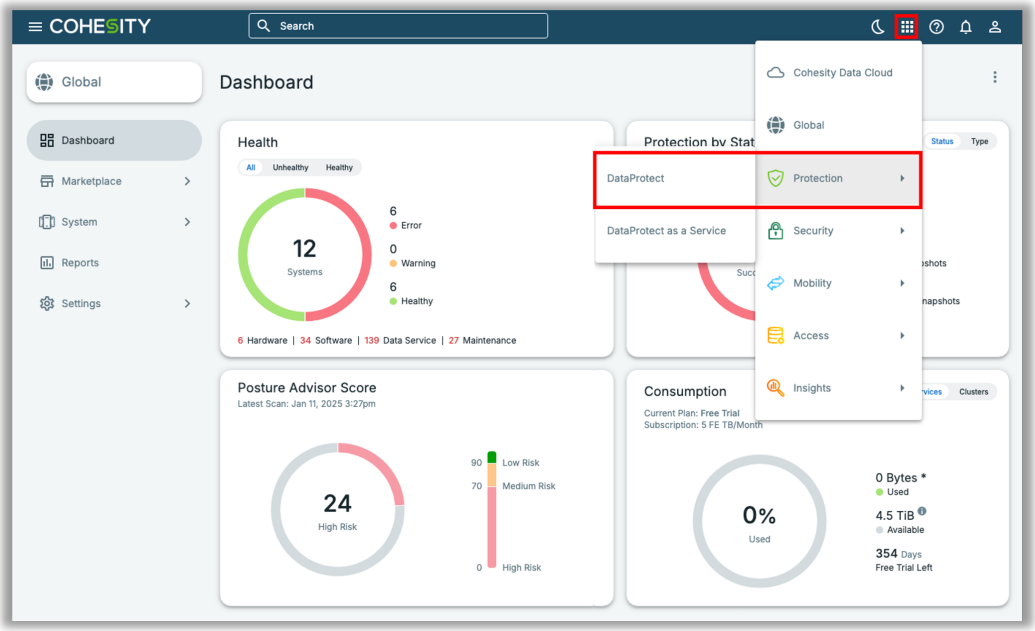


- If you are not receiving the message *{"text": "Success", "code": "0"}* or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

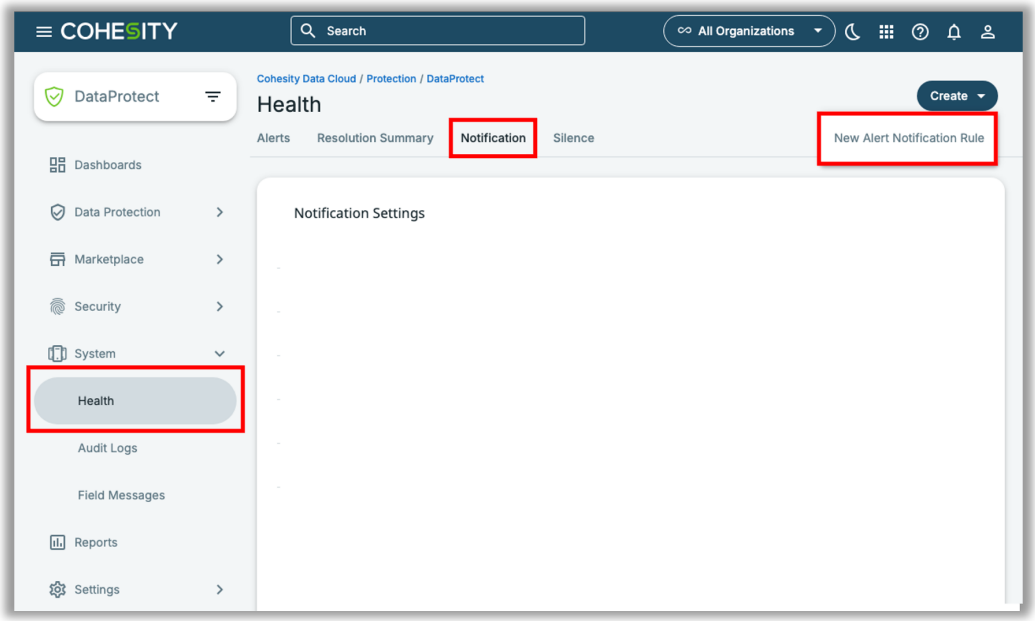
7. Configure alert notification with webhook on Cohesity Data Cloud.
   a. Login to Cohesity Data Cloud.



   b. Go to **DataProtect** under **Protection**.



c. Click **System** > **Health** > **Notification and then Create** > **New Alert Notification Rule**.



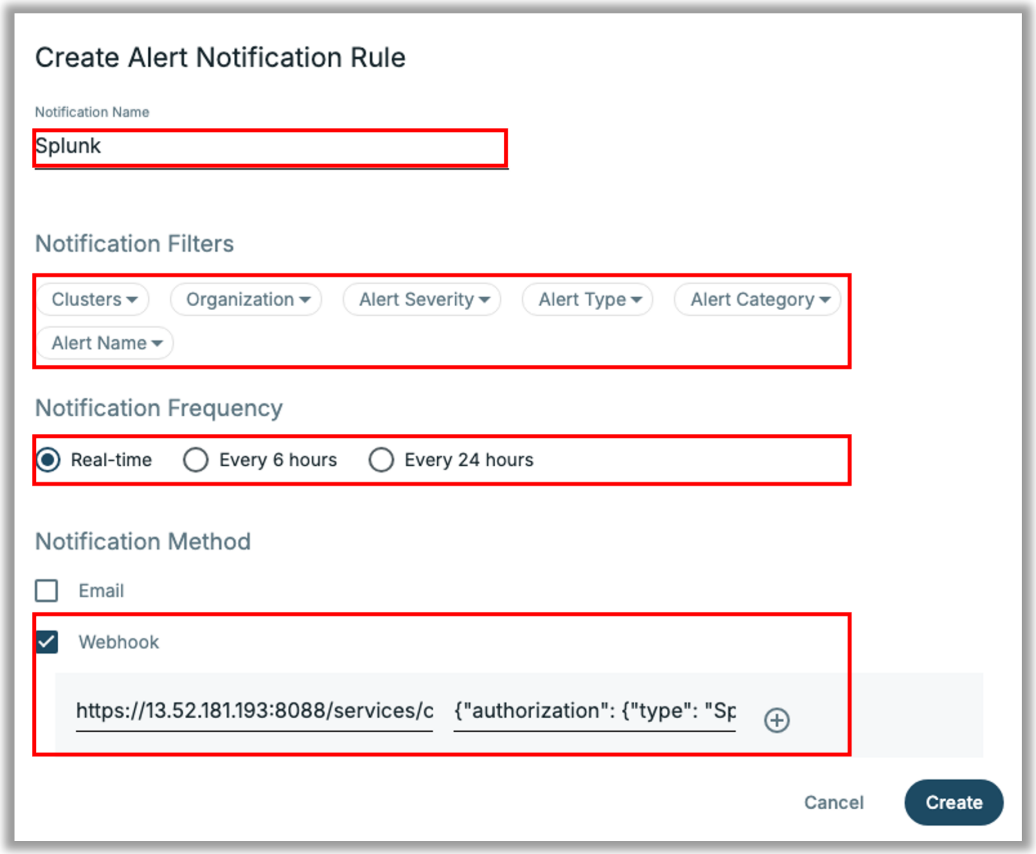
d. Provide the **Notification Name**, select the **Notification Filters** and **Notification Frequency**, choose **Webhook** as the **Notification Method** and provide the **Webhook URL** and **Options** as below:

URL:
https://<Your Splunk IP>:8088/services/collector/raw

Options:
{"authorization": {"type": "Splunk","credentials": "*<HEC Token>*"}}

NOTE For Splunk Trials:

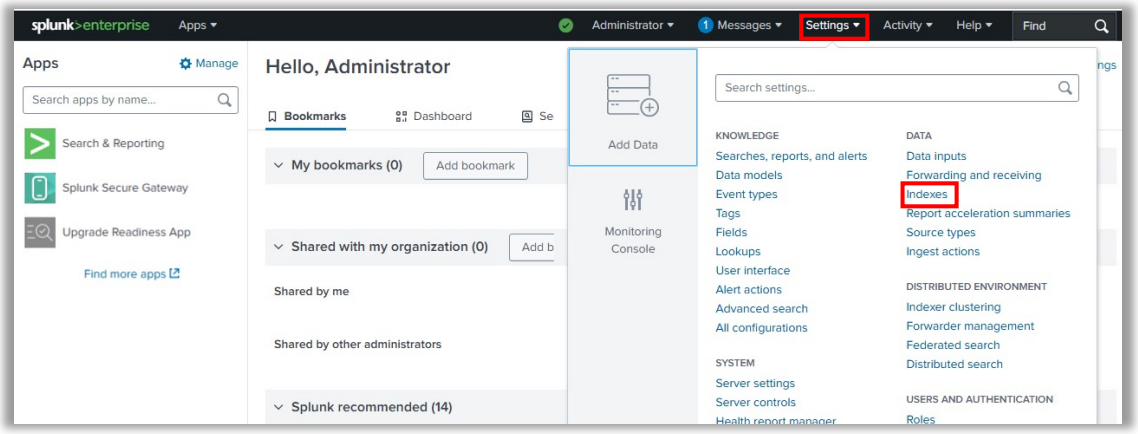
- Alert notifications from Cohesity to Splunk via Webhook requires a valid certificate at the Splunk side.
- Splunk trials might use expired/invalid certificates, which may lead to TLS certificate verification failure, in which case the alert notifications will not be sent from Cohesity to Splunk.
- Ensure you have a valid certificate installed or available at your Splunk Enterprise.



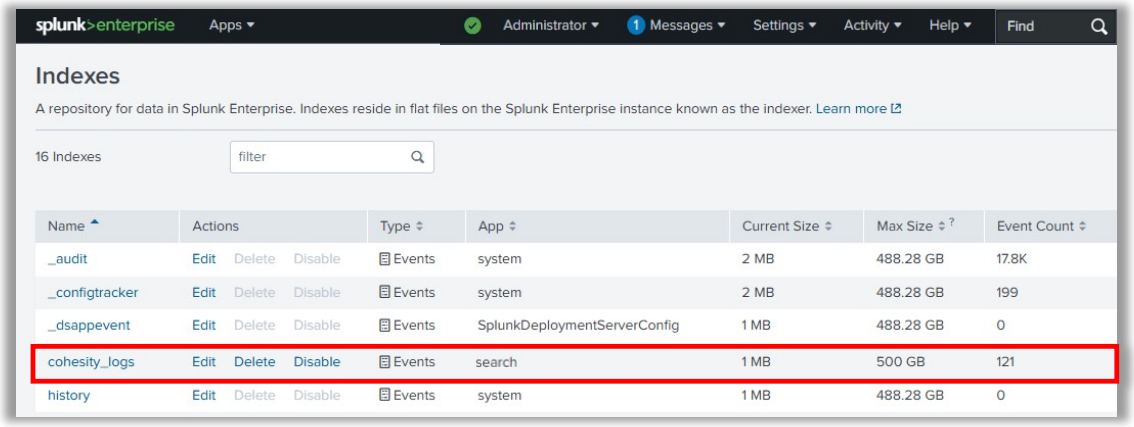
NOTE:

- Use Clusters, Organization, Alert Severity, Alert Type, Alert Category or Alert Name to filter out the selective alerts you want to send to Splunk.
- If you do not select any value for Clusters, Organization, Alert Severity, Alert Type, Alert Category or Alert Name, then all the alerts generated by Cohesity will be sent to Splunk.

8. Validate data received from Cohesity on Splunk Enterprise.
   a. Click **Indexes** under **Data** in **Settings.**



b. Verify logs are being pushed to your index by checking the Event Count.

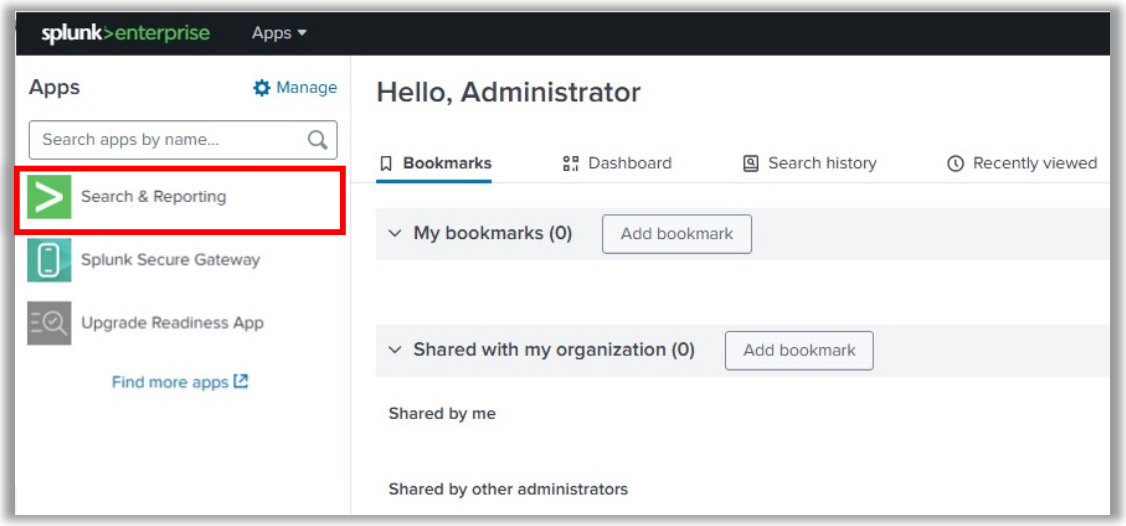


NOTE:

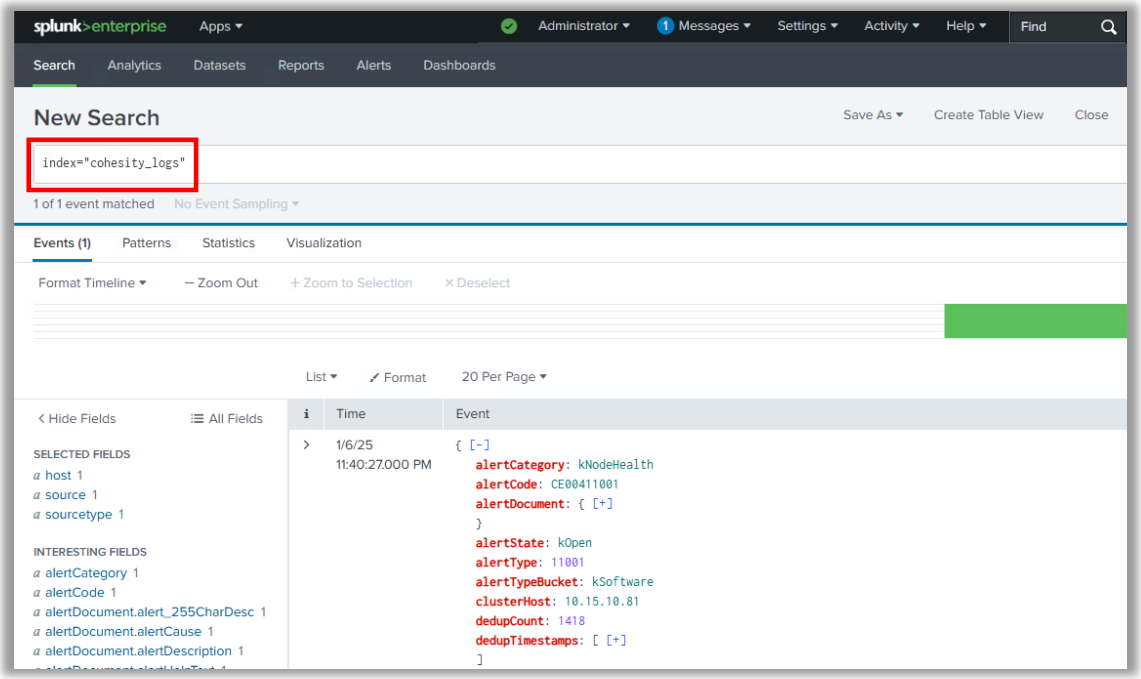
- Alerts and logs will be pushed from Cohesity to Splunk in real time. However, it is not immediate. Sometimes it takes more time for the data to be transmitted to Splunk. If you are not seeing the events after significant amount of time, then there could be an issue in HEC configuration. Edit your HEC to fix the issue.

9. Search, alert and visualize.

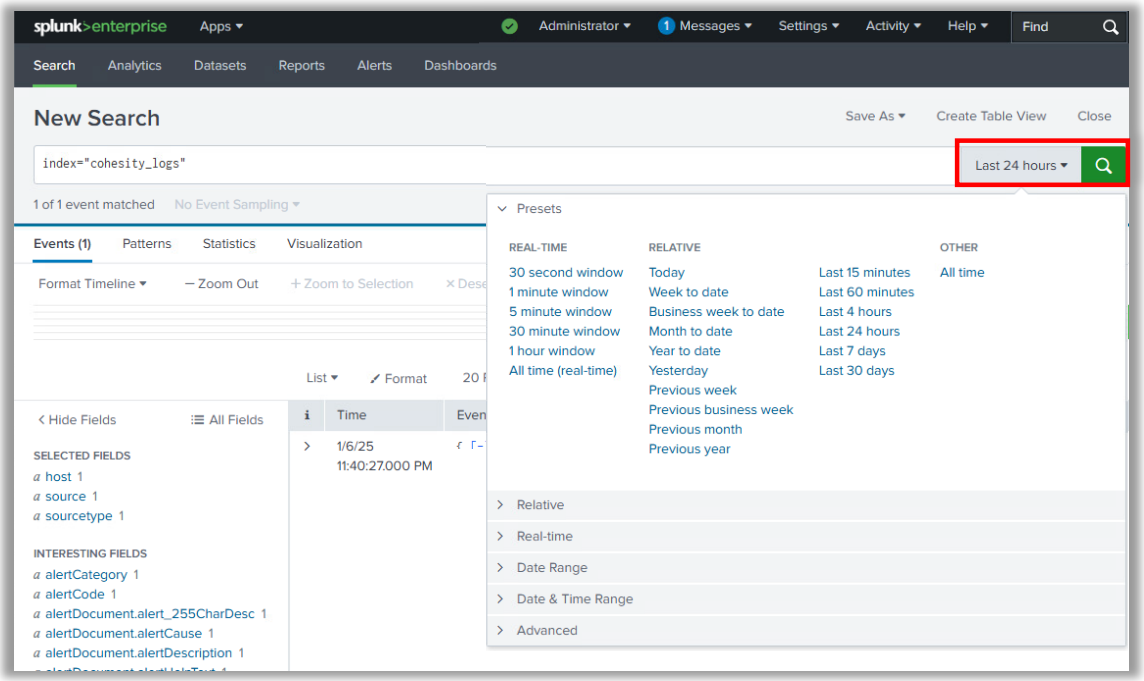
a. From Splunk Web Home, click Search & Reporting.



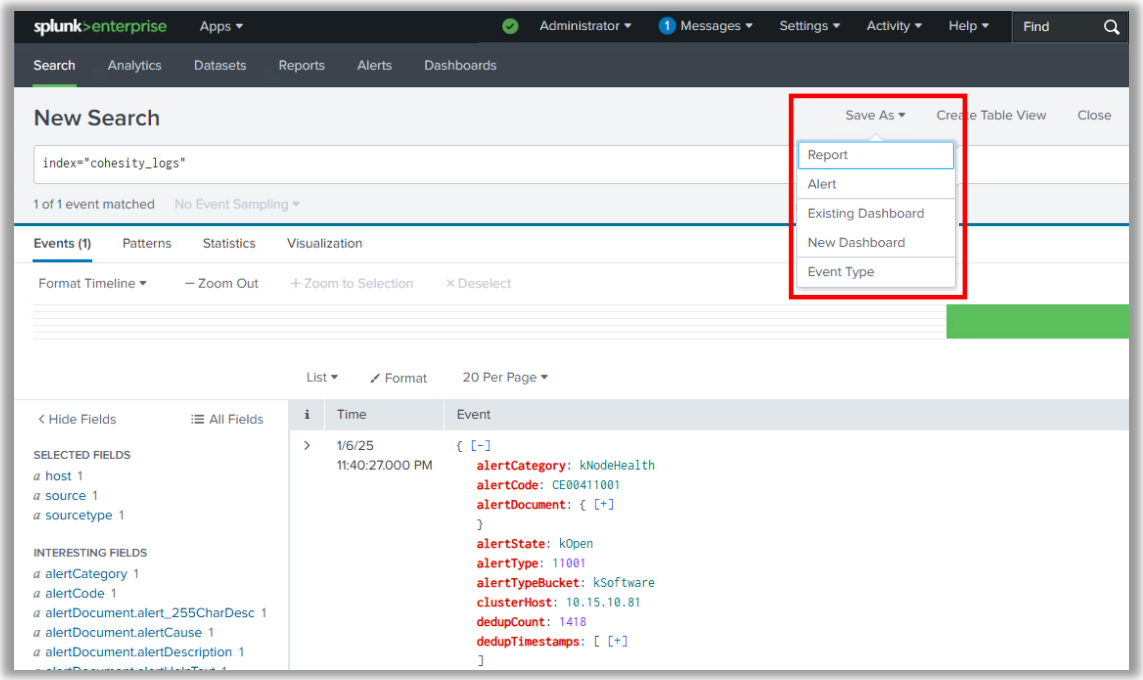
b. Run search query to filter logs.



c. Filter search results based on time.



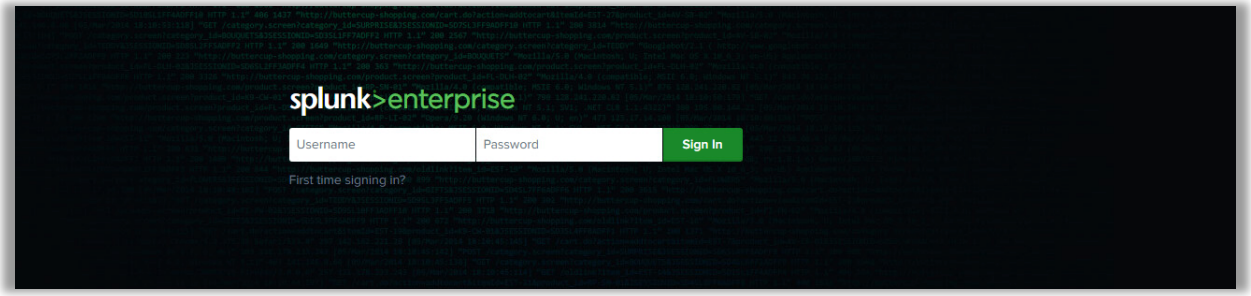
d. Alert and visualize.



NOTE: **For more details,** refer to the Search and Reporting section.

DataProtect as a Service [Cohesity SaaS Service]

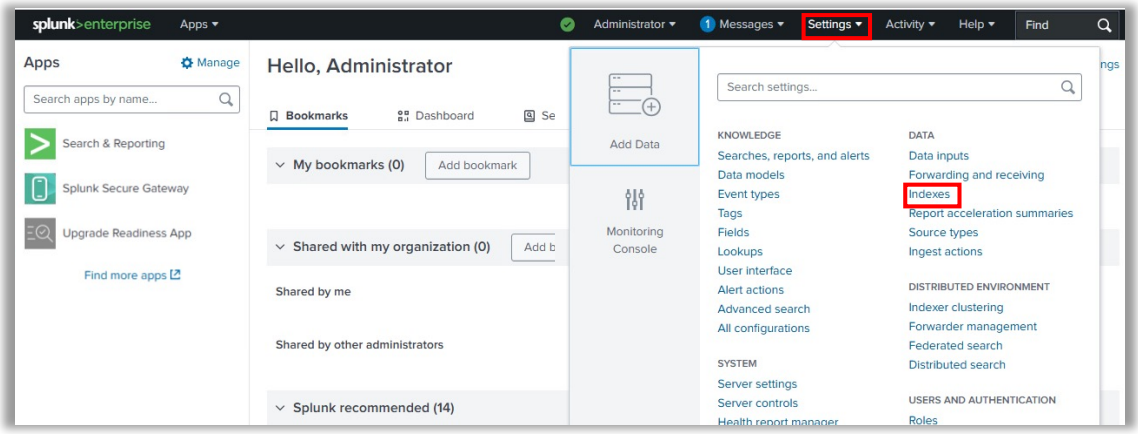
1. Login to your Splunk Enterprise Instance.



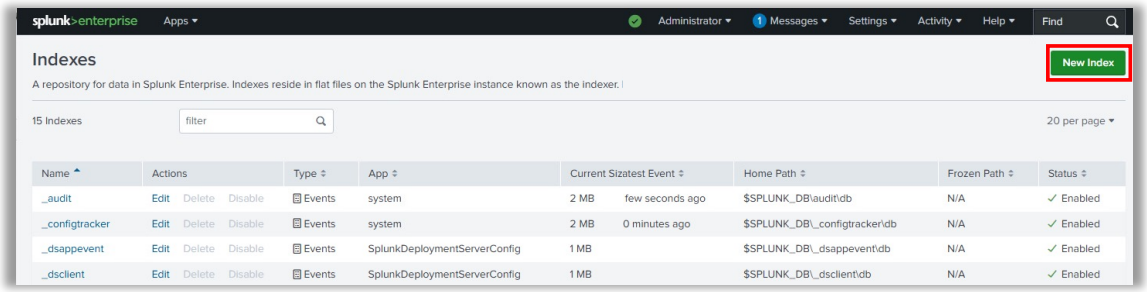
2. Create a new index to store Cohesity logs.

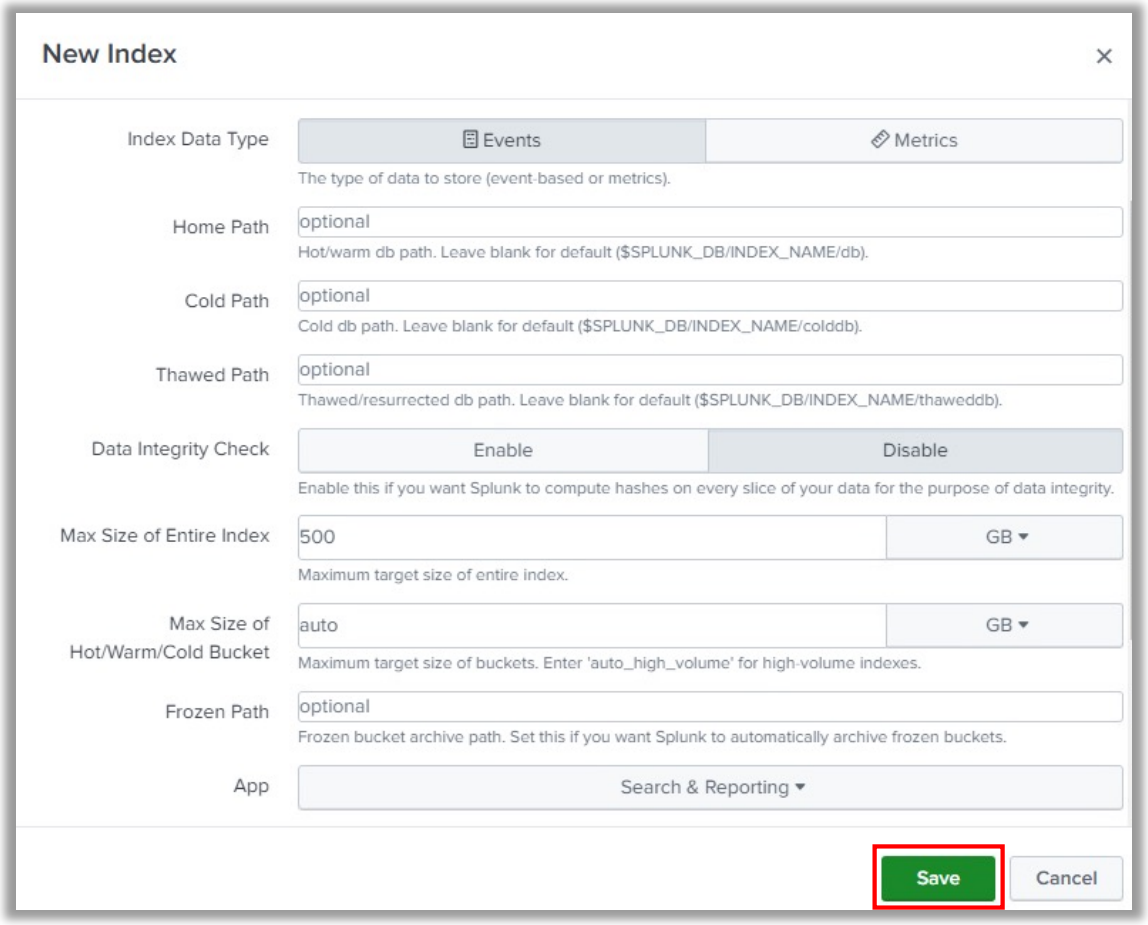
   This is an optional, however, recommended step. You can use an already existing index in your Splunk instance. But it is advised to create and use a new index specific to Cohesity logs and alerts

3. Click **Indexes** under **Data** in **Settings**.

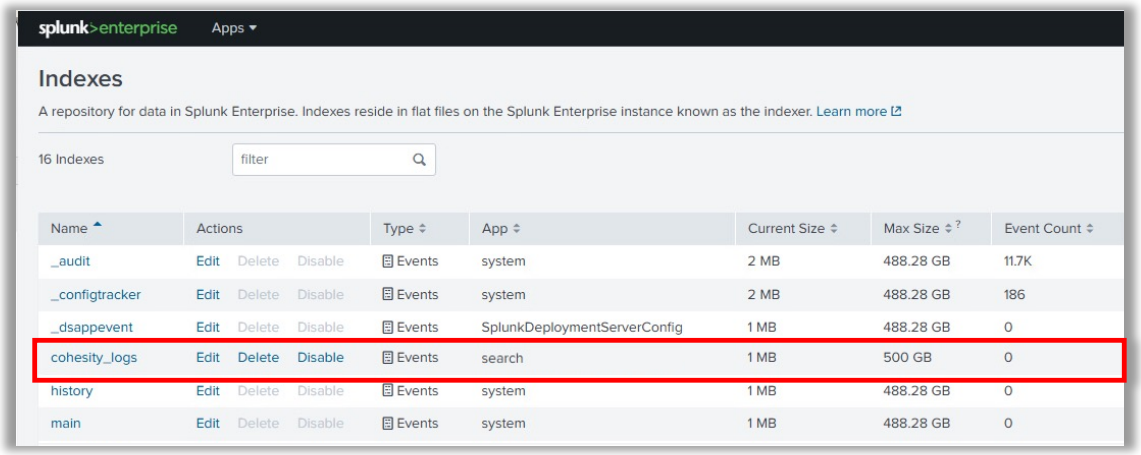


a. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save.**



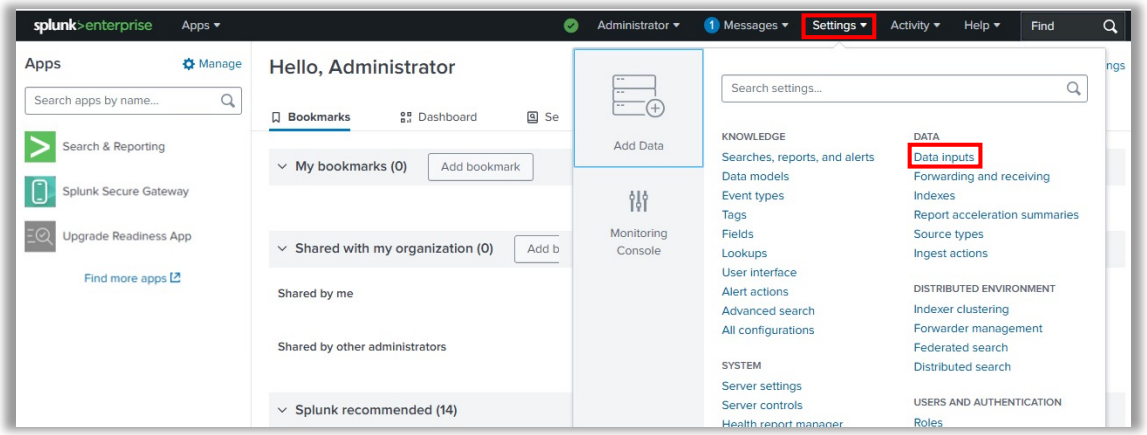


b. You can see the newly created index under Indexes

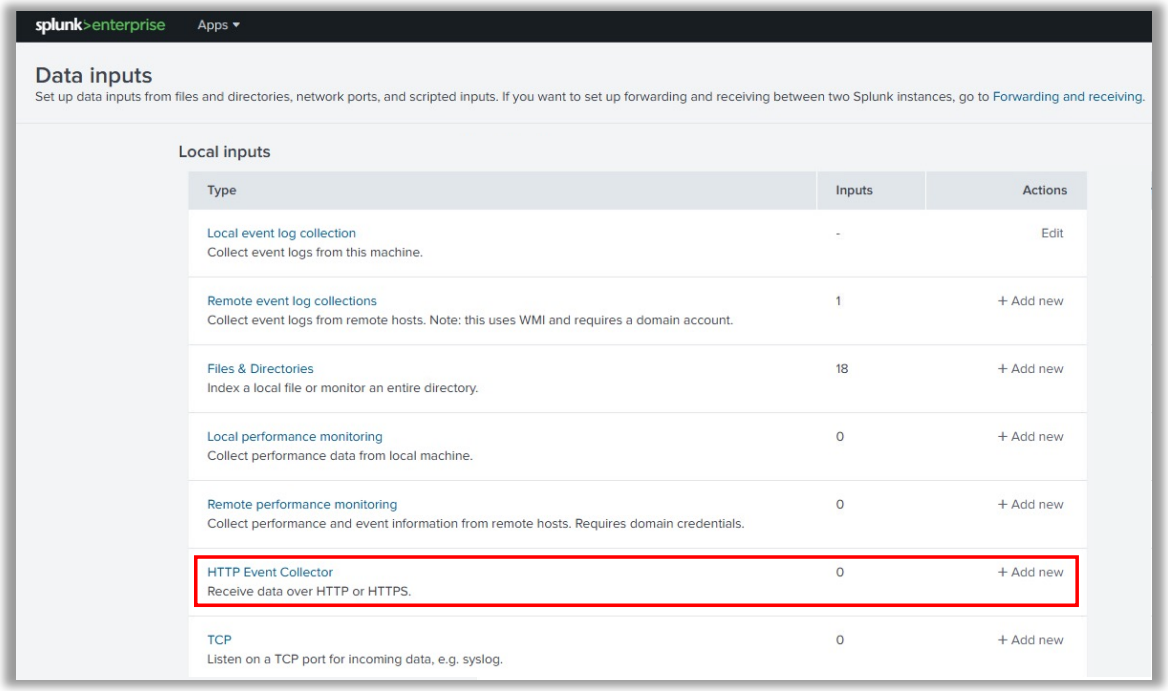


4. Configure HTTP Event Collector to receive data from Cohesity.

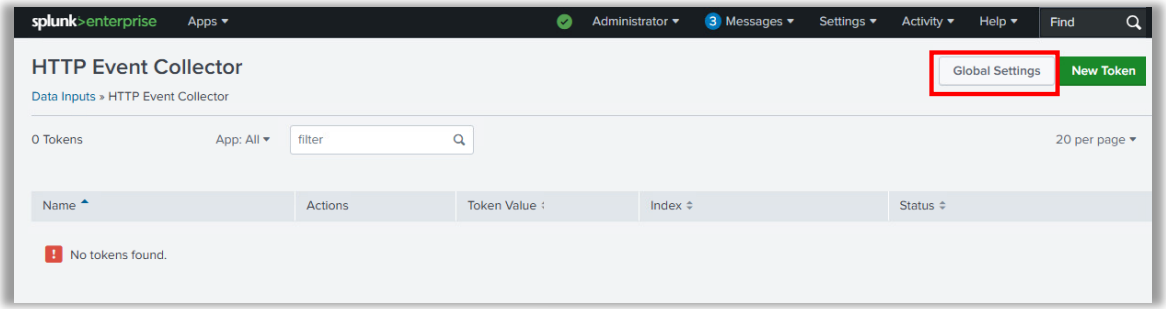
   a. Click **Data Inputs** under **Data** in **Settings**.

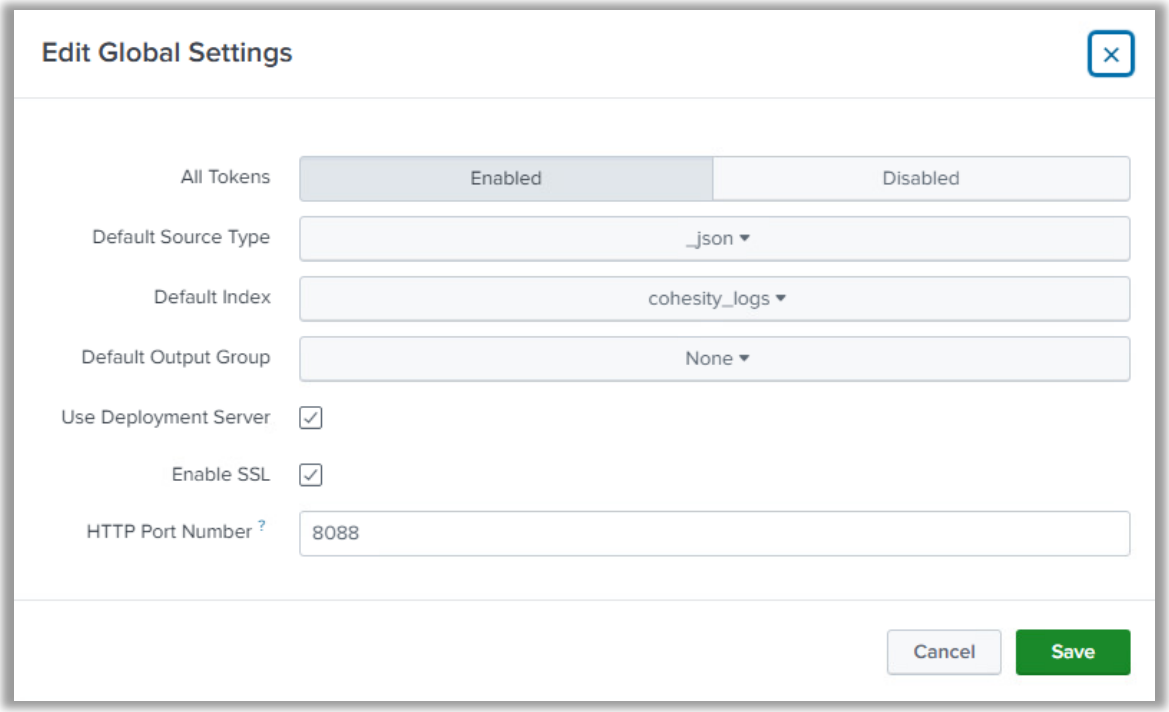


   b. Click **HTTP Event Collector**.



c. Click **Global Settings**.

