

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

General Information	4
Purpose and Scope	4
Intended Audience	4
How to use this Guide	4
Cohesity and Splunk Integration	5
Overview	5
Integration Types	6
Integration Workflow	7
<i>Cohesity Splunk Add-on Integration Workflow</i>	7
<i>Webhook Integration Workflow</i>	7
Webhook Integration Overview	8
Quick Webhook Integration in 5 Steps	9
Supported Alerts	10
Webhook Integration v/s Cohesity Splunk Add-on	12
Integrate Cohesity with Splunk Enterprise	13
Self-managed Cohesity Clusters	13
<i>Integration via Cohesity add-on</i>	13
<i>Integration via Webhook</i>	24
Cohesity Data Cloud	40
<i>DataProtect [Self-managed clusters managed from Cohesity Data Cloud]</i>	40
<i>DataProtect as a Service [Cohesity SaaS Service]</i>	57
Integrate Cohesity with Splunk Cloud	74
Self-managed Cohesity Clusters	74
Cohesity Data Cloud	90
<i>DataProtect [Self-managed clusters managed from Cohesity Data Cloud]</i>	90
<i>DataProtect as a Service [Cohesity SaaS Service]</i>	107
Search and Reporting	123
Troubleshooting	131

Frequently Asked Questions	134
Leveraging Cohesity as a storage for Splunk Enterprise	135
Your Feedback	136
About the Authors	136
Document Version History	136

Figures

Figure 1: Cohesity and Splunk Integration	5
Figure 2: Cohesity and Splunk Integration Types	6
Figure 3: Cohesity Add-on Integration Workflow	7
Figure 4: Webhook Integration Workflow	7
Figure 5: Webhook Integration Overview	8

Tables

Table 1: Cohesity and Splunk Compatibility Matrix	5
Table 2: Cohesity and Splunk Integration Matrix	6
Table 3: Cohesity-supported Alerts	10
Table 4: Cohesity and Splunk Alert Compatibility Matrix	11
Table 5: Webhook Integration v/s Cohesity Splunk Add-on	12

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

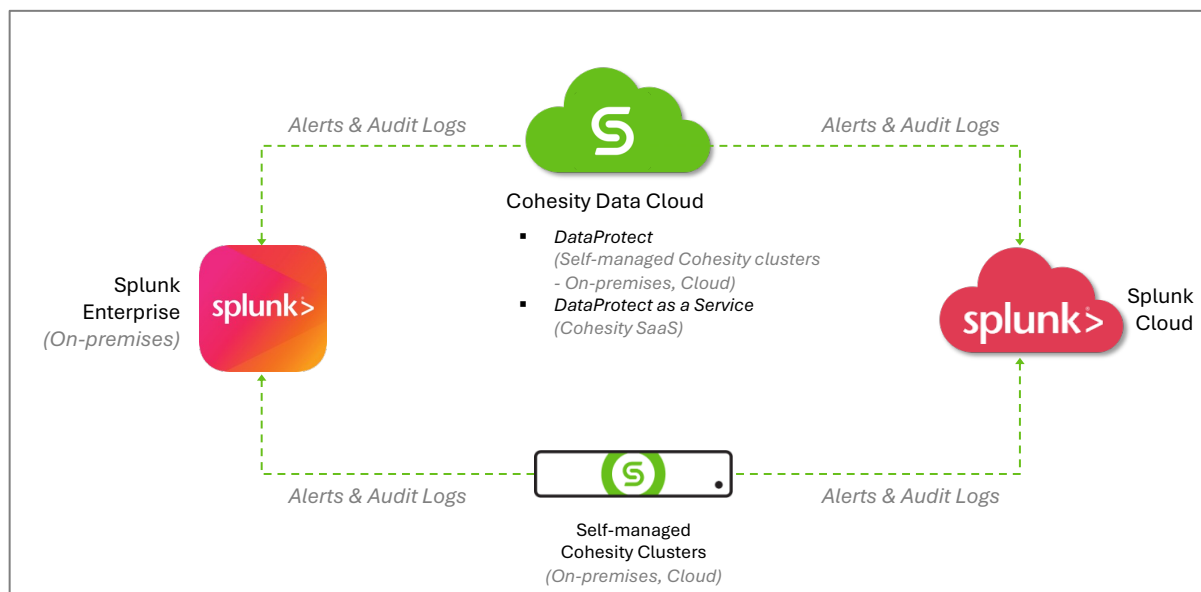


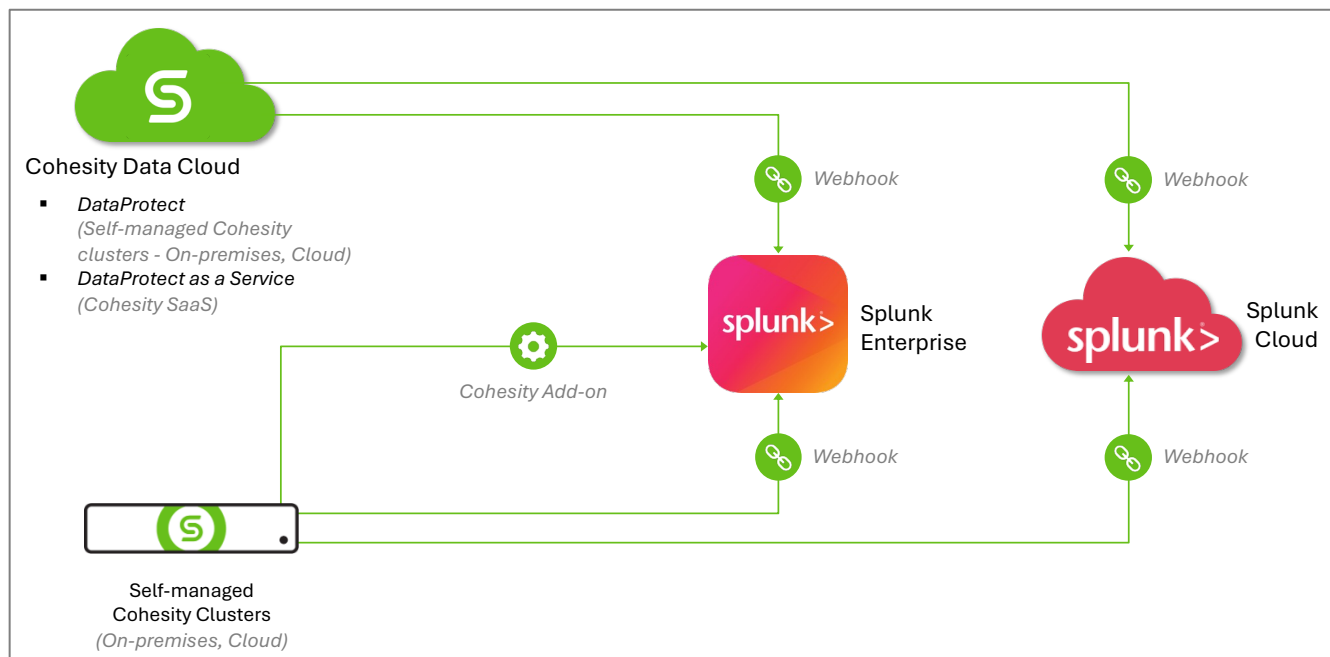
Table 1: Cohesity and Splunk Compatibility Matrix

	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



- 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.
- 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).

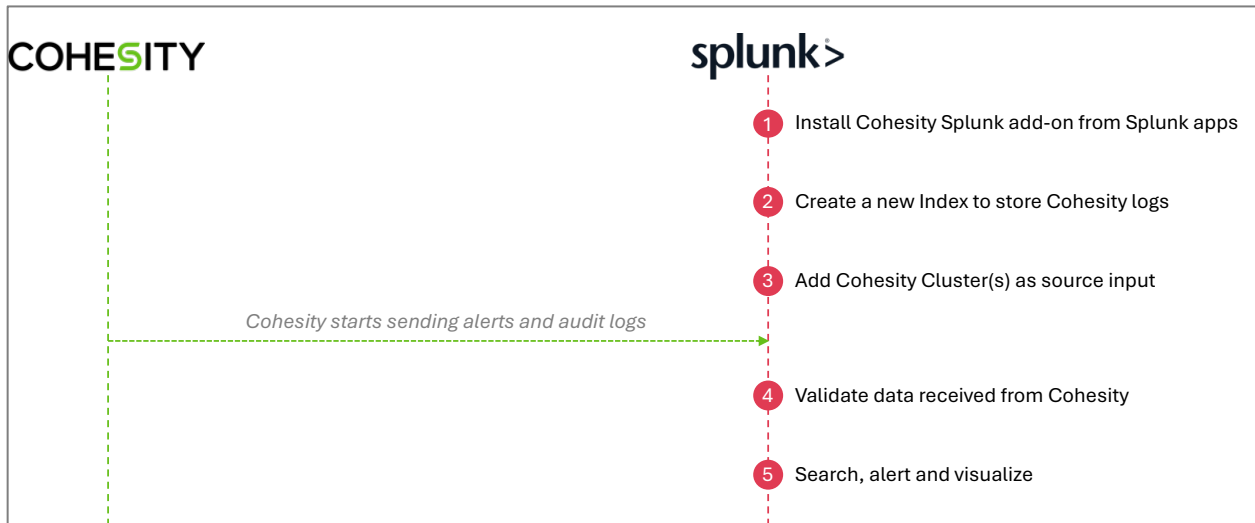
Table 2: Cohesity and Splunk Integration Matrix

		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

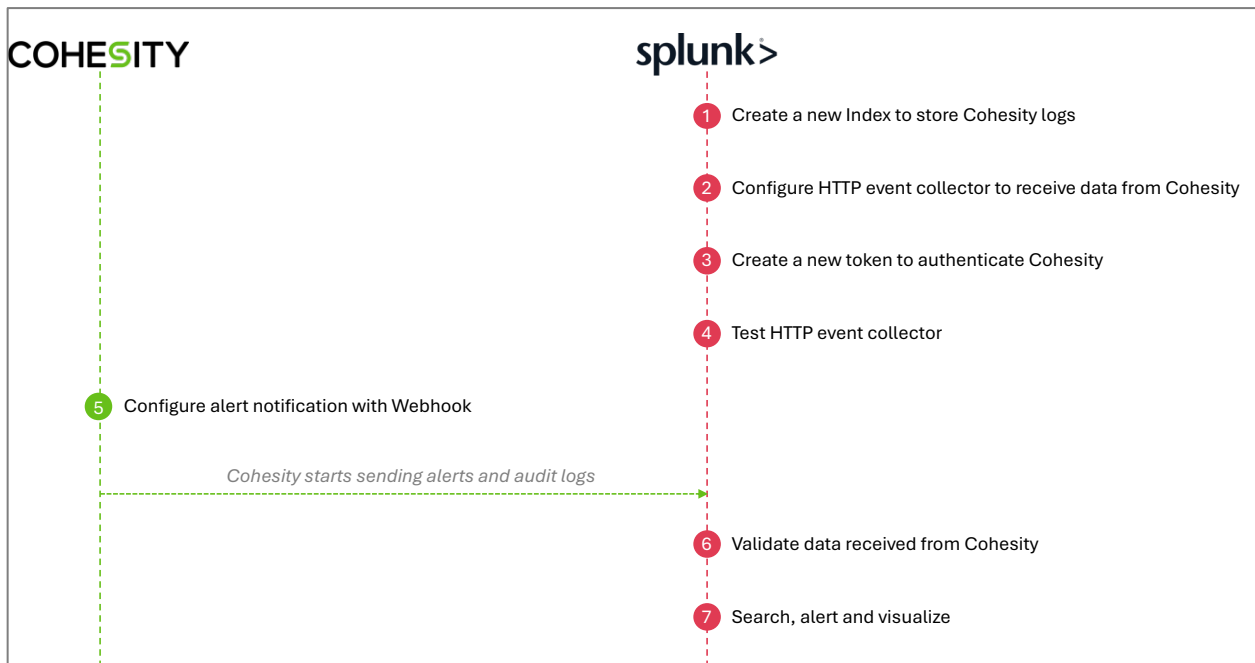
Cohesity Splunk Add-on Integration Workflow