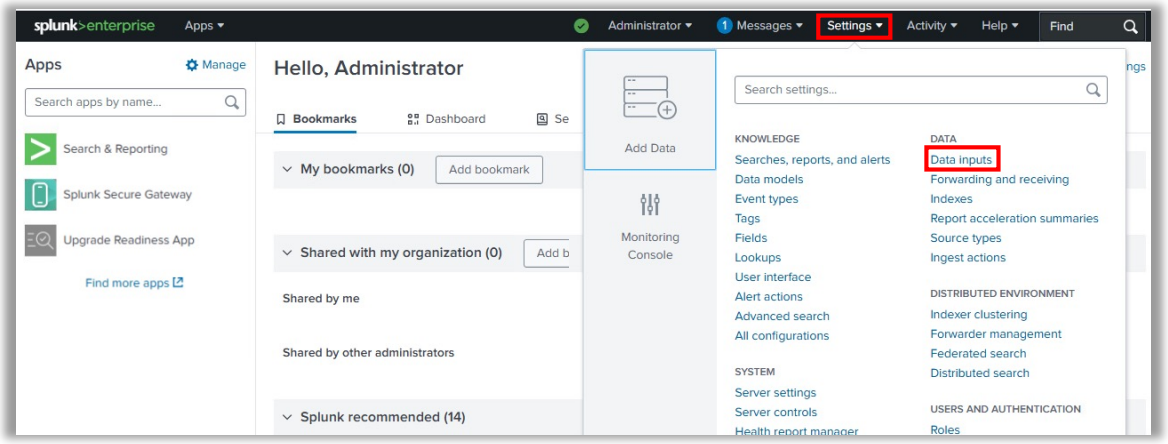




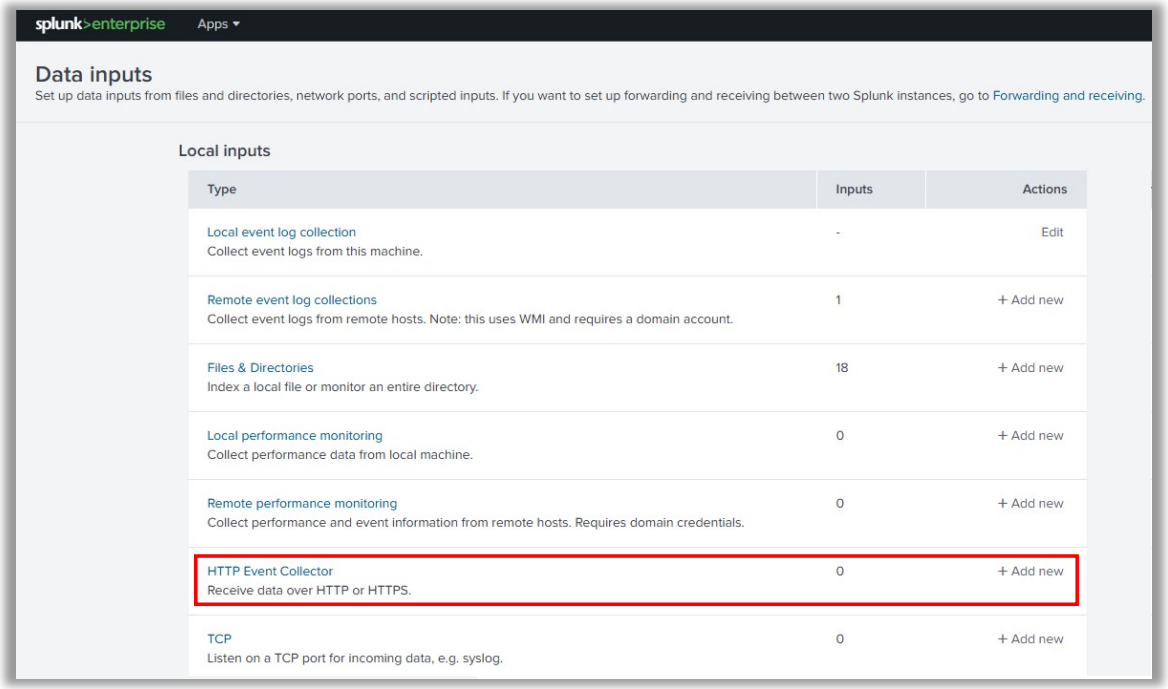
- Select **Enabled** for **All Tokens.**
- Select the **Default Source Type** as **_json** (If it is not shown under the dropdown, then type _json in search bar to bring it up).
- Select the **Default index** as the new index we created exclusively for Cohesity logs and alerts under step 1.
- By default, **SSL** is enabled with default **Port 8088**. You can disable SSL or modify the default port. The general recommendation is to enable SSL.

5. Create a new token to authenticate Cohesity.

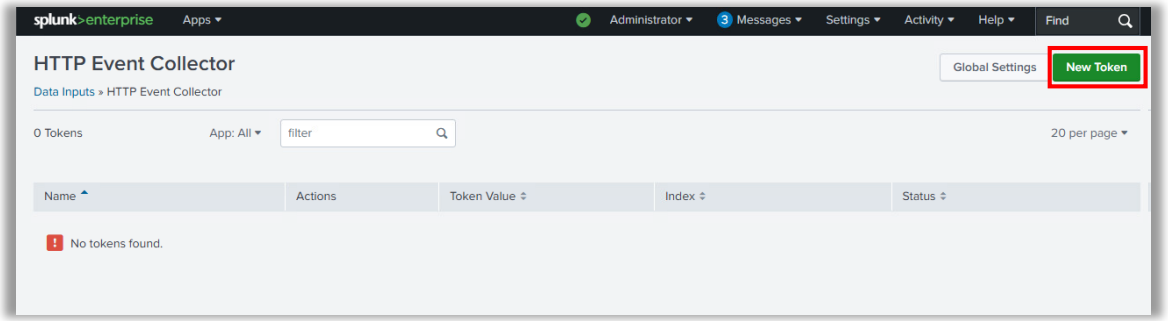
   a. Click **Data Inputs** under **Data** in **Settings**.



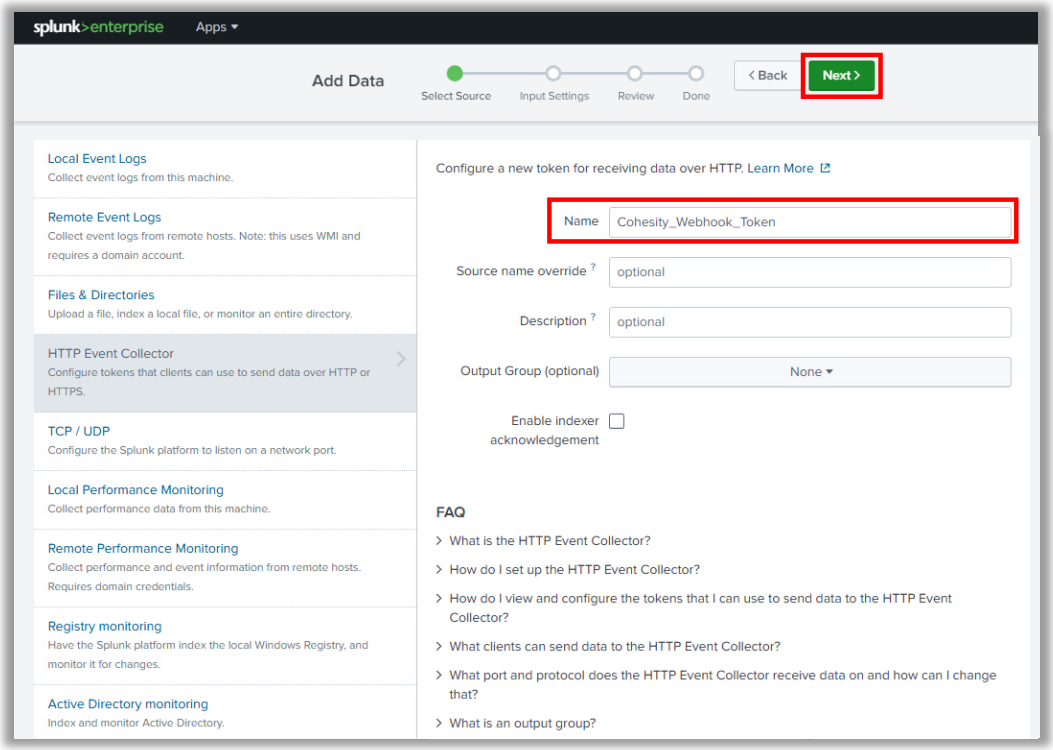
   b. Click **HTTP Event Collector**.



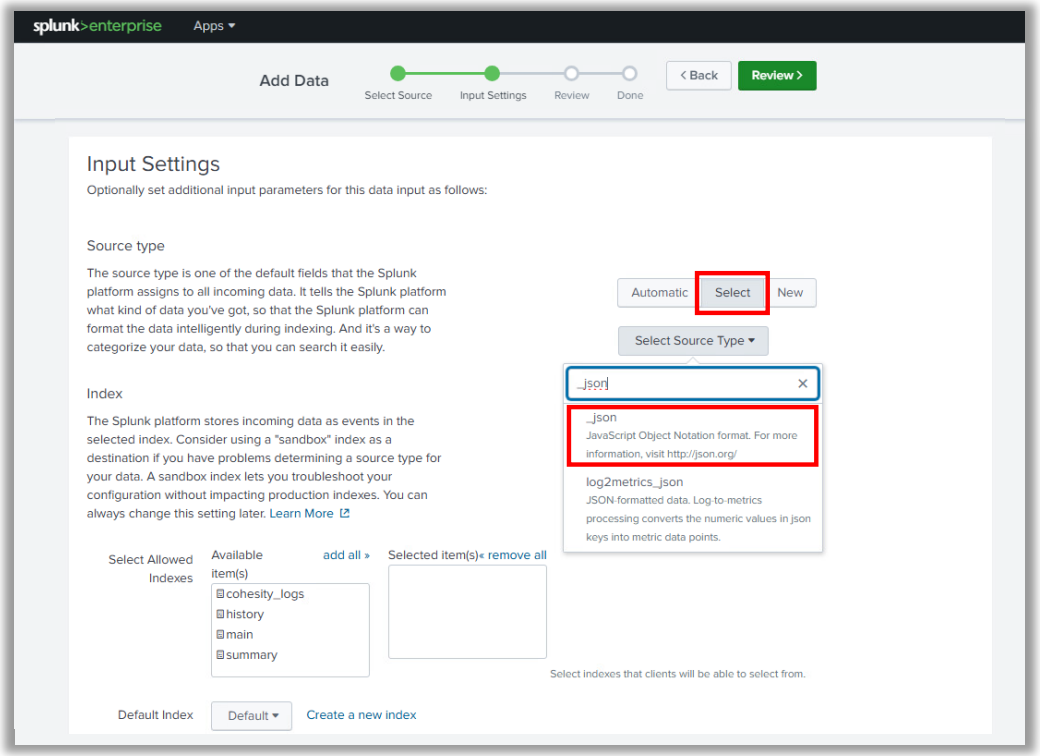
   c. Click **New Token.**



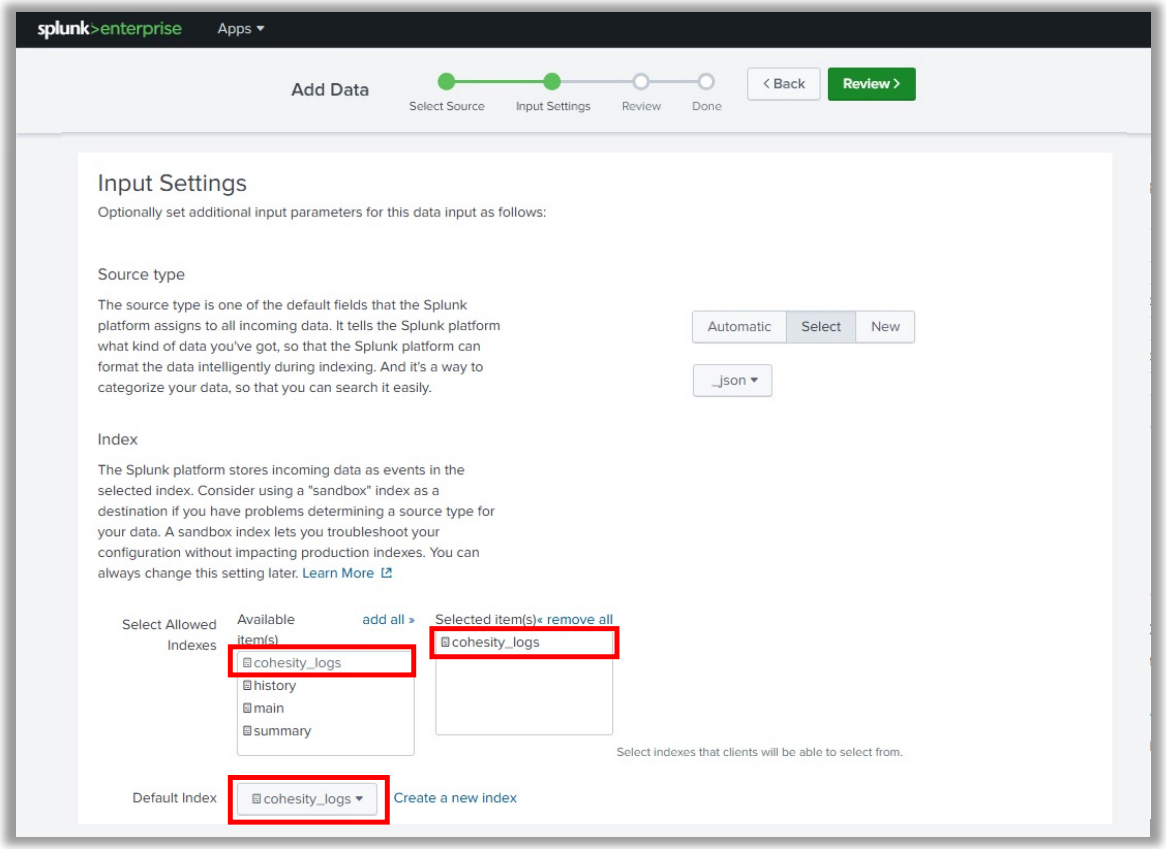
d. Provide a unique **Name** for your token and click **Next.**



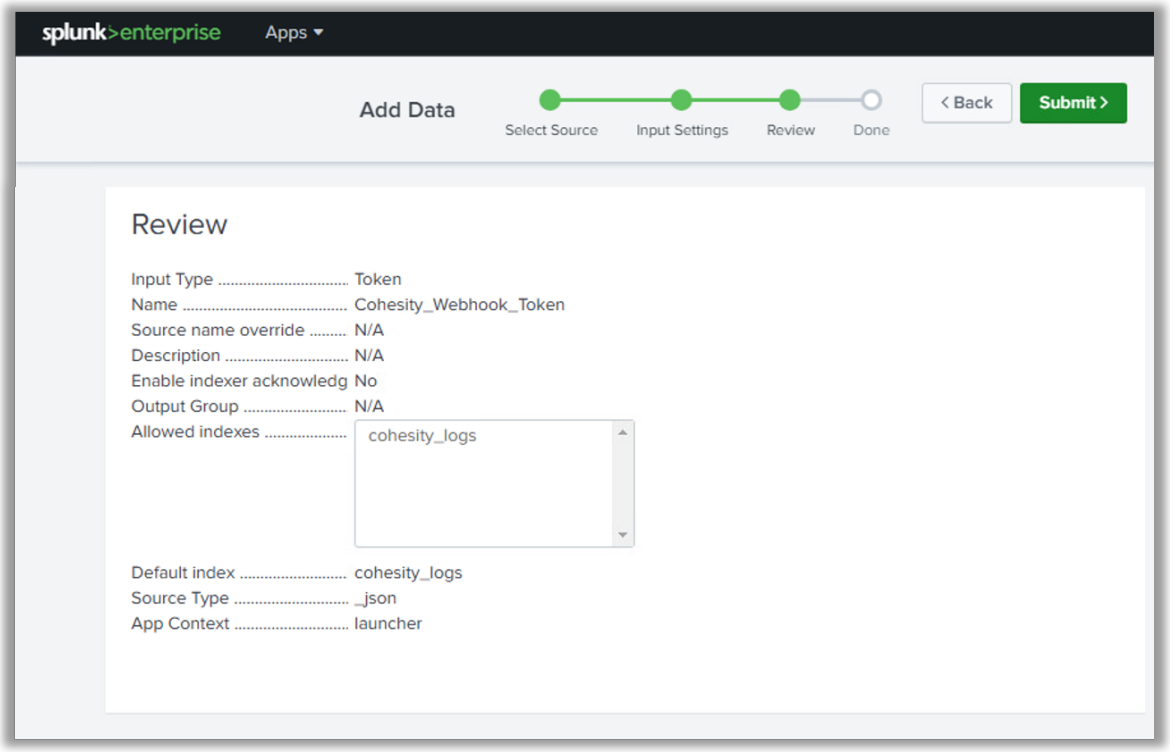
e. Under **Input Settings**, For **Source Type**, choose **Select** and then click **Select Source Type,** Select **_json** from the dropdown. If it is not shown under the dropdown, then type **_json** in search bar to bring it up.



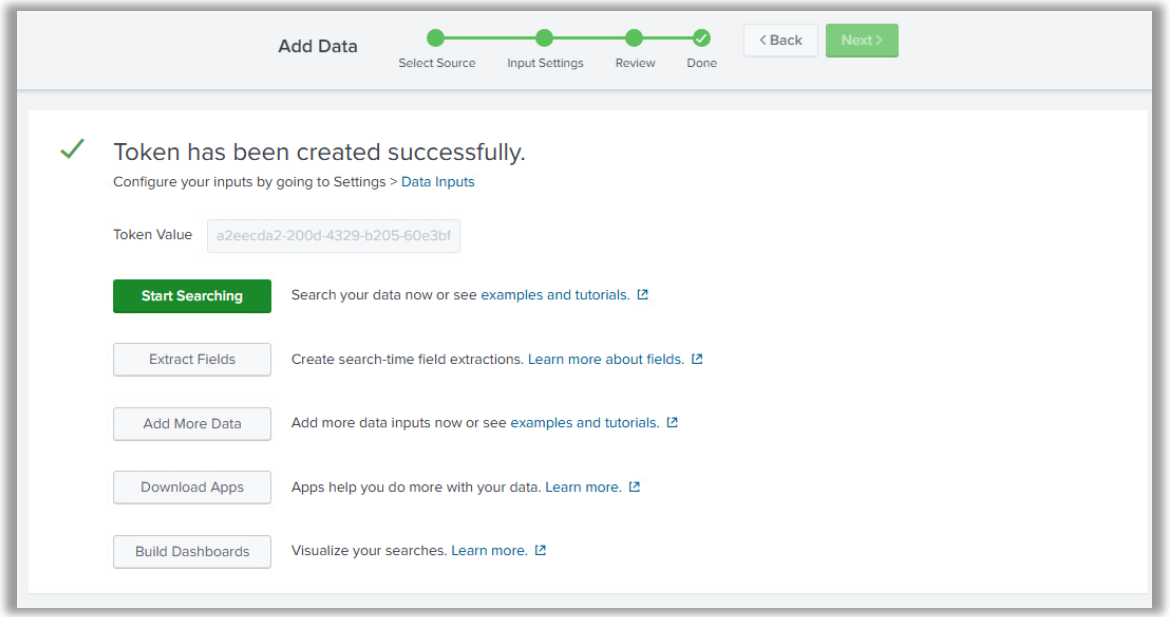
f. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.



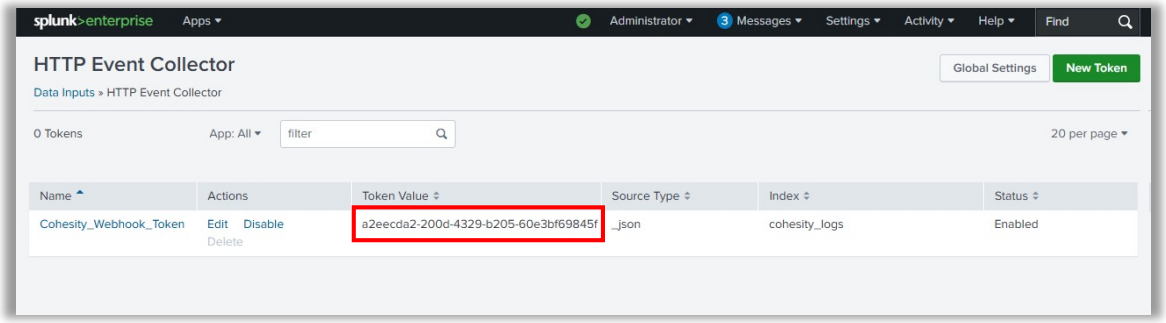
g. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.



h. Click **Submit** to successfully create the token.



i. Once the Token is created, go back to **HTTP Event Collector Page** and verify the Token created. Copy the **Token Value** (Which we will need while configuring the Webhook on Cohesity side).



6. Check HEC endpoint is accessible.

   a. Open the below URL in a browser.

   ```
   https://<your_splunk_ip>:8088/services/collector/health
   ```

   b. If you get the below json response, then your HEC endpoint is accessible and properly configured.

   ```
   {"text":"HEC is healthy","code":17}
   ```

   c. If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Revisit previous steps to configure the HEC properly.

7. Test HTTP Event Collector on any system

   a. Test the HTTP Event Collector using a curl request from cmd prompt / terminal on any system as shown below:

   ```
   curl -k "https://<your Splunk IP>:8088/services/collector/raw" \
        -H "Authorization: Splunk <HEC Token>" \
        -H "Content-Type: application/json" \
        -d '{"alert": "Test Alert", "alertId": "0000"}'
   ```

   - Your Splunk IP – is the IP address of the system where your Splunk Enterprise is running.
   - HEC Token – is the Token Value of the HTTP Event Collector Token you created in previous step.

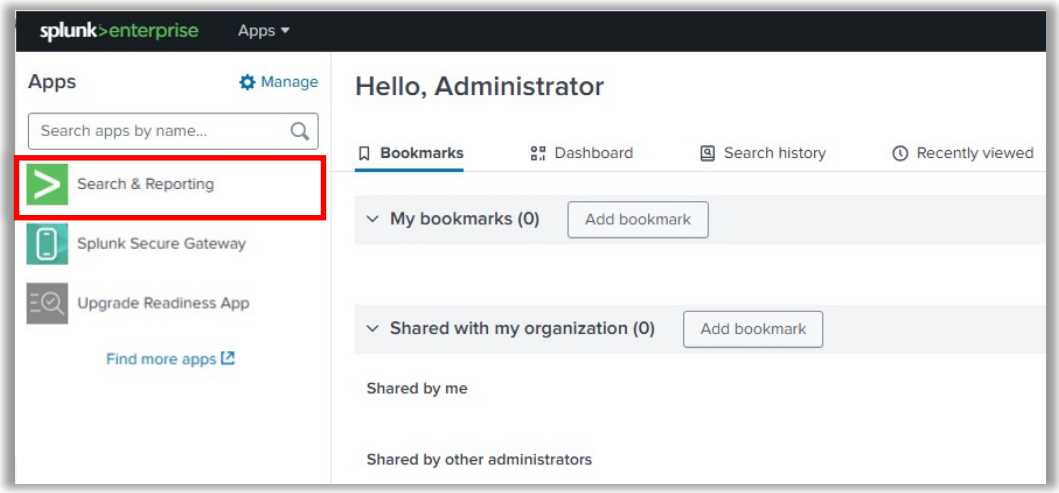
     Once the curl command executes successfully, it must return the message *{"text": "Success", "code": "0"}* as shown below.

NOTE:

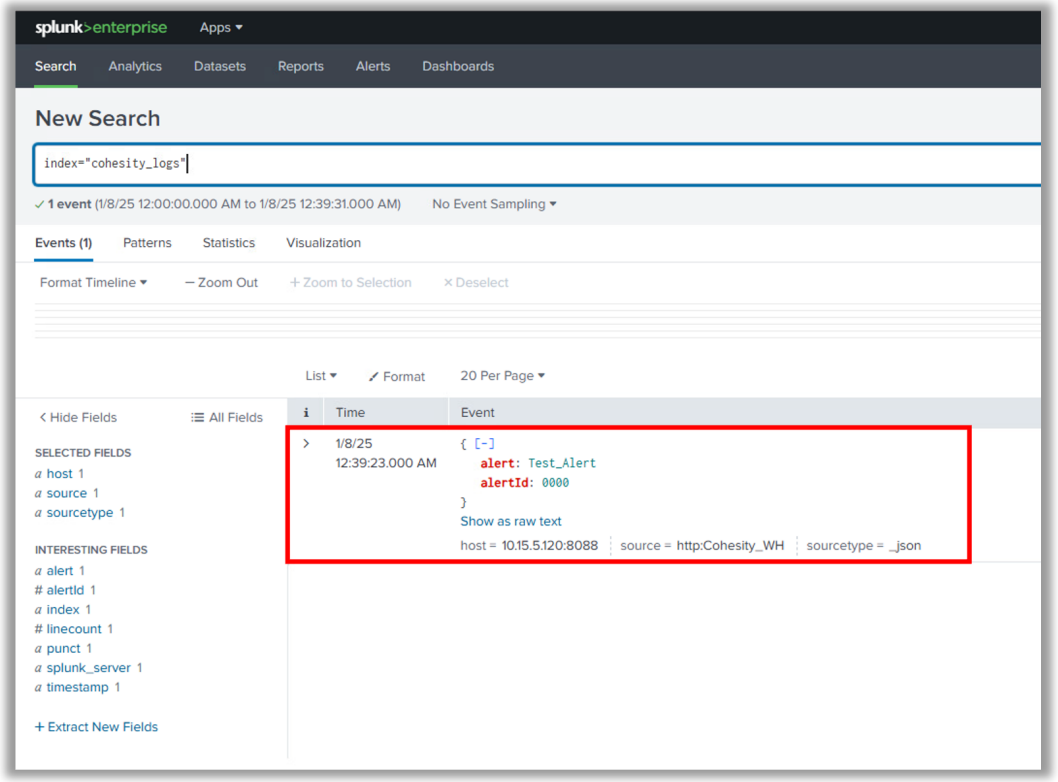
- If you are not receiving the message *{"text": "Success", "code": "0"}* or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

b. Verify the data is successfully received on Splunk.

i. From Splunk Web Home console, click Search & Reporting.



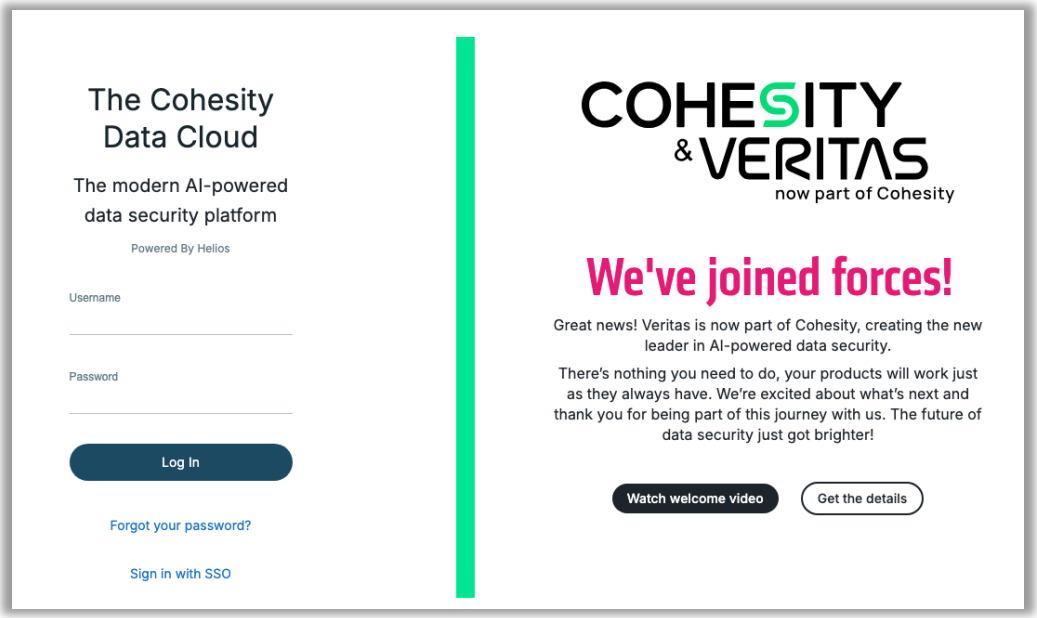
ii. Run search query to filter logs. You must see the event sent by curl command in Splunk



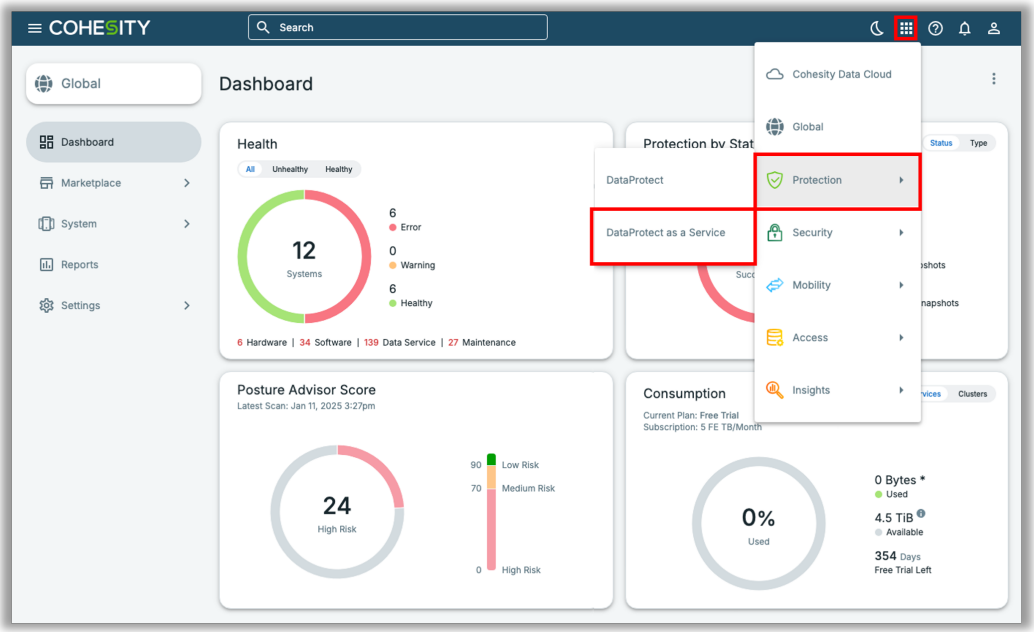
NOTE:

- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

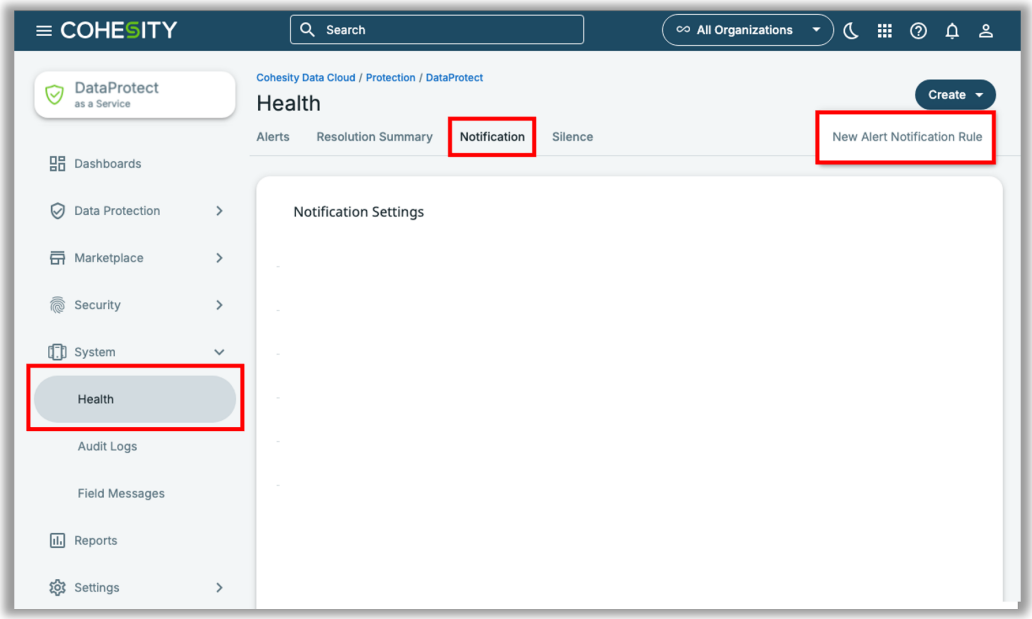
8. Configure alert notification with webhook on Cohesity Data Cloud
   a. Login to Cohesity Data Cloud.



   b. Go to **Protection > DataProtect as a Service**.



c. Click **Health** > **Notification** and then **Create** > **New Alert Notification Rule**.



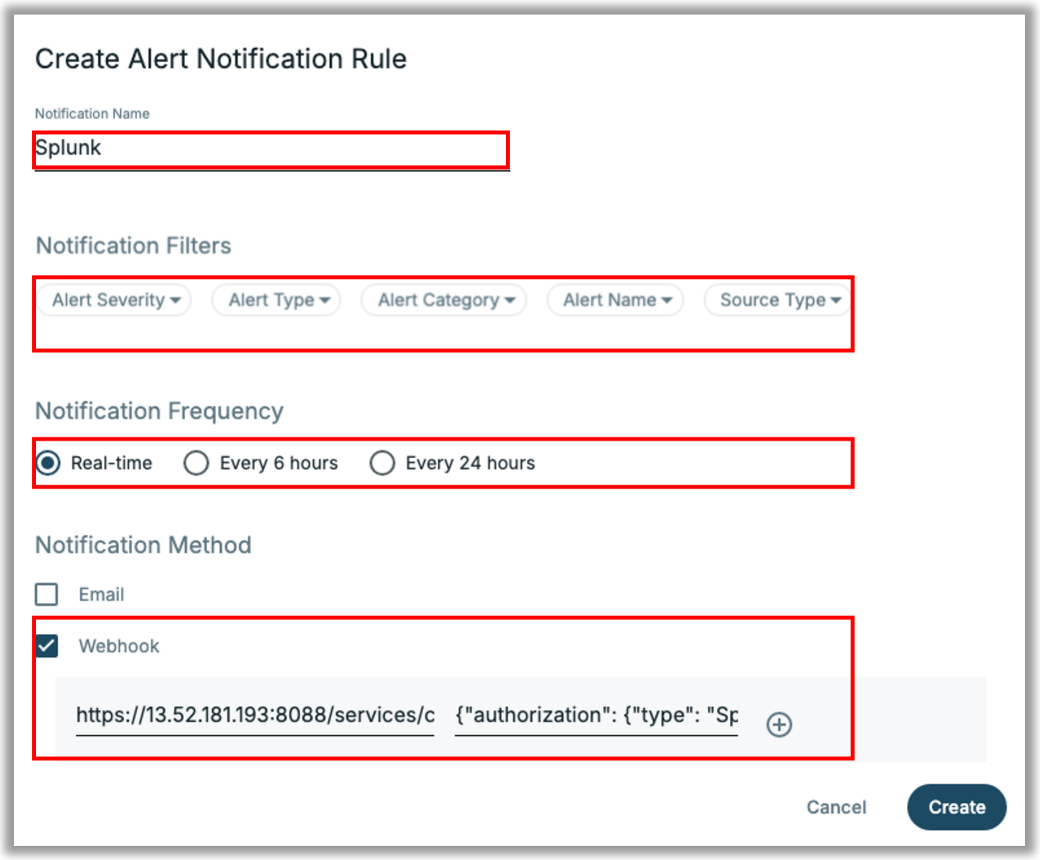
d. Provide the **Notification Name**, Select the **Notification Filters** and **Notification Frequency**, choose **Webhook** as the **Notification Method** and provide the Webhook **URL** and **Options** as below:

URL:
https://<Your Splunk IP>:8088/services/collector/raw

Options:
{"authorization": {"type": "Splunk","credentials": "*<HEC Token>*"}}

NOTE For Splunk Trials:

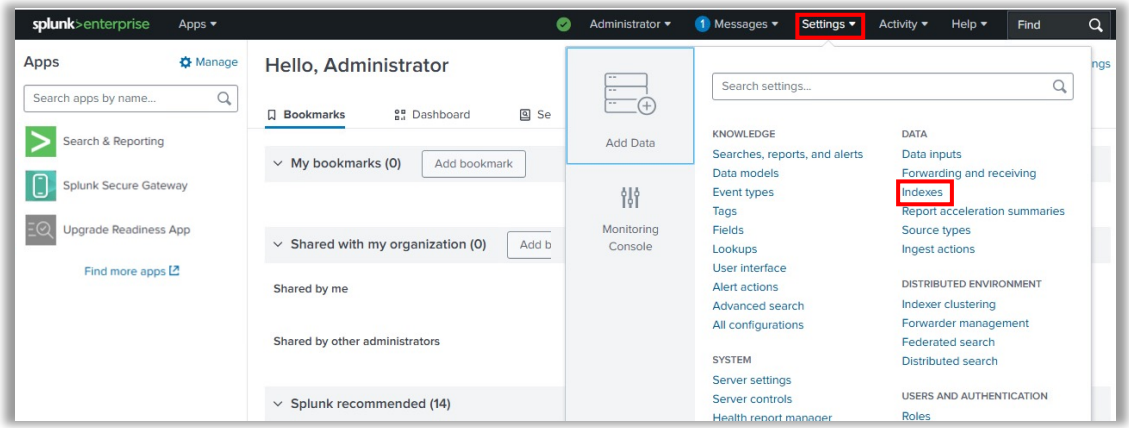
- Alert notifications from Cohesity to Splunk via Webhook requires a valid certificate at the Splunk side.
- Splunk trials might use expired/invalid certificates, which may lead to TLS certificate verification failure, in which case the alert notifications will not be sent from Cohesity to Splunk.
- Ensure you have a valid certificate installed or available at your Splunk Enterprise.



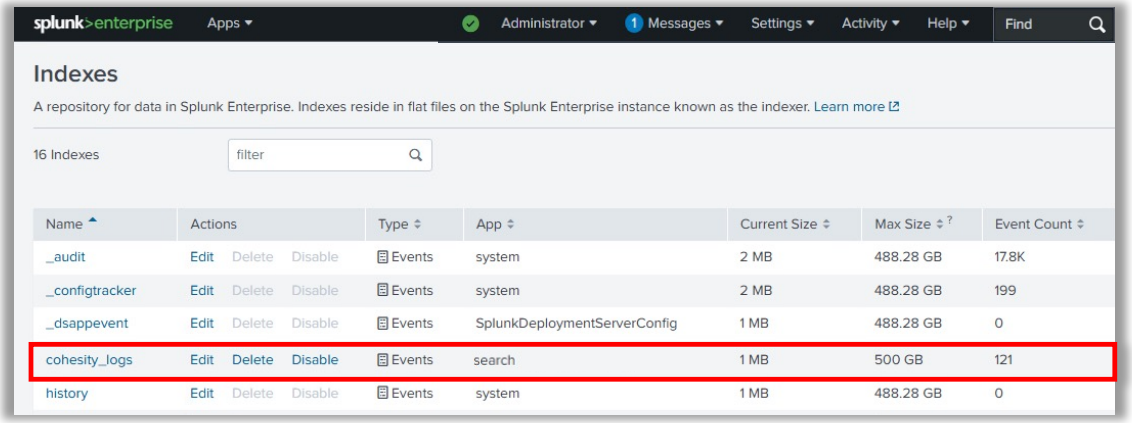
NOTE:

- Use Alert Severity, Alert Type, Alert Category, Alert Name or Source Type to filter out the selective alerts you want to send to Splunk
- If you do not select any value for Alert Severity, Alert Type, Alert Category, Alert Name or Source Type, then all the alerts generated by Cohesity will be sent to Splunk

9. Validate data received from Cohesity on Splunk Enterprise.
   a. Click **Indexes** under **Data** in **Settings.**

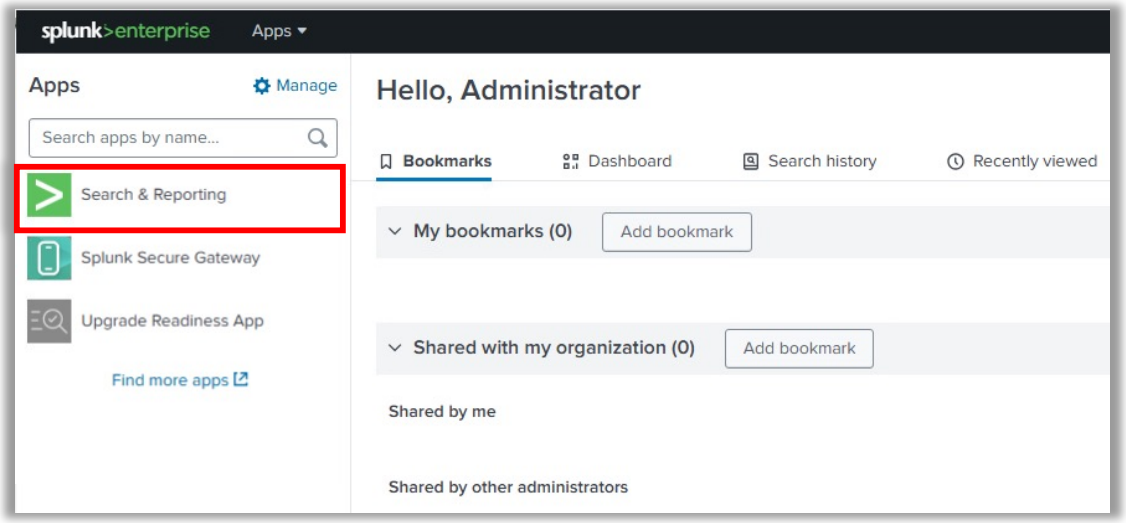


b. Verify logs are being pushed to your index by checking the Event Count.

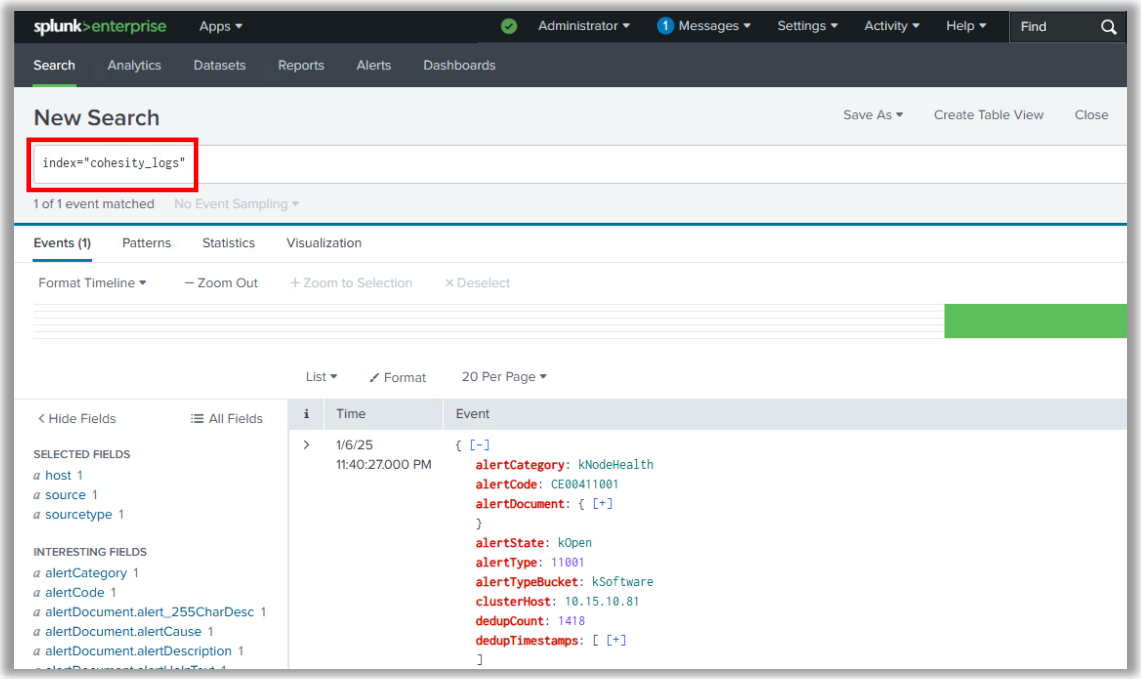


10. Search, alert and visualize.

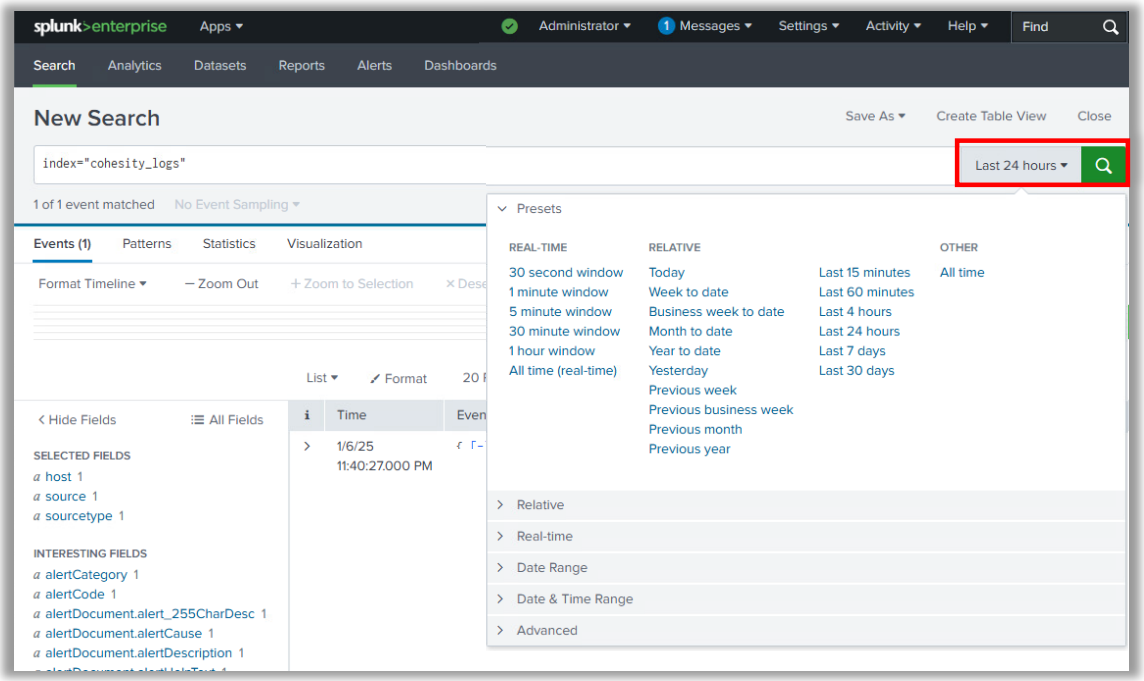
a. From Splunk Web Home, click Search & Reporting.



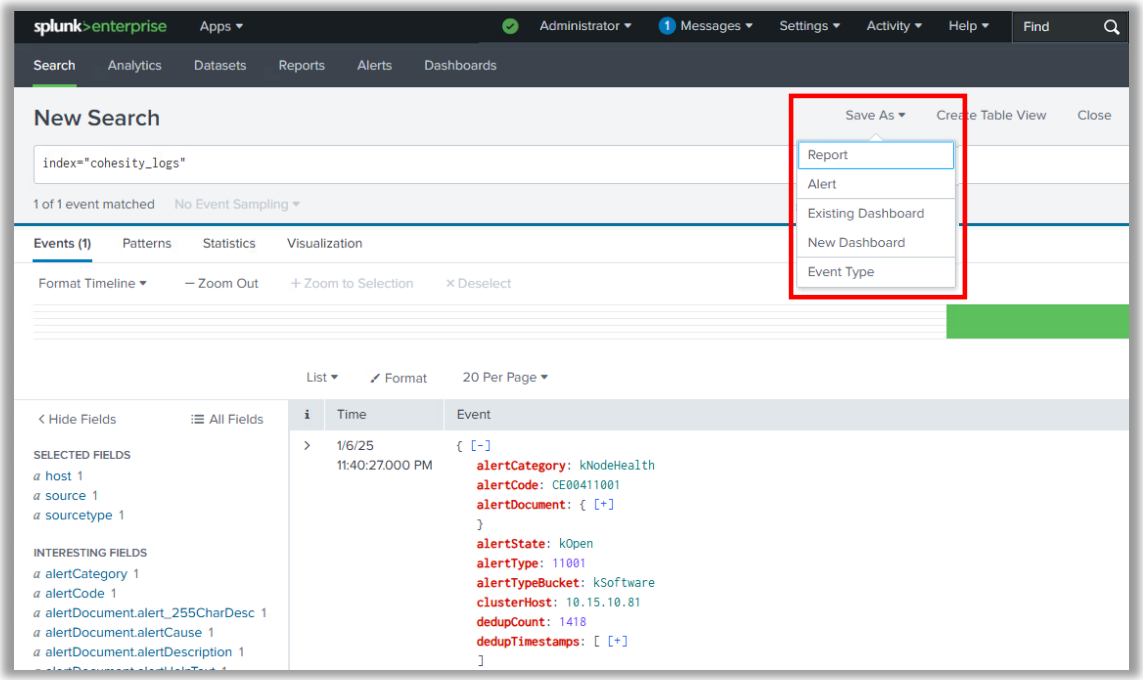
b. Run search query to filter logs.



c. Filter search results based on time.



d. Alert and visualize.

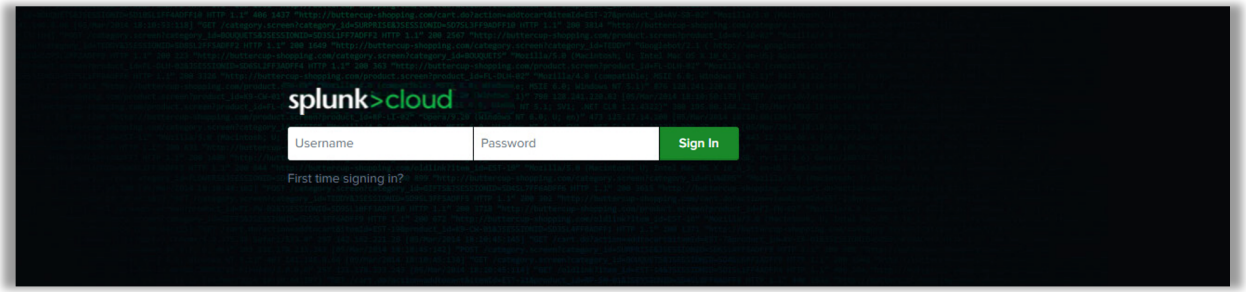


NOTE: **For more details,** refer to the Search and Reporting section.

Integrate Cohesity with Splunk Cloud

Self-managed Cohesity Clusters

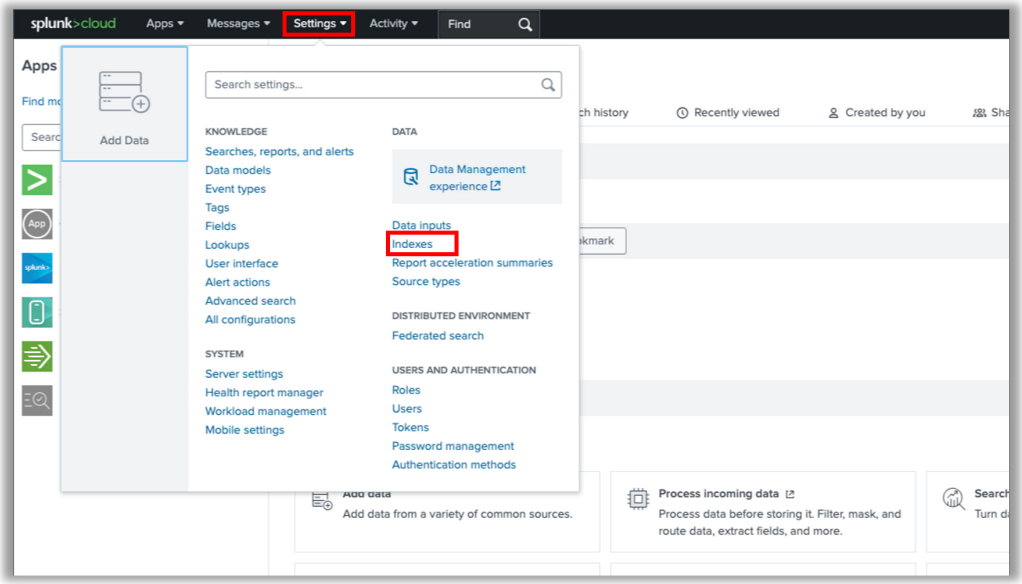
1. Login to your Splunk Cloud Instance.



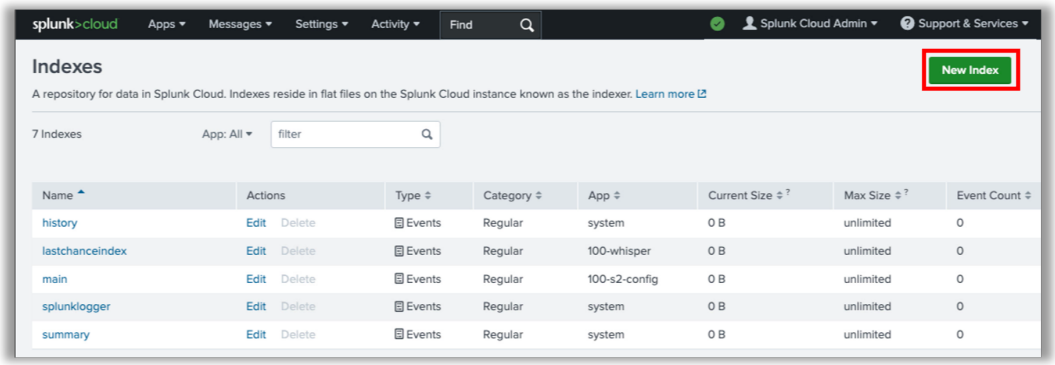
2. Create a new index to store Cohesity logs.

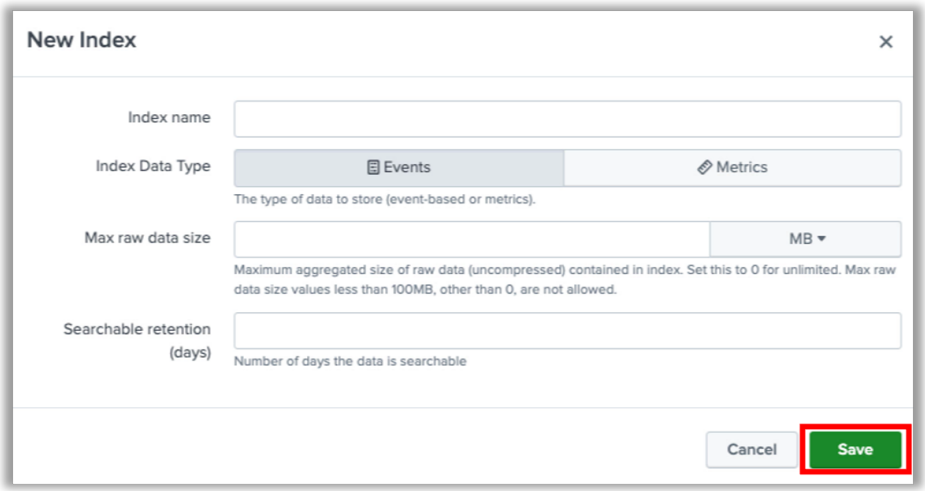
   This is an optional, however, recommended step. You can use already existing index in your Splunk instance. But it is advised to create and use a new index specific to Cohesity logs and alerts

   a. Click **Indexes** under **Data** in **Settings.**

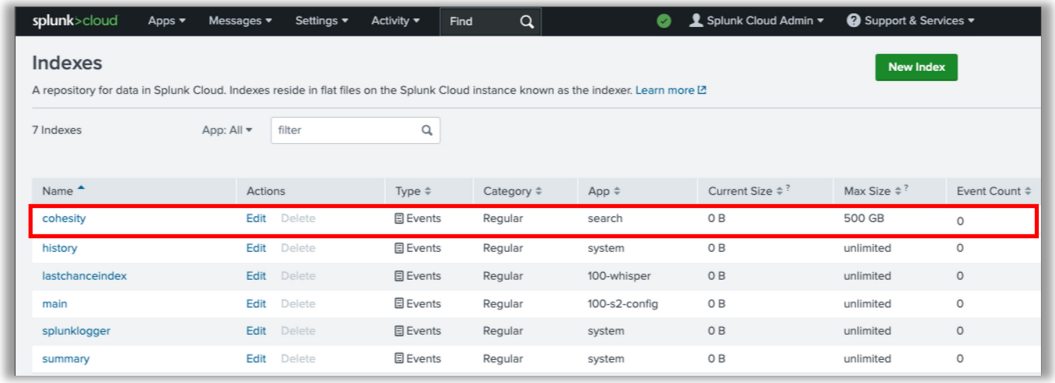


b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type**. Define the maximum size and retention for data and click **Save.**

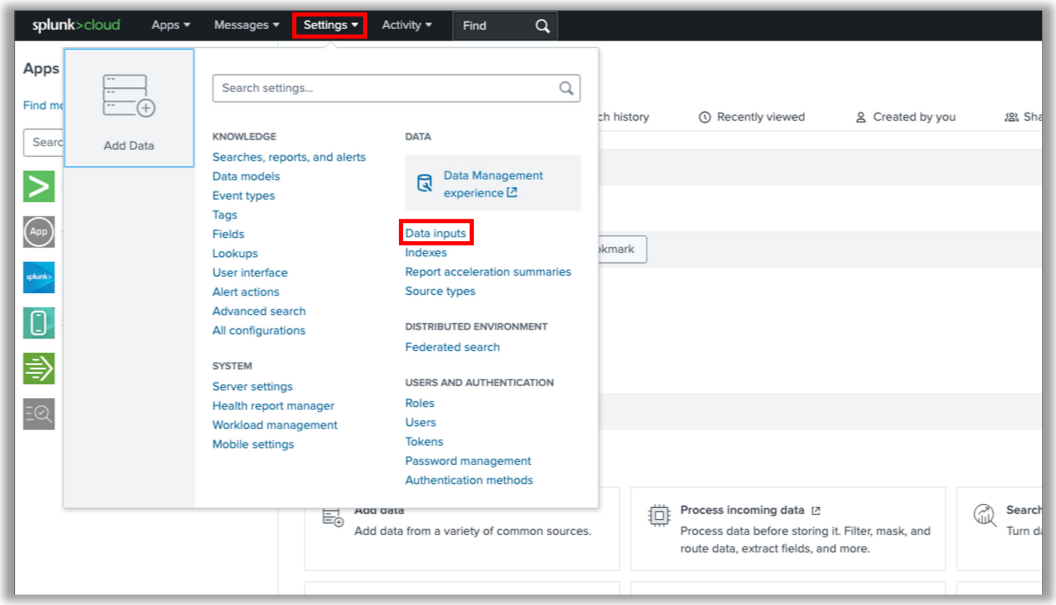




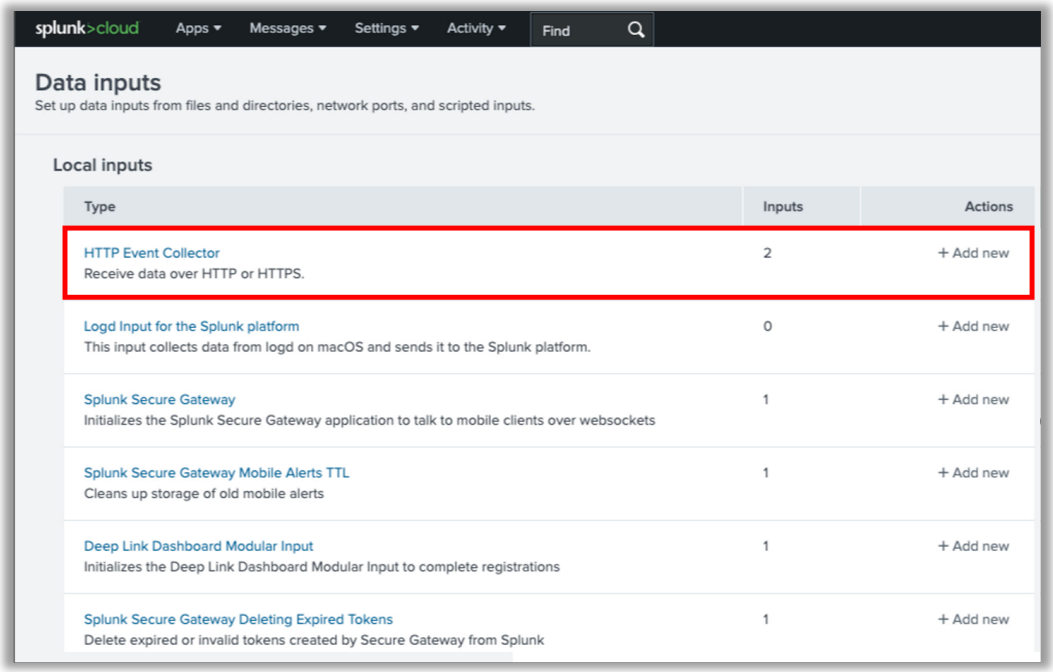
c. You can see the newly created index under Indexes.



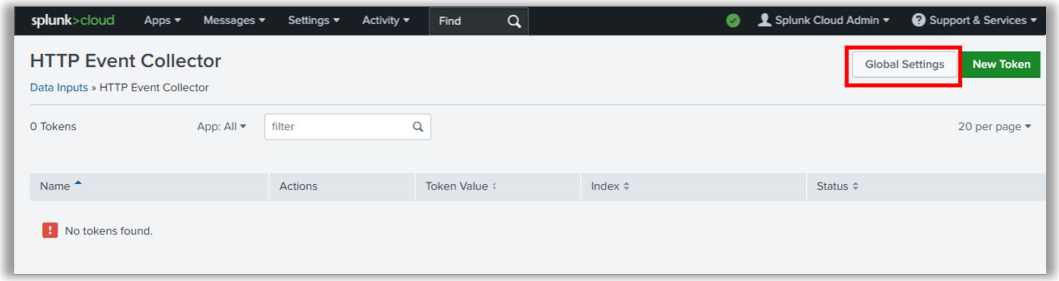
3. Configure HTTP Event Collector to receive data from Cohesity.
   a. Click **Data Inputs** under **Data** in **Settings**.

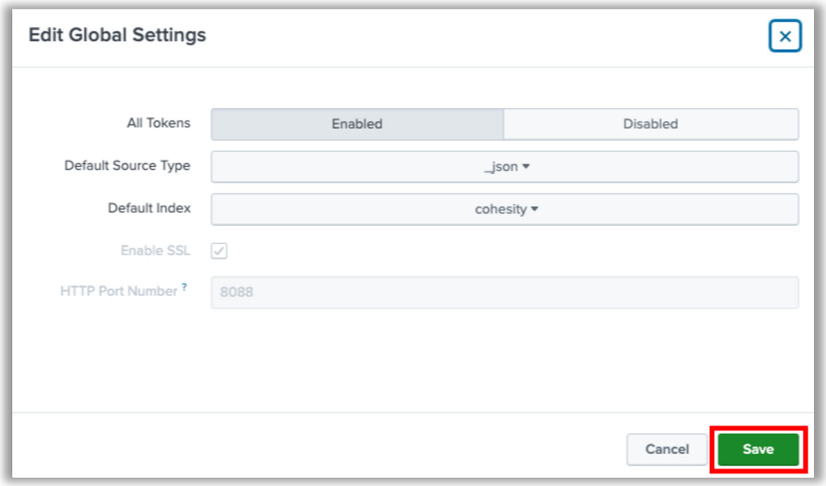


   b. Click **HTTP Event Collector**.



c. Click **Global Settings** and fill in all requested details and click **Save.**

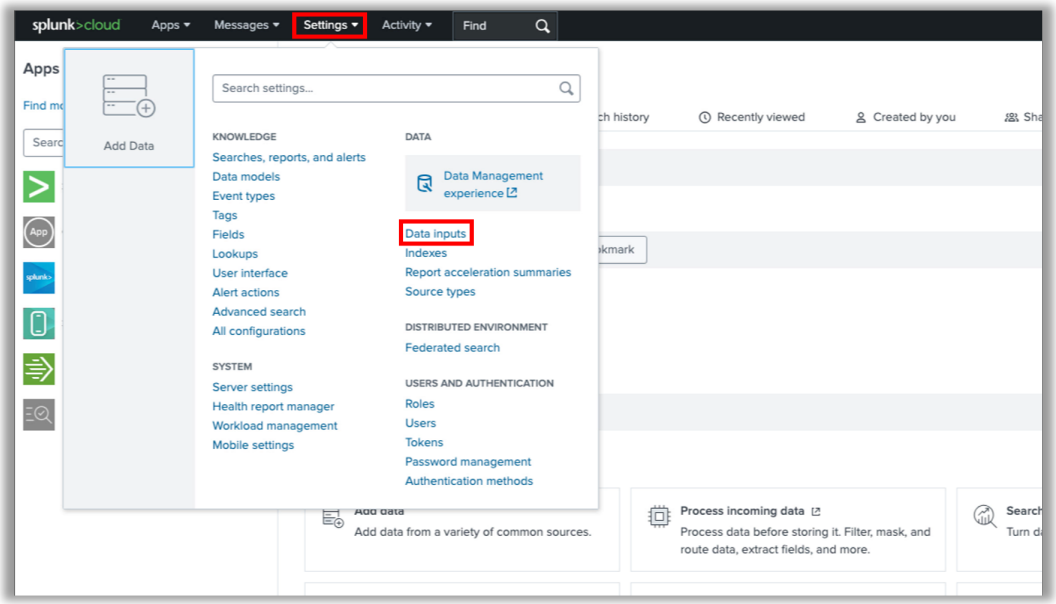




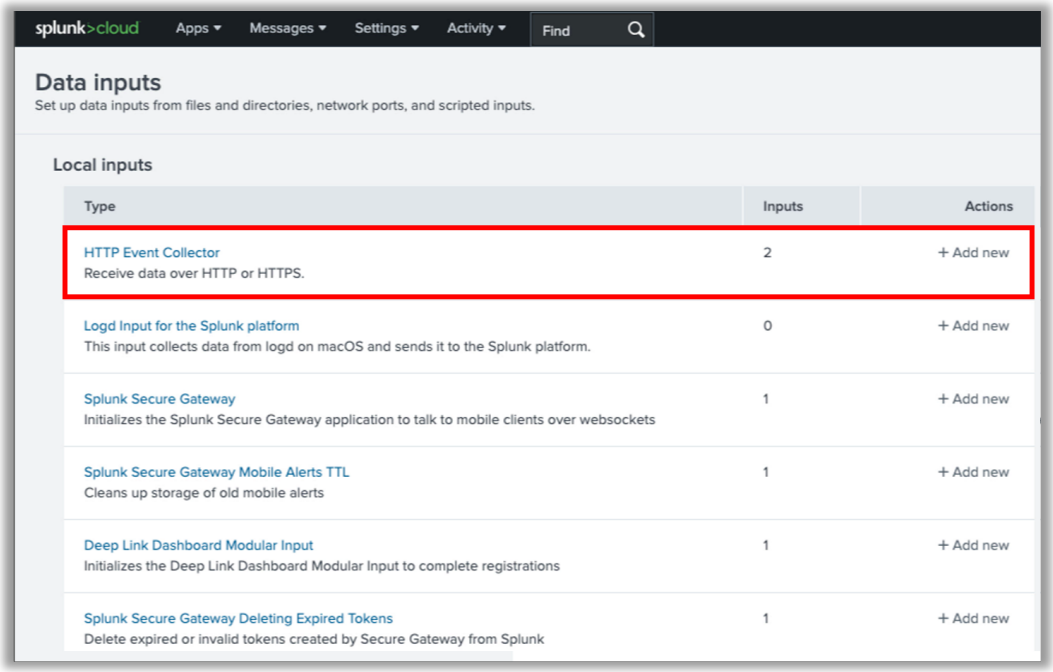
- Select Enabled for All Tokens.
- Select the Default Source Type as _json (If it is not shown under the dropdown, then type _json in search bar to bring it up).
- Select the Default index as the new index we created exclusively for Cohesity logs and alerts under step 1.
- By default, SSL is enabled with default Port 8088. You can disable SSL or modify the default port. The general recommendation is to enable SSL.

4. Create a new token to authenticate Cohesity.

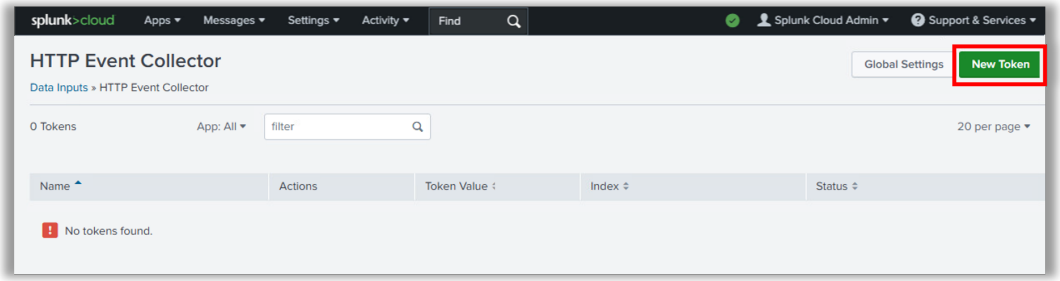
a. Click **Data Inputs** under **Data** in **Settings**.



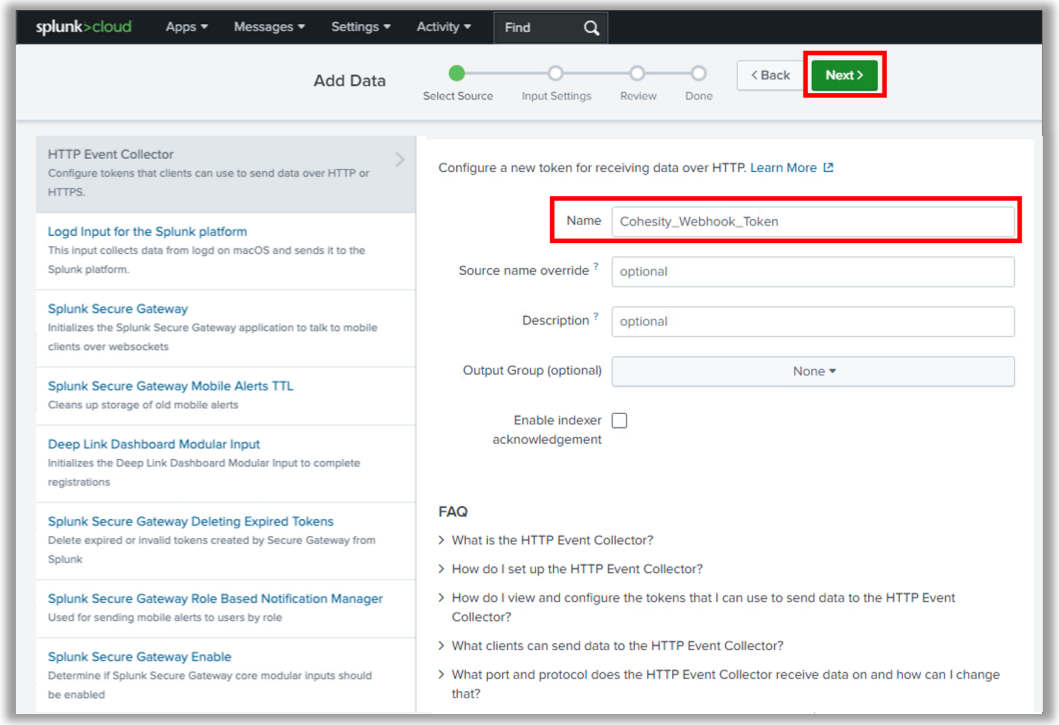
b. Click **HTTP Event Collector**.



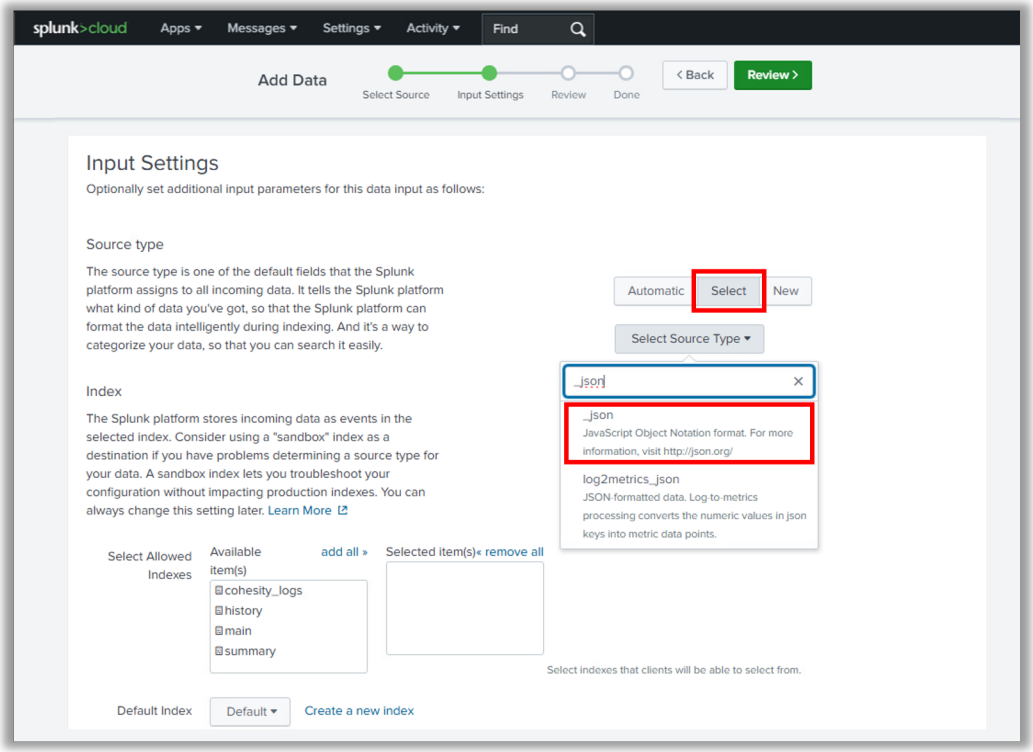
c. Click **New Token**.



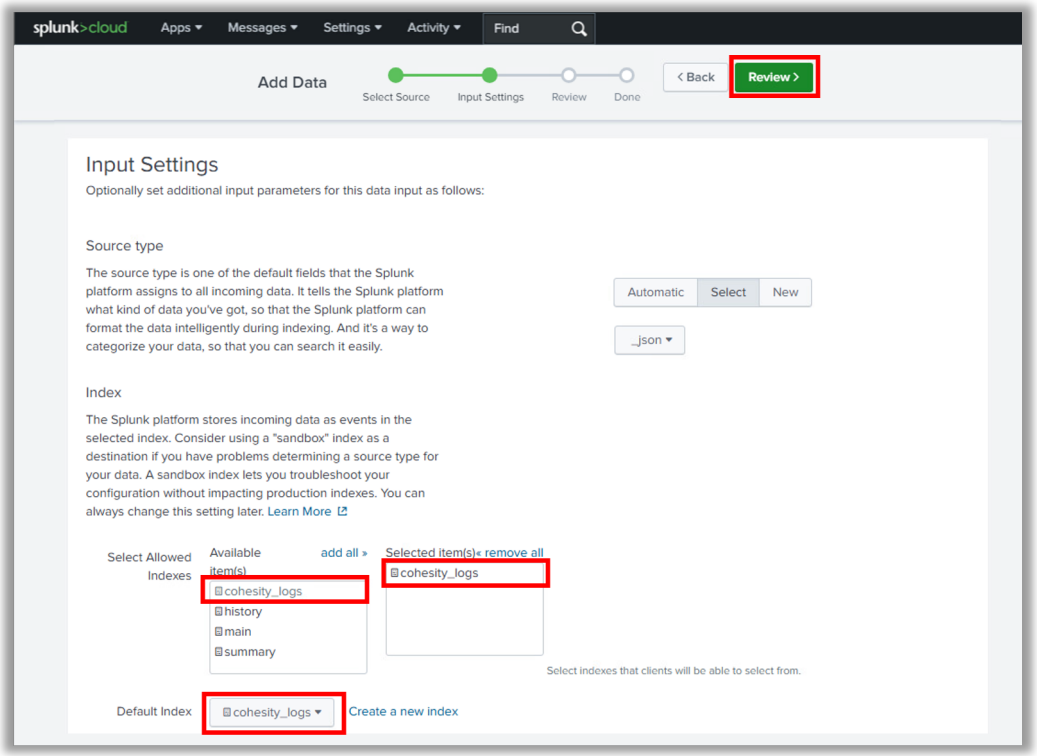
d. Provide a unique **Name** for your token and click **Next.**



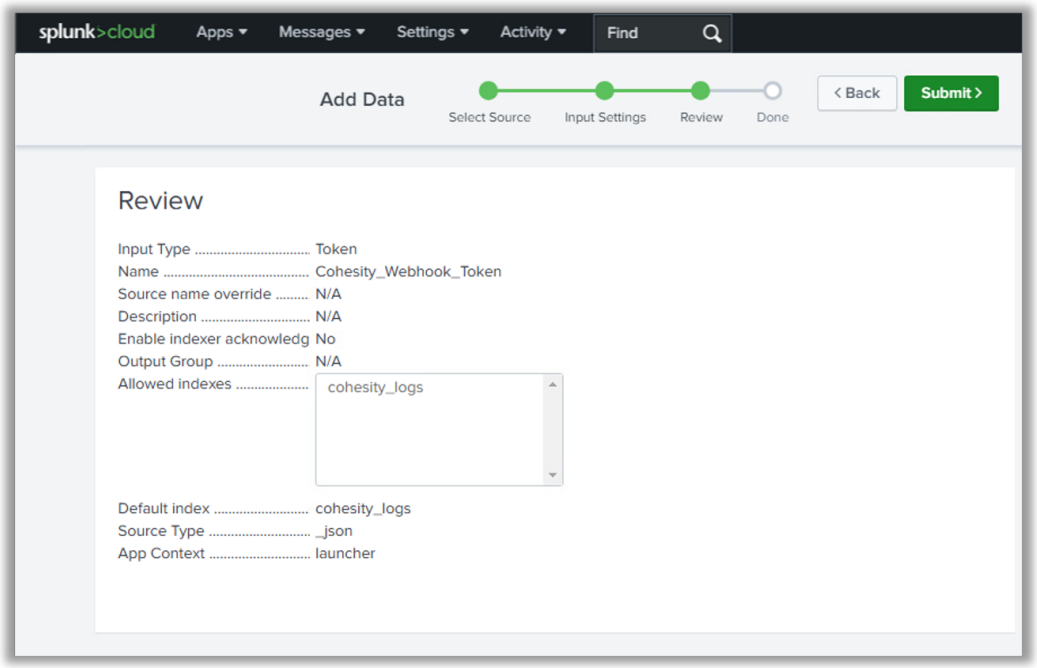
e. Under **Input Settings**, For **Source Type**, choose **Select** and then click **Select Source Type,** Select **_json** from the dropdown. If it is not shown under the dropdown, then type **_json** in search bar to bring it up.