Figure 3: Cohesity Add-on Integration Workflow



Webhook Integration Workflow

Figure 4: Webhook Integration Workflow



Webhook Integration Overview

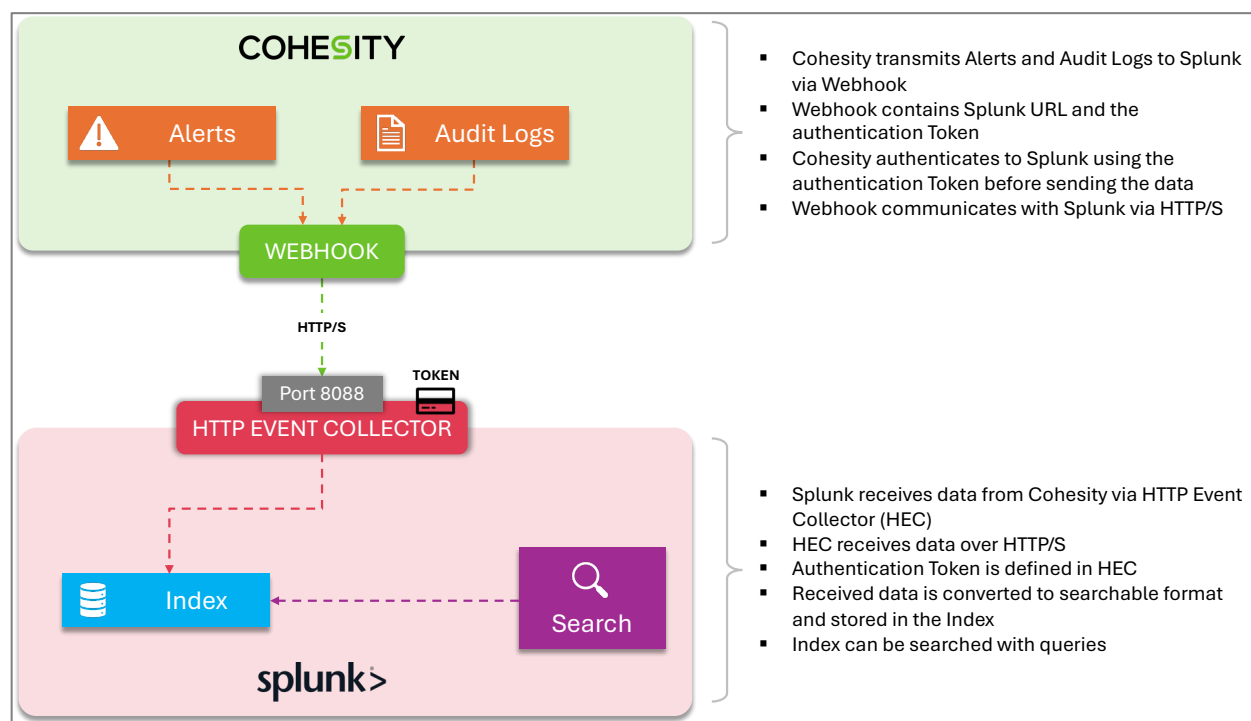
A webhook integration of Cohesity with Splunk requires defining an HTTP Event Collector on the Splunk side and defining a webhook on the Cohesity side. This integration consists of the following components:

- **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 **webhook** 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.
- Click **Search** and **Reporting**.
 - 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		<ul style="list-style-type: none"> Hardware Alerts Software Alerts Data Service Alerts Maintenance Alerts
Cohesity Data Cloud	DataProtect	<ul style="list-style-type: none"> Hardware Alerts Software Alerts Data Service Alerts Maintenance Alerts Security Alerts (Data Ingest Anomaly, Threat Detection, Data Classification)
	DataProtect as a Service	<ul style="list-style-type: none"> 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

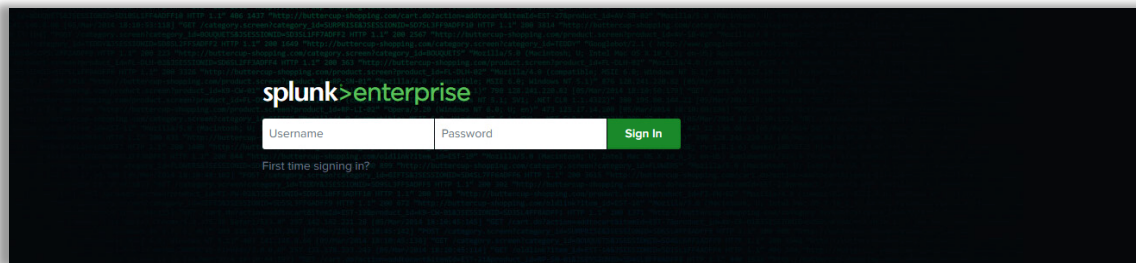
Webhook Integration	Cohesity Splunk Add-on
Uses HTTP Callbacks	Uses REST APIs
Configured at Cohesity side	Configured at Splunk side
Pushes alerts from Cohesity to Splunk	Pulls alerts from Cohesity into Splunk
Works with both Self-managed Cohesity clusters and Cohesity Data Cloud	Works only with Self-managed 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

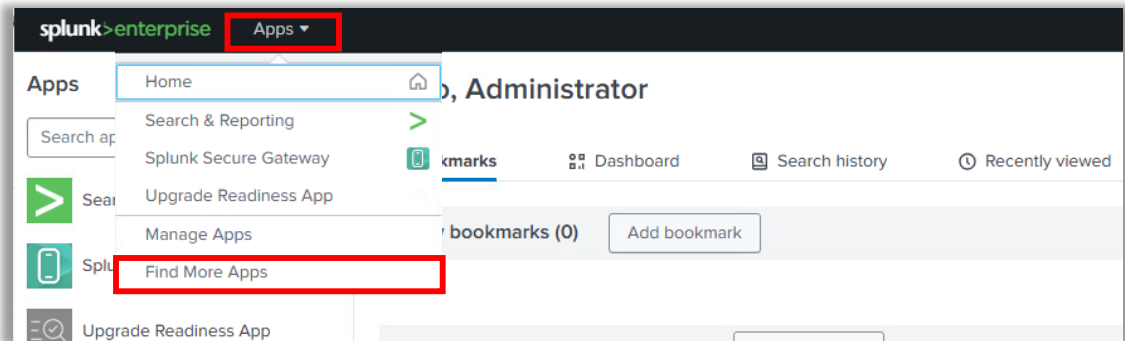
Self-managed Cohesity Clusters

Integration via Cohesity add-on

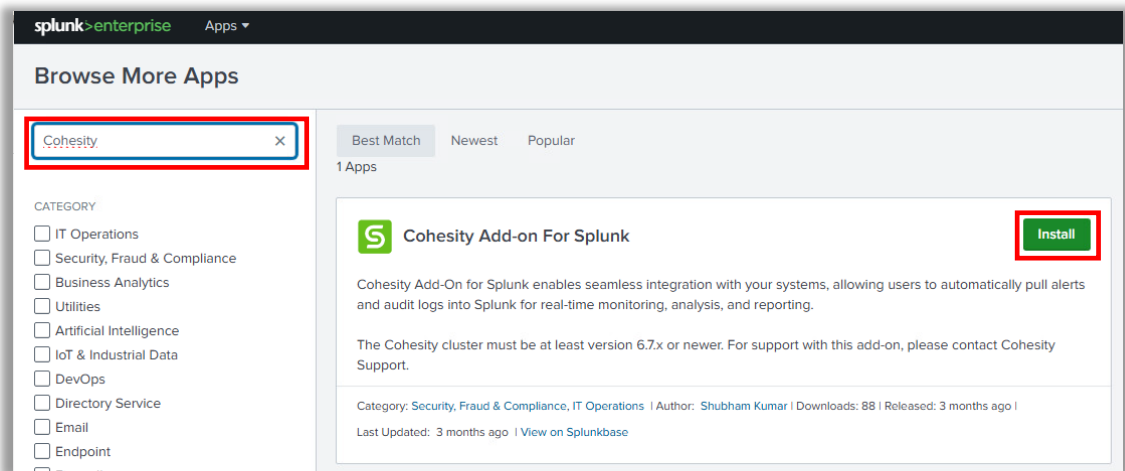
1. Install the Cohesity Splunk Add-on.
 - a. Login to your Splunk Enterprise Instance.



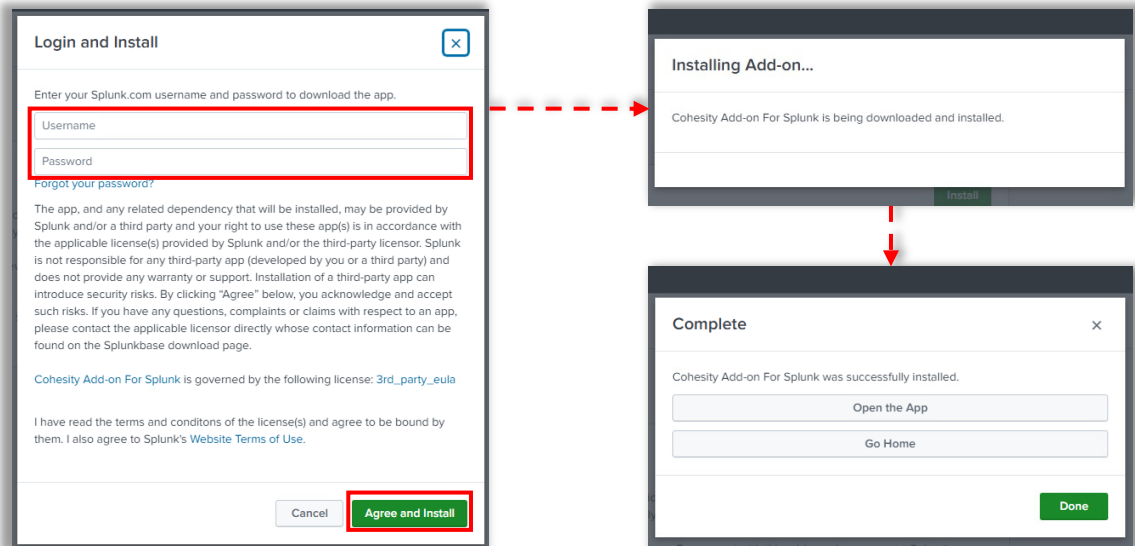
- b. Click **Find More Apps** under **Apps**.



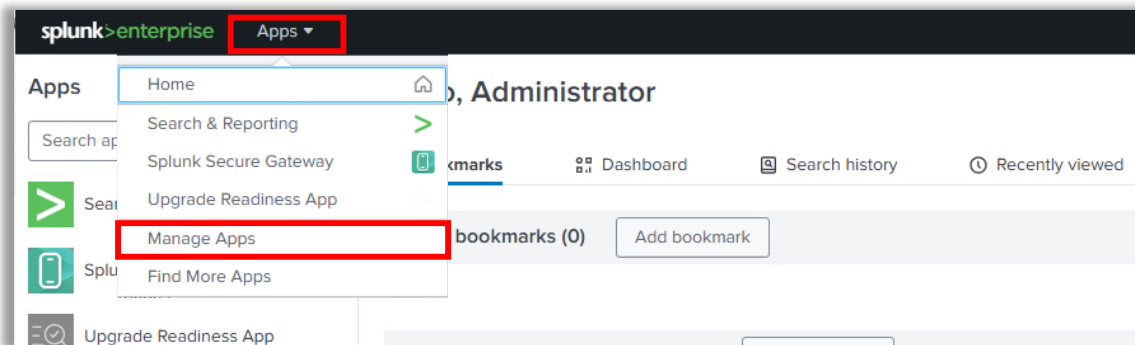
- c. Search for **Cohesity Add-on For Splunk** and click **Install**.



- 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.

Apps

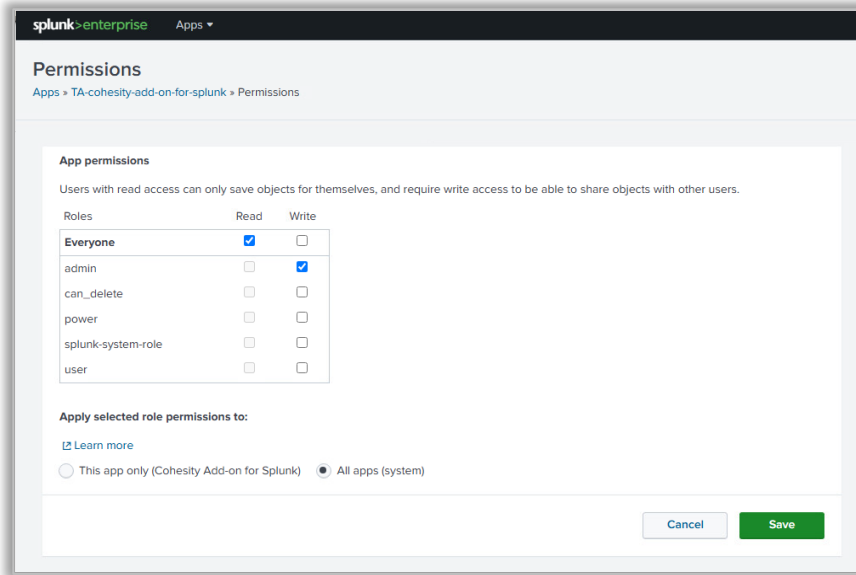
Showing 1-24 of 24 items

filter

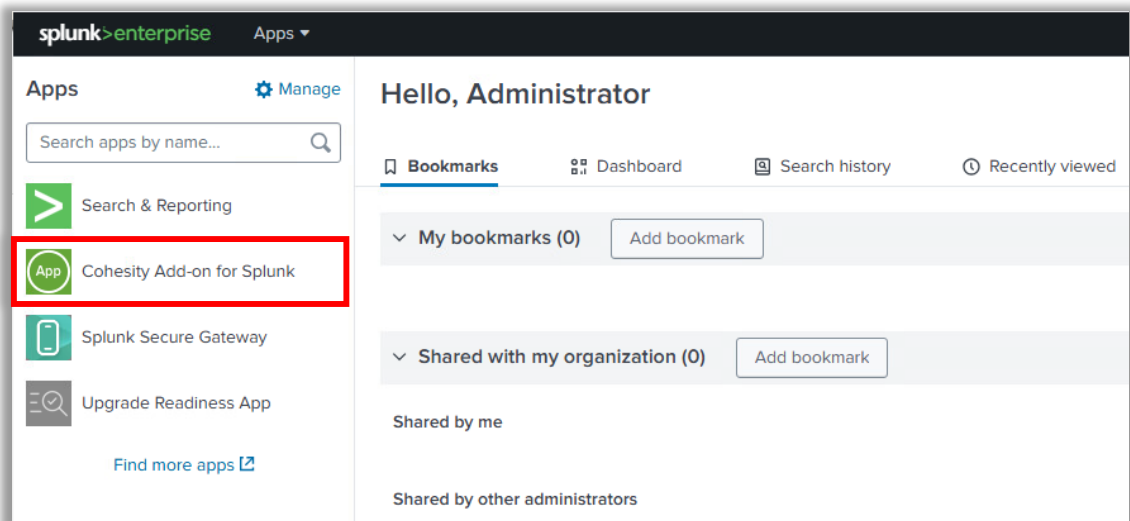
Name	Folder name	Version	Update checking	Visible	Sharing	Status
SplunkDeploymentServerConfig	SplunkDeploymentServerConfig		Yes	No	App Permissions	Enabled Disable
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable
Cohesity Add-on for Splunk	TA-cohesity-add-on-for-splunk	1.1	Yes	Yes	Global Permissions	Enabled Disable
Log Event Alert Action	alert_logevent	9.3.1	Yes	No	App Permissions	Enabled