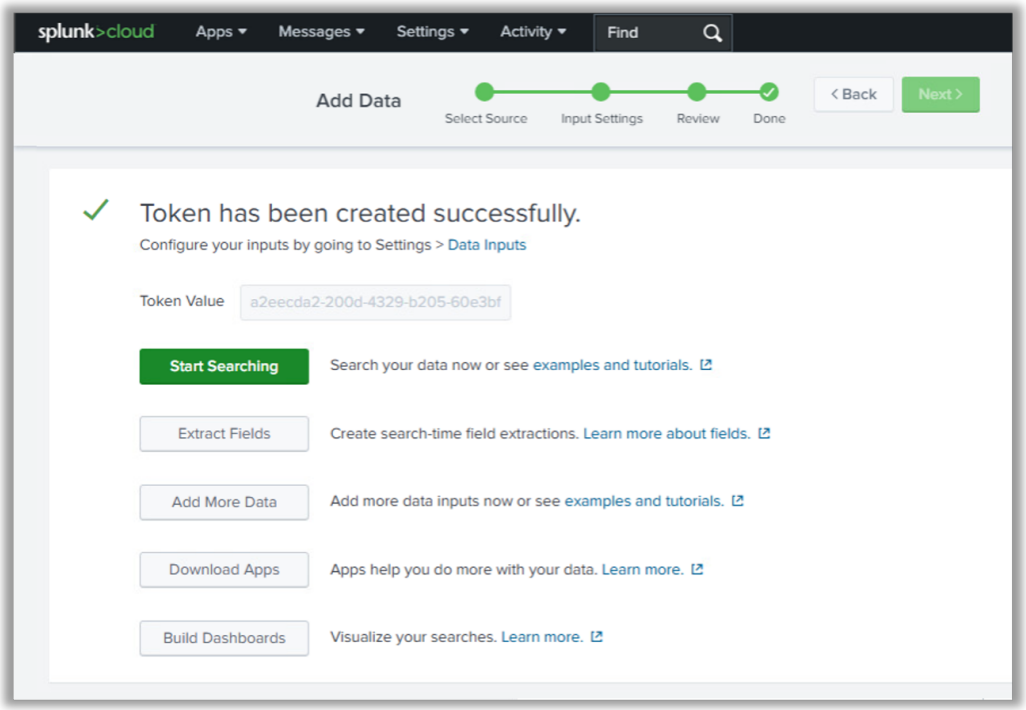
f. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.



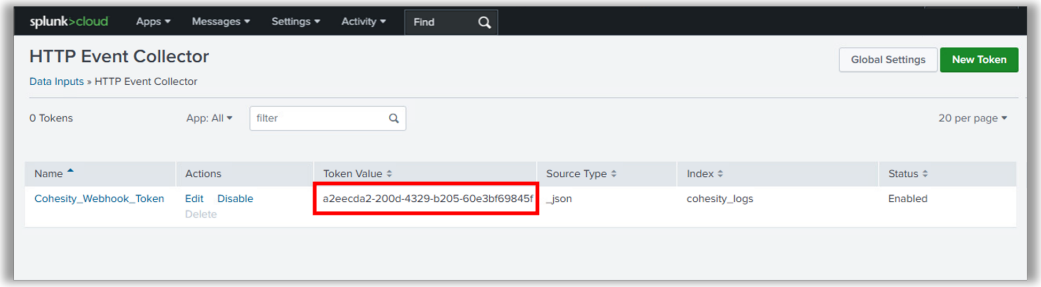
g. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.



h. Click **Submit** to successfully create the token.



i. Once the Token is created, go back to **HTTP Event Collector Page** and verify the Token created. Copy the **Token Value** (Which we will need while configuring the Webhook on Cohesity side).



5. Check HEC endpoint is accessible.

a. Open the below URL in a browser

```
https://<your_domain>.splunkcloud.com:8088/services/collector/health
```

b. If you get the below json response, then your HEC endpoint is accessible and properly configured

```
{"text":"HEC is healthy","code":17}
```

c. If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Revisit previous steps to configure the HEC properly.

6. Test HTTP Event Collector on any system.

   a. Test the HTTP Event Collector using a curl request from cmd prompt / terminal on any system as shown below:

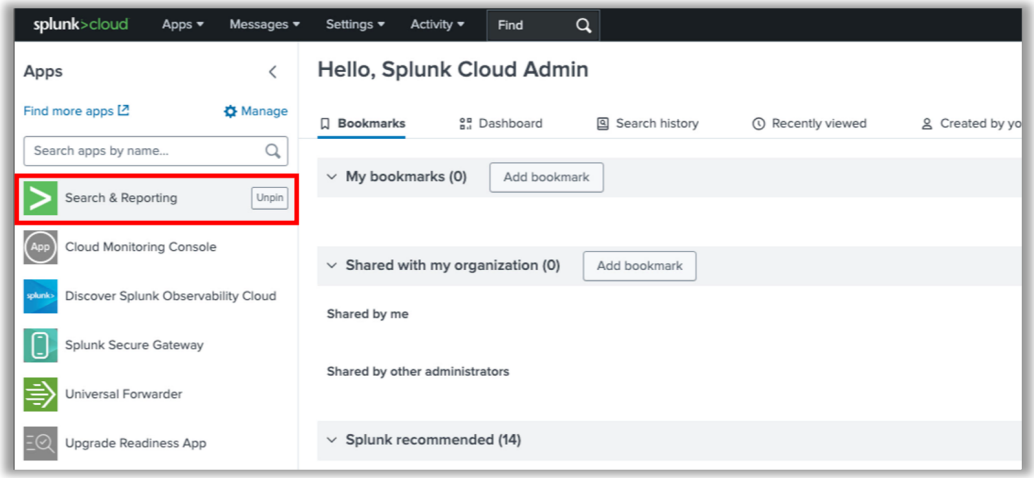
```
curl -k "https://<your_domain>.splunkcloud.com:8088/services/collector/raw" \
     -H "Authorization: Splunk <HEC Token>" \
     -H "Content-Type: application/json" \
     -d '{"alert": "Test Alert", "alertId": "0000"}'
```

   - Your domain – is your unique domain in your Splunk cloud. The link is same as your Splunk cloud access URL.
   - HEC Token – is the Token Value of the HTTP Event Collector Token you created in previous step.
   - Once the curl command executes successfully, it must return the message *{"text": "Success", "code": "0"}* as shown below:

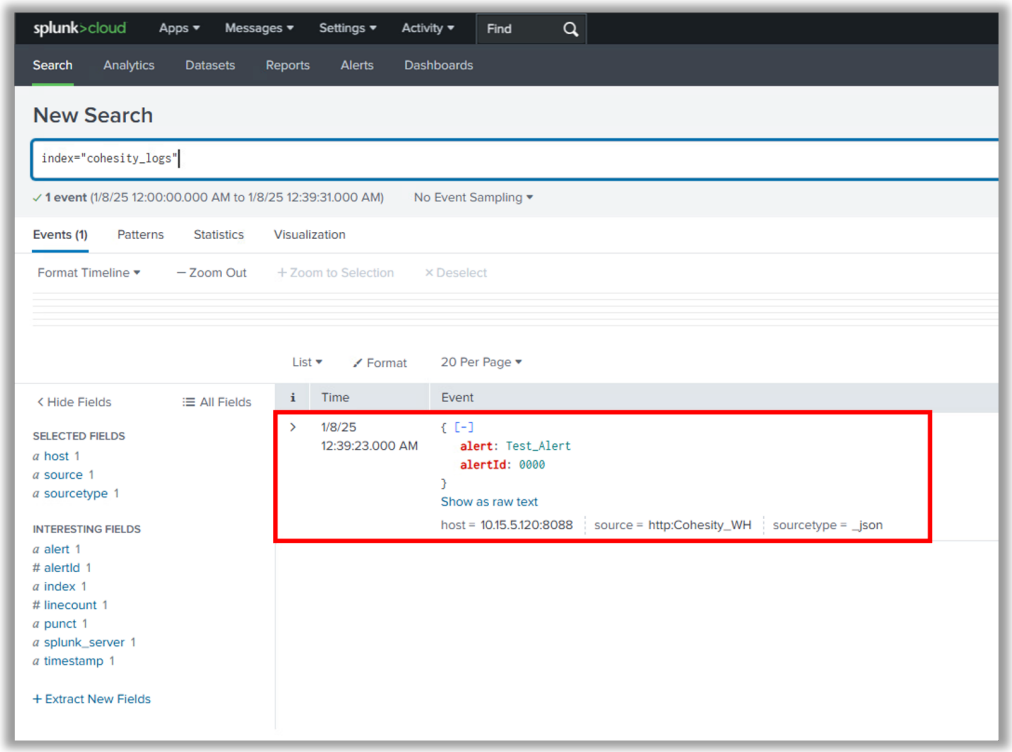
> **NOTE:**
>
> - If you are not receiving the message *{"text": "Success", "code": "0"}* or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration
> - Visit Troubleshooting for more details.

   b. Verify the data is successfully received on Splunk.

      i. From Splunk Web Home console, click Search & Reporting.



ii. Run search query to filter logs. You must see the event sent by curl command in Splunk.

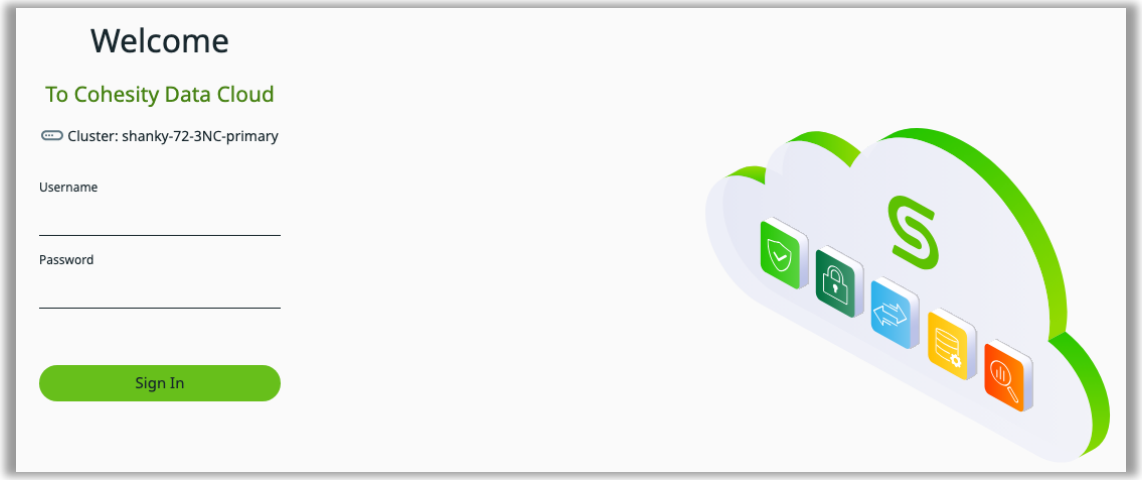


NOTE:

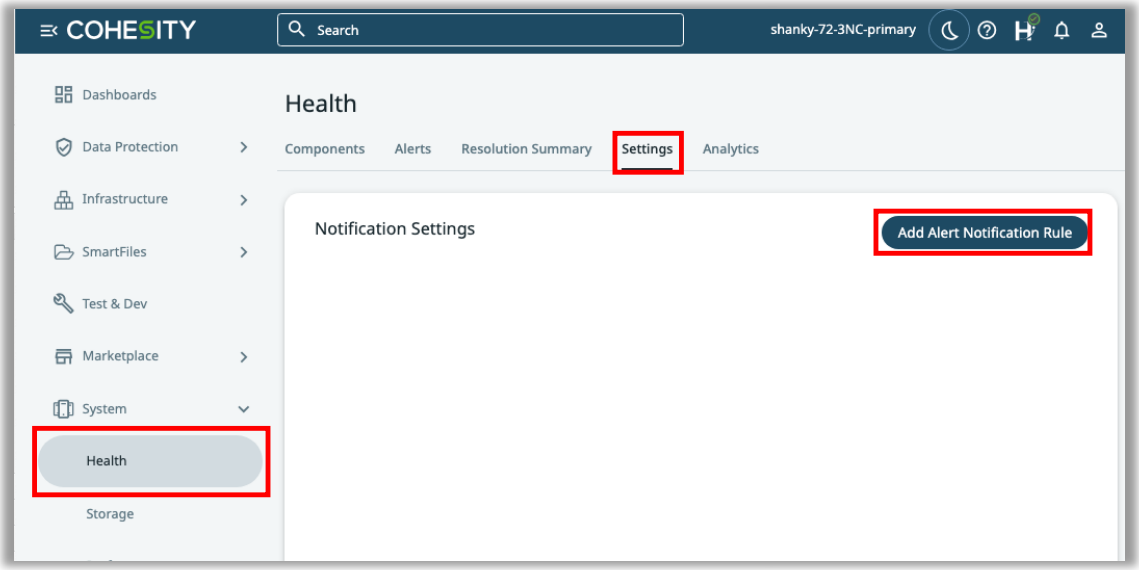
- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

7. Configure alert notification with webhook on Cohesity Cluster.

a. Login to your Cohesity Cluster from Cluster UI.



b. Click **System** > **Health** > **Settings** and then **Add Alert Notification Rule.**



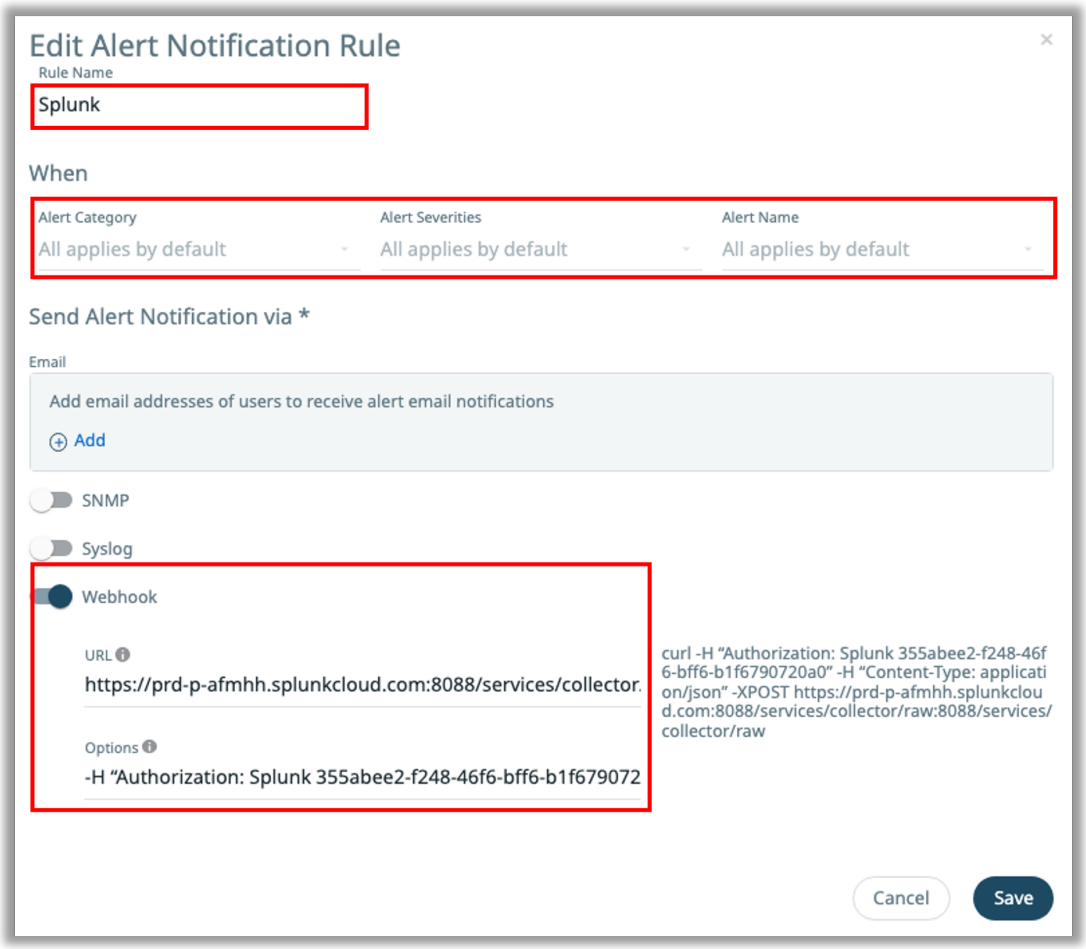
c. Provide the **Rule Name**, choose required **Alert Category**, **Alert Severities** and **Alert Name**, choose **Webhook** as alert notification type and provide the Webhook **URL** and **Options** as below:

URL:
https://<Your Domain>.splunkcloud.com:8088/services/collector/raw

Options:
-H “Authorization: Splunk *<HEC Token>*” -H “Content-Type: application/json”

NOTE For Splunk Trials:

- Alert notifications from Cohesity to Splunk via Webhook requires a valid certificate at the Splunk side.
- Splunk trials might use expired/invalid certificates, which may lead to TLS certificate verification failure, in which case the alert notifications will not be sent from Cohesity to Splunk.
- Contact Splunk support to get your certificate issue resolved.

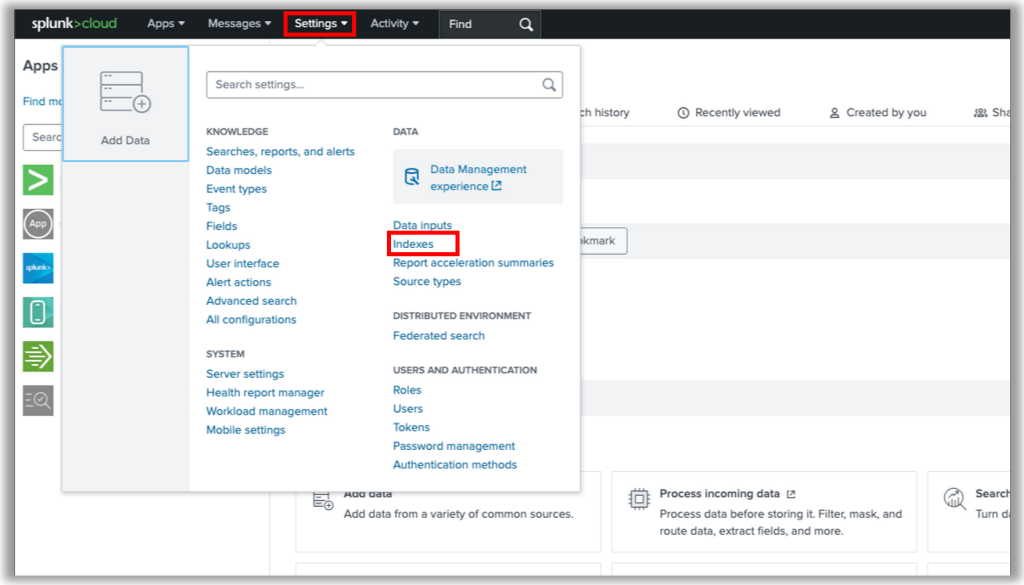


NOTE:

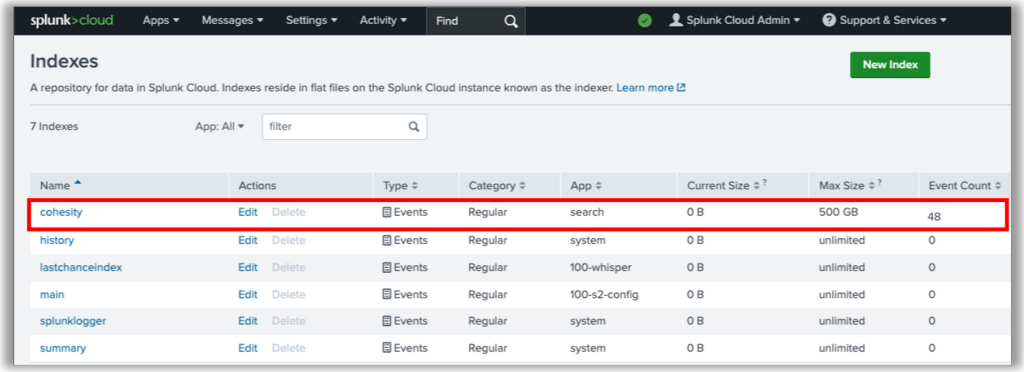
- Use Alert Category, Alert Severities or Alert Name to filter out the selective alerts you want to send to Splunk.
- If you do not select any value for Alert Category, Alert Severities or Alert Name, then all the alerts generated by Cohesity will be sent to Splunk.
- You can see the corresponding curl command framed on the Cluster UI based on your entered URL and Options for Webhook. You can test that curl command on cmd prompt / terminal of any system. Revisit step 5 to know more details.

8. Validate data received from Cohesity on Splunk Cloud.

   a. Click **Indexes** under **Data** in **Settings.**



   b. Verify logs are being pushed to your index by checking the Event Count.

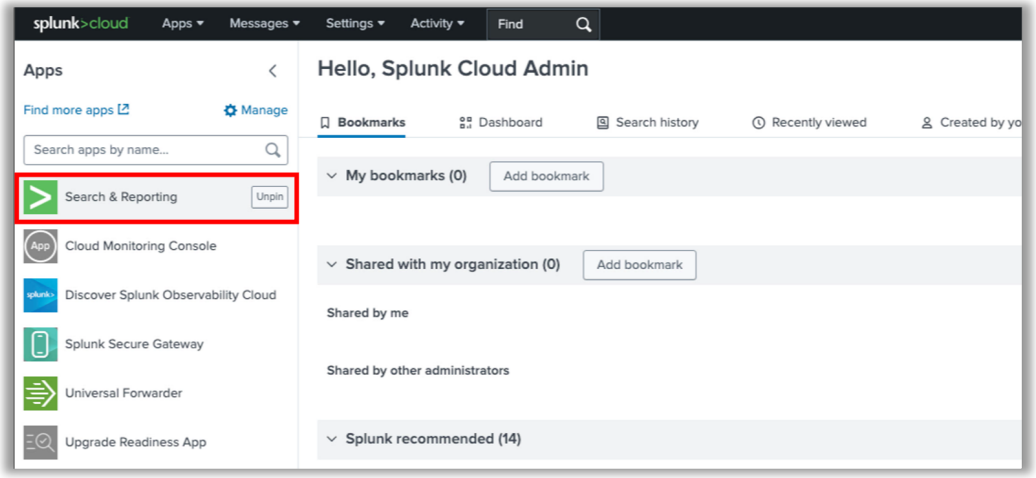


NOTE:

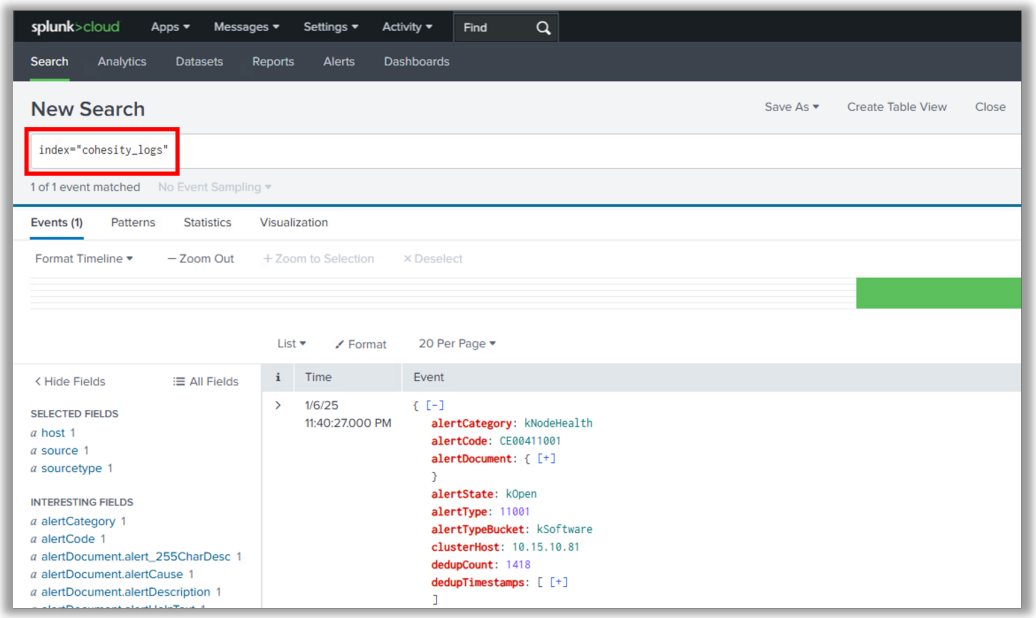
- Alerts and logs will be pushed from Cohesity to Splunk in real time. However, it is not immediate. Sometimes it takes more time for the data to be transmitted to Splunk. If you are not seeing the events after significant amount of time, then there could be an issue in HEC configuration. Edit your HEC to fix the issue.

9. Search, alert and visualize.

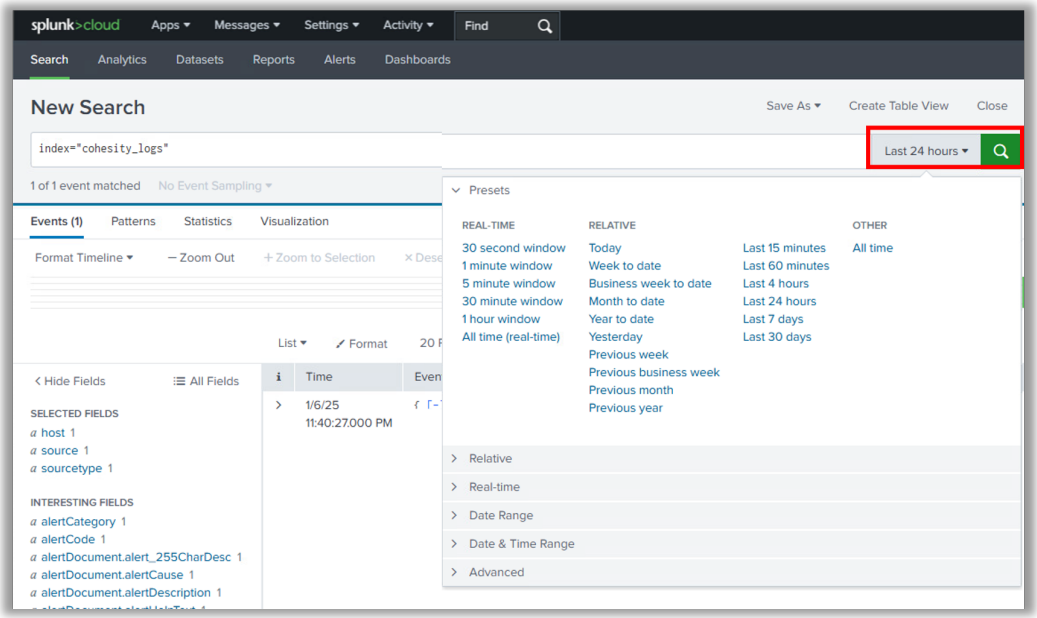
   c. From Splunk Web Home, click Search & Reporting.



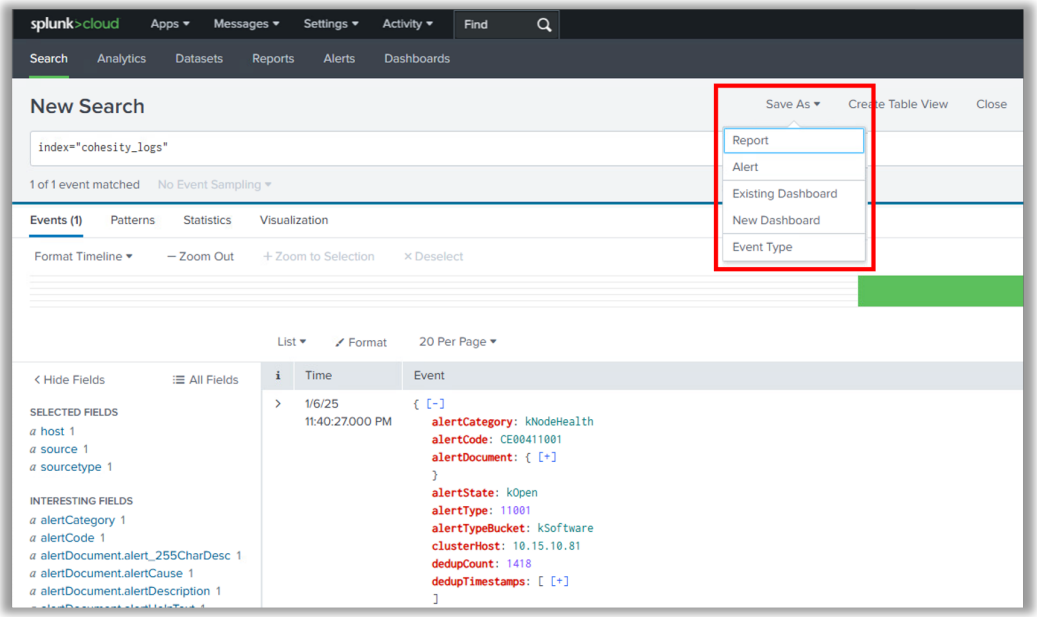
   d. Run search query to filter logs.



e. Filter search results based on time.



f. Alert and visualize.

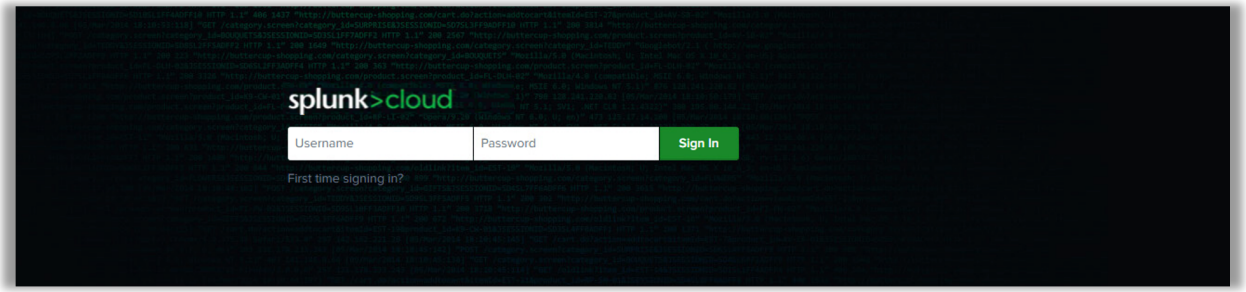


NOTE: **For more details,** refer to the Search and Reporting section.

Cohesity Data Cloud

DataProtect [Self-managed clusters managed from Cohesity Data Cloud]

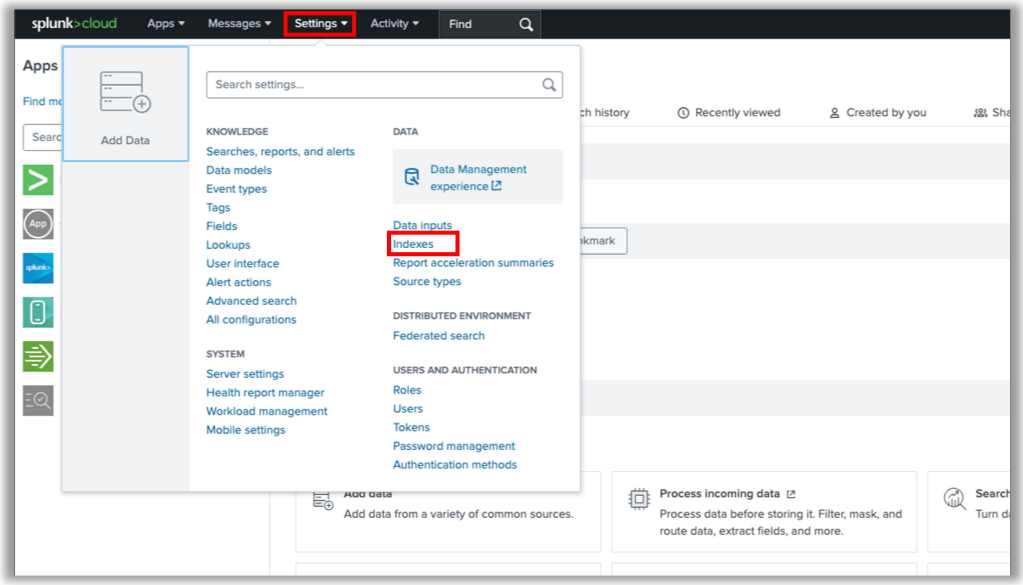
1. Login to your Splunk Cloud Instance.



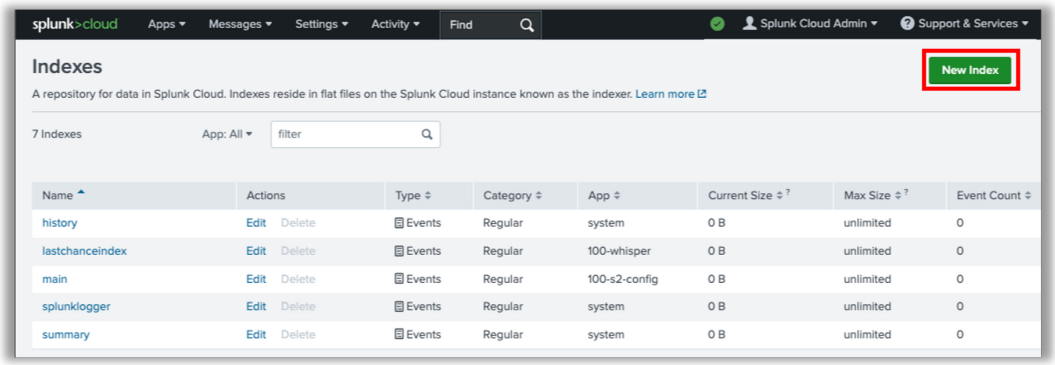
2. Create a new index to store Cohesity logs.

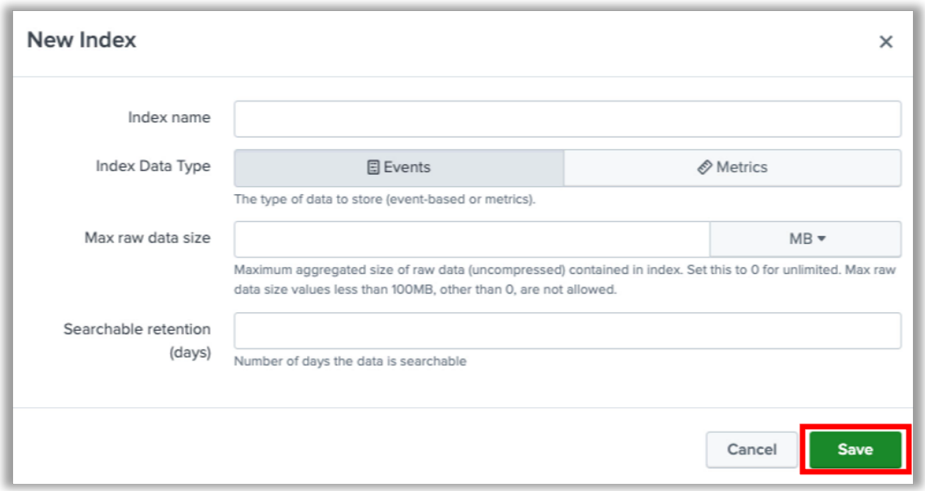
   This is an optional, however, recommended step. You can use already existing index in your Splunk instance. But it is advised to create and use a new index specific to Cohesity logs and alerts

   a. Click **Indexes** under **Data** in **Settings.**

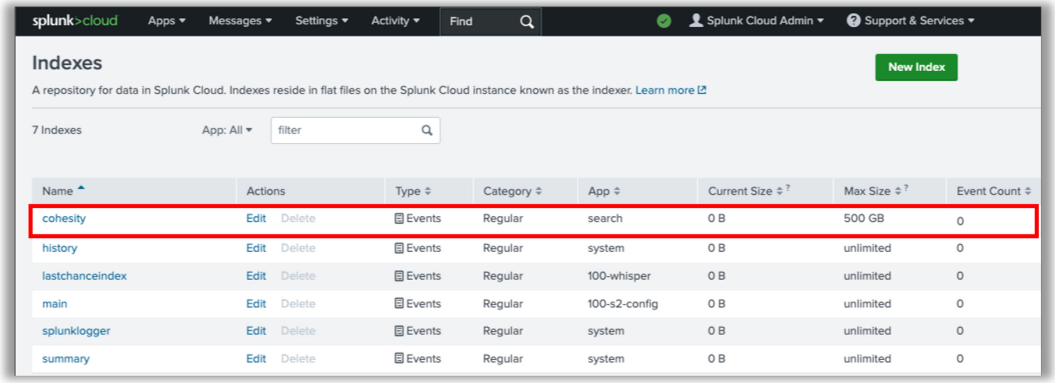


b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save.**

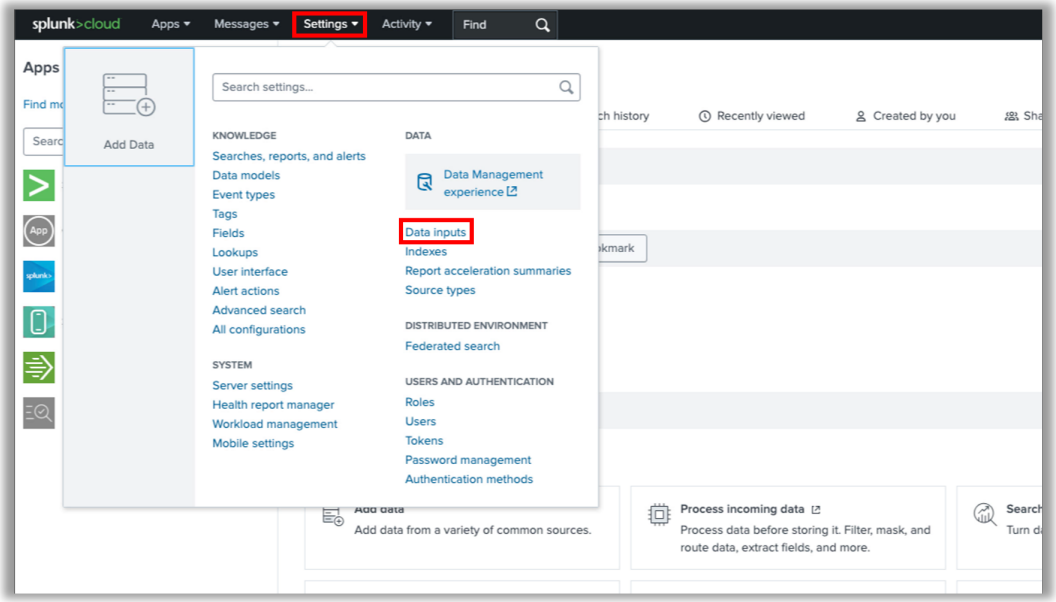




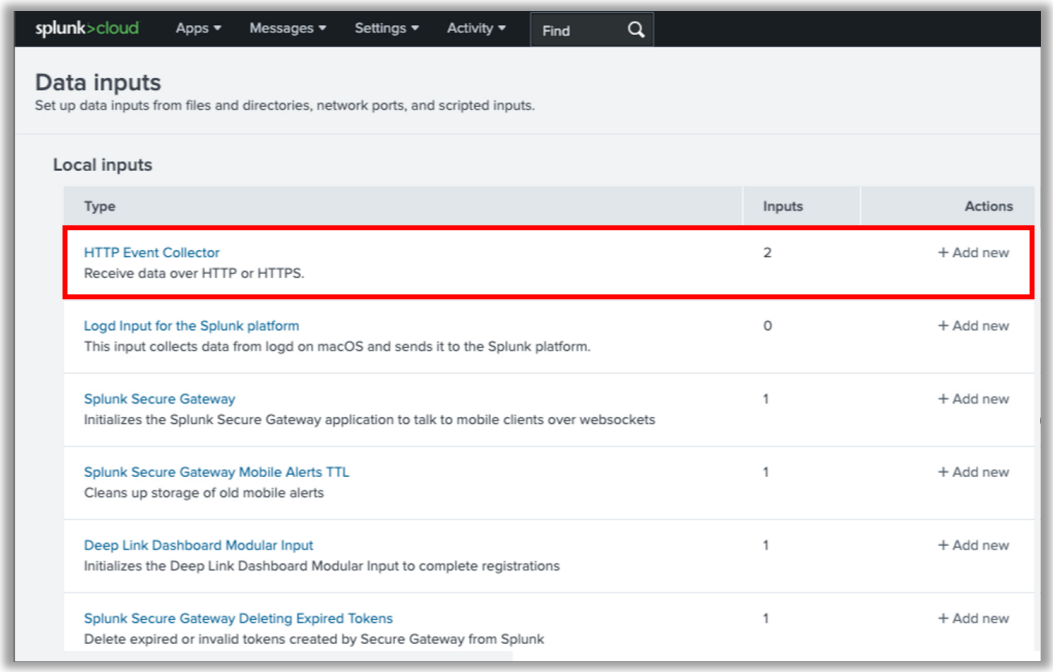
c. You can see the newly created index under Indexes.