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

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



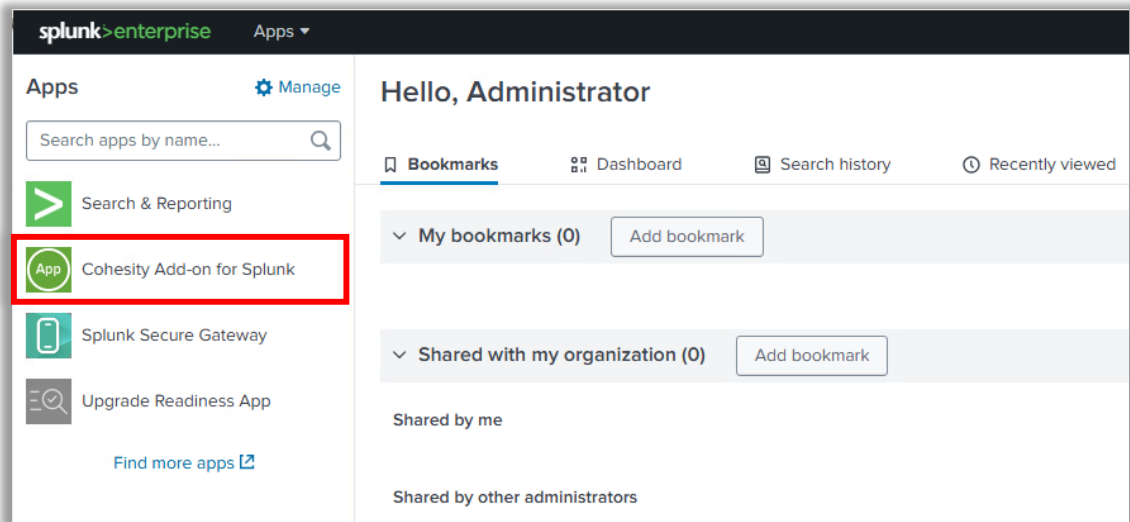
- d. On the Splunk Home Page, **Cohesity Add-on for Splunk** must be available.



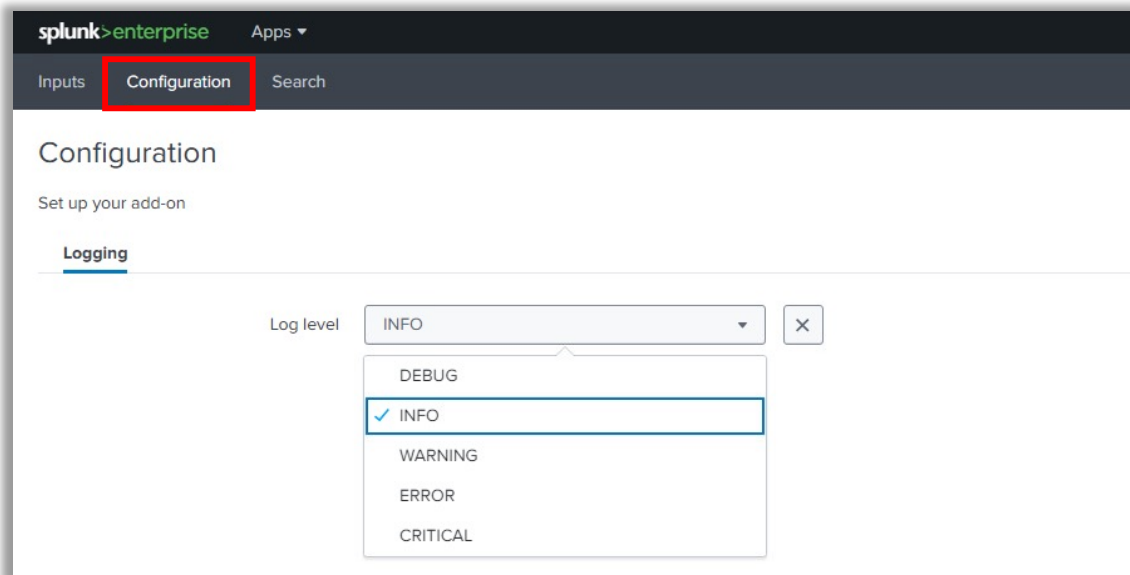
NOTE: If the add-on is not visible in the home page, then the add-on might still be getting installed. Wait for some time and then try again. If the add-on is still not visible, then the installation could have been interrupted. Try to reinstall the add-on again.

3. Configure Cohesity Splunk Add-On.

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



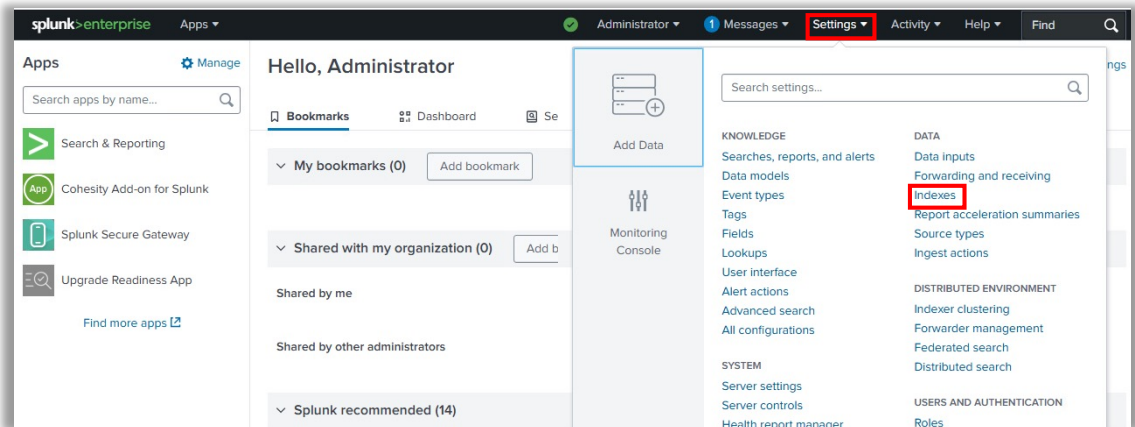
- b. Click **Configuration** and set up the desired **Log Level**. By default, **Info** is selected.



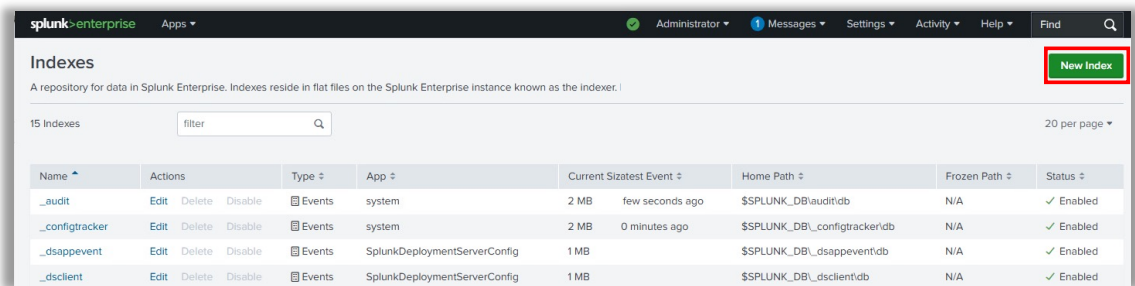
4. Create a new index to store Cohesity logs.
This is an optional however, recommended step. Create a new index to store Cohesity alerts and logs.

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**.

New Index ✕

Index Data Type Events Metrics

The type of data to store (event-based or metrics).

Home Path

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path

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 GB ▾

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket GB ▾

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App

Save
Cancel

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.

splunk>enterprise Apps ▾

Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. [Learn more](#)

16 Indexes

Name ▲	Actions	Type ▾	App ▾	Current Size ▾	Max Size ▾?	Event Count ▾
._audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	117K
._configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	186
._dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	Events	TA-cohesity-add-on-for-splunk	1 MB	500 GB	0
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0

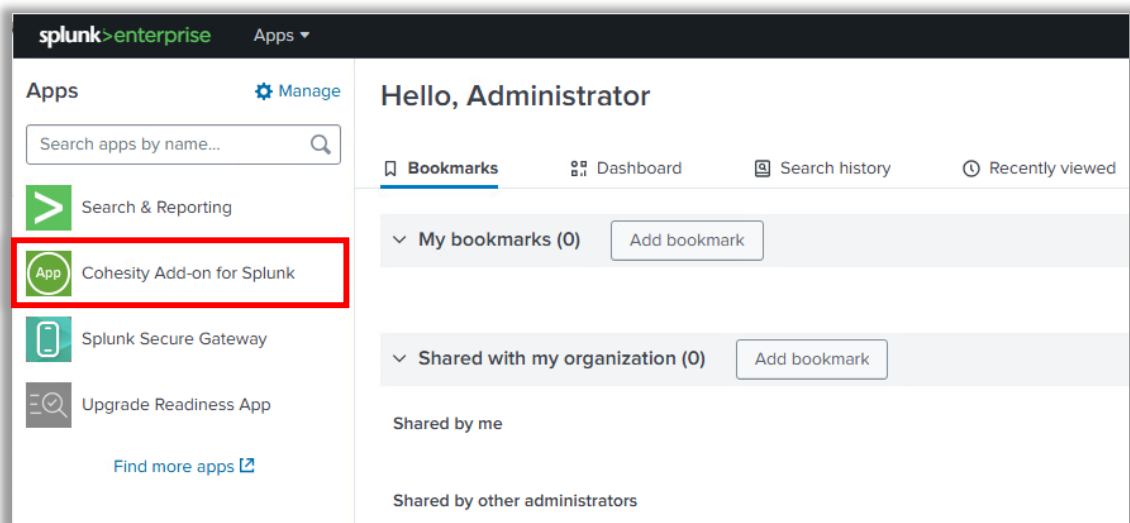
5. Add self-managed Cohesity Cluster(s) as source input.

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

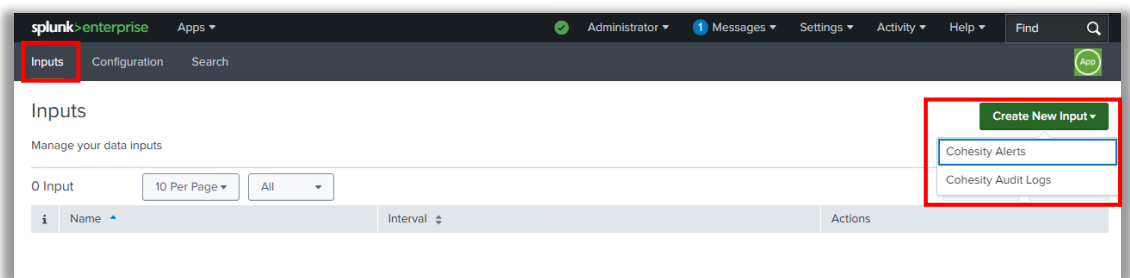
NOTE:

- 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**.

Add Cohesity Alerts ✕

***Name**
Enter a unique name for the data input

***Interval**
Time interval of input in seconds.

***Index**

***Cluster FQDN**

***Cohesity User**

***Password**

***User Domain**

- **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

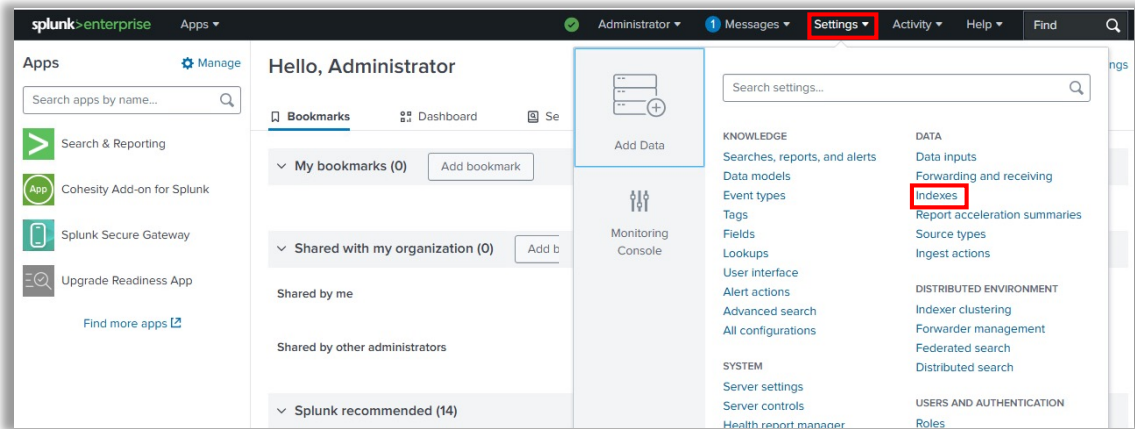
- d. You can see the newly created source inputs under Inputs.

i	Name	Interval	Index	Status
>	Cohesity_Alerts	60	cohesity_logs	Enabled
>	Cohesity_Audit_Logs	60	cohesity_logs	Enabled

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**.



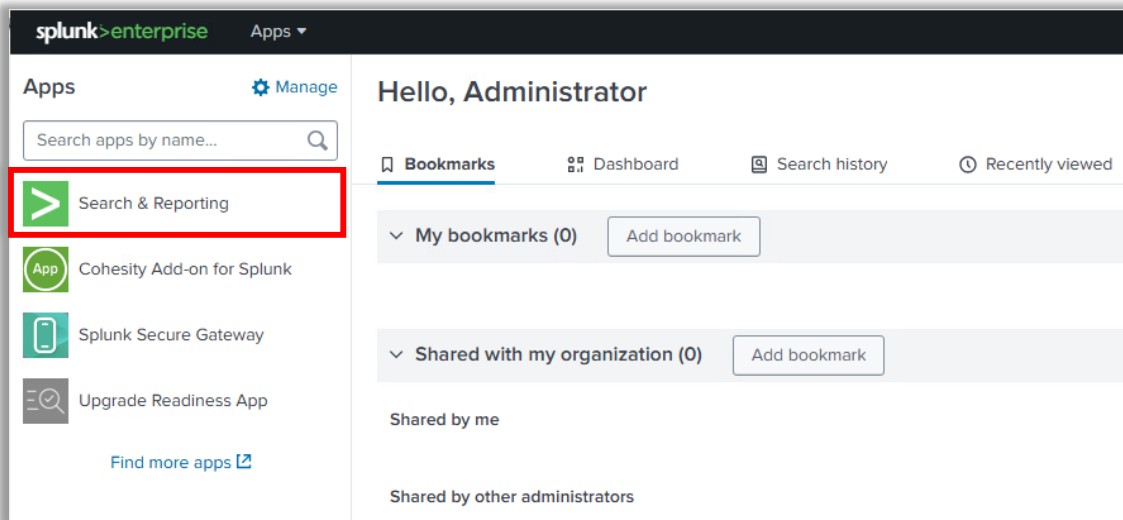
- b. Verify logs are being pushed to your index by checking the Event Count

Name	Actions	Type	App	Current Size	Max Size	Event Count
__audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	17.8K
__configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	199
__dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	Events	TA-cohesity-add-on-for-splunk	1 MB	500 GB	121
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0

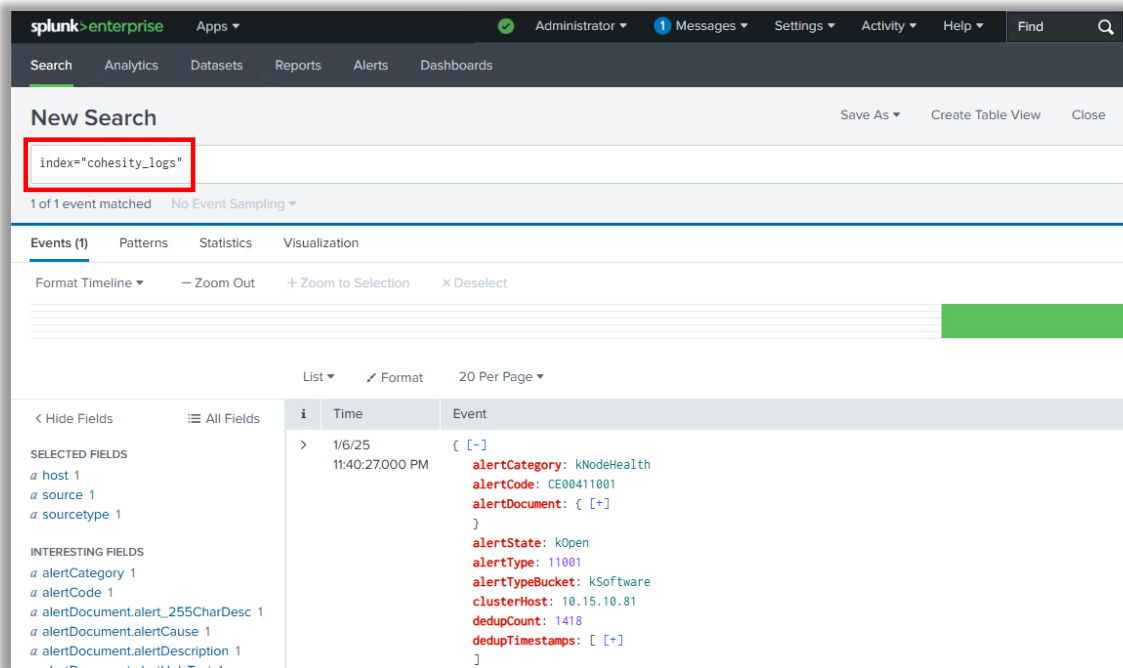
NOTE: Alerts and logs will be pulled from Cohesity to Splunk after the time-interval you have defined while creating the source input in step 5. Wait till the time interval elapses before you see the increase in event count. If you are not seeing the events even after the time interval elapse, then there 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.

The screenshot shows the Splunk Enterprise interface. At the top, the search bar contains the query `index=*cohesity_logs`. To the right of the search bar, a dropdown menu is open, showing the 'Last 24 hours' filter selected. Below the search bar, the search results are displayed in a table format. The table has columns for 'Time' and 'Event'. The 'Time' column shows the date and time of the event, and the 'Event' column shows the event details. The 'Presets' dropdown menu is open, showing various time-based filters such as '30 second window', '1 minute window', '5 minute window', '30 minute window', '1 hour window', 'All time (real-time)', 'Today', 'Week to date', 'Business week to date', 'Month to date', 'Year to date', 'Yesterday', 'Previous week', 'Previous business week', 'Previous month', and 'Previous year'.

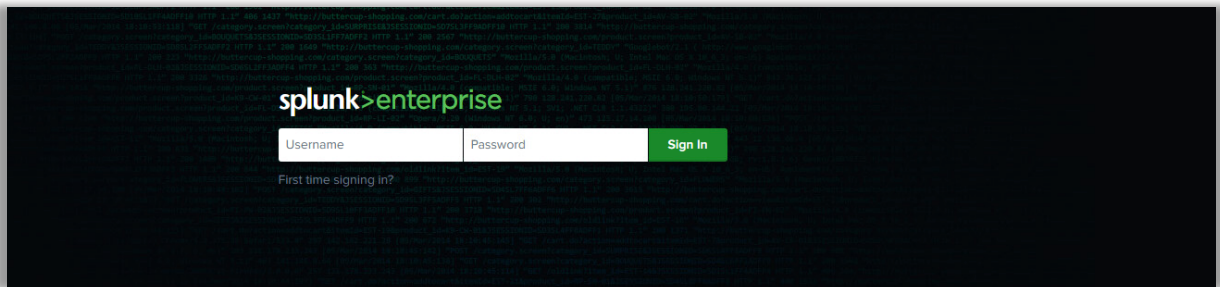
d. Alert and visualize.

The screenshot shows the Splunk Enterprise interface. At the top, the search bar contains the query `index=*cohesity_logs`. To the right of the search bar, a dropdown menu is open, showing the 'Report' action selected. Below the search bar, the search results are displayed in a table format. The table has columns for 'Time' and 'Event'. The 'Time' column shows the date and time of the event, and the 'Event' column shows the event details. The 'Report' dropdown menu is open, showing various actions such as 'Report', 'Alert', 'Existing Dashboard', 'New Dashboard', and 'Event Type'.

NOTE: For more details, refer to the [Search and Reporting](#) section.

Integration via Webhook

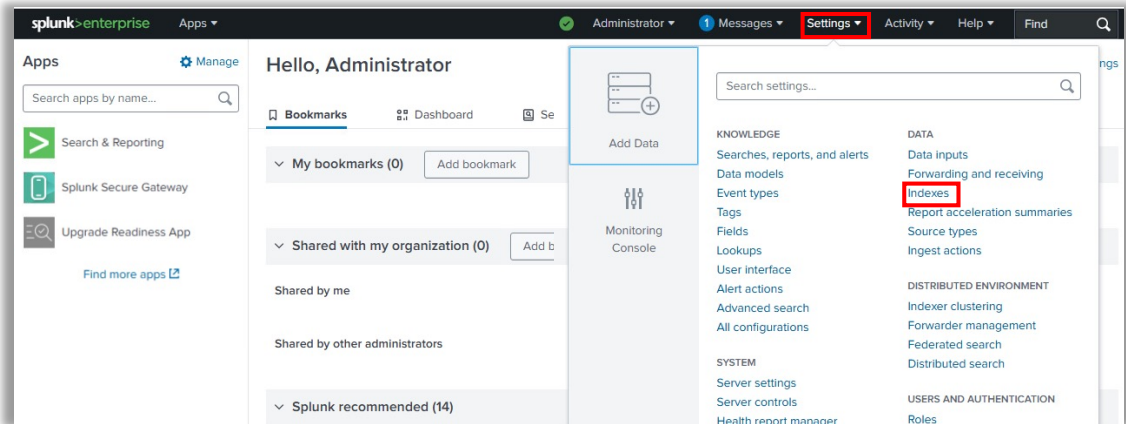
1. Login to your Splunk Enterprise Instance.



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.

15 Indexes 20 per page

Name	Actions	Type	App	Current Size	Latest 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.

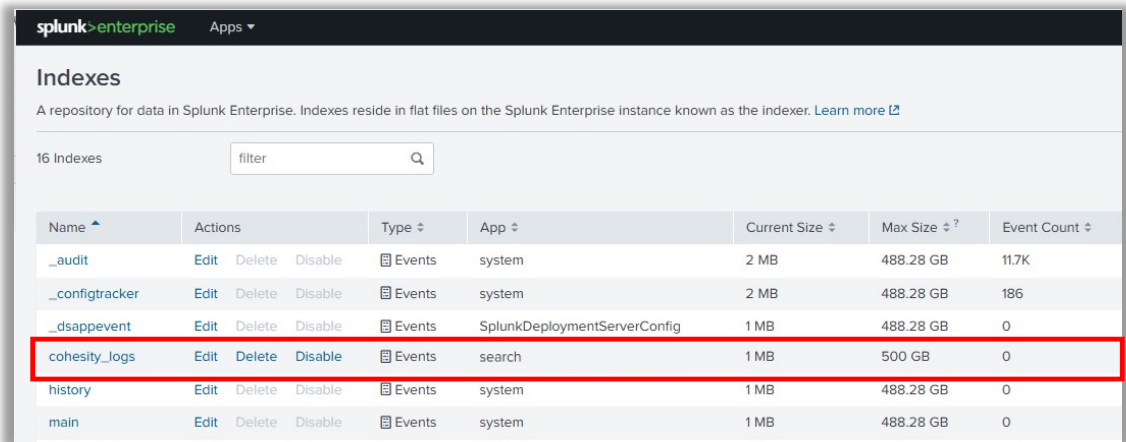
Max Size of Entire Index: 500 GB
Maximum target size of entire index.

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

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

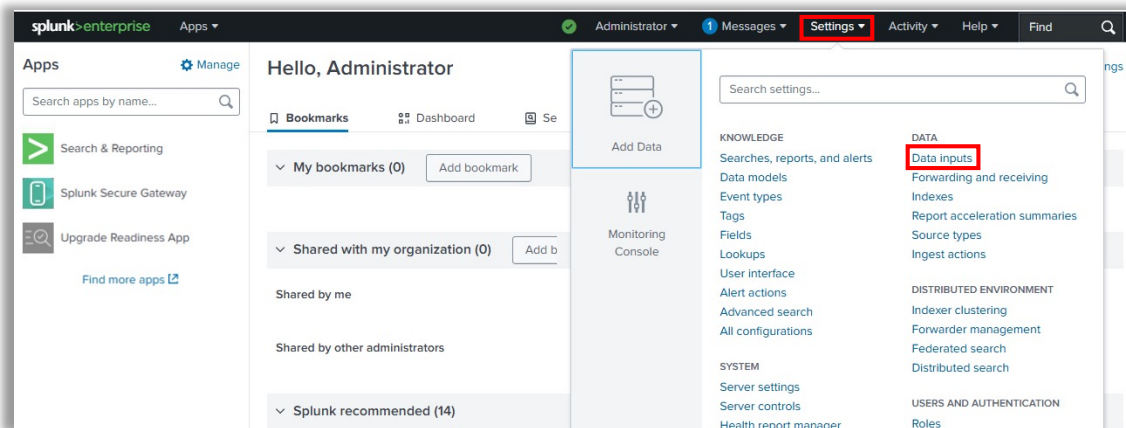


The screenshot shows the Splunk Enterprise 'Indexes' page. A table lists various indexes. The 'cohesity_logs' index is highlighted with a red border. The table has columns for Name, Actions, Type, App, Current Size, Max Size, and Event Count.