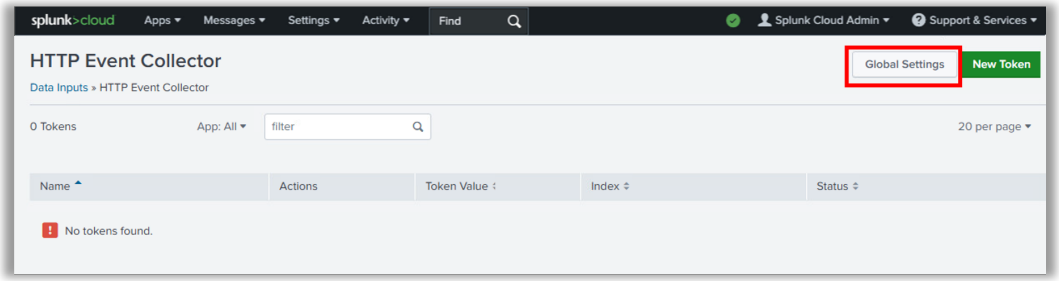
3. Configure HTTP Event Collector to receive data from Cohesity.
   a. Click **Data Inputs** under **Data** in **Settings**.

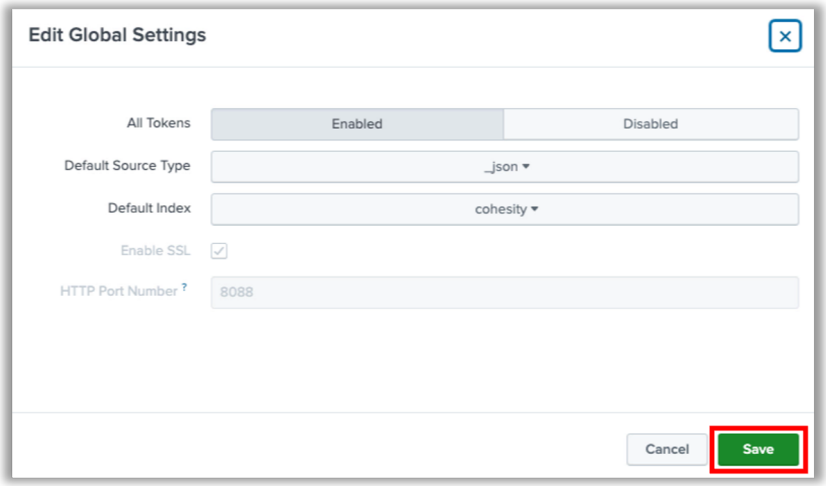


   b. Click **HTTP Event Collector**.



c. Click **Global Settings** and fill in all requested details and click **Save.**

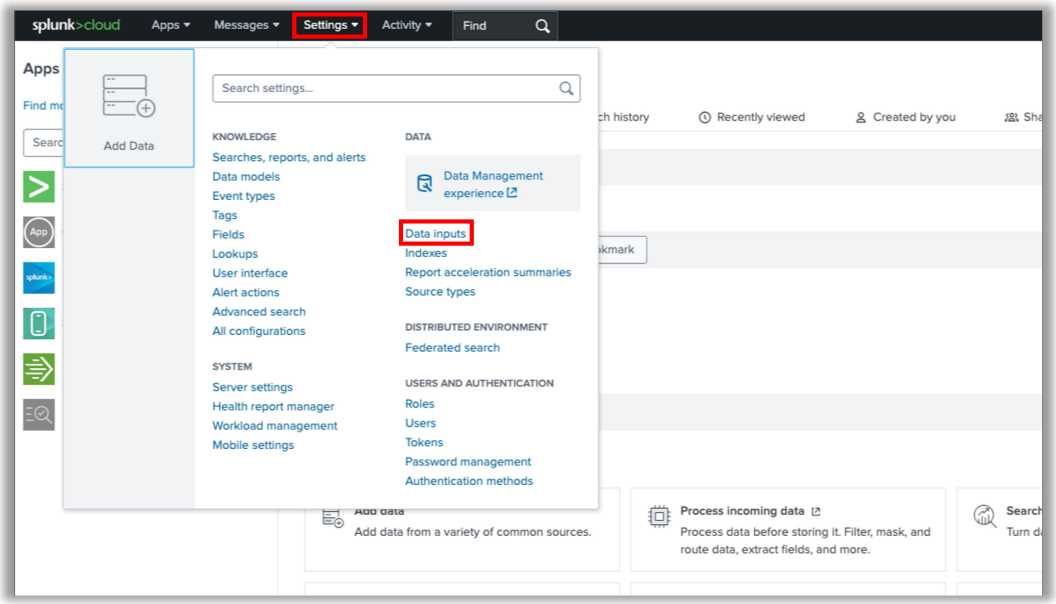




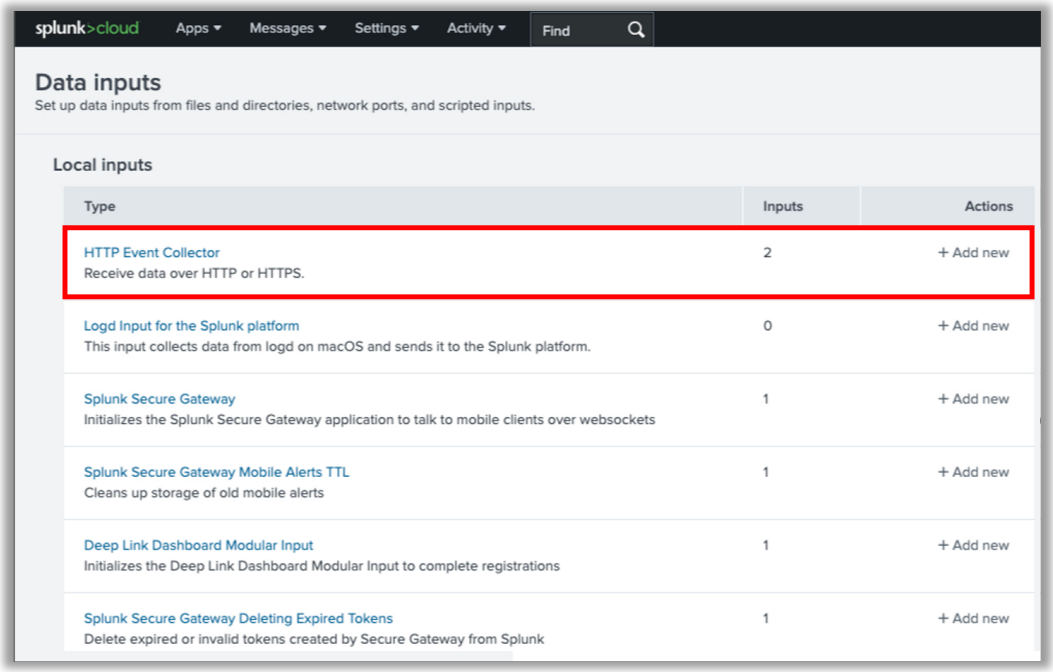
- Select Enabled for All Tokens.
- Select the Default Source Type as _json (If it is not shown under the dropdown, then type _json in search bar to bring it up).
- Select the Default index as the new index we created exclusively for Cohesity logs and alerts under step 1.
- By default, SSL is enabled with default Port 8088. You can disable SSL or modify the default port. The general recommendation is to enable SSL.

4. Create a new token to authenticate Cohesity.

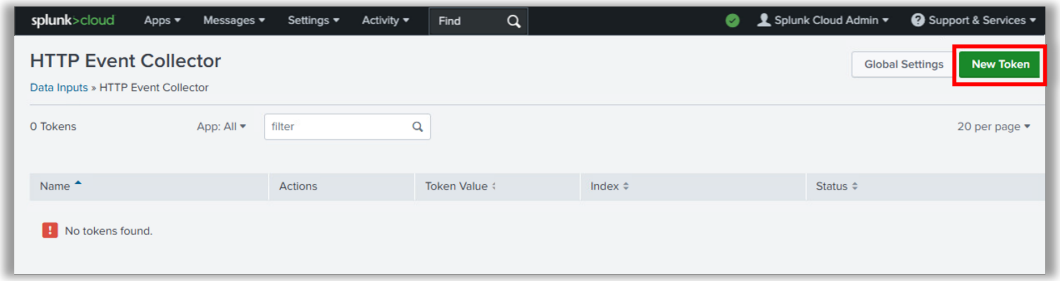
a. Click **Data Inputs** under **Data** in **Settings**.



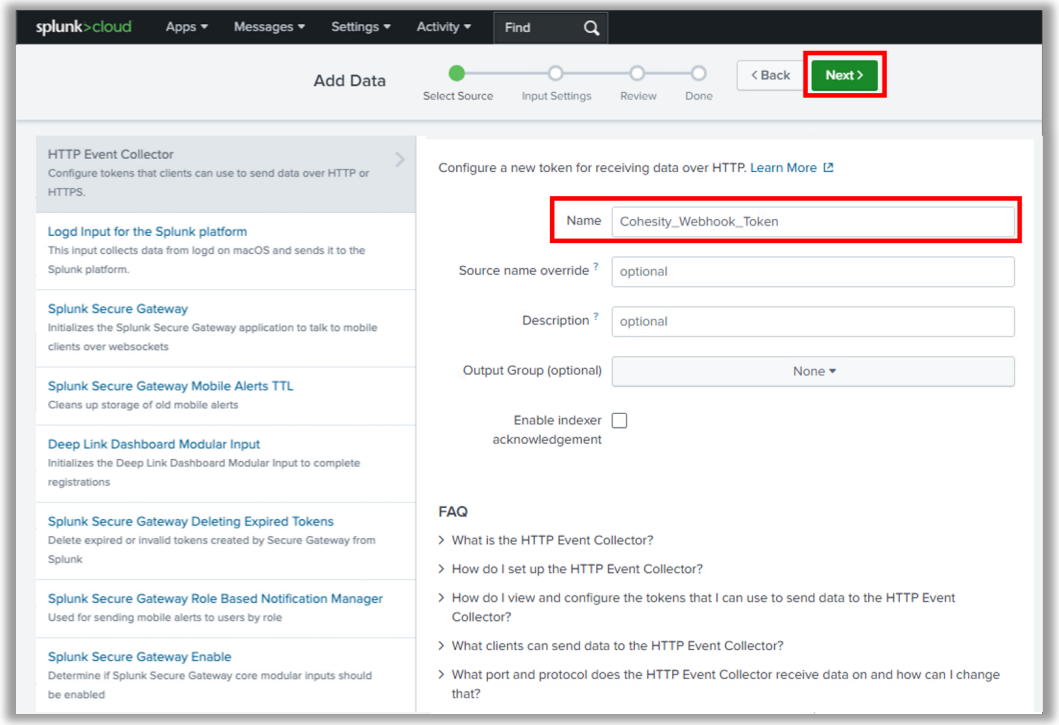
b. Click **HTTP Event Collector**.



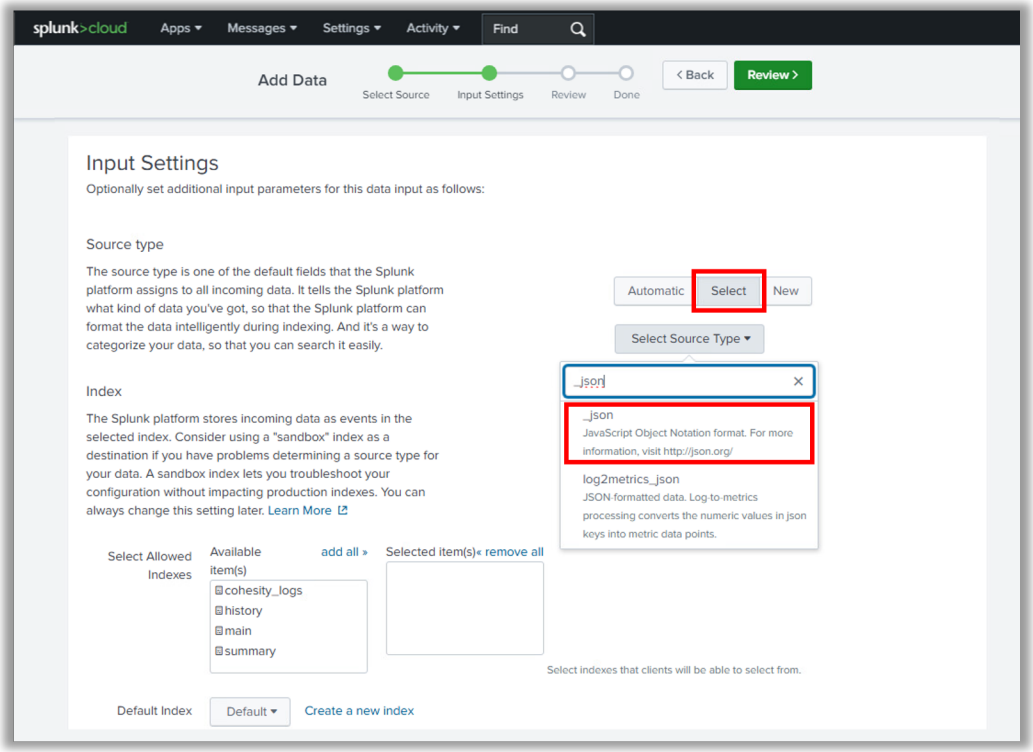
c. Click **New Token.**



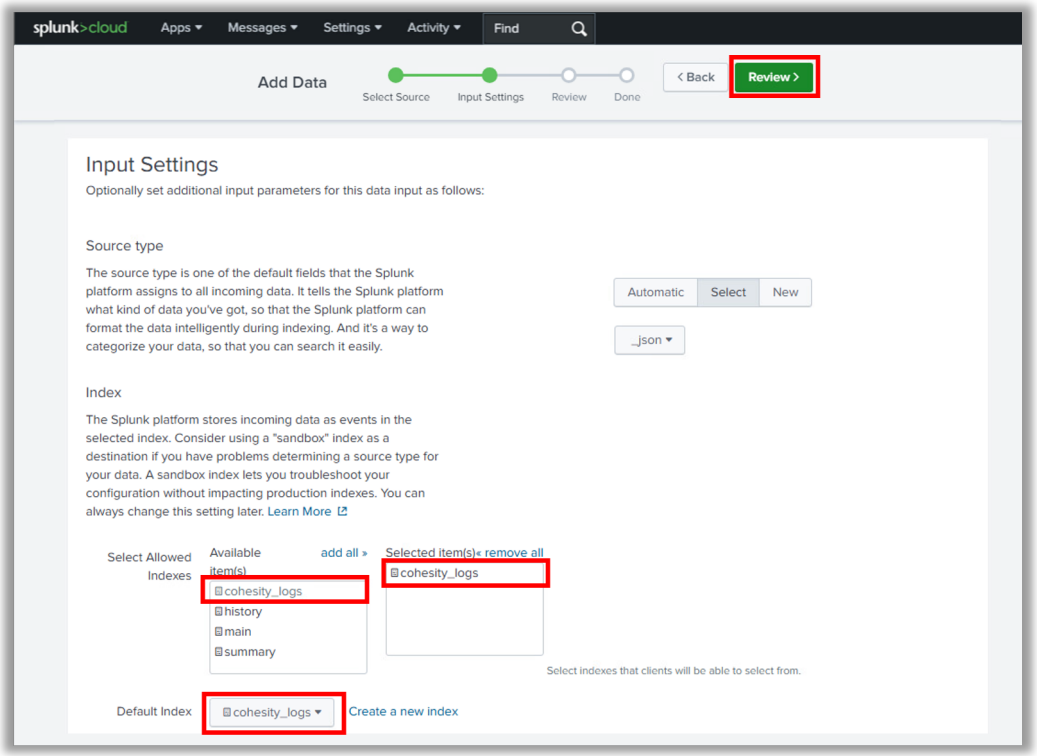
d. Provide a unique **Name** for your token and click **Next** .



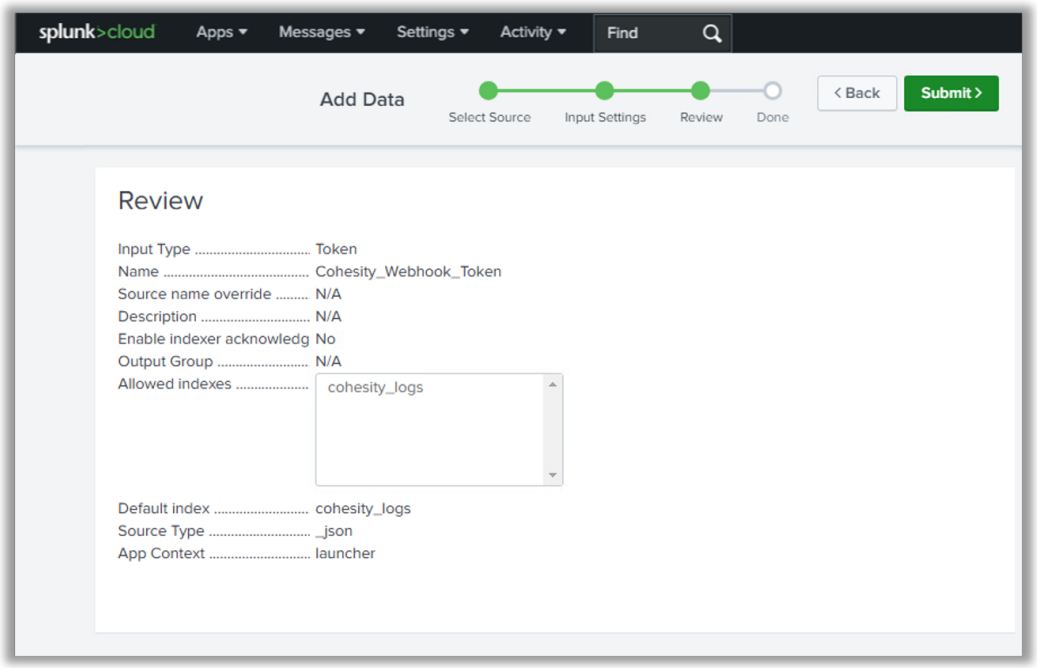
e. Under **Input Settings**, For **Source Type**, choose **Select** and then click **Select Source Type,** Select **_json** from the dropdown. If it is not shown under the dropdown, then type **_json** in search bar to bring it up.



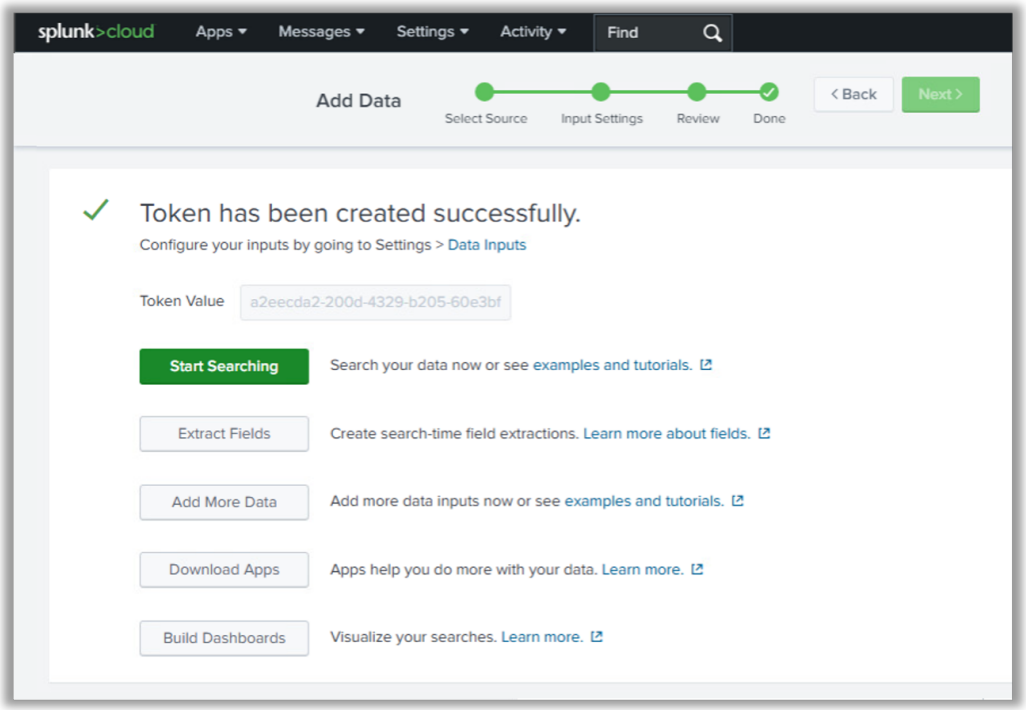
f. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.



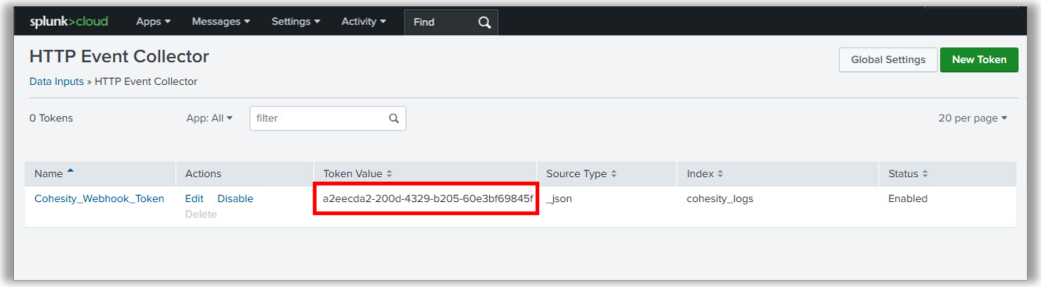
g. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.



h. Click **Submit** to successfully create the token.



i. Once the Token is created, go back to **HTTP Event Collector Page** and verify the Token created. Copy the **Token Value** (Which we will need while configuring the Webhook on Cohesity side).



5. Check HEC endpoint is accessible.

a. Open the below URL in a browser.

```
https://<your_domain>.splunkcloud.com:8088/services/collector/health
```

b. If you get the below json response, then your HEC endpoint is accessible and properly configured.

```
{"text":"HEC is healthy","code":17}
```

c. If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Revisit previous steps to configure the HEC properly.

6. Test HTTP Event Collector on any system.

   a. Test the HTTP Event Collector using a curl request from cmd prompt / terminal on any system as shown below:

```
curl -k "https://<your_domain>.splunkcloud.com:8088/services/collector/raw" \
     -H "Authorization: Splunk <HEC Token>" \
     -H "Content-Type: application/json" \
     -d '{"alert": "Test Alert", "alertId": "0000"}'
```

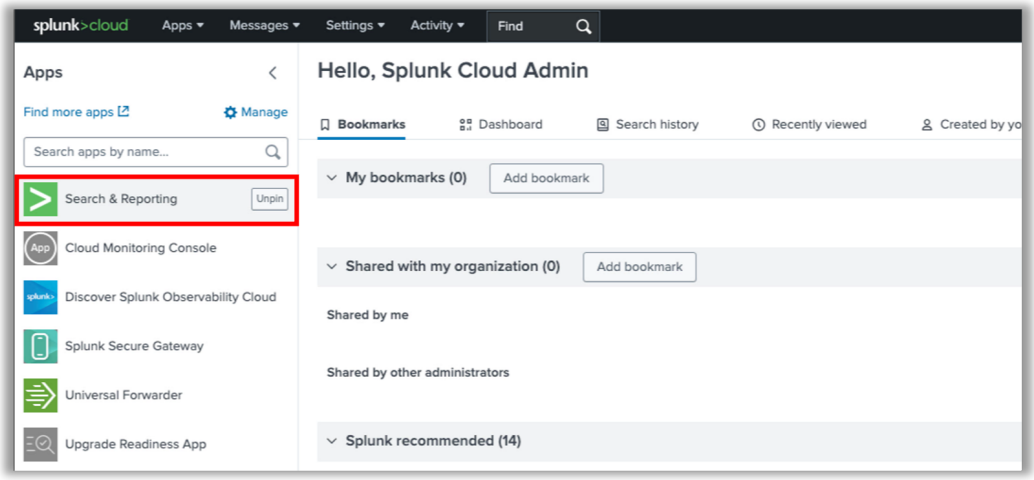
   - Your domain – is your unique domain in your Splunk cloud. The link is same as your Splunk cloud access URL.
   - HEC Token – is the Token Value of the HTTP Event Collector Token you created in previous step.
   - Once the curl command executes successfully, it must return the message *{"text": "Success", "code": "0"}* as shown below:

NOTE:

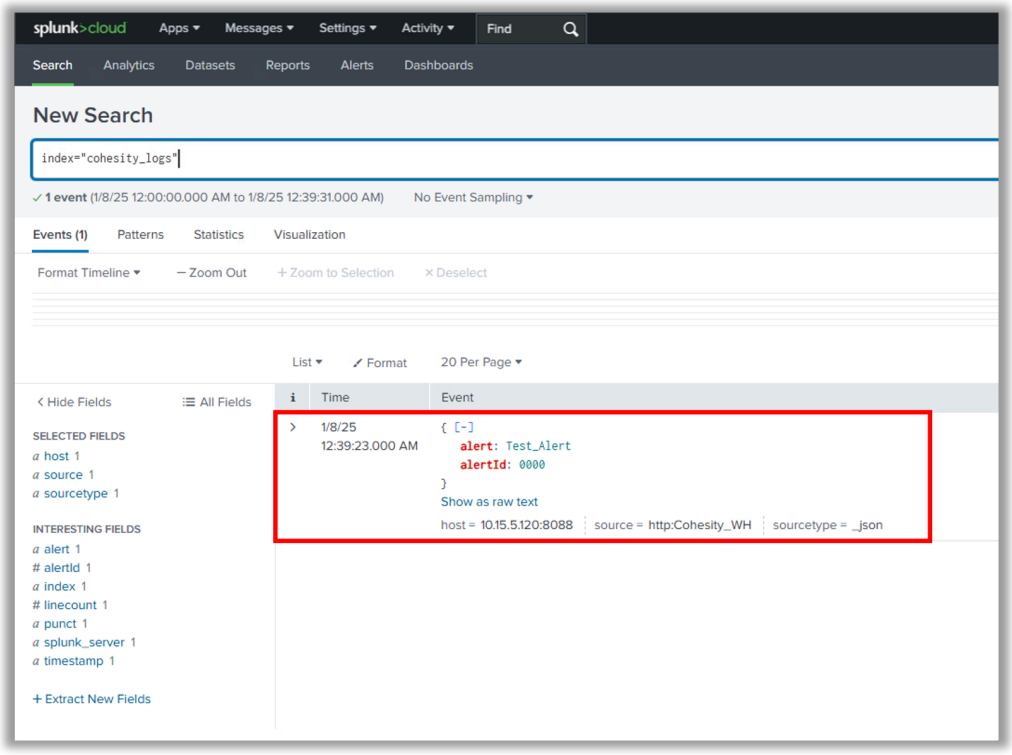
- If you are not receiving the message *{"text": "Success", "code": "0"}* or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

   b. Verify the data is successfully received on Splunk.

      i. From Splunk Web Home console, click Search & Reporting.



ii. Run search query to filter logs. You must see the event sent by curl command in Splunk.

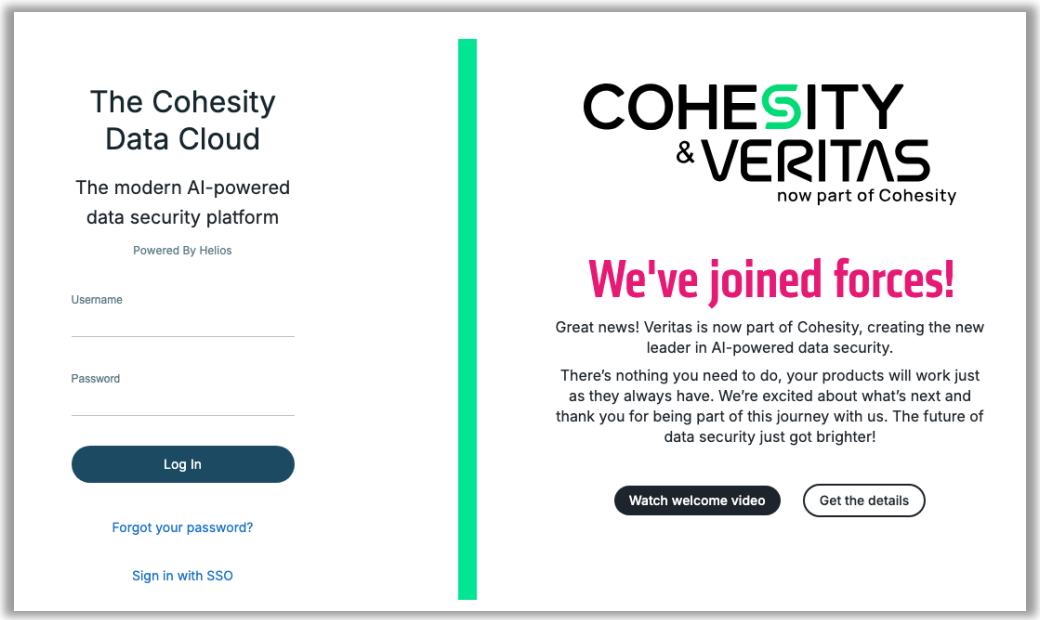


NOTE:

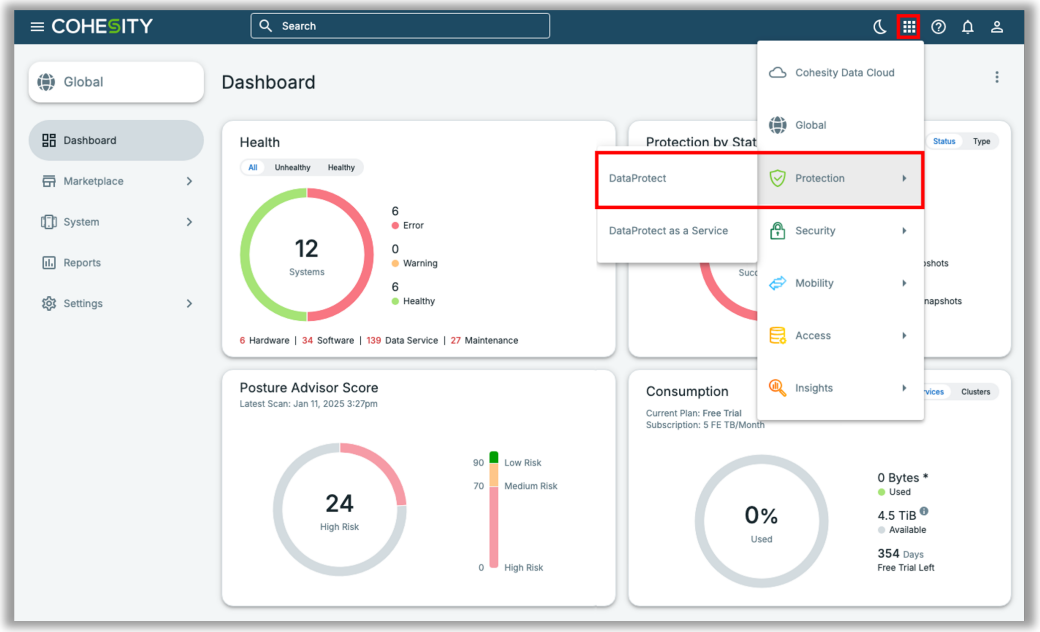
- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

7. Configure alert notification with webhook on Cohesity Data Cloud.

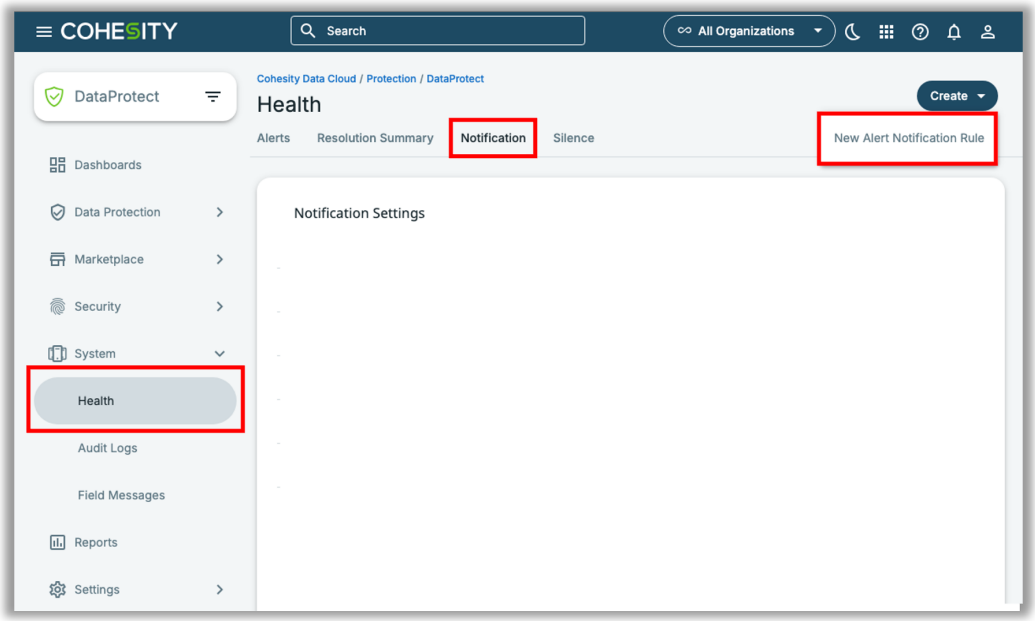
a. Login to Cohesity Data Cloud.



b. Go to **DataProtect** under **Protection**.



c. Click **System** > **Health** > **Notification** and then **Create** > **New Alert Notification Rule**.



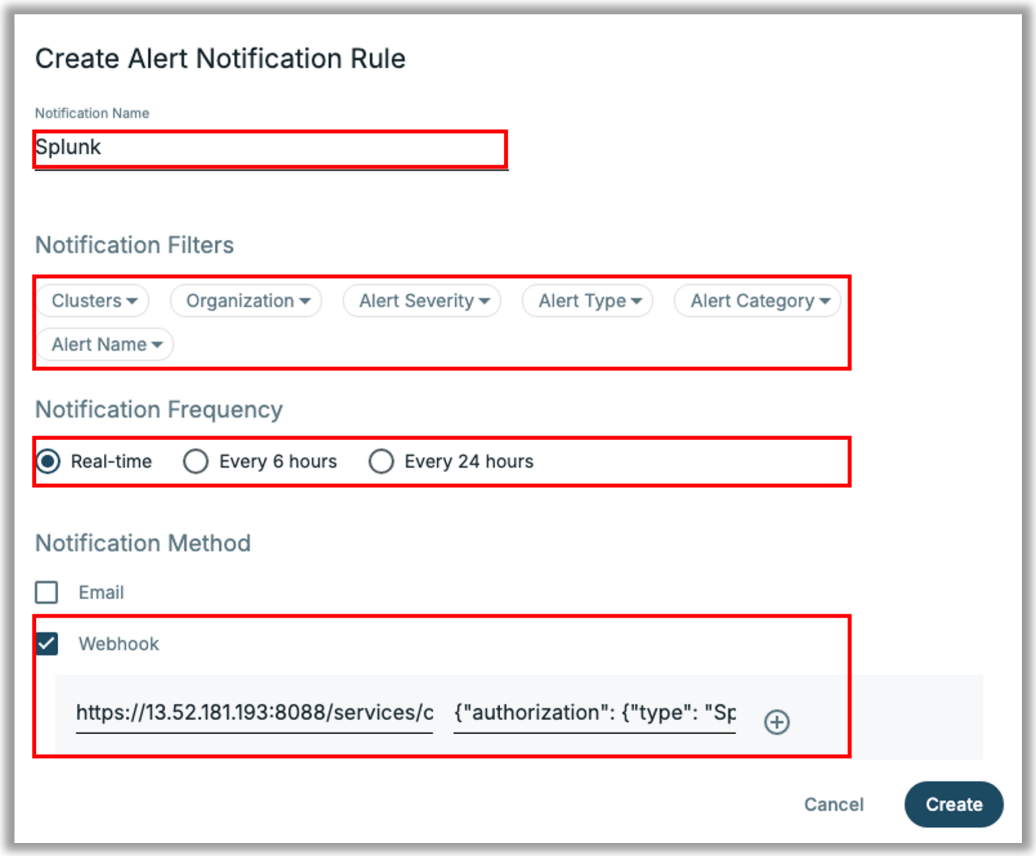
d. Provide the **Notification Name**, Select the **Notification Filters** and **Notification Frequency**, choose **Webhook** as the **Notification Method** and provide the Webhook **URL** and **Options** as below:

URL:
https://<Your Domain>.splunkcloud.com:8088/services/collector/raw

Options:
{"authorization": {"type": "Splunk","credentials": "*<HEC Token>*"}}

NOTE For Splunk Trials:

- Alert notifications from Cohesity to Splunk via Webhook requires a valid certificate at the Splunk side.
- Splunk trials might use expired/invalid certificates, which may lead to TLS certificate verification failure, in which case the alert notifications will not be sent from Cohesity to Splunk.
- Contact Splunk support to get your certificate issue resolved.

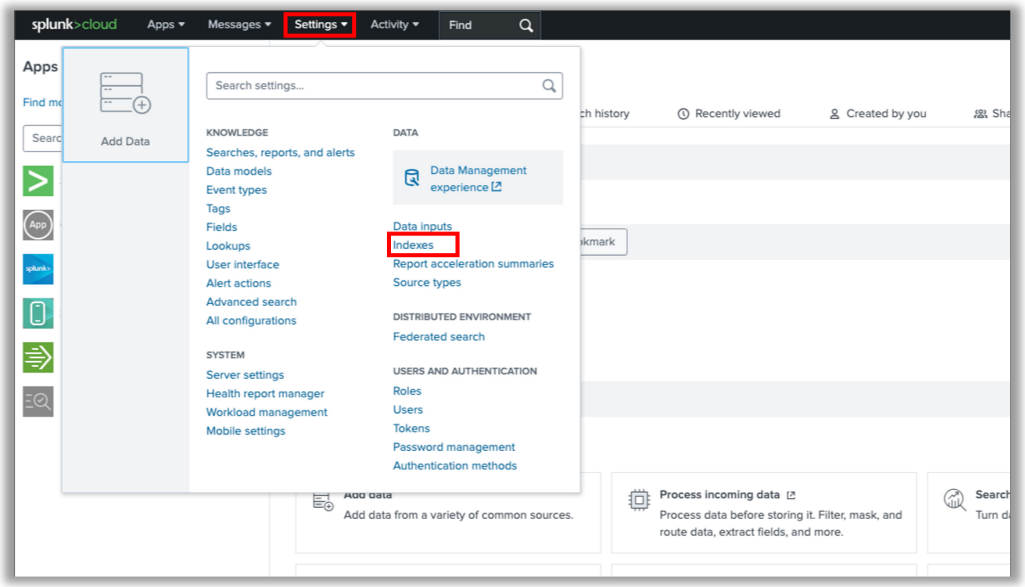


NOTE:

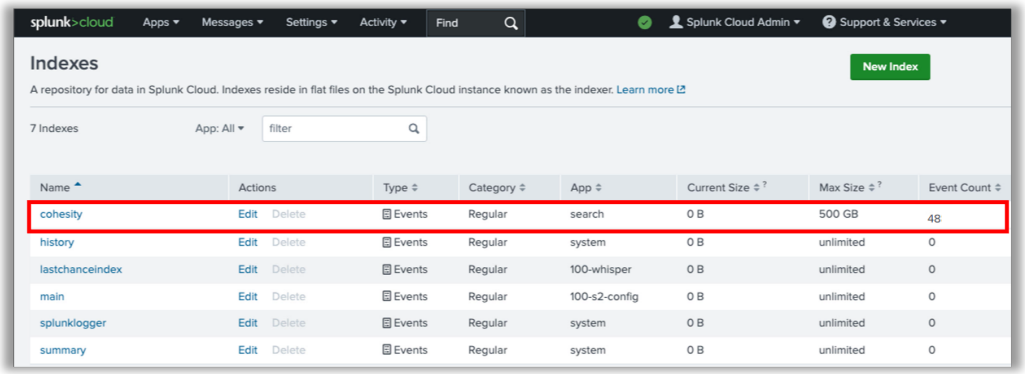
- Use Clusters, Organization, Alert Severity, Alert Type, Alert Category or Alert Name to filter out the selective alerts you want to send to Splunk.
- If you do not select any value for Clusters, Organization, Alert Severity, Alert Type, Alert Category or Alert Name, then all the alerts generated by Cohesity will be sent to Splunk.

8. Validate data received from Cohesity on Splunk Cloud.

e. Click **Indexes** under in **Data Settings**.



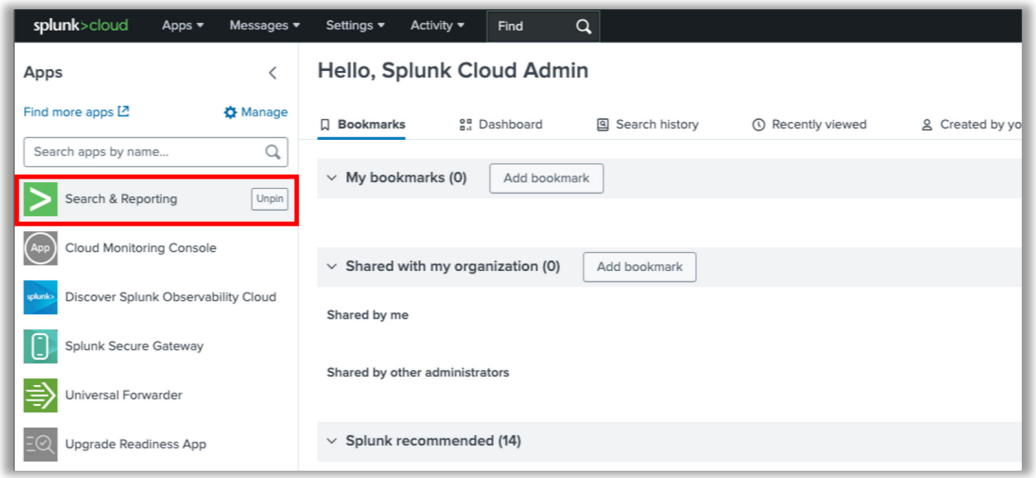
f. Verify logs are being pushed to your index by checking the Event Count.



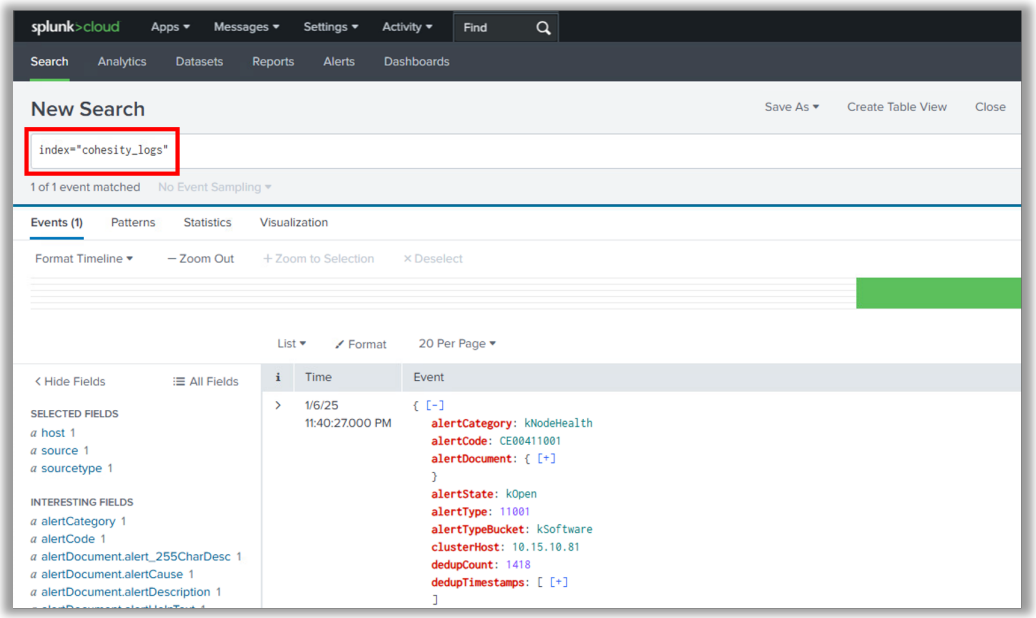
NOTE: Alerts and logs will be pushed from Cohesity to Splunk in real time. However, it is not immediate. Sometimes it takes more time for the data to be transmitted to Splunk. If you are not seeing the events after significant amount of time, then there could be an issue in HEC configuration. Edit your HEC to fix the issue.

9. Search, alert and visualize.

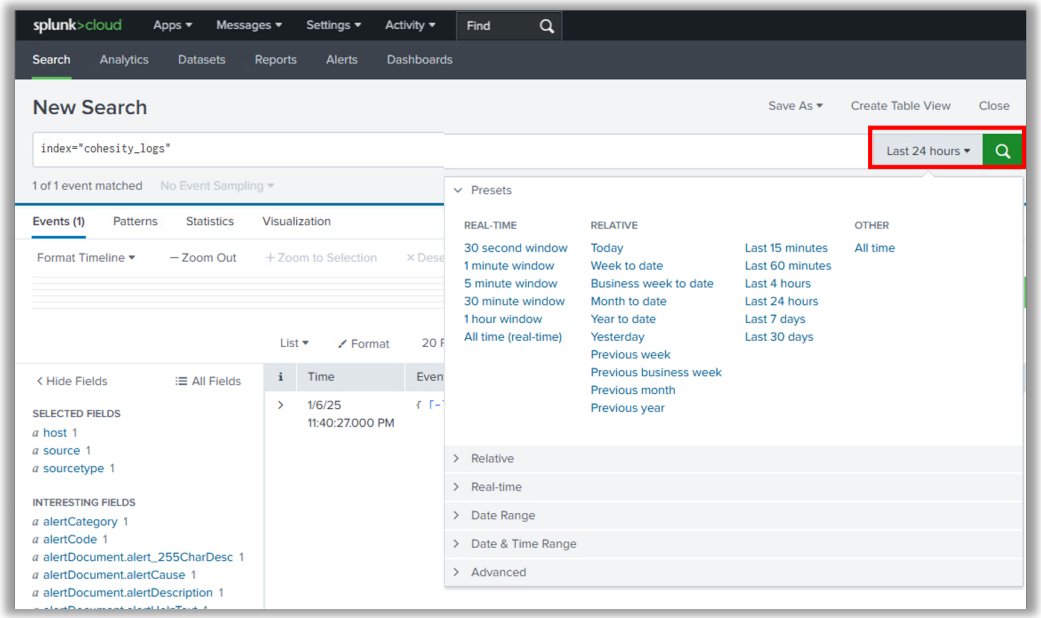
a. From Splunk Web Home, click Search & Reporting.



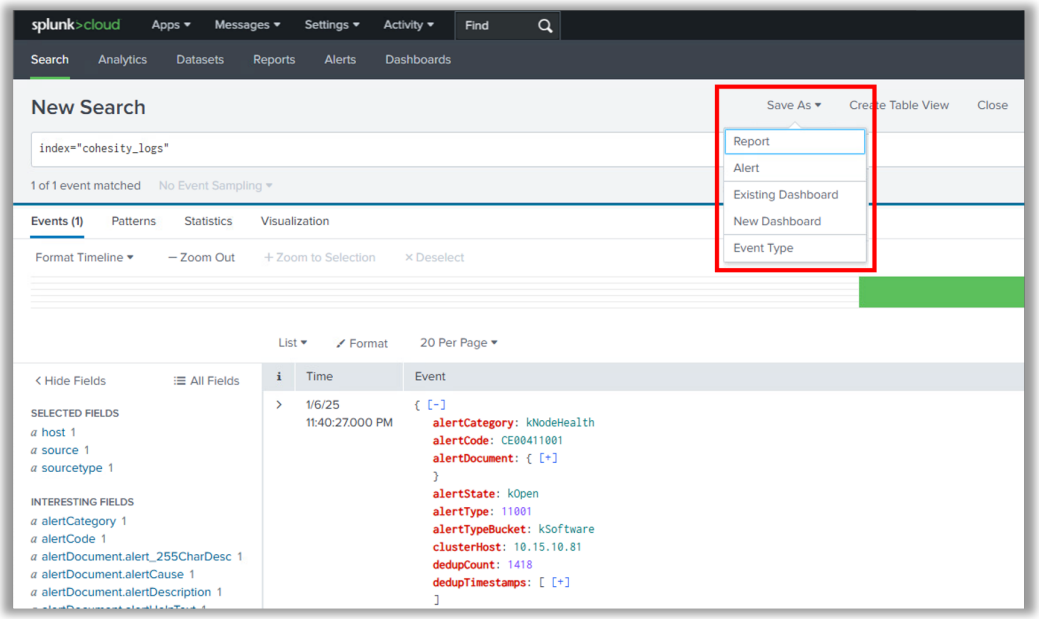
b. Run search query to filter logs.



c. Filter search results based on time.



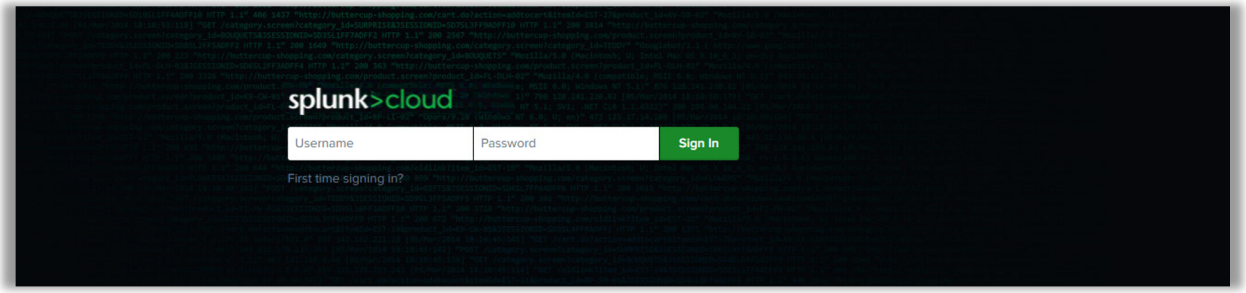
10. Alert and visualize.



NOTE: **For more details,** refer to the Search and Reporting section.

DataProtect as a Service [Cohesity SaaS Service]

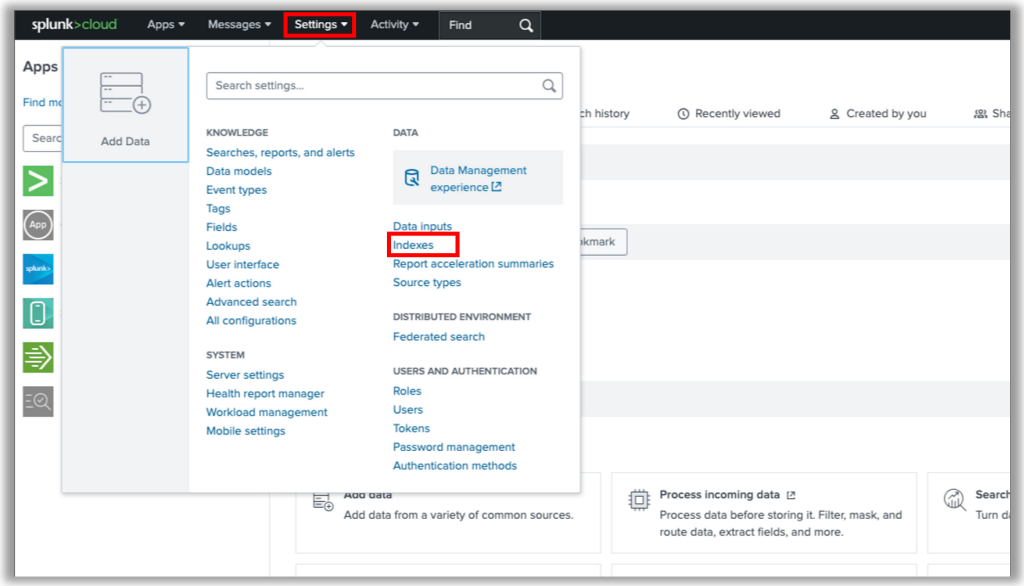
1. Login to your Splunk Cloud Instance.



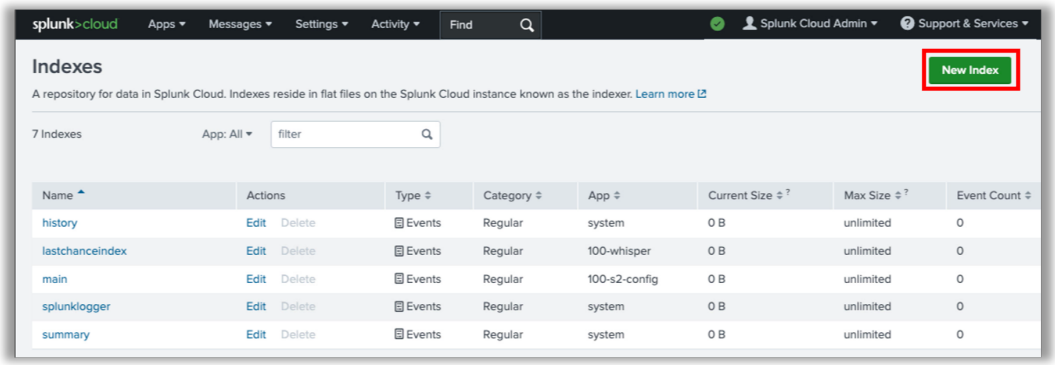
2. Create a new index to store Cohesity logs.

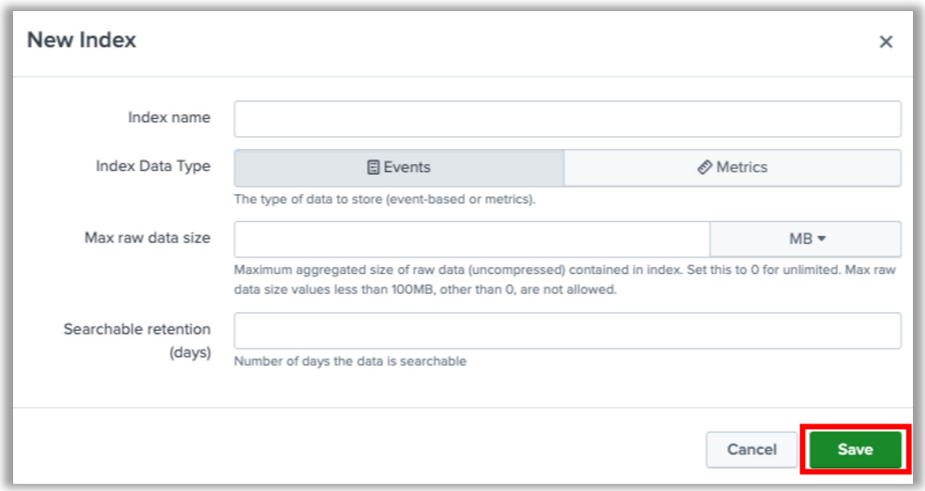
   This is an optional, however, recommended step. You can use already existing index in your Splunk instance. But it is advised to create and use a new index specific to Cohesity logs and alerts

   a. Click **Indexes** under **Data** in **Settings.**

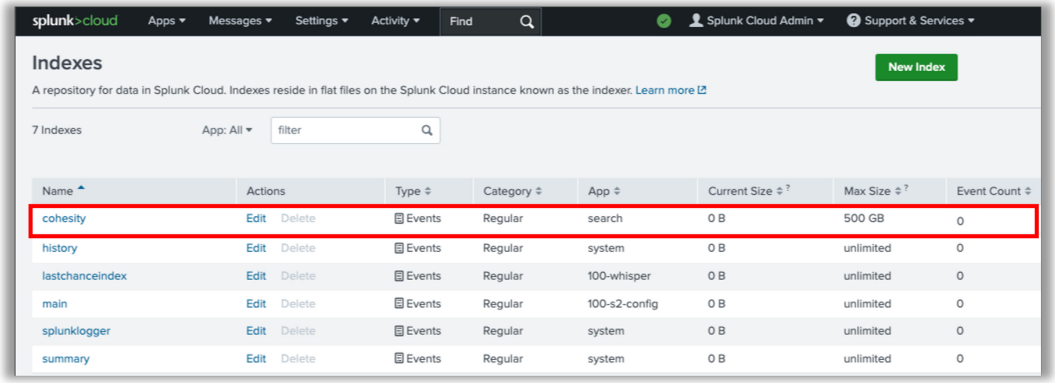


b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save.**

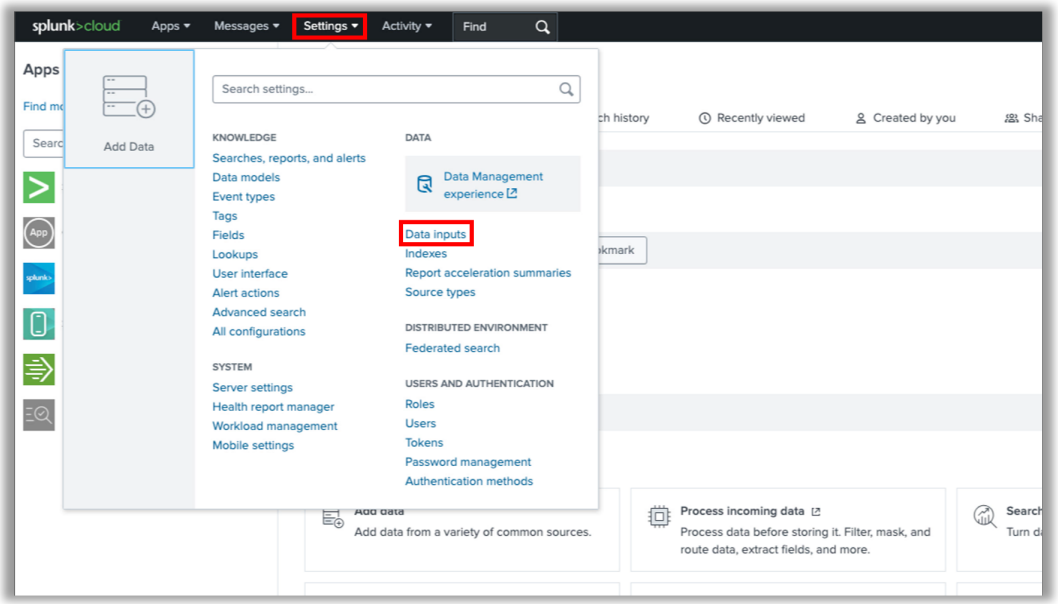




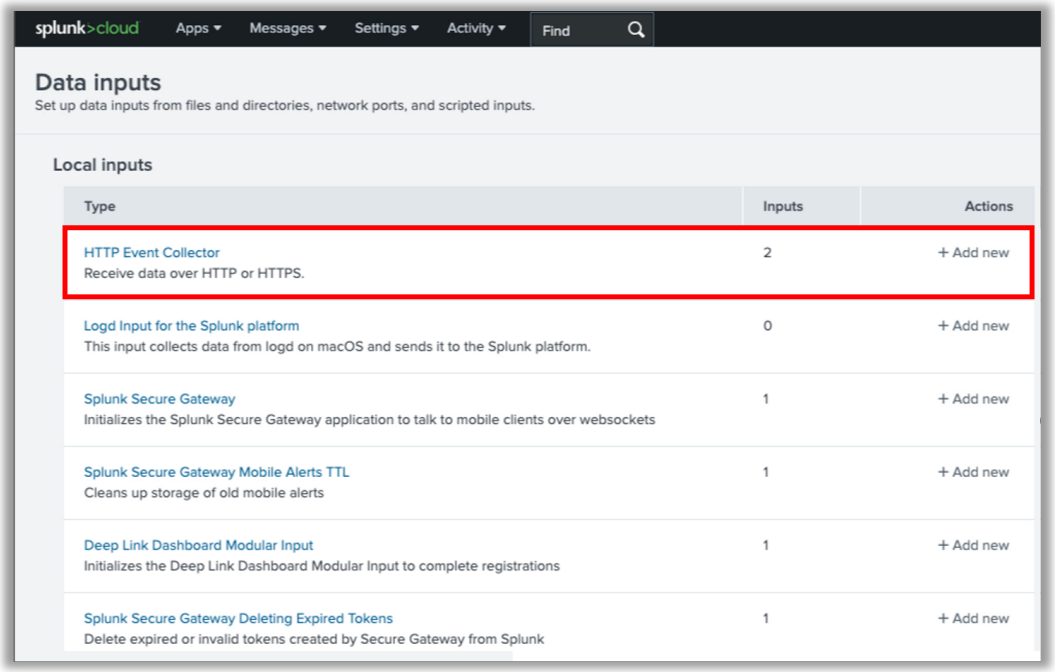
c. You can see the newly created index under Indexes.



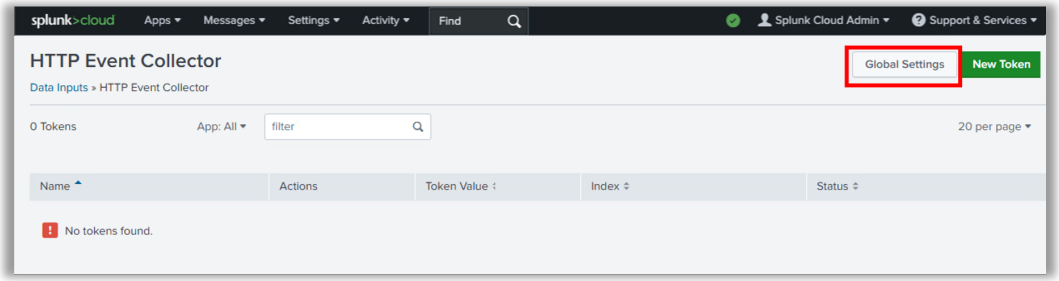
3. Configure HTTP Event Collector to receive data from Cohesity.
   a. Click **Data Inputs** under **Data** in **Settings**.

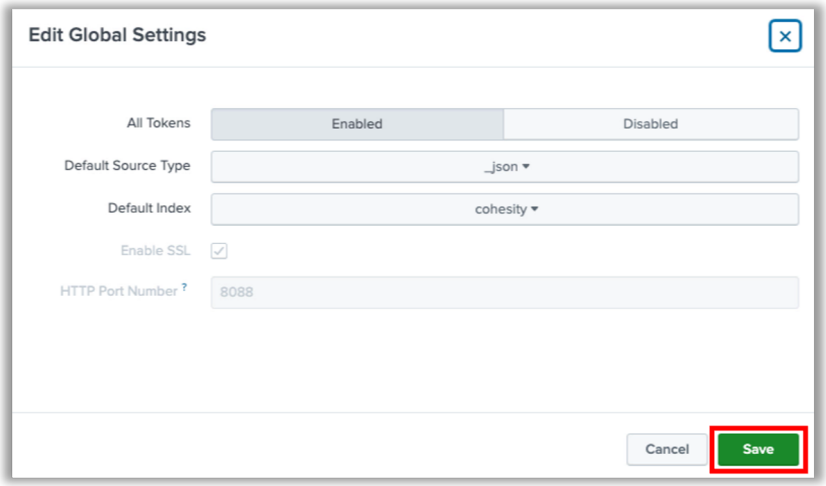


   b. Click **HTTP Event Collector**.



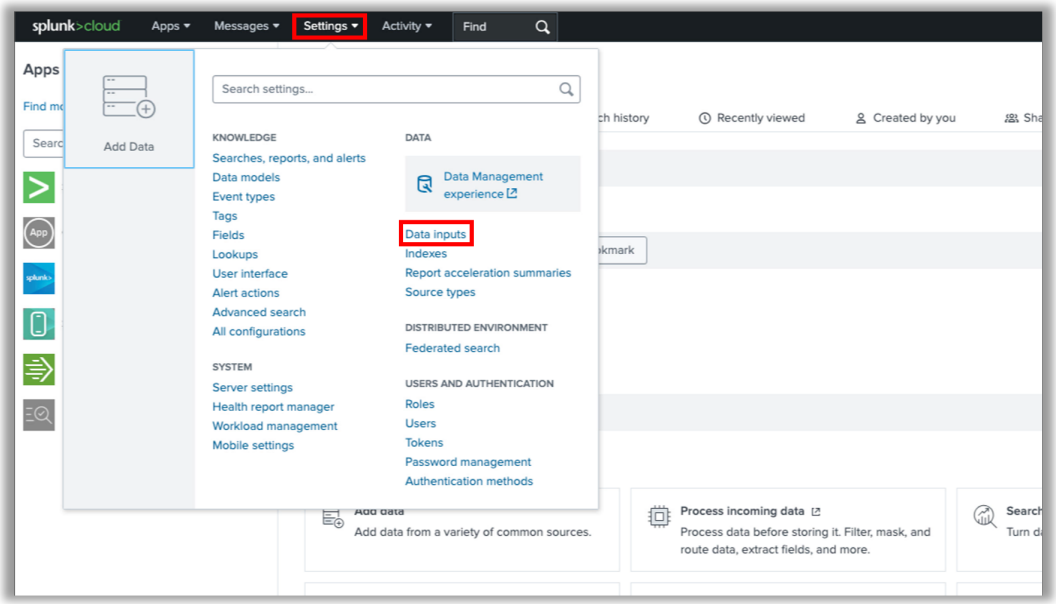
c. Click **Global Settings** and fill in all requested details and click **Save.**



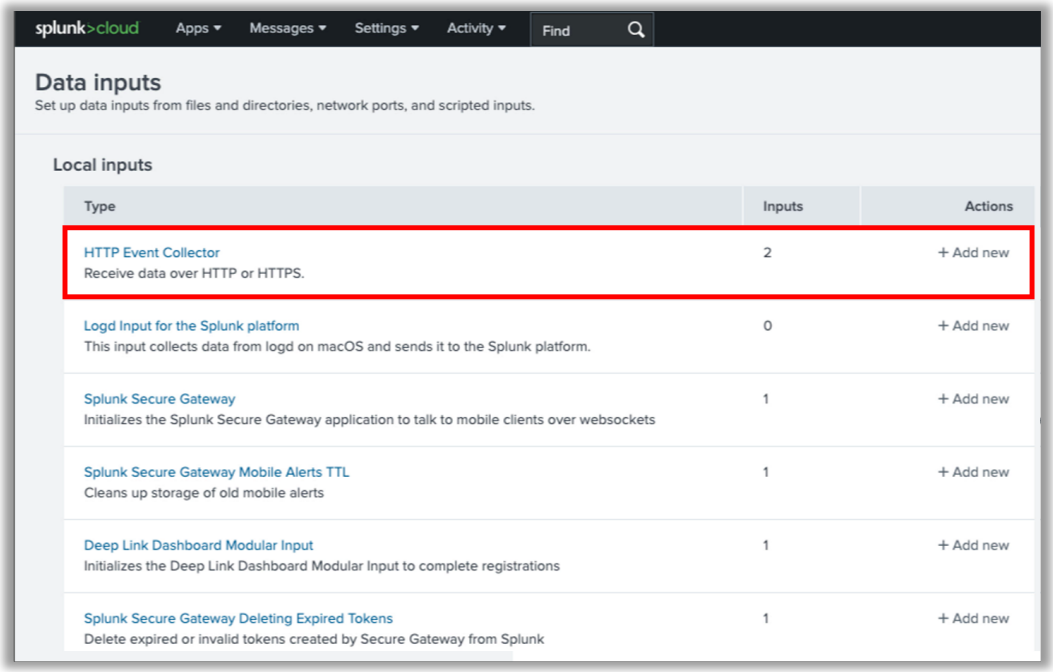


- Select **Enabled** for **All Tokens.**
- Select the **Default Source Type** as **_json** (If it is not shown under the dropdown, then type _json in search bar to bring it up).
- Select the **Default index** as the new index we created exclusively for Cohesity logs and alerts under step 1.
- By default, **SSL** is enabled with default **Port 8088**. You can disable SSL or modify the default port. The general recommendation is to enable SSL.

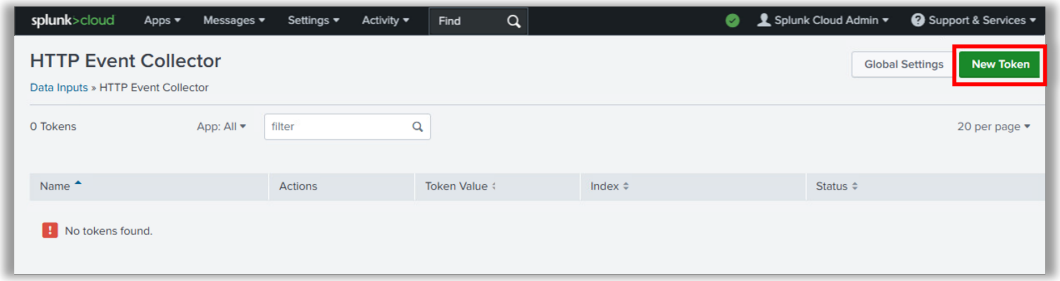
4. Create a new token to authenticate Cohesity.
   a. Click **Data Inputs** under **Data** in **Settings**.



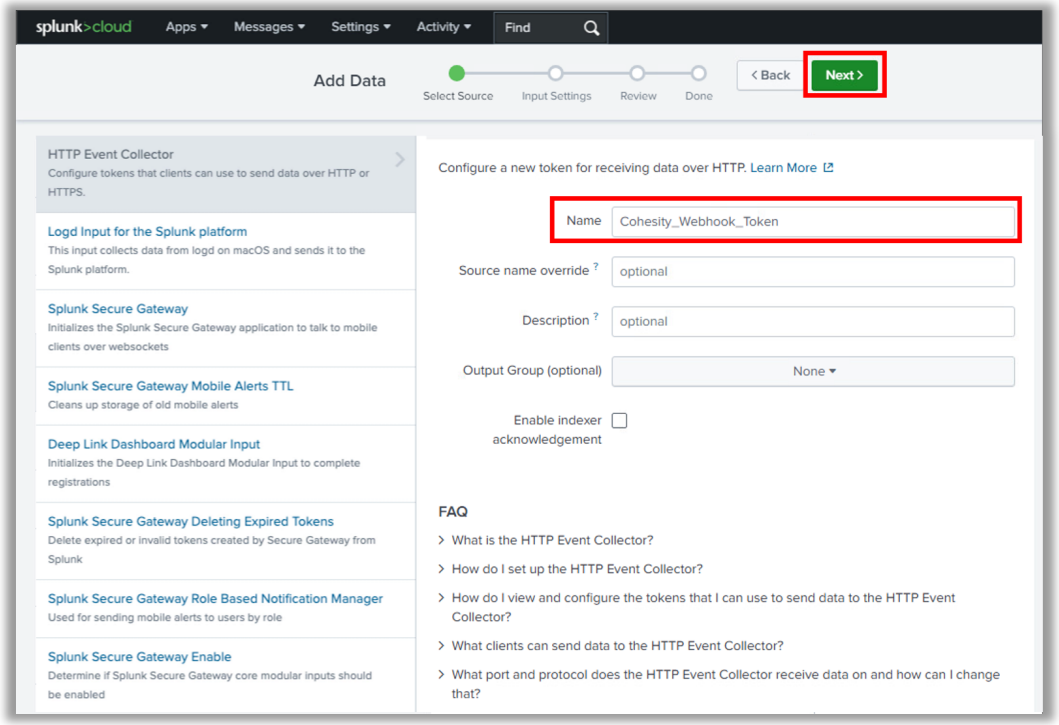
   b. Click **HTTP Event Collector.**



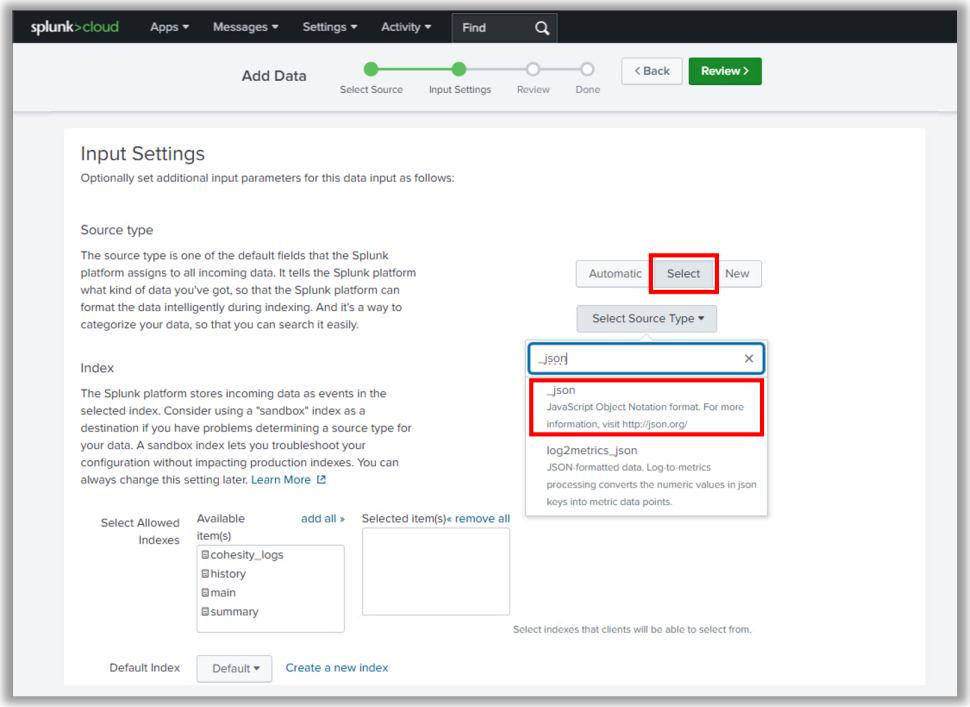
c. Click **New Token.**



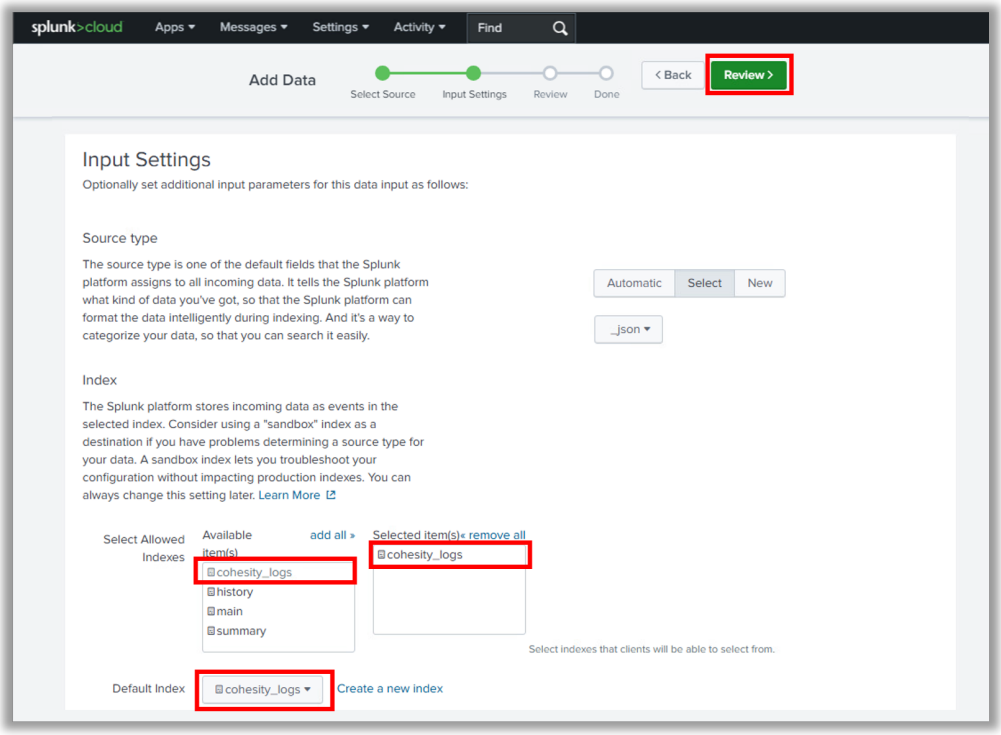
d. Provide a unique **Name** for your token and click **Next.**



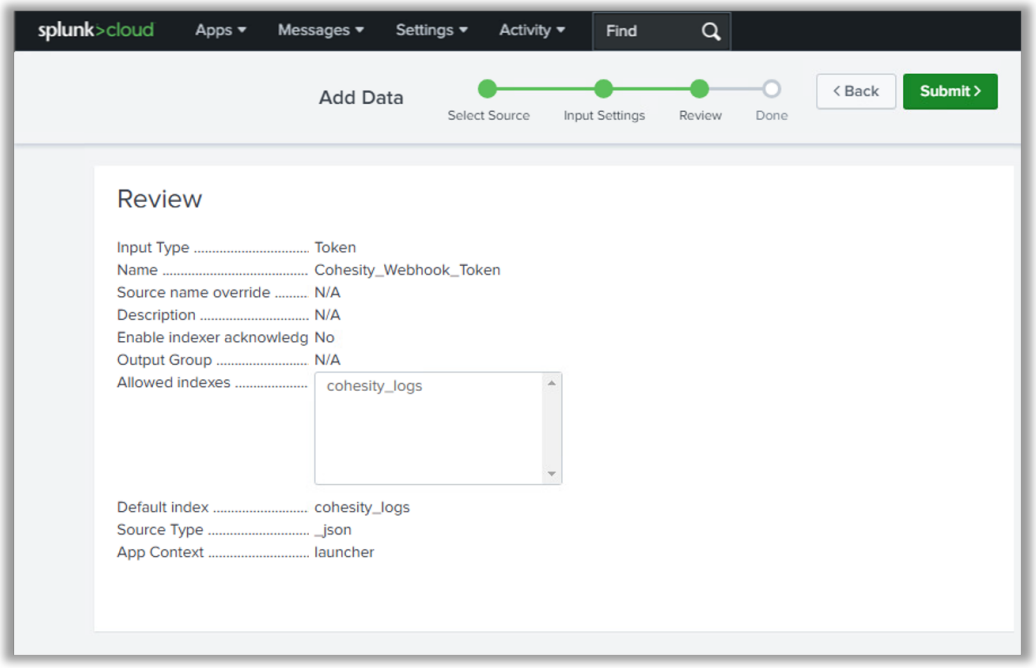
e. Under **Input Settings**, For **Source Type**, choose **Select** and then click **Select Source Type,** Select **_json** from the dropdown. If it is not shown under the dropdown, then type **_json** in search bar to bring it up.