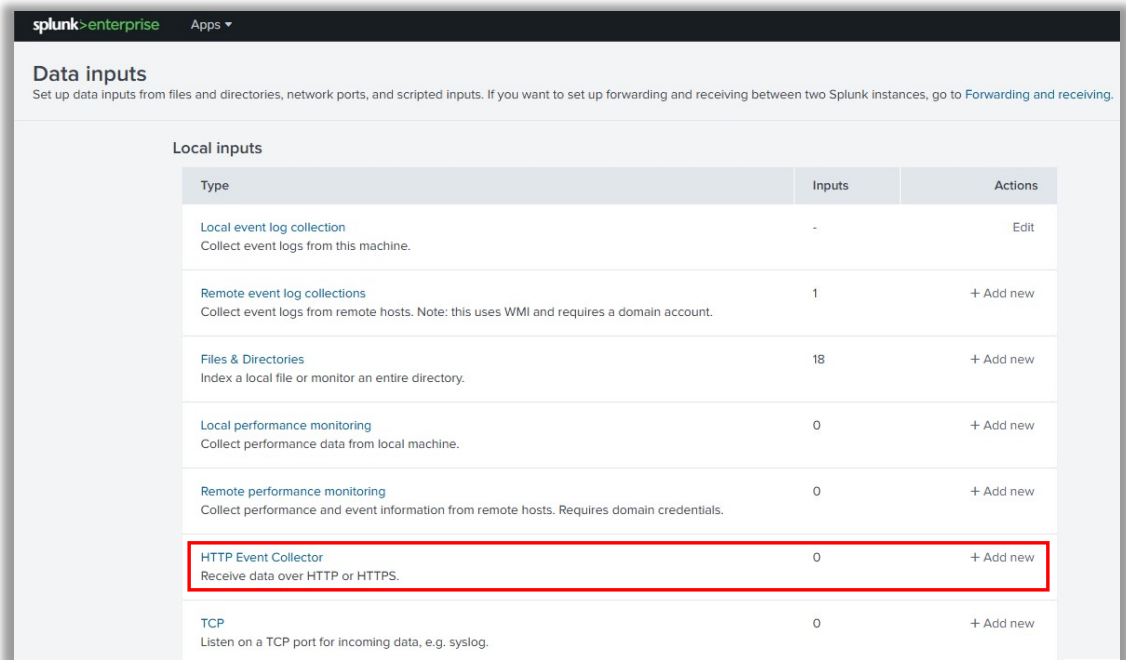
Name	Actions	Type	App	Current Size	Max Size	Event Count
._audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	11.7K
._configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	186
._dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	Events	search	1 MB	500 GB	0
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0

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

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



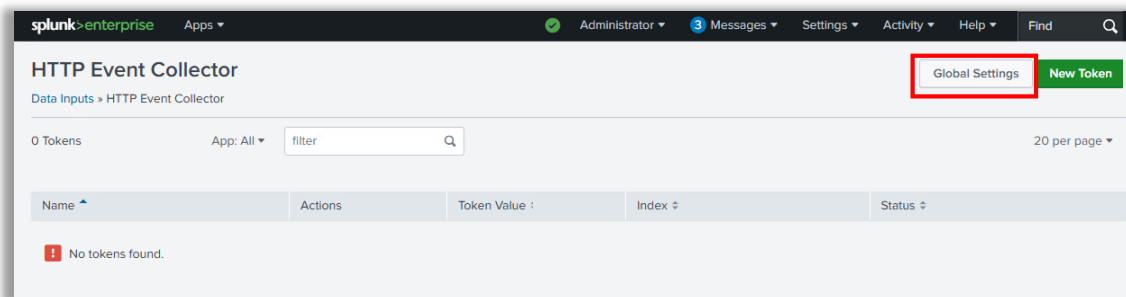
- b. Click **HTTP Event Collector**.



The screenshot shows the Splunk Enterprise interface for configuring data inputs. The page title is "Data inputs" with a subtitle: "Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#)." Below this is a section for "Local inputs" containing a table with the following data:

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	18	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new

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



The screenshot shows the Splunk Enterprise interface for configuring the HTTP Event Collector. The page title is "HTTP Event Collector" with a subtitle: "Data Inputs > HTTP Event Collector". In the top right corner, there are two buttons: "Global Settings" (highlighted with a red box) and "New Token". Below the buttons, there is a search bar and a table with the following data:

Name	Actions	Token Value	Index	Status
No tokens found.				

Edit Global Settings

All Tokens: Enabled

Default Source Type: `_json`

Default Index: `cohesity_logs`

Default Output Group: None

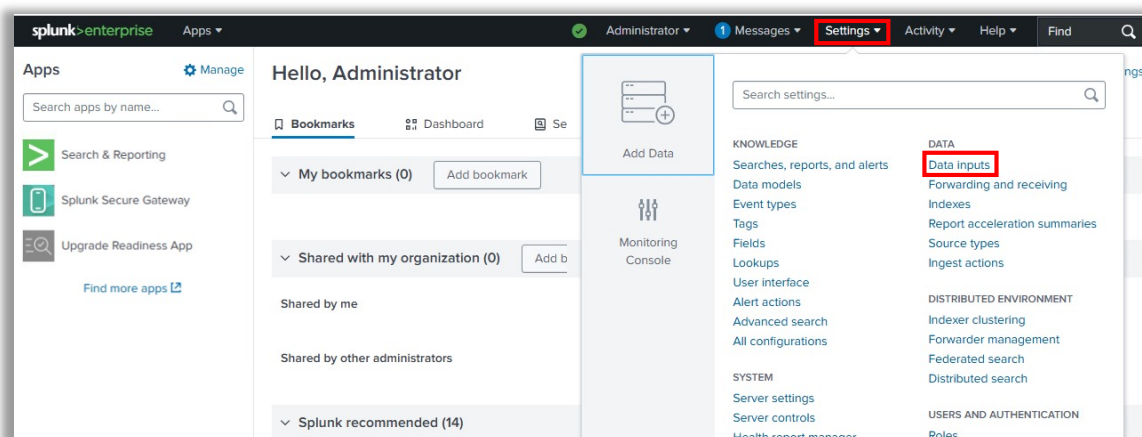
Use Deployment Server:

Enable SSL:

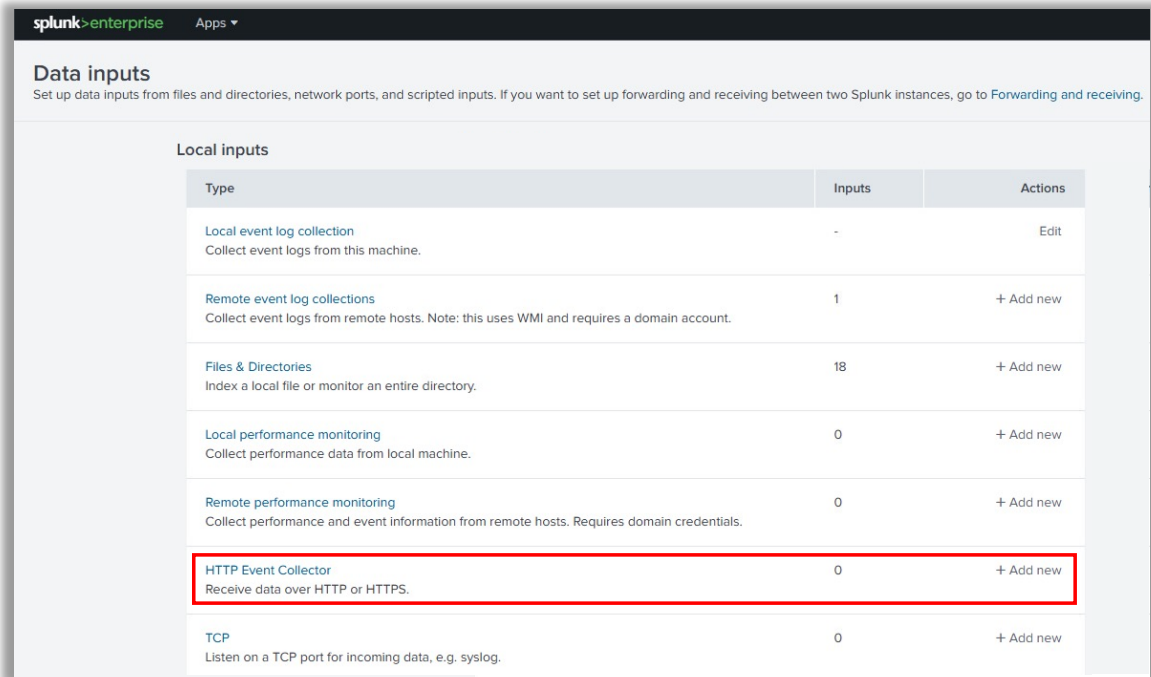
HTTP Port Number: 8088

Cancel 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**.



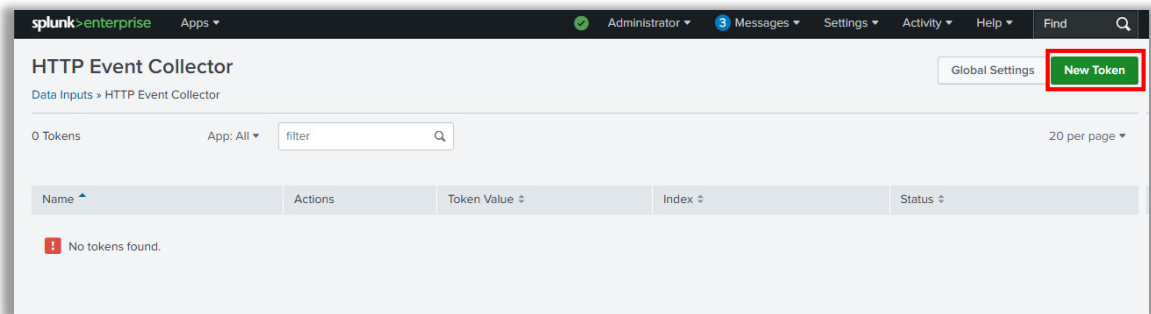
b. Click **HTTP Event Collector**.



The screenshot shows the Splunk Enterprise interface for configuring data inputs. The page title is "Data inputs" with a subtitle: "Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving." Below this, there is a section for "Local inputs" containing a table of input types.

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	18	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new

c. Click **New Token**.



The screenshot shows the Splunk Enterprise interface for the HTTP Event Collector configuration page. The page title is "HTTP Event Collector" with a subtitle: "Data Inputs > HTTP Event Collector". In the top right corner, there are two buttons: "Global Settings" and "New Token", with the "New Token" button highlighted by a red box. Below the buttons, there is a section for "0 Tokens" with a search filter and a "20 per page" dropdown. A table with columns "Name", "Actions", "Token Value", "Index", and "Status" is shown, but it contains no data. A message at the bottom left of the table area says "No tokens found."

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

The screenshot shows the 'Add Data' configuration page in Splunk Enterprise. The progress bar indicates the 'Input Settings' step is active. On the left, the 'HTTP Event Collector' option is selected. The main configuration area shows a 'Name' field containing 'Cohesity_Webhook_Token', which is highlighted with a red box. Below it are fields for 'Source name override?', 'Description?', and 'Output Group (optional)'. There is also an 'Enable indexer acknowledgement' checkbox. A 'Next >' button is highlighted in red in the top right corner.

- 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.

The screenshot shows the 'Input Settings' page in Splunk Enterprise. The progress bar indicates the 'Input Settings' step is active. The 'Source type' dropdown is set to 'Select', which is highlighted with a red box. Below it, the 'Select Source Type' dropdown is open, showing a search for '_json'. The '_json' option is selected and highlighted with a red box. Below the dropdown, there is a table for 'Select Allowed Indexes' with columns for 'Available Item(s)' and 'Selected Item(s)'. The 'Default Index' is set to 'Default'.

- 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.

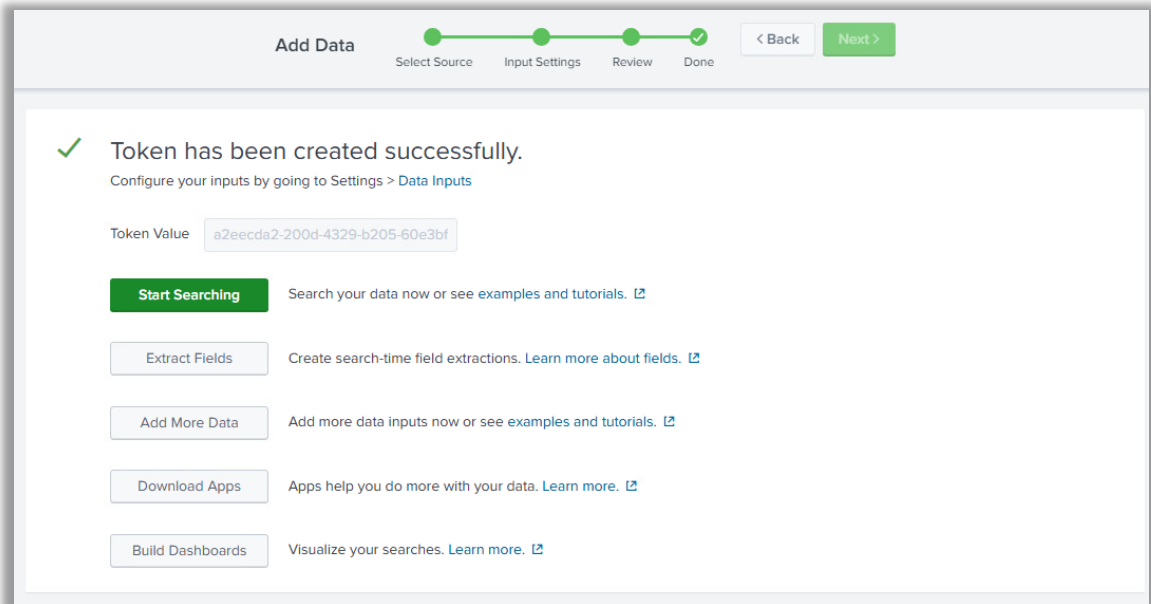
The screenshot shows the 'Input Settings' page in Splunk. The progress bar at the top indicates the current step is 'Input Settings'. The 'Index' section is highlighted, showing a list of available indexes: @cohesity_logs, @history, @main, and @summary. The @cohesity_logs index is selected and moved to the 'Selected item(s)' list. The 'Default Index' dropdown is also set to @cohesity_logs. The 'Source type' is set to '_json'.