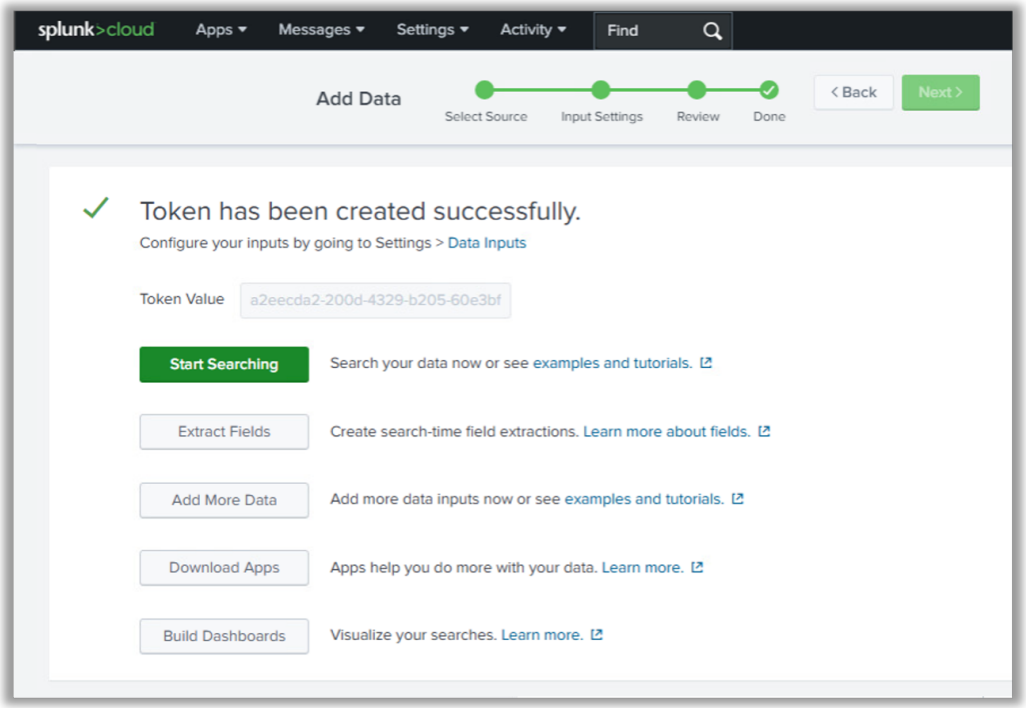
f. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.



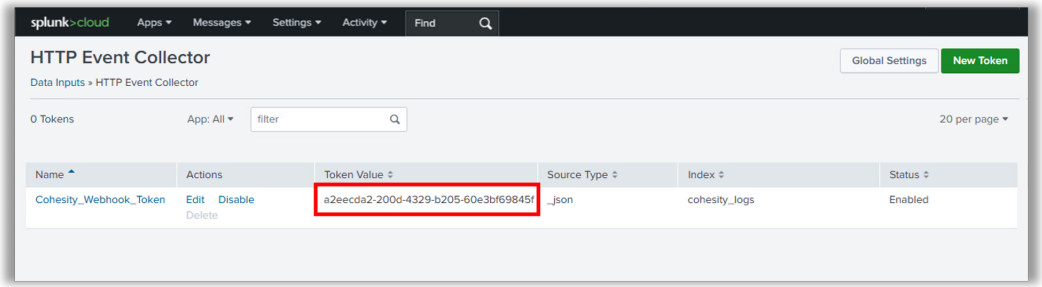
g. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.



h. Click **Submit** to successfully create the token.



i. Once the Token is created, go back to **HTTP Event Collector Page** and verify the Token created. Copy the **Token Value** (Which we will need while configuring the Webhook on Cohesity side).



5. Check HEC endpoint is accessible.

   a. Open the below URL in a browser

   ```
   https://<your_domain>.splunkcloud.com:8088/services/collector/health
   ```

   b. If you get the below json response, then your HEC endpoint is accessible and properly configured

   ```
   {"text":"HEC is healthy","code":17}
   ```

   c. If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Revisit previous steps to configure the HEC properly

6. Test HTTP Event Collector on any system.

   d. Test the HTTP Event Collector using a curl request from cmd prompt / terminal on any system as shown below:

   ```
   curl -k "https://<your_domain>.splunkcloud.com:8088/services/collector/raw" \
        -H "Authorization: Splunk <HEC Token>" \
        -H "Content-Type: application/json" \
        -d '{"alert": "Test Alert", "alertId": "0000"}'
   ```

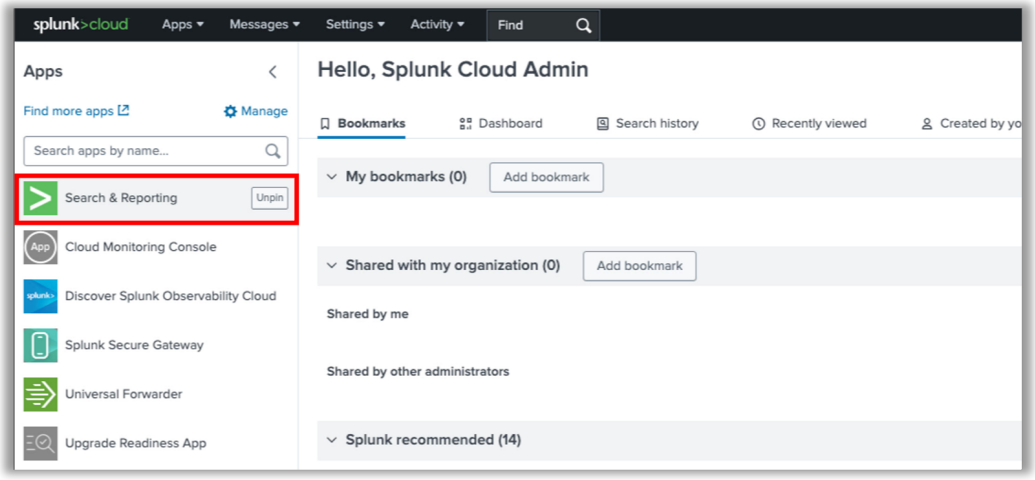
   - Your domain – is your unique domain in your Splunk cloud. The link is same as your Splunk cloud access URL.
   - HEC Token – is the Token Value of the HTTP Event Collector Token you created in previous step.
   - Once the curl command executes successfully, it must return the message *{"text": "Success", "code": "0"}* as shown below:

NOTE:

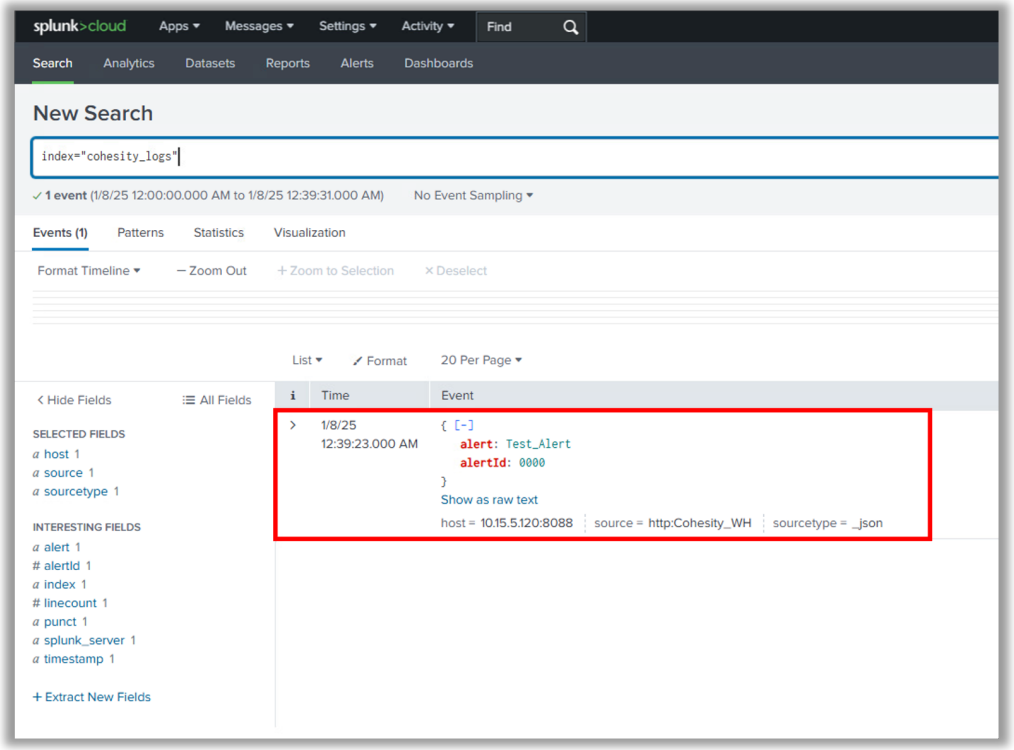
- If you are not receiving the message *{"text": "Success", "code": "0"}* or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration
- Visit Troubleshooting for more details.

e. Verify the data is successfully received on Splunk.

i. From Splunk Web Home console, click Search & Reporting.



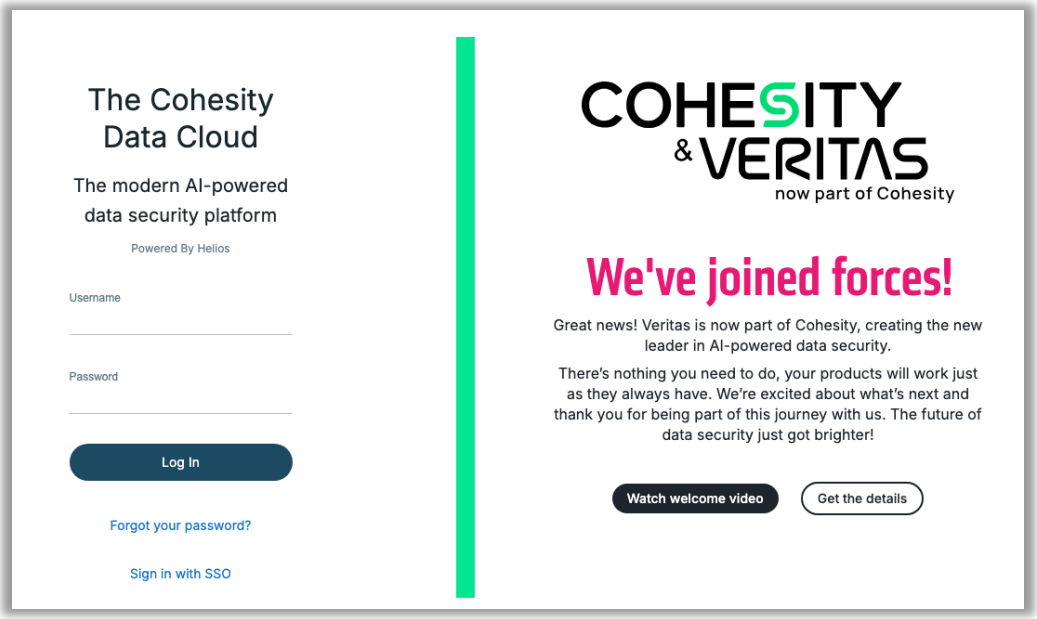
ii. Run search query to filter logs. You must see the event sent by curl command in Splunk.



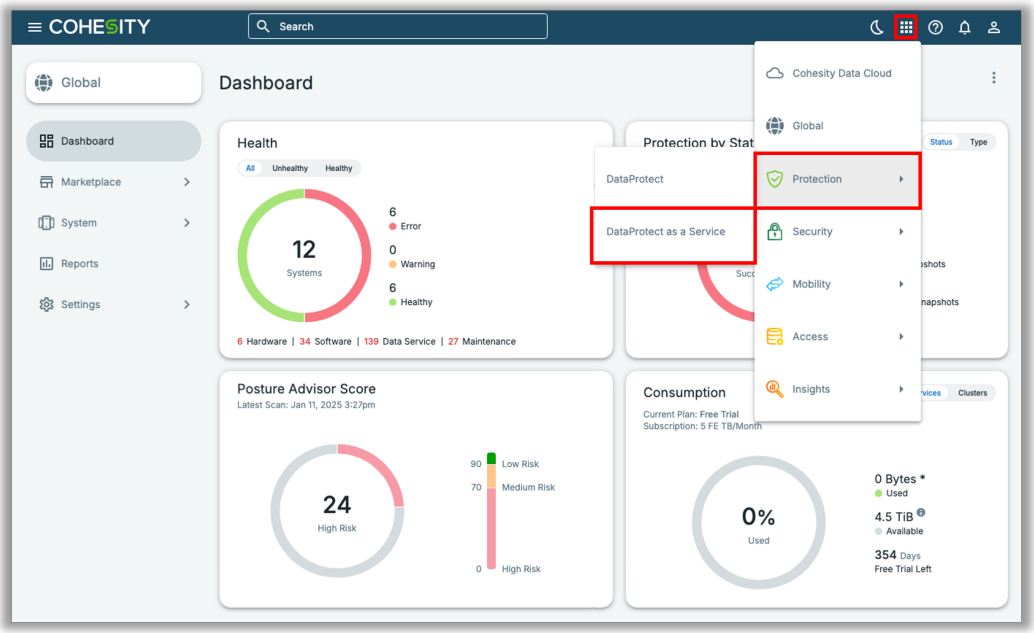
NOTE:

- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit Troubleshooting for more details.

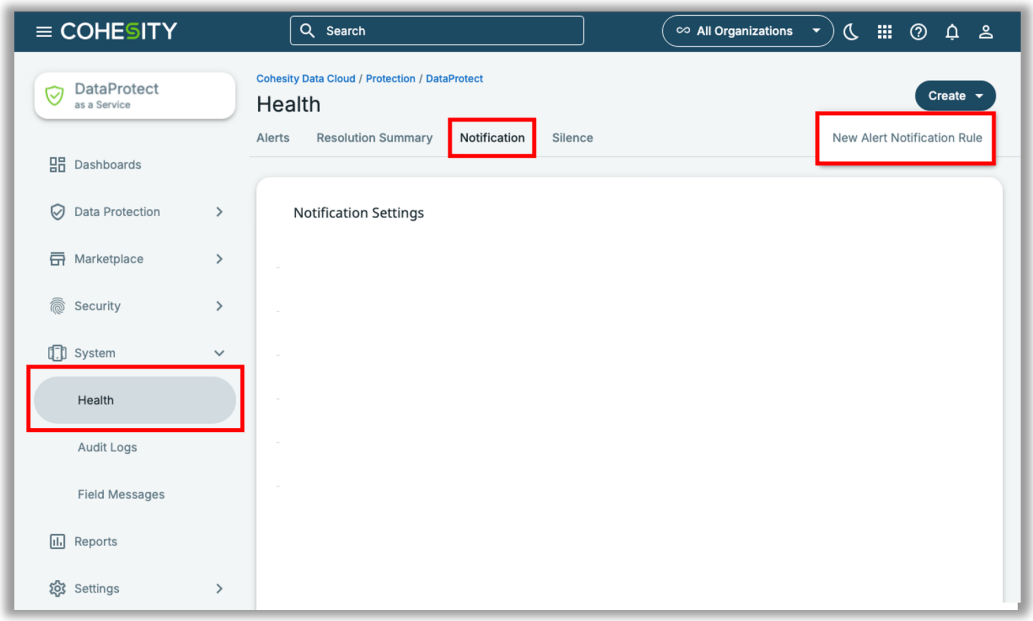
7. Configure alert notification with webhook on Cohesity Data Cloud.
   a. Login to Cohesity Data Cloud.



   b. Go to **DataProtect as a Service** under **Protection.**



c. Click **Health** > **Notification** and then **Create** > **New Alert Notification Rule.**



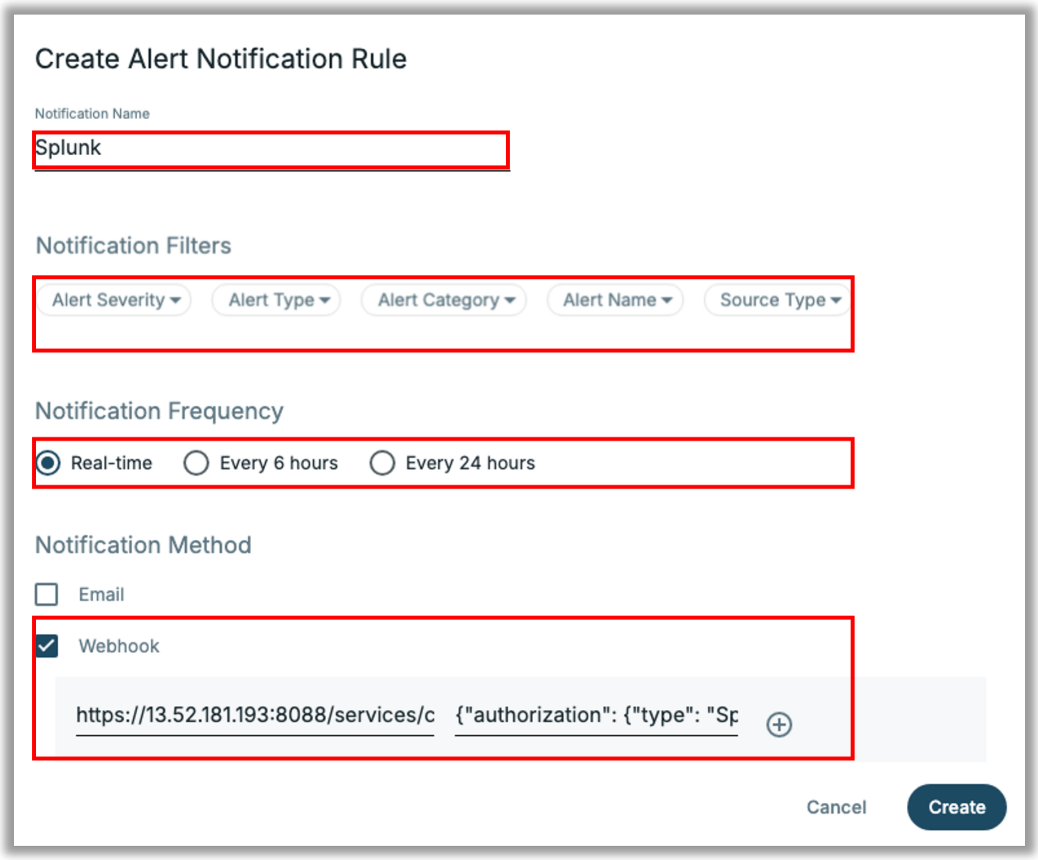
d. Provide the **Notification Name**, Select the **Notification Filters** and **Notification Frequency**, choose **Webhook** as the **Notification Method** and provide the Webhook **URL** and **Options** as below:

URL:
https://<Your Domain>.splunkcloud.com:8088/services/collector/raw

Options:
{"authorization": {"type": "Splunk","credentials": "*<HEC Token>*"}}

NOTE For Splunk Trials:

- Alert notifications from Cohesity to Splunk via Webhook requires a valid certificate at the Splunk side.
- Splunk trials might use expired/invalid certificates, which may lead to TLS certificate verification failure, in which case the alert notifications will not be sent from Cohesity to Splunk.
- Contact Splunk support to get your certificate issue resolved.

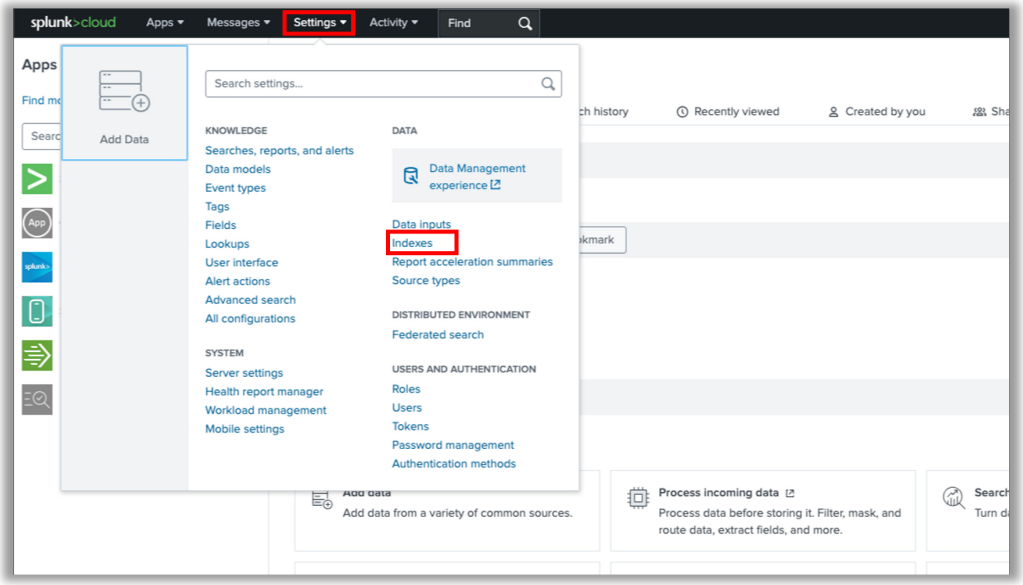


NOTE:

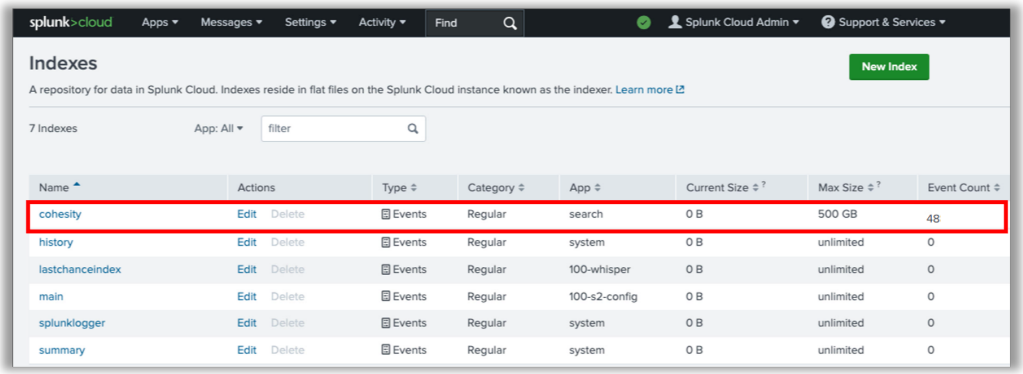
- Use Alert Severity, Alert Type, Alert Category, Alert Name or Source Type to filter out the selective alerts you want to send to Splunk.
- If you do not select any value for Alert Severity, Alert Type, Alert Category, Alert Name or Source Type, then all the alerts generated by Cohesity will be sent to Splunk.

8. Validate data received from Cohesity on Splunk Cloud.

a. Click **Indexes** under **Data** in **Settings.**



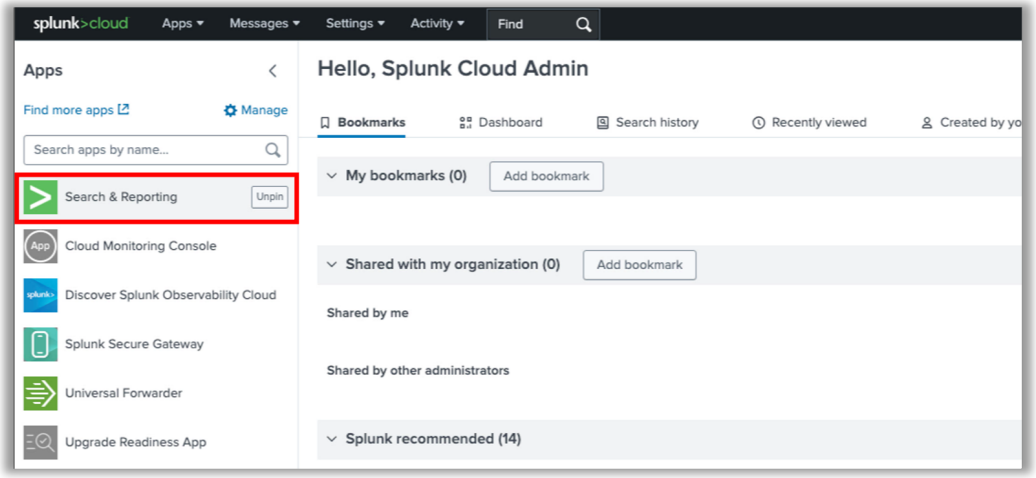
b. Verify logs are being pushed to your index by checking the Event Count.



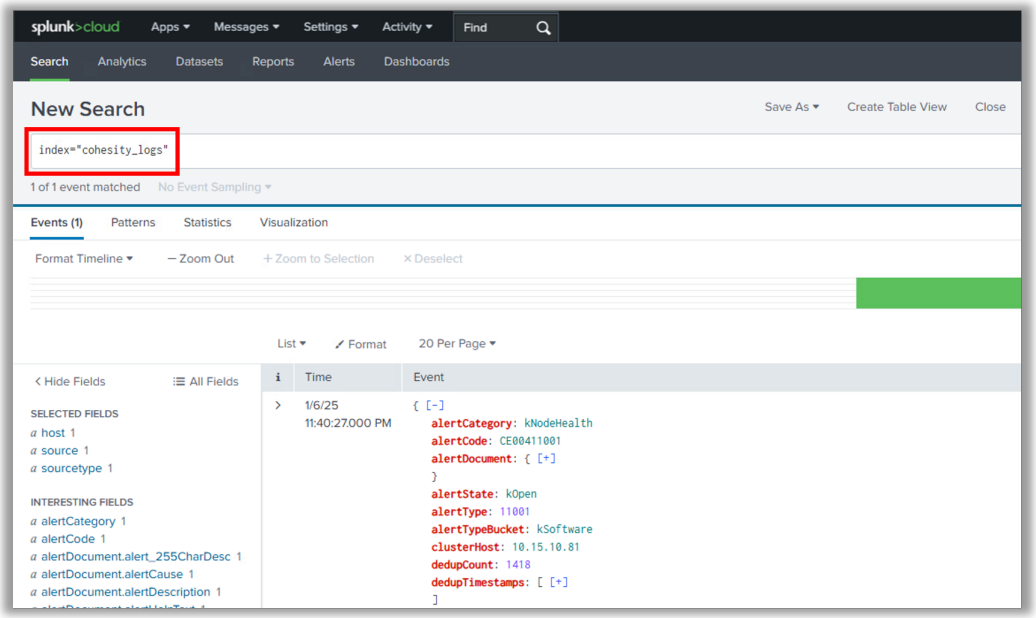
NOTE: Alerts and logs will be pushed from Cohesity to Splunk in real time. However, it is not immediate. Sometimes it takes more time for the data to be transmitted to Splunk. If you are not seeing the events after significant amount of time, then there could be an issue in HEC configuration. Edit your HEC to fix the issue.

9. Search, alert and visualize.

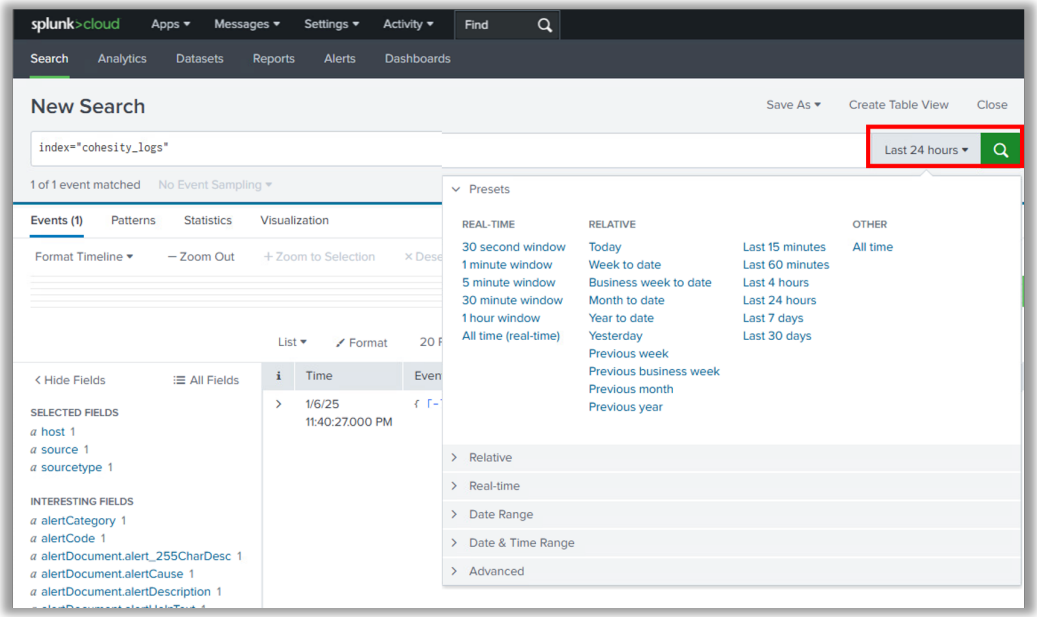
   a. From Splunk Web Home, click Search & Reporting.



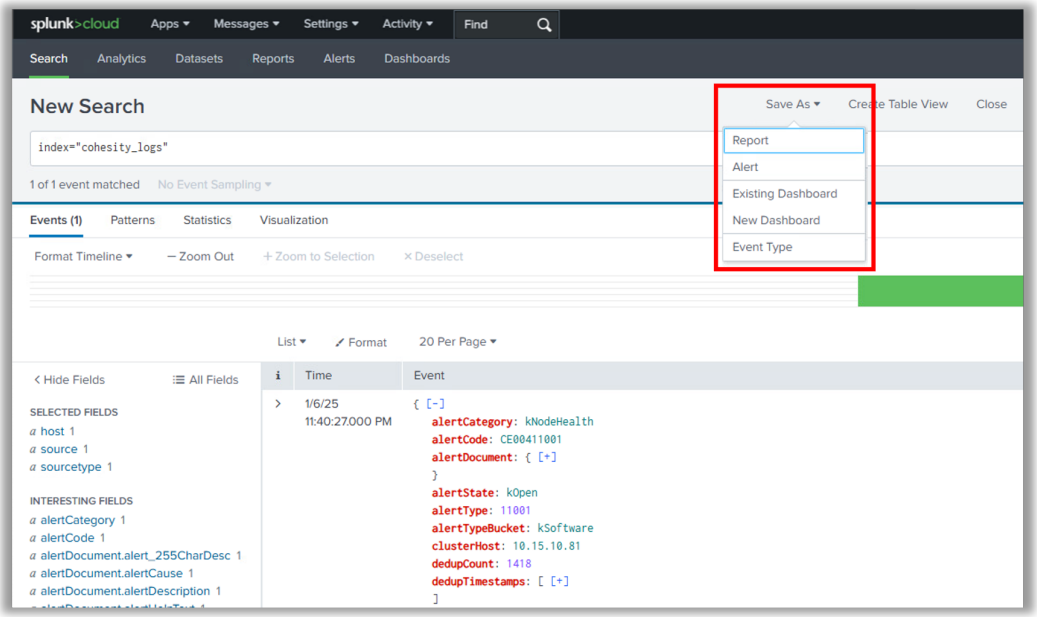
   b. Run search query to filter logs.



c. Filter search results based on time.



d. Alert and visualize.



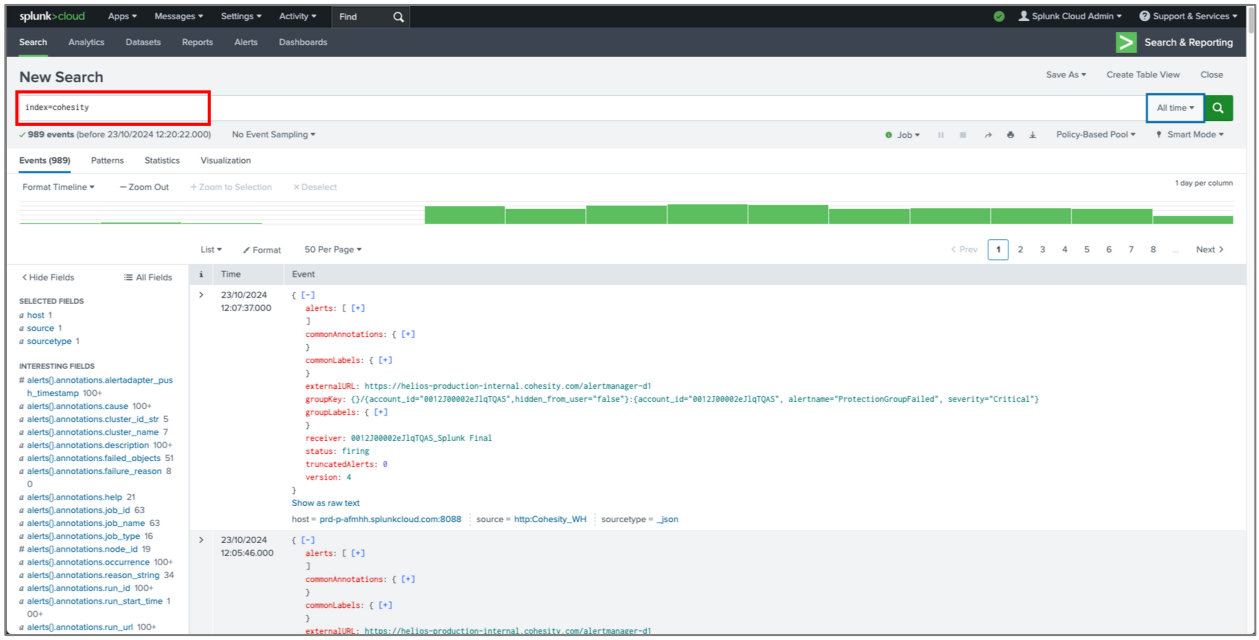
NOTE: **For more details,** refer to the Search and Reporting section.

Search and Reporting

1. **By Index**: Search for data that was sent to a specific index. Use the index that you selected during the HEC token setup.

Search Query
index=<*your_index_name*>

Example
index=”cohesity”

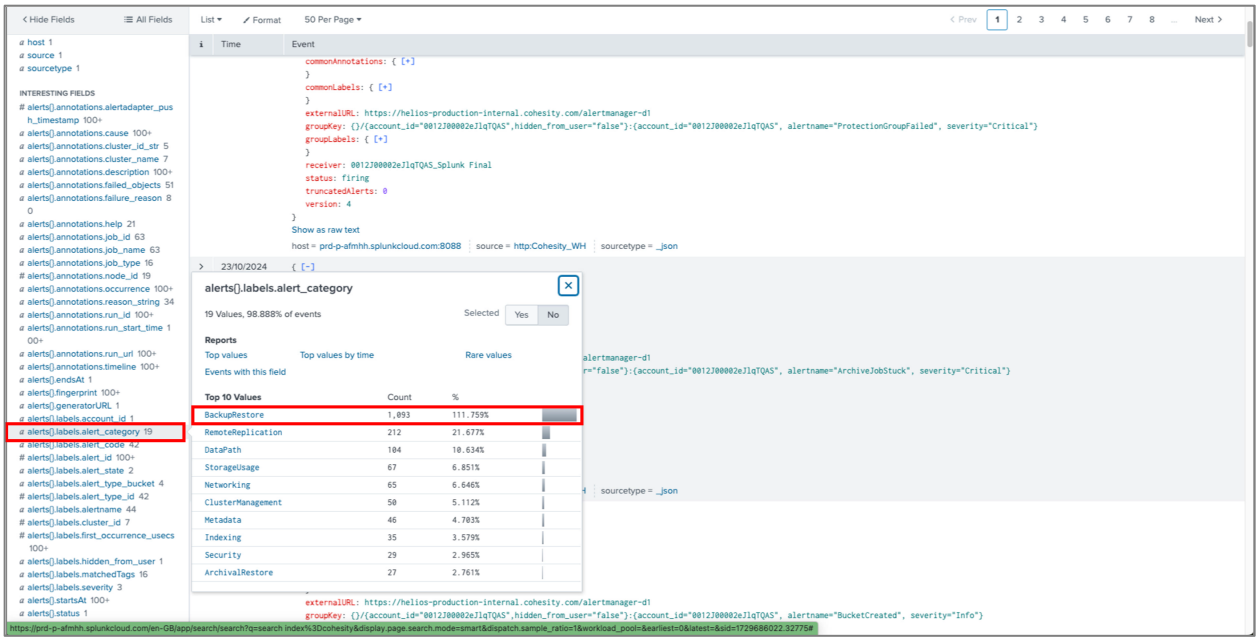


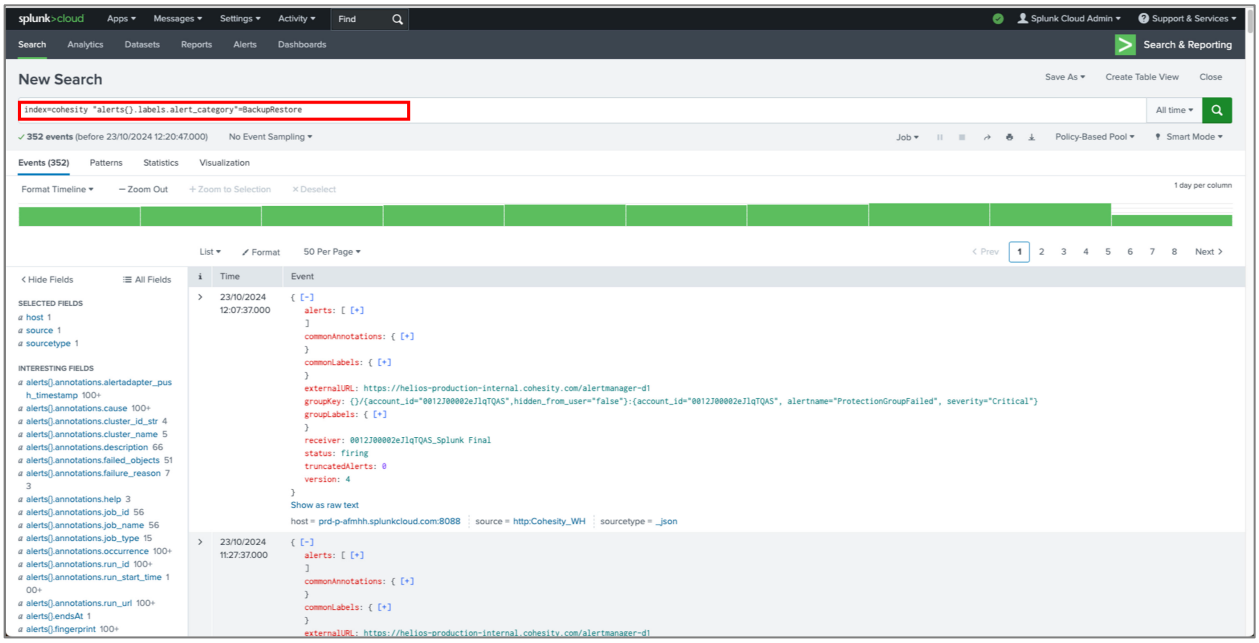
By Alert Category: Search for alerts for a particular Alert Category like “*BackupRestore*”

Search Query
index=<*your_index_name*> “alerts{}.labels.alert_category”=<*alert_category*>

Example
index=”cohesity” “alerts{}.labels.alert_category”=BackupRestore

If you are not sure about the formatting of the search query, then simply click the data on the left tab to frame the search query automatically. In this case click on **alerts{}.labels.alert_category**, which will prompt you with available alert categories, from which you must select the required alert category, which in this case is **BackupRestore.**

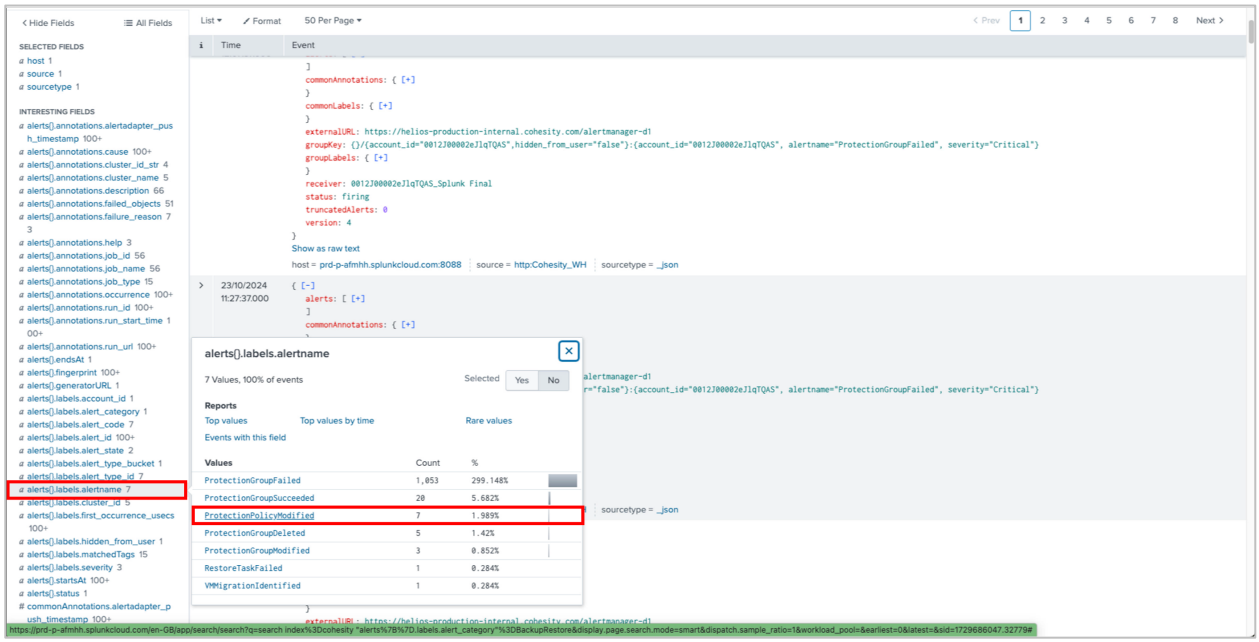

alerts{}.labels.alert_category
19 Values, 98.888% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
BackupRestore 1,093 111.759%
RemoteReplication 212 21.677%
DataPath 104 10.634%
StorageUsage 67 6.851%
Networking 65 6.646%
ClusterManagement 50 5.112%
Metadata 46 4.703%
Indexing 35 3.579%
Security 29 2.965%
ArchivalRestore 27 2.761%

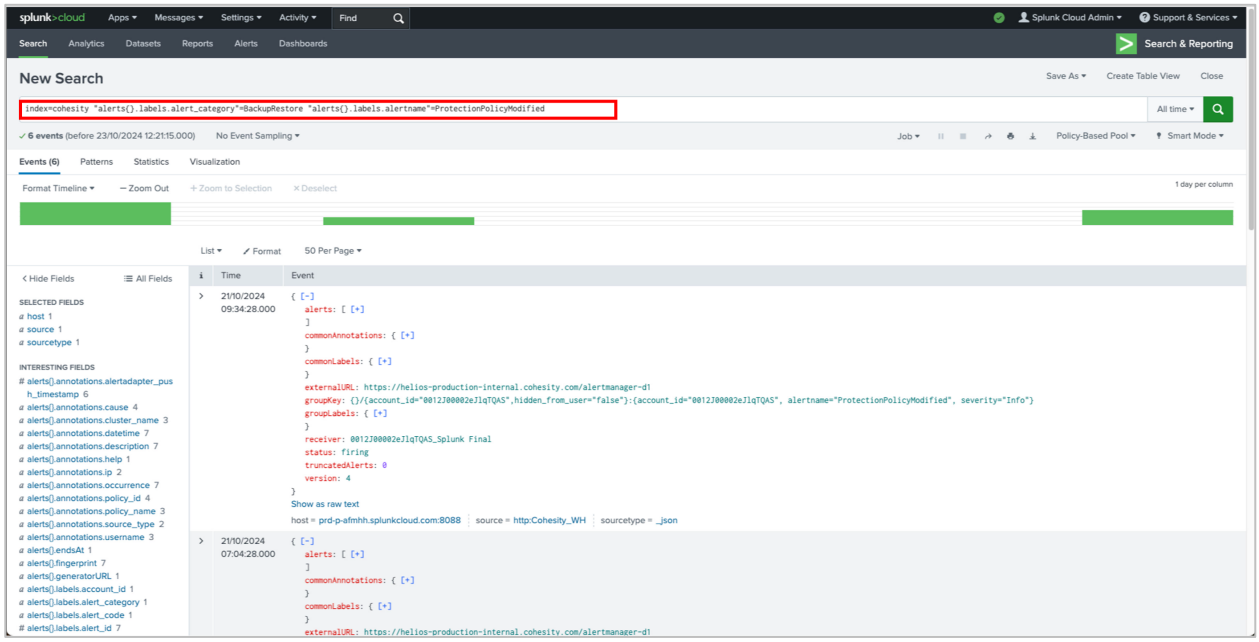

splunk>cloud
Search & Reporting
New Search
index=cohesity "alerts{}.labels.alert_category"=BackupRestore
352 events (before 23/10/2024 12:20:47.000)
Events (352)
Patterns
Statistics
Visualization

2. **By Alert Name**: Search for alerts for a particular Alert Name like "*ProtectionPolicyModified*".

Search Query
index=<*your_index_name*> "alerts{}.labels.alertname"=<*alert_name*>

Example
index="cohesity" "alerts{}.labels.alert_category"=ProtectionPolicyModified

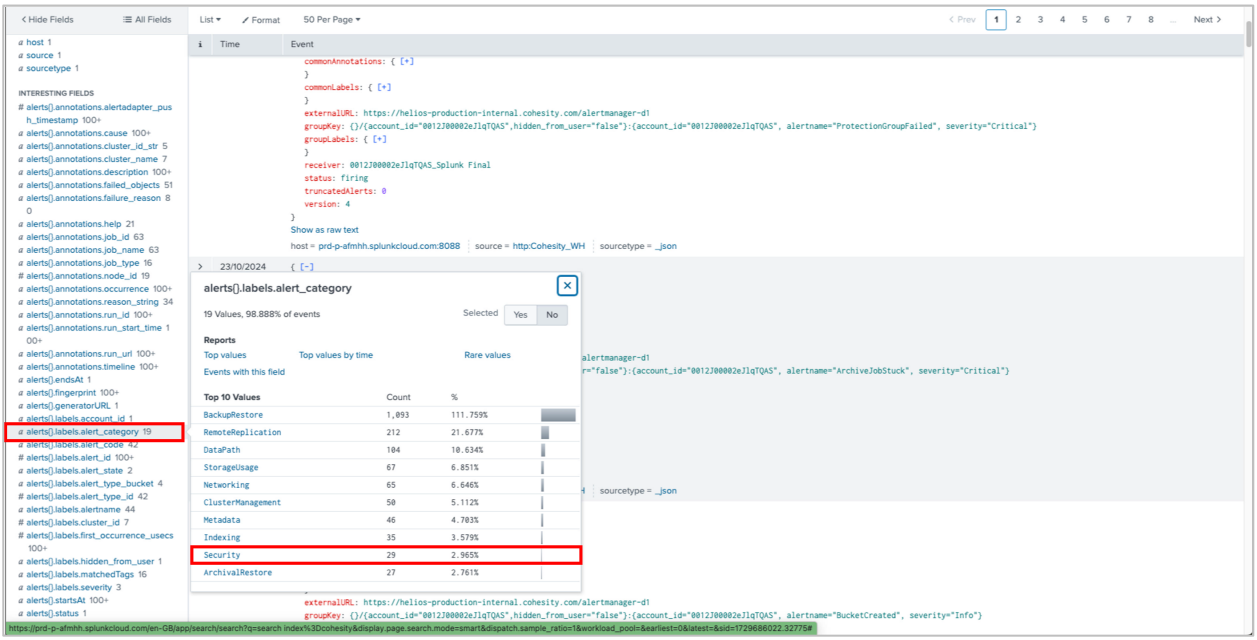


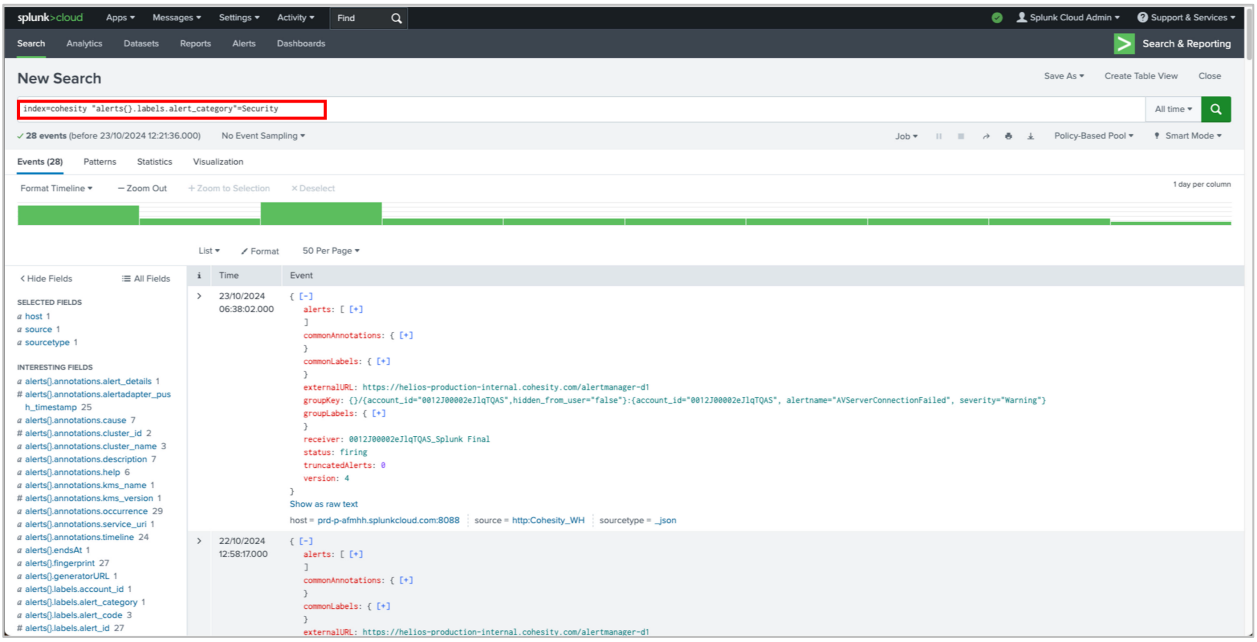


3. **Security Alerts**: Search for All Security alerts.

Search Query
index=<*your_index_name*> “alerts{}.labels.alert_category”=**Security**

Example
index=”cohesity” “alerts{}.labels.alert_category”=Security



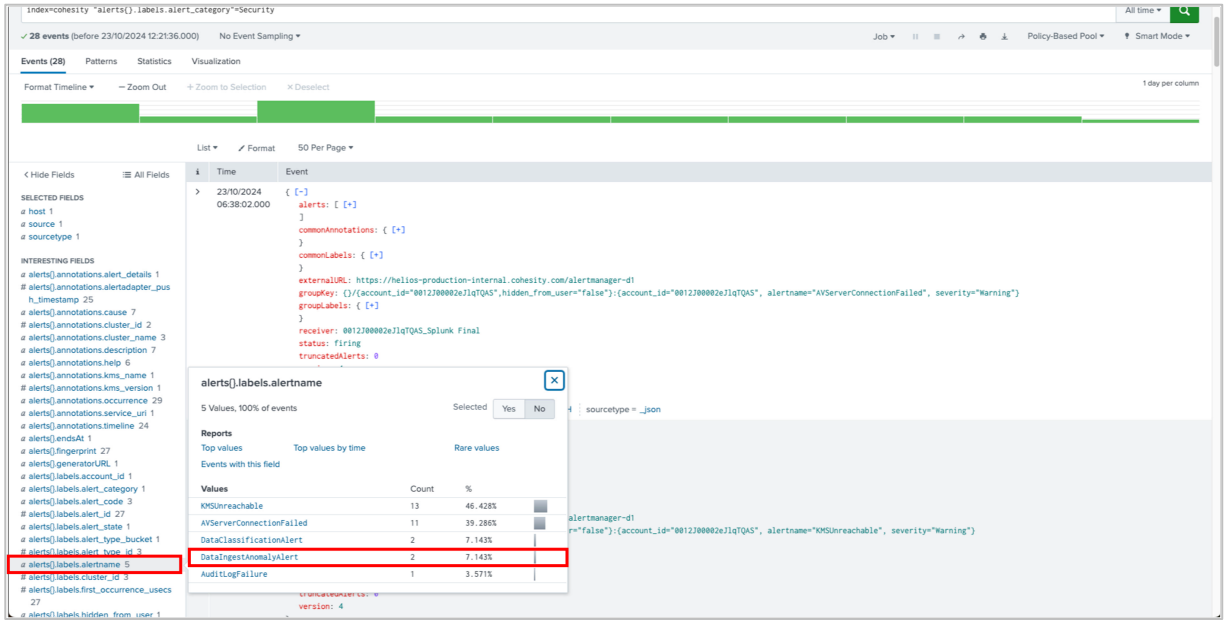


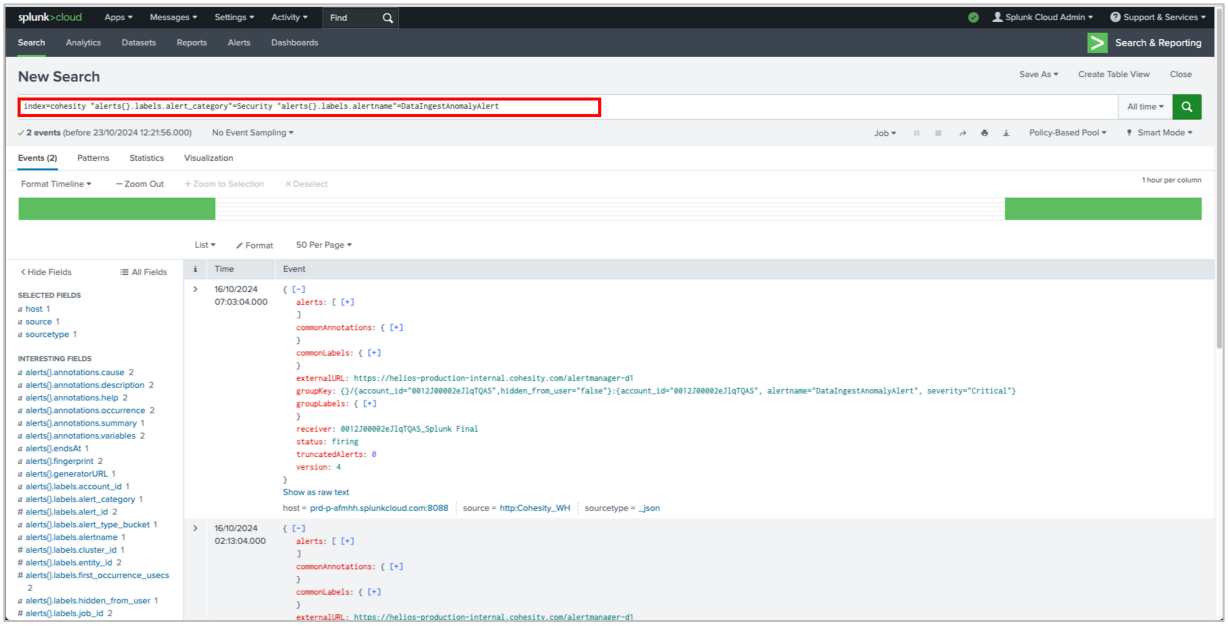
4. **Specific Security Alerts**: Search for particular Security Alerts like "*DataIngestAnomalyAlert*" or "*DataClassificationAlert*".

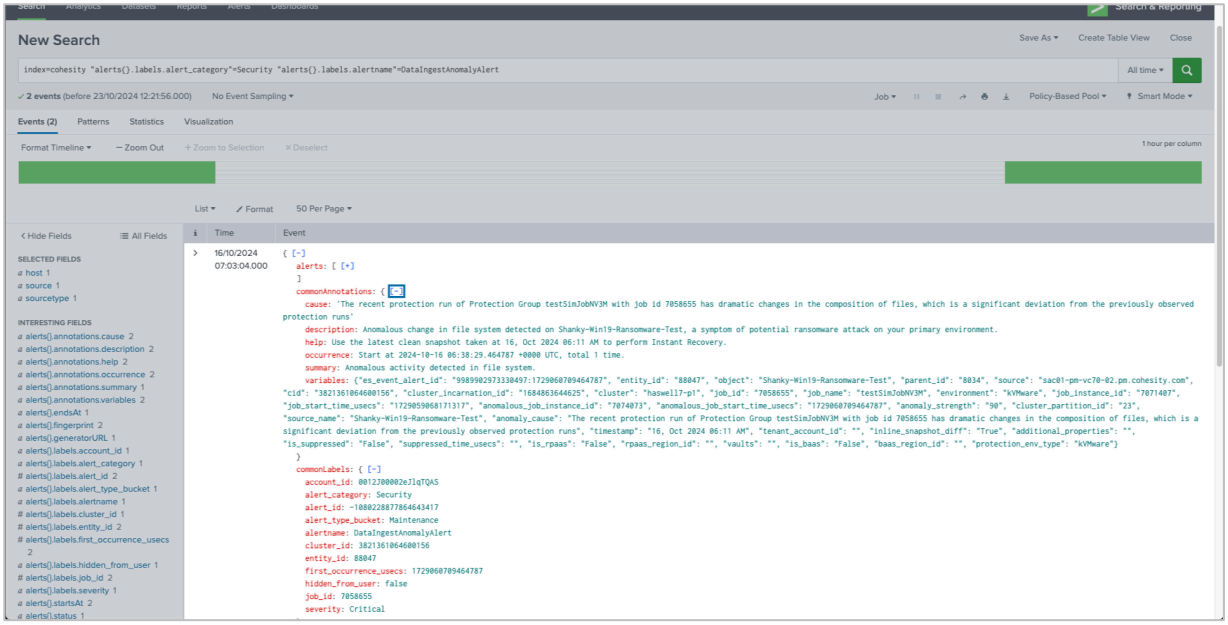
   a. **DataIngestAnomalyAlert**

Search Query
index=*<your_index_name>* "alerts{}.labels.alert_category"=**Security** "alerts{}.labels.alertname"= DataIngestAnomalyAlert

Example
index="cohesity" "alerts{}.labels.alert_category"=Security "alerts{}.labels.alertname"=DataIngestAnomalyAlert



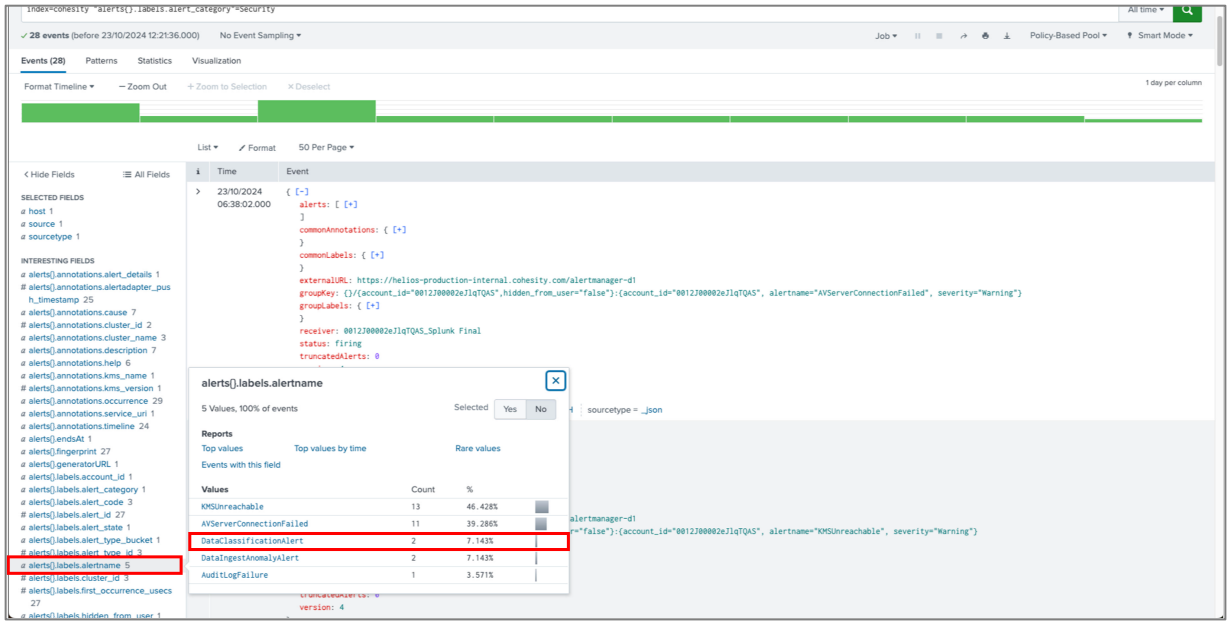


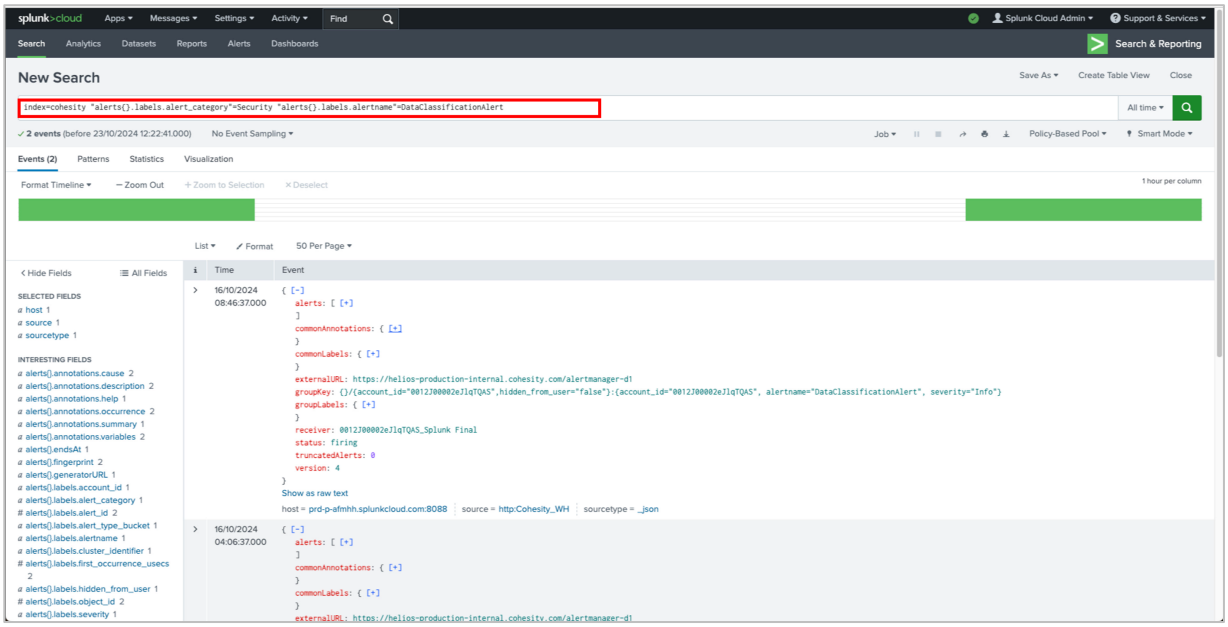


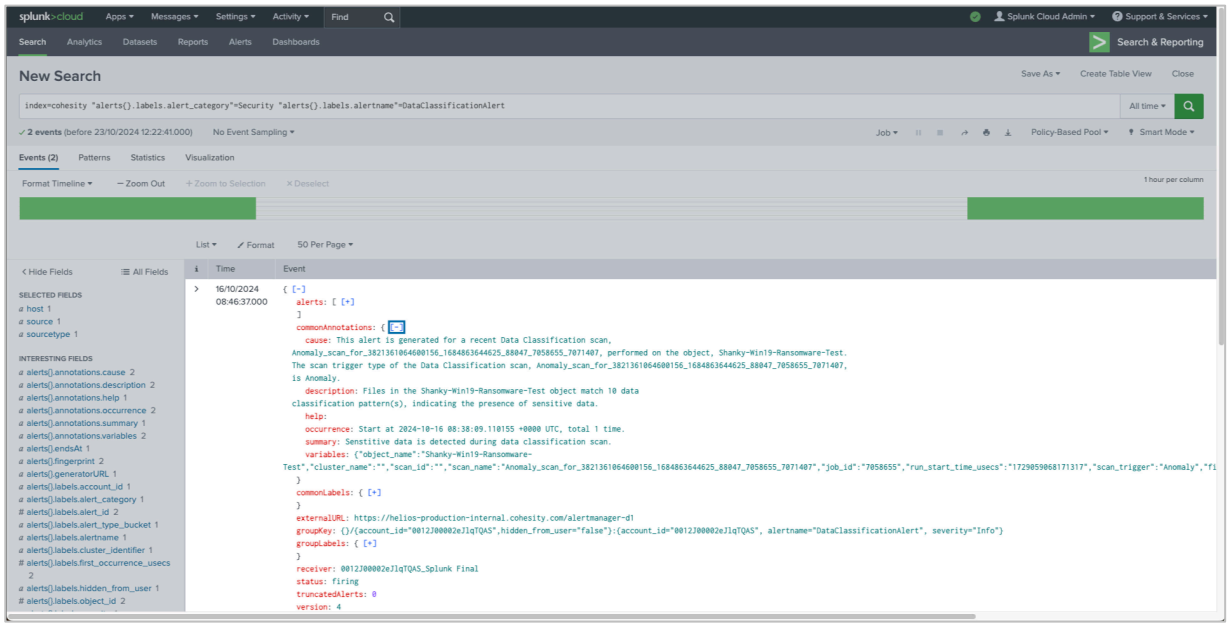
b. **DataClassificationAlert**

Search Query
index=<*your_index_name*> “alerts{}.labels.alert_category”=**Security** “alerts{}.labels.alertname”= DataClassificationAlert

Example
index=”cohesity” “alerts{}.labels.alert_category”=Security “alerts{}.labels.alertname”=DataClassificationAlert


index=cohesity "alerts{}.labels.alert_category"=Security
28 events (before 23/10/2024 12:21:36.000)
No Event Sampling
Events (28)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 day per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
alerts{}.annotations.alert_details 1
alerts{}.annotations.alertadapter_push_timestamp 25
alerts{}.annotations.cause 7
alerts{}.annotations.cluster_id 2
alerts{}.annotations.cluster_name 3
alerts{}.annotations.description 7
alerts{}.annotations.help 6
alerts{}.annotations.kms_name 1
alerts{}.annotations.kms_version 1
alerts{}.annotations.occurrence 29
alerts{}.annotations.service_url 1
alerts{}.annotations.timeline 24
alerts{}.endsAt 1
alerts{}.fingerprint 27
alerts{}.generatorURL 1
alerts{}.labels.account_id 1
alerts{}.labels.alert_category 1
alerts{}.labels.alert_code 3
alerts{}.labels.alert_id 27
alerts{}.labels.alert_state 1
alerts{}.labels.alert_type_bucket 1
alerts{}.labels.alert_type_id 3
alerts{}.labels.alertname 5
alerts{}.labels.cluster_id 3
alerts{}.labels.first_occurrence_usecs 27
Time
Event
23/10/2024 06:38:02.000
alerts{}.labels.alertname
5 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
KMSUnreachable 13 46.428%
AVServerConnectionFailed 11 39.286%
DataClassificationAlert 2 7.143%
DataIngestAnomalyAlert 2 7.143%
AuditLogFailure 1 3.571%
sourcetype = _json


splunk>cloud
Apps
Messages
Settings
Activity
Find
Splunk Cloud Admin
Support & Services
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=cohesity "alerts{}.labels.alert_category"=Security "alerts{}.labels.alertname"=DataClassificationAlert
All time
2 events (before 23/10/2024 12:22:41.000)
No Event Sampling
Job
Policy-Based Pool
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
alerts{}.annotations.cause 2
alerts{}.annotations.description 2
alerts{}.annotations.help 1
alerts{}.annotations.occurrence 2
alerts{}.annotations.summary 1
alerts{}.annotations.variables 2
alerts{}.endsAt 1
alerts{}.fingerprint 2
alerts{}.generatorURL 1
alerts{}.labels.account_id 1
alerts{}.labels.alert_category 1
alerts{}.labels.alert_id 2
alerts{}.labels.alert_type_bucket 1
alerts{}.labels.alertname 1
alerts{}.labels.cluster_identifier 1
alerts{}.labels.first_occurrence_usecs 2
alerts{}.labels.hidden_from_user 1
alerts{}.labels.object_id 2
alerts{}.labels.severity 1
Time
Event
16/10/2024 08:46:37.000
externalURL: https://helios-production-internal.cohesity.com/alertmanager-d1
groupKey: {}/{account_id="0012J00002eJlqTQAS",hidden_from_user="false"}:{account_id="0012J00002eJlqTQAS", alertname="DataClassificationAlert", severity="Info"}
receiver: 0012J00002eJlqTQAS_Splunk Final
status: firing
truncatedAlerts: 0
version: 4
Show as raw text
host = prd-p-afmhh.splunkcloud.com:8088
source = http:Cohesity_WH
sourcetype = _json
16/10/2024 04:06:37.000


splunk>cloud
Apps
Messages
Settings
Activity
Find
Splunk Cloud Admin
Support & Services
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=cohesity "alerts{}.labels.alert_category"=Security "alerts{}.labels.alertname"=DataClassificationAlert
All time
2 events (before 23/10/2024 12:22:41.000)
No Event Sampling
Job
Policy-Based Pool
Smart Mode
Events (2)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
alerts{}.annotations.cause 2
alerts{}.annotations.description 2
alerts{}.annotations.help 1
alerts{}.annotations.occurrence 2
alerts{}.annotations.summary 1
alerts{}.annotations.variables 2
alerts{}.endsAt 1
alerts{}.fingerprint 2
alerts{}.generatorURL 1
alerts{}.labels.account_id 1
alerts{}.labels.alert_category 1
alerts{}.labels.alert_id 2
alerts{}.labels.alert_type_bucket 1
alerts{}.labels.alertname 1
alerts{}.labels.cluster_identifier 1
alerts{}.labels.first_occurrence_usecs 2
alerts{}.labels.hidden_from_user 1
alerts{}.labels.object_id 2
Time
Event
16/10/2024 08:46:37.000
{ [-]
alerts: [[+]
]
commonAnnotations: { [-]
cause: This alert is generated for a recent Data Classification scan, Anomaly_scan_for_3821361064600156_1684863644625_88047_7058655_7071407, performed on the object, Shanky-Win19-Ransomware-Test. The scan trigger type of the Data Classification scan, Anomaly_scan_for_3821361064600156_1684863644625_88047_7058655_7071407, is Anomaly.
description: Files in the Shanky-Win19-Ransomware-Test object match 10 data classification pattern(s), indicating the presence of sensitive data.
help:
occurrence: Start at 2024-10-16 08:38:09.110155 +0000 UTC, total 1 time.
summary: Senstitive data is detected during data classification scan.
variables: {"object_name":"Shanky-Win19-Ransomware-Test","cluster_name":"","scan_id":"","scan_name":"Anomaly_scan_for_3821361064600156_1684863644625_88047_7058655_7071407","job_id":"7058655","run_start_time_usecs":"1729059068171317","scan_trigger":"Anomaly","fi
}
commonLabels: { [+]
}
externalURL: https://helios-production-internal.cohesity.com/alertmanager-d1
groupKey: {}/{account_id="0012J00002eJlqTQAS",hidden_from_user="false"}:{account_id="0012J00002eJlqTQAS", alertname="DataClassificationAlert", severity="Info"}
groupLabels: { [+]
}
receiver: 0012J00002eJlqTQAS_Splunk Final
status: firing
truncatedAlerts: 0
version: 4

Troubleshooting

If alerts are not received at Splunk, ensure the Webhook URL, HEC Token and data format are correct

- **Verify HEC is enabled**: Ensure HTTP Event Collector (HEC) is enabled in Global Settings.
  - Go to **Settings** > **Data Inputs** > **HTTP Event Collector.**
  - Check Global Settings and ensure that All Tokens is set to Enabled.
- Check HEC endpoint is accessible:
  - Open the below URL in a browser.

    For Splunk Enterprise
    https://<your_splunk_ip>:8088/services/collector/health

    For Splunk Cloud
    https://<your_splunk_cloud_domain>:8088/services/collector/health
  - If you get the below json response, then your HEC endpoint is accessible and properly configured.

    ```
    {"text":"HEC is healthy","code":17}
    ```
  - If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Try with HTTP (non-SSL version of URL) instead of HTTPS, and if it works then the issue is specific to SSL/TLS.
- **Check Splunk's Internal Logs** for any errors related to data ingestion:
  - Run this search to see if there are any issues with HEC:

    ```
    index=_internal sourcetype=”splunkd” “HTTP Event Collector”
    ```
  - This query should show any issues or errors related to the HEC, such as token problems, data format errors or failed data ingestion.
- Monitor Index
  - Check status of your index to ensure that it is receiving data and there is no issue with its storage capacity or retention settings.
  - Navigate to **Settings** > **Data** > **Indexes** and check if your index is ingesting data by verifying the event count. If the index count remains zero, it indicates that data is not being ingested.
- Check for Incorrect Index:
  - Make sure you are searching for the correct index. Try running broad search on all indexes just to confirm.

    ```
    index=*
    ```
- Check if data is arriving in the wrong index:
  - Sometimes, data may be ingested into an unintended index if there's a configuration issue.
  - Search across multiple indexes using the following:

    ```
    index=main OR index=lastchanceindex OR index=history OR <your_custom_index>
    ```
- Confirm Webhook URL Configuration:
  - Double-check your Webhook URL is correct, including HEC token.

- Make sure there are no typos in the URL or Token.

  URL
  For Splunk Enterprise
  https://<your_splunk_ip>:8088:/services/collector/raw

  For Splunk Cloud
  https://<your_splunk_cloud_domain>:8088:/services/collector/raw

  Options:
  {"authorization": {"type": "Splunk","credentials": "<your_HEC_Token>"}}

  - **Protocol**: Use https if HEC is configured for SSL (which is by default).
  - **Port**: The default port for HEC is 8088. Ensure this is the correct port and accessible.
  - **Path**: The path must be **/services/collector/raw**. Any deviation will result in “URL not found” error.

- Check firewall and network:
  - Ensure your Splunk instance is accessible from Cohesity. Ensure there are no network restrictions, firewalls or security rules blocking communication between Cohesity and Splunk.
  - You can use tools like **telnet** to check if **8088** port is open.

    For Splunk Enterprise
    telnet <your_splunk_IP> 8088

    For Splunk Cloud
    telnet <your_splunk_cloud_domain> 8088

  - If this fails, it means that either the Splunk instance is not accessible via that port or network/firewall restrictions are in place.
  - If a firewall, proxy or other network security tool is blocking SSL/TLS traffic on port 8088 then it might require manual approval for outbound connections to port 8088.
- Try different Ports
  - Port 8088 is standard for HEC. If your organization has specific configurations, then check with you IT team for proper port.
- Test from a different network
  - If possible, try connecting from a different network to see if it is a network specific issue.
- Check Permissions and Index Configuration:
  - Ensure that the index you created has the correct permissions and is writable.
  - Go to **Settings** > **Indexes** and check that the index is enabled and has enough disk space.
- Additional Testing:
  - Send a manual test event to the HEC using a tool like cURL or Postman and ensure Splunk is receiving data.

```
For Splunk Enterprise
curl -k “https://<your Splunk IP>:8088/services/collector/raw” \
     -H “Authorization: Splunk <HEC Token>” \
     -H “Content-Type: application/json” \
     -d ‘{“alert”: “Test Alert”, “alertId”: “0000”}’

For Splunk Cloud
curl -k “https://<your Splunk cloud domain >:8088/services/collector/raw” \
     -H “Authorization: Splunk <HEC Token>” \
     -H “Content-Type: application/json” \
     -d ‘{“alert”: “Test Alert”, “alertId”: “0000”}’
```

  - The curl command must return the message *{“text”: “Success”, “code”: “0”}.*
  - If the test event appears in Splunk, and your Cohesity alerts are not appearing, then the issue is with the Webhook configuration.

- Search Time Range:
  - Sometimes events might not appear due to mismatch in the time range being searched. Expand the time range in the search bar to “**All Time**” or “**Last 24 hours**”.
- Contact Support:
  - If everything appears correct, and you still cannot access the HEC endpoint, contact Cohesity Support.

Frequently Asked Questions

Q: Can Cohesity send data to Splunk Enterprise *(On-premises)*?

A: Yes

Q: Can Cohesity send data to Splunk Cloud?

A: Yes

Q: What data can Cohesity send to Splunk?

A: Cohesity can send Alerts and Audit Logs to Splunk

Q: Can Cohesity send Internal Cluster Logs to Splunk?
A: No

Q: Can Cohesity send Activity Logs to Splunk?
A: No

Q: What is the difference between Cohesity add-on and Webhook Integration?

A: Cohesity Add-on is a Splunk app installed on your Splunk enterprise, and it pulls the alerts and logs from individual self-managed cluster; whereas Webhook integration works via HTTP callbacks and pushes alerts and logs from self-managed clusters as well as Cohesity Data Cloud to Splunk.

Q: When should I use Cohesity add-on v/s Webhook Integration?

A: Use Cohesity add-on, only if you have self-managed Cohesity clusters managed locally and are not using Cohesity Data Cloud. For all other scenarios use Webhook integration.

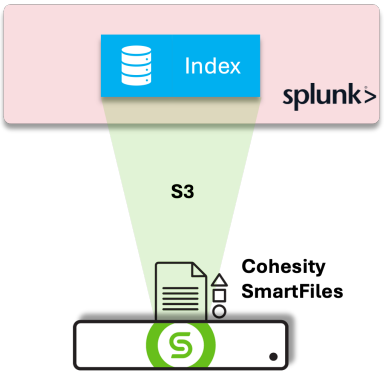
Q: Does Cohesity send Security alerts to Splunk?

A: Yes. Only if you have DataHawk SKUs (ThreatProtection and DataClassification) and are using Cohesity Data Cloud to manage your Cohesity Clusters.

Q: Does this integration work if I am using Splunk trial?

A: Yes, but make sure you have valid certificate at the Splunk side for successful integration. *In case of Splunk cloud, contact Splunk support to get the certificate issue resolved.*

Leveraging Cohesity as a storage for Splunk Enterprise



Cohesity can be used as external storage for Splunk Enterprise to store indexed data.

As indexed data volume increases, demand for scalable storage increases. Splunk SmartStore provides a way to use remote object sources to store indexed data. Cohesity can serve as an object store for Splunk Enterprise to store the indexed data.

For further details refer Leverage Cohesity's Web-Scale Architecture for Splunk.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Shashanka SR, Sr. Solutions Architect - Focuses on Security, Cohesity Gaia and GSI.

Other major contributors include:

- Surya Swaminathan, Security
- Karthick Radhakrishnan, Director, Solution Architecture
- Damien Philip, Field CTO
- Kamal Deka, Product Management
- Eleonor Lee, Product Marketing
- Sudeep Reddy Gaddam, Engineering
- Shubham Kumar, Engineering

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.1	Aug 2025	Republished with latest template.
1.0	Jan 2025	First full release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.