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

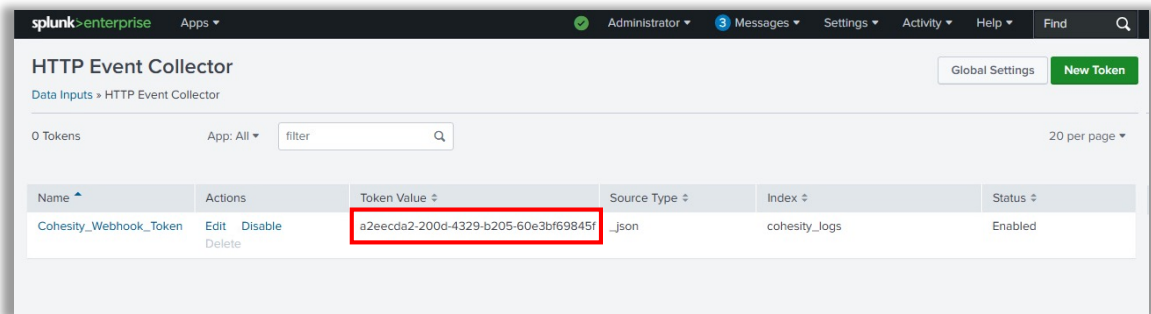
The screenshot shows the 'Review' page in Splunk. The progress bar at the top indicates the current step is 'Review'. The configuration details are as follows:

Input Type	Token
Name	Cohesity_Webhook_Token
Source name override	N/A
Description	N/A
Enable indexer acknowledgment	No
Output Group	N/A
Allowed indexes	cohesity_logs
Default index	cohesity_logs
Source Type	_json
App Context	launcher

- 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:



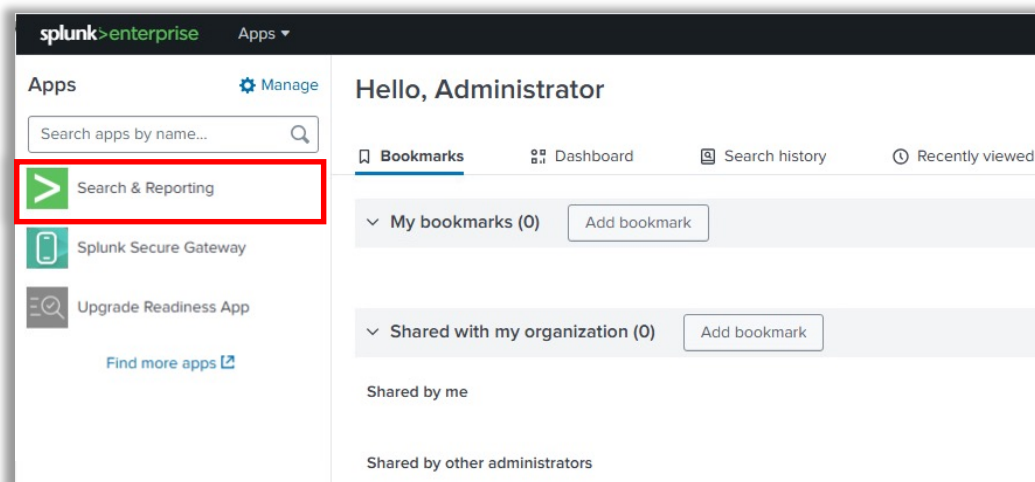
```
shashanka.sr@COH-J6CJPK74WG ~ % curl -k "https://10.15.5.120:8088/services/collector/raw" \
-H "Authorization: Splunk c37725f2-299e-4f03-929d-12f0d8f0254c" \
-H "Content-Type: application/json" \
-d '{"alert": "Test_Alert", "alertId": "0000"}'
{"text": "Success", "code": "0"}
shashanka.sr@COH-J6CJPK74WG ~ %
```

NOTE:

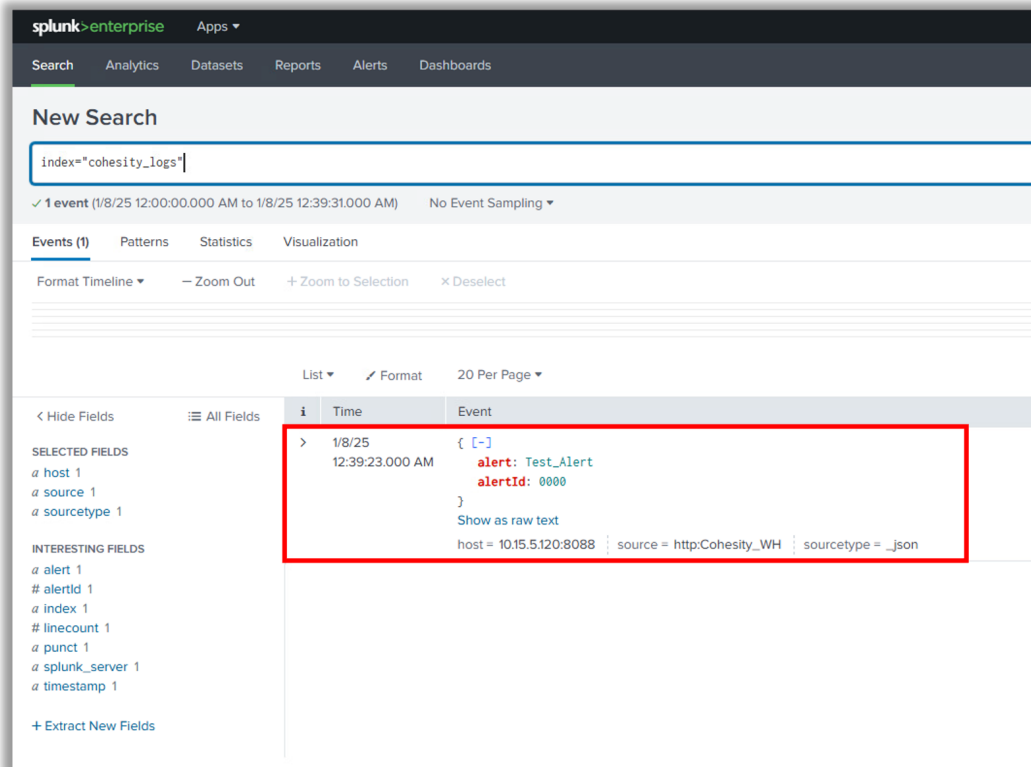
- If you are not receiving the message `{"text": "Success", "code": "0"}` or receiving some other message, then there is some issue with the HTTP Event Collector configuration.
- Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

- 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.



The screenshot shows the Splunk Enterprise interface. At the top, the search bar contains the query `index="cohesity_logs"`. Below the search bar, it indicates 1 event found for the time range 1/8/25 12:00:00.000 AM to 1/8/25 12:39:31.000 AM. The event is displayed in a table with the following details:

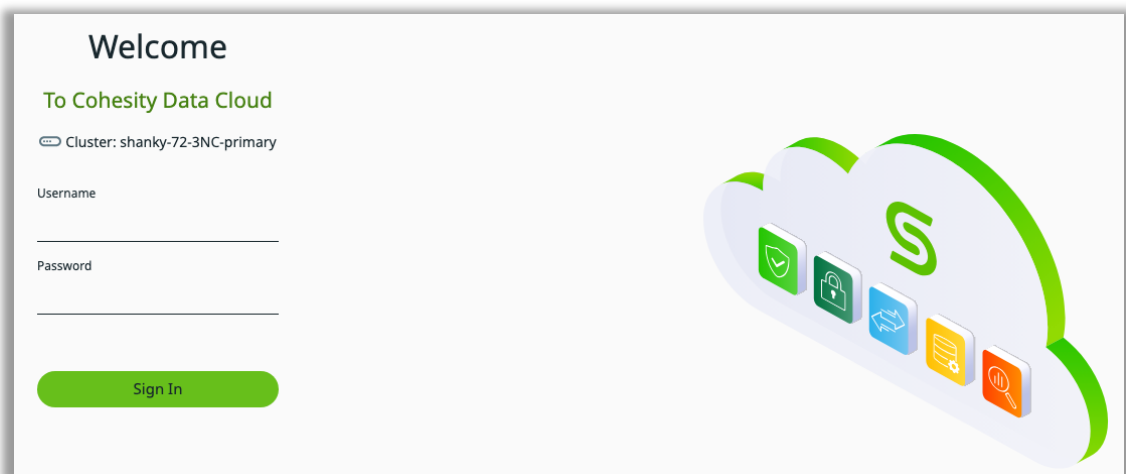
i	Time	Event
>	1/8/25 12:39:23.000 AM	{ [-] alert: Test_Alert alertId: 0000 } Show as raw text host = 10.15.5.120:8088 source = http:Cohesity_WH sourcetype = _json

The event details are highlighted with a red box. The interface also shows a list of selected fields (host, source, sourcetype) and interesting fields (alert, alertId, index, linecount, punct, splunk_server, timestamp).

NOTE:

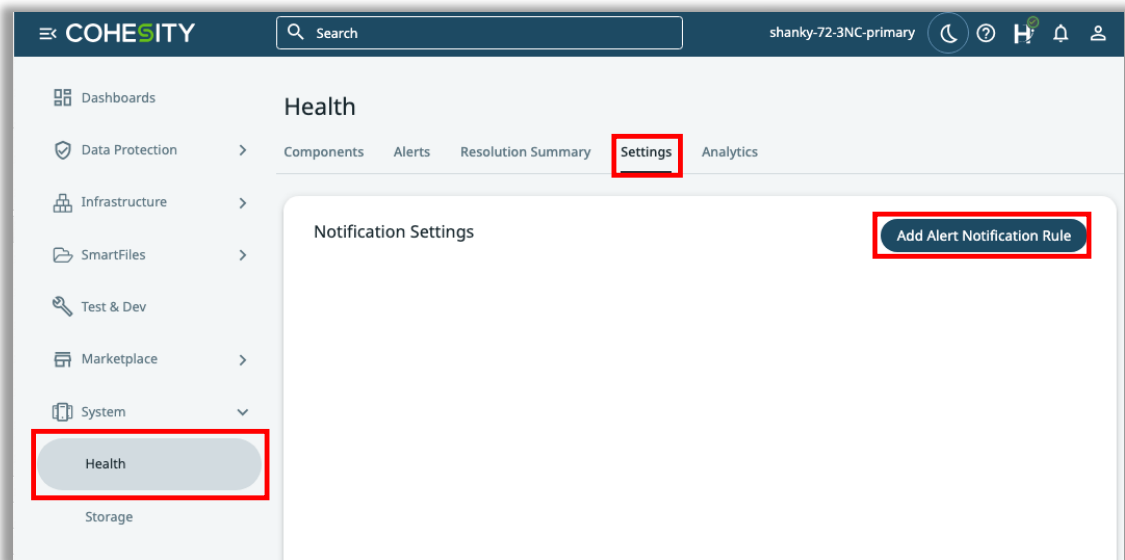
- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

7. Configure alert notification with webhook On Cohesity Cluster.
 - a. Login to your Cohesity Cluster from Cluster UI.



The screenshot shows the 'Welcome' page of the Cohesity Cluster UI. The page title is 'Welcome To Cohesity Data Cloud'. Below the title, it displays the cluster name: 'Cluster: shanky-72-3NC-primary'. There are input fields for 'Username' and 'Password', and a green 'Sign In' button. On the right side, there is a graphic of a cloud with various icons representing different services or features.

- 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"

Add Alert Notification Rule ✕

Rule Name

Splunk

When

Alert Category	Alert Severities	Alert Name
All applies by default	All applies by default	All applies by default

Send Alert Notification via *

Email

Add email addresses of users to receive alert email notifications
+ Add

SNMP

Syslog

Webhook

URL ⓘ

Options ⓘ

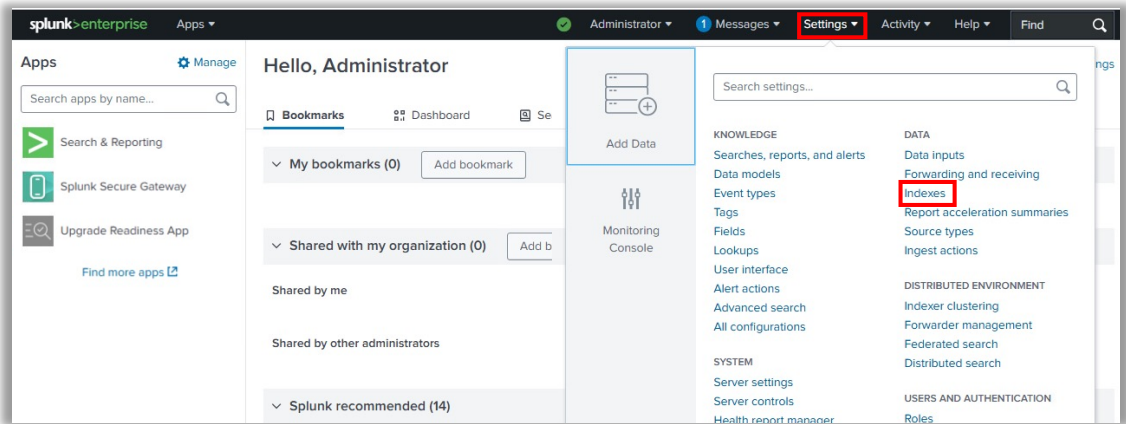
```
curl -H "Authorization: Splunk 355abee2-f248-46f6-bff6-b1f6790720a0" -H "Content-Type: application/json" -XPOST http://10.15.5.120:8088/services/collector/raw
```

Cancel
Save

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**.

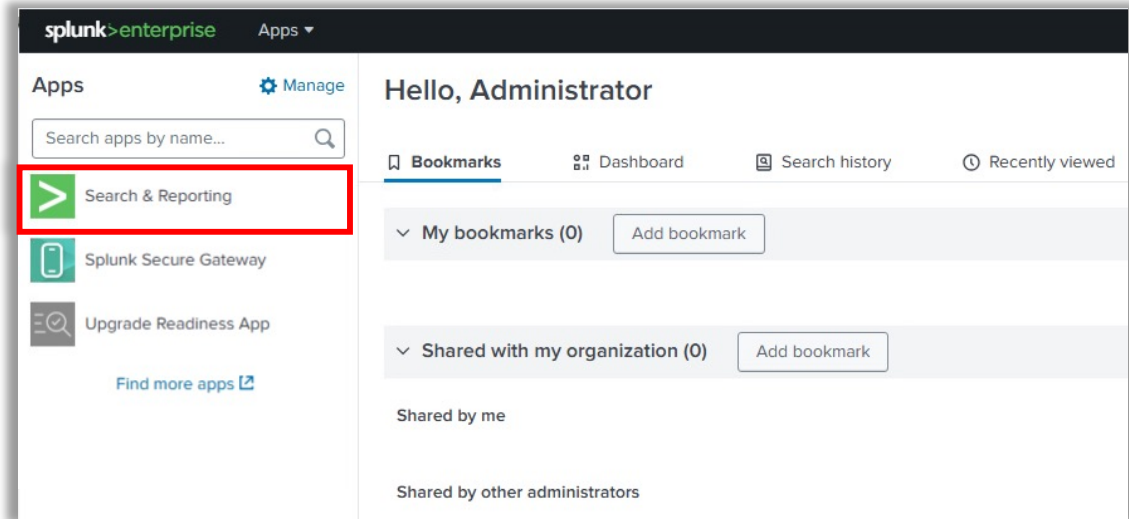


- b. Verify logs are being pushed to your index by checking the Event Count.

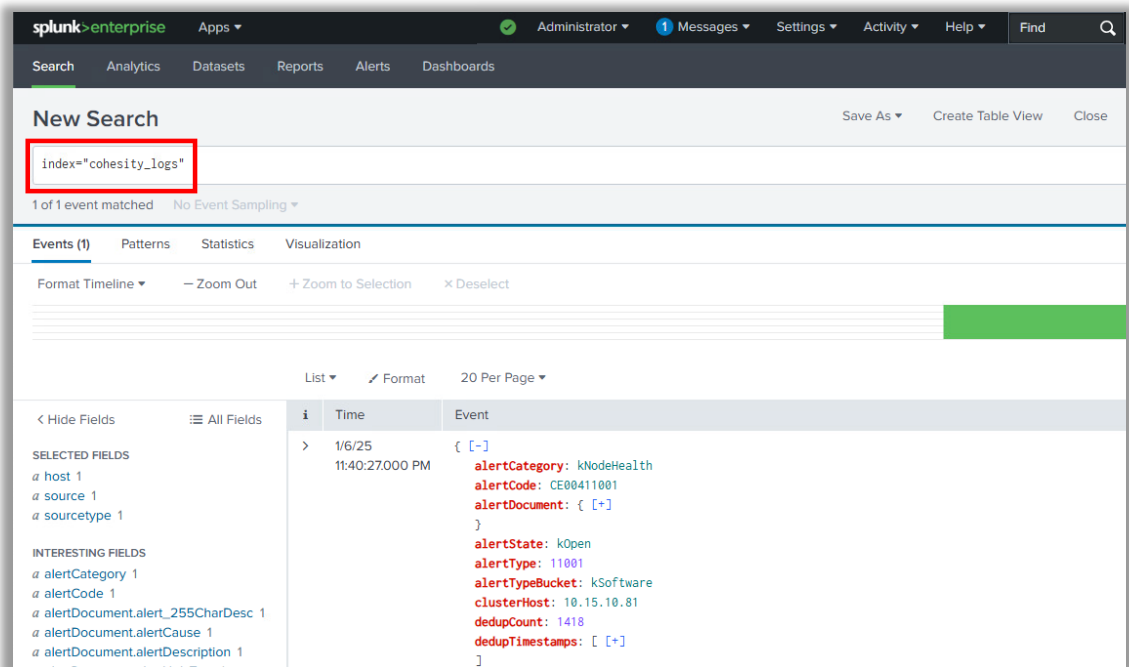
Name	Actions	Type	App	Current Size	Max Size	Event Count
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	17.8K
_configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	199
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	Events	search	1 MB	500 GB	121
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0

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.

The screenshot shows the Splunk Enterprise interface with a search for `index=*cohesity_logs`. The search results show 1 of 1 event matched. A dropdown menu is open, showing various time filters under the 'Presets' section. The 'Last 24 hours' filter is highlighted in red. The search results table shows a single event with the following fields:

Time	Event
1/6/25 11:40:27.000 PM	

d. Alert and visualize.

The screenshot shows the Splunk Enterprise interface with a search for `index=*cohesity_logs`. The search results show 1 of 1 event matched. A dropdown menu is open, showing various actions under the 'Save As' section. The 'Report' action is highlighted in red. The search results table shows a single event with the following fields:

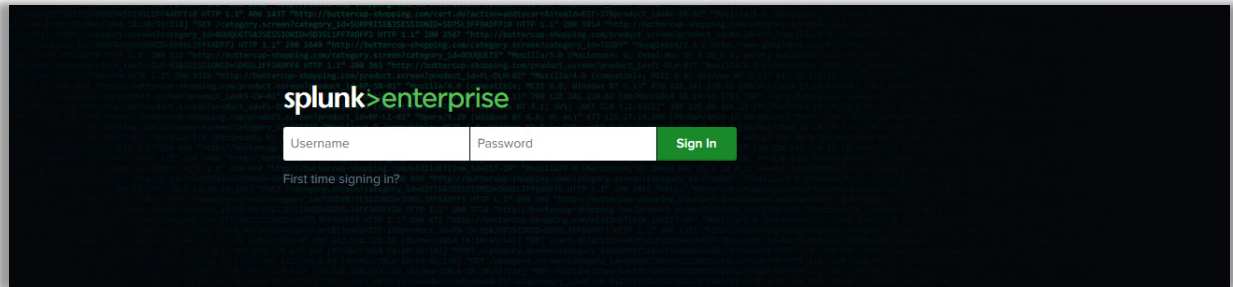
Time	Event
1/6/25 11:40:27.000 PM	<pre>{ [-] alertCategory: kNodeHealth alertCode: CE00411001 alertDocument: { [+]} alertState: kOpen alertType: 11001 alertTypeBucket: kSoftware clusterHost: 10.15.10.81 dedupCount: 1418 dedupTimestamps: [+]} }</pre>

NOTE: For more details, refer to the [Search and Reporting](#) section.

Cohesity Data Cloud

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

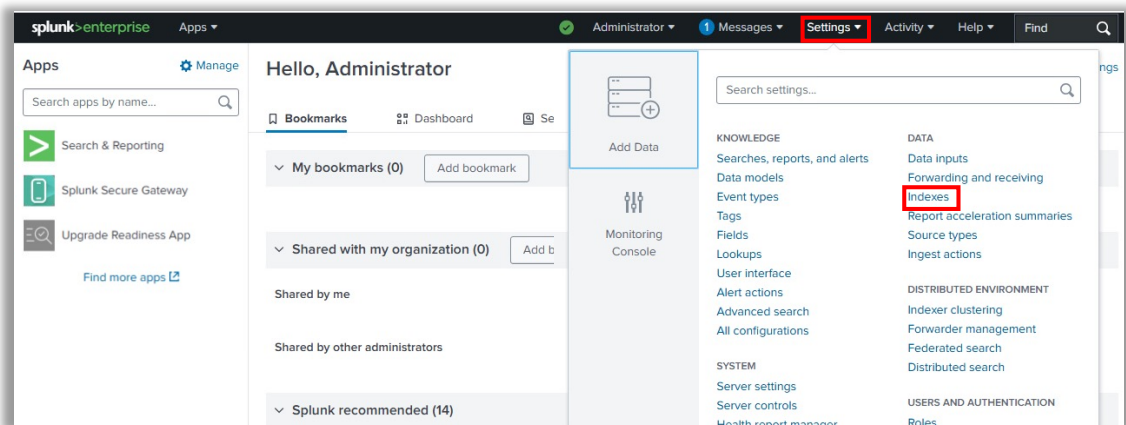
1. Login to your Splunk Enterprise Instance.



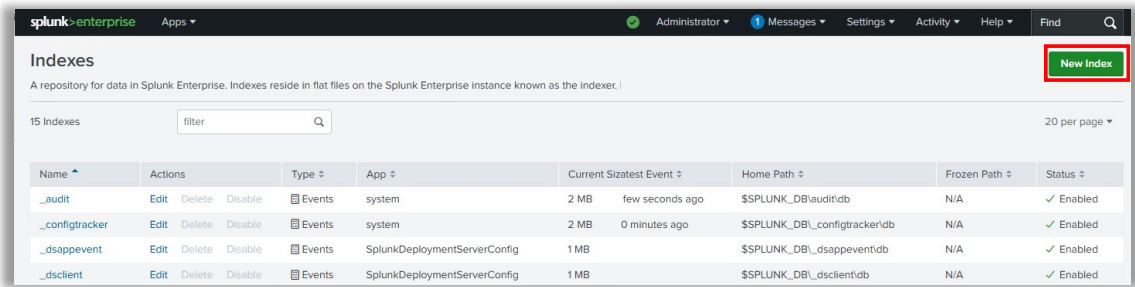
2. Create a new index to store Cohesity logs.

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**.

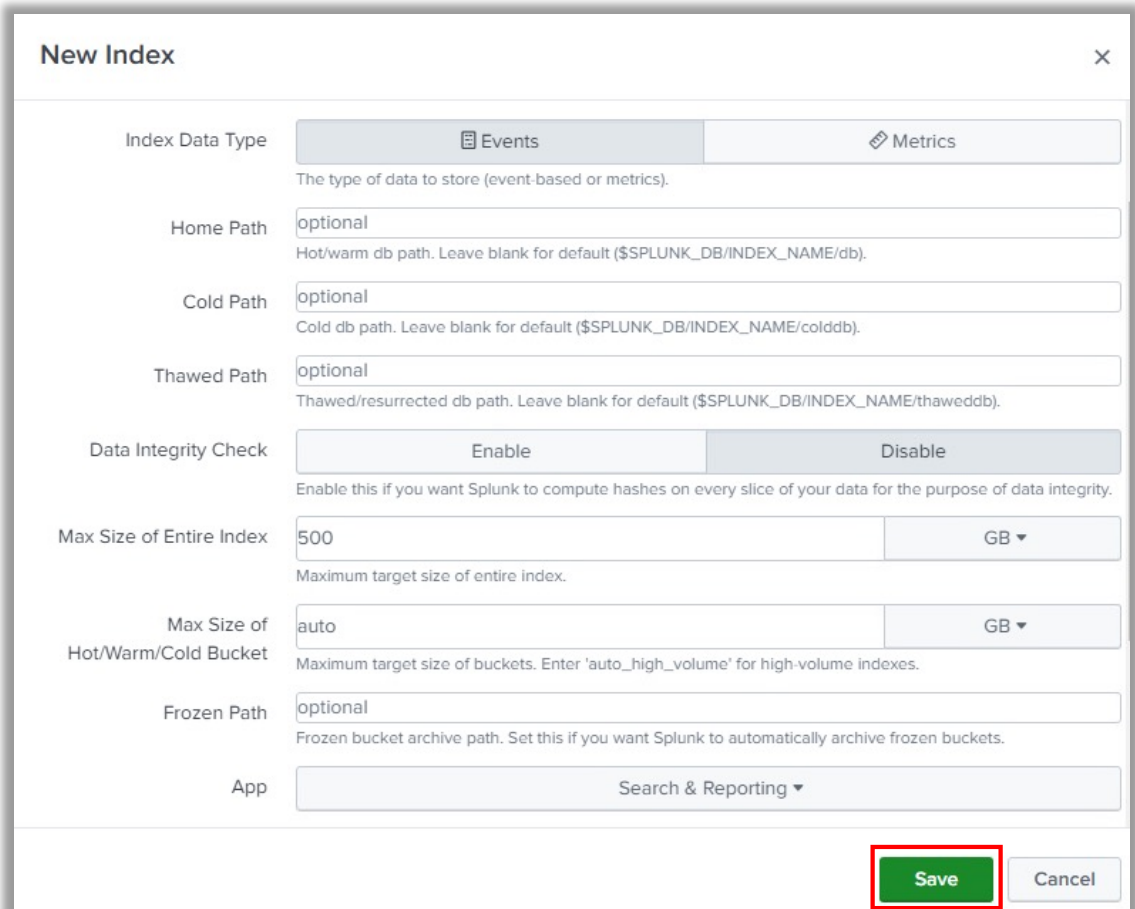


- b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save**.



The screenshot shows the Splunk Enterprise interface for managing indexes. The 'New Index' button is highlighted with a red box. Below the button is a table listing existing indexes.

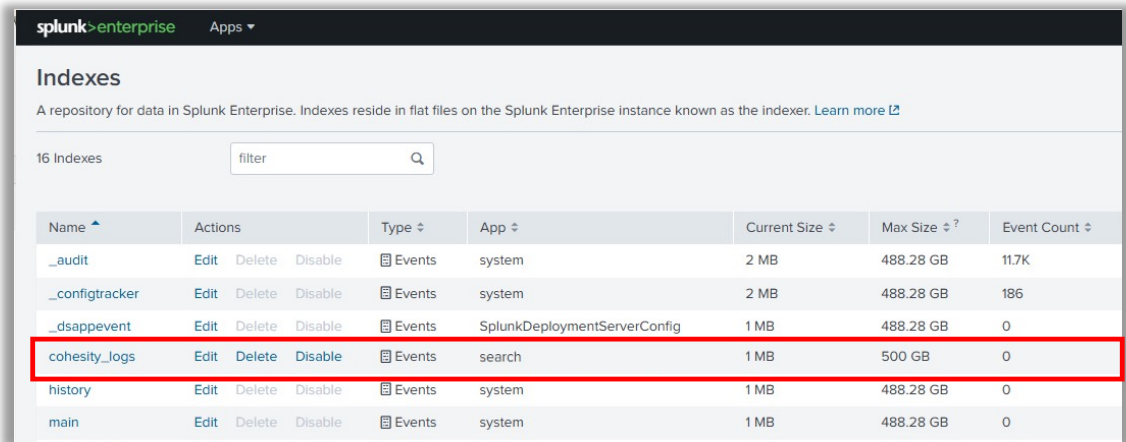
Name	Actions	Type	App	Current Size	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	2 MB	few seconds ago	\$SPLUNK_DB/audit/db	N/A	Enabled
_configtracker	Edit Delete Disable	Events	system	2 MB	0 minutes ago	\$SPLUNK_DB/_configtracker/db	N/A	Enabled
_dsappevent	Edit Delete 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



The screenshot shows the 'New Index' configuration form. The 'Save' button is highlighted with a red box. The form contains the following fields and options:

- Index Data Type:** Events (selected), Metrics
- Home Path:** optional (text input)
- Cold Path:** optional (text input)
- Thawed Path:** optional (text input)
- Data Integrity Check:** Enable (selected), Disable
- Max Size of Entire Index:** 500 (text input), GB (dropdown)
- Max Size of Hot/Warm/Cold Bucket:** auto (text input), GB (dropdown)
- Frozen Path:** optional (text input)
- App:** Search & Reporting (dropdown)

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

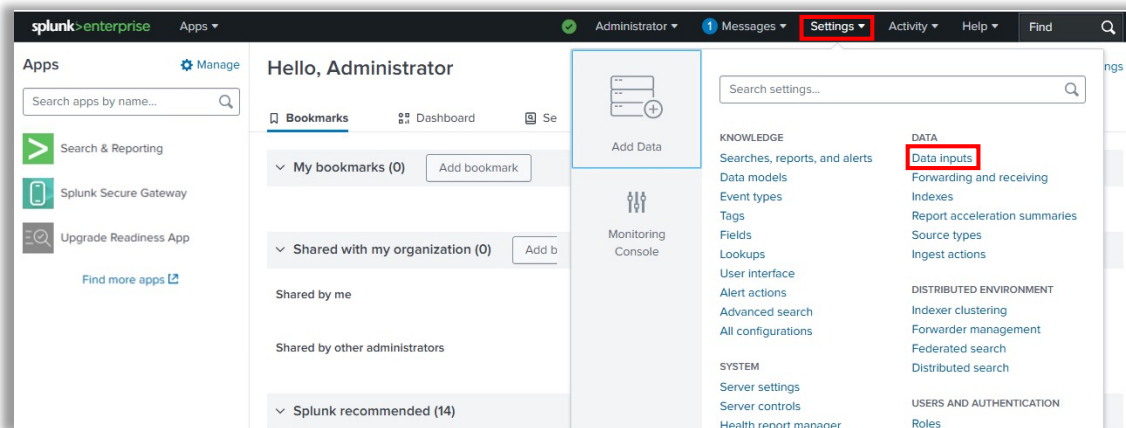


The screenshot shows the Splunk Enterprise 'Indexes' page. A table lists 16 indexes. The 'cohesity_logs' index is highlighted with a red border. The table columns are Name, Actions, Type, App, Current Size, Max Size, and Event Count.

Name	Actions	Type	App	Current Size	Max Size	Event Count
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	11.7K
_configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	186
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	Events	search	1 MB	500 GB	0
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0

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

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



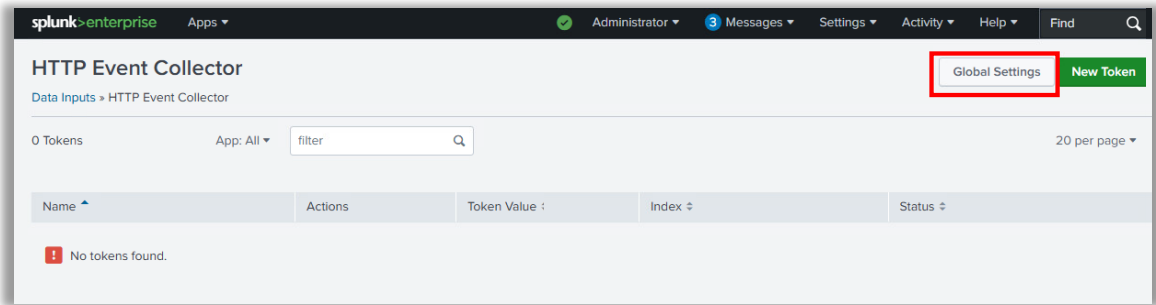
b. Click **HTTP Event Collector**.

The screenshot shows the Splunk Enterprise interface for configuring data inputs. The page title is "Data inputs" with a subtitle: "Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#)." Below this, there is a section for "Local inputs" containing a table with columns for "Type", "Inputs", and "Actions".

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
Files & Directories Index a local file or monitor an entire directory.	18	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new



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



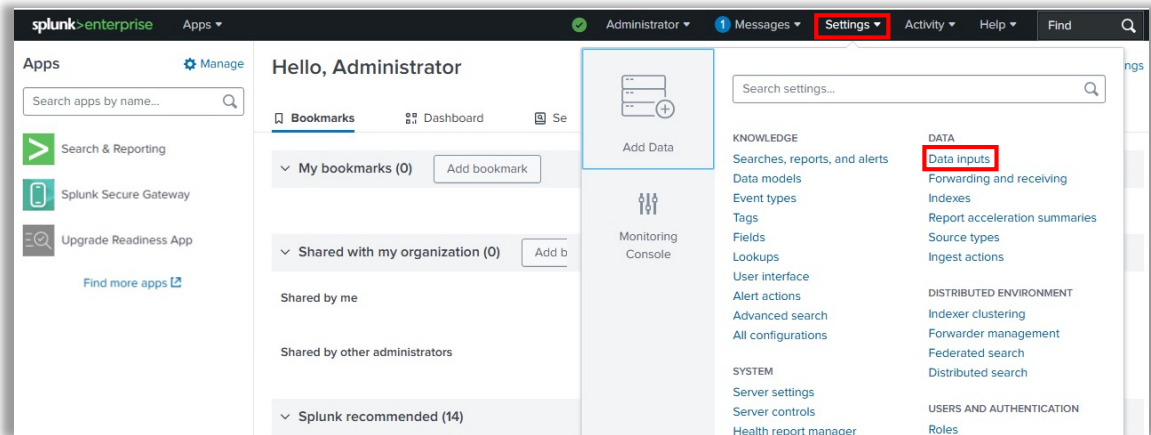
The 'Edit Global Settings' dialog box contains the following configuration options:

- All Tokens:** A toggle switch currently set to 'Enabled'.
- Default Source Type:** A dropdown menu set to '_json'.
- Default Index:** A dropdown menu set to 'cohesity_logs'.
- Default Output Group:** A dropdown menu set to 'None'.
- Use Deployment Server:** A checkbox that is checked.
- Enable SSL:** A checkbox that is checked.
- HTTP Port Number:** A text input field containing the value '8088'.

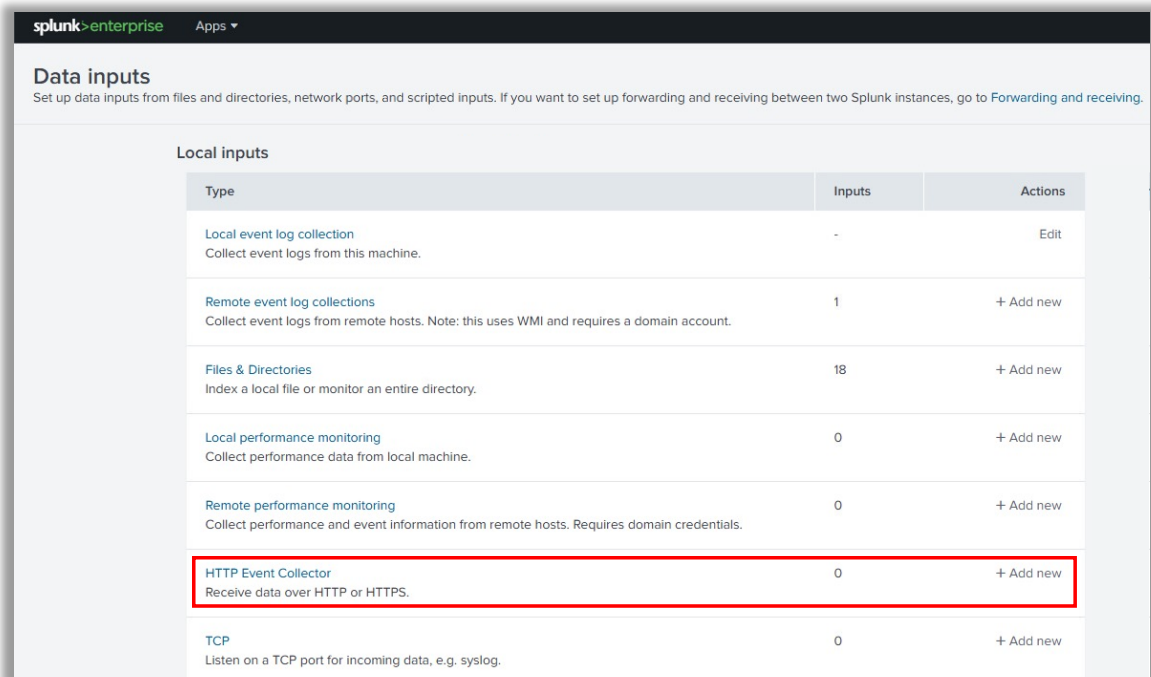
At the bottom right of the dialog, there are 'Cancel' and 'Save' buttons.

- 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.

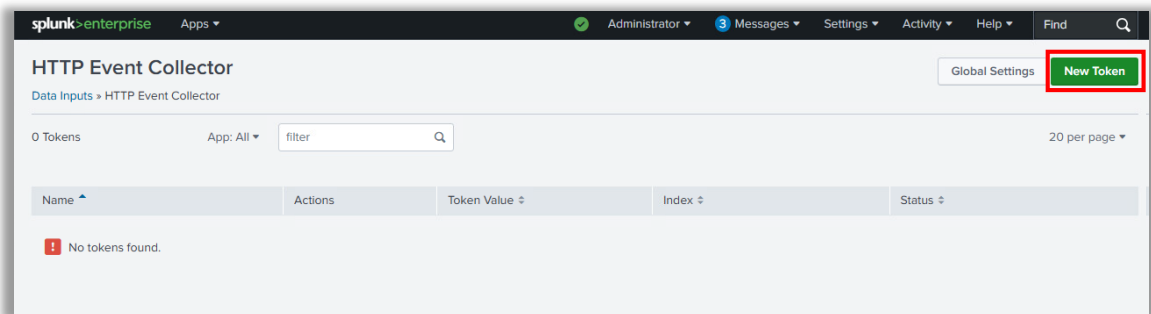
- d. Click **Data Inputs** under **Data** in **Settings**.



- e. Click **HTTP Event Collector**.



- f. Click **New Token**.



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

splunk>enterprise Apps ▾

Add Data ● ○ ○ ○ < Back Next >

Select Source Input Settings Review Done

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector >
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring
Have the Splunk platform index the local Windows Registry, and monitor it for changes.

Active Directory monitoring
Index and monitor Active Directory.

Configure a new token for receiving data over HTTP. [Learn More](#)

Name Cohesity_Webhook_Token

Source name override? optional

Description? optional

Output Group (optional) None ▾

Enable indexer acknowledgement

FAQ

- > What is the HTTP Event Collector?
- > How do I set up the HTTP Event Collector?
- > How do I view and configure the tokens that I can use to send data to the HTTP Event Collector?
- > What clients can send data to the HTTP Event Collector?
- > What port and protocol does the HTTP Event Collector receive data on and how can I change that?
- > What is an output group?

- 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.

The screenshot displays the Splunk Enterprise interface for configuring data input. At the top, the 'Add Data' process is shown with four steps: Select Source, Input Settings (current), Review, and Done. The 'Input Settings' section provides instructions on setting input parameters. Under 'Source type', there are buttons for 'Automatic', 'Select' (highlighted in red), and 'New'. A 'Select Source Type' dropdown menu is open, showing a search bar with '_json' and a list of results. The '_json' option is highlighted in red, with a description: 'JavaScript Object Notation format. For more information, visit http://json.org/'. Below this, there are options for 'log2metrics_json' and 'JSON-formatted data'. The 'Index' section shows a list of available indexes: cohesity_logs, history, main, and summary. A 'Default Index' dropdown is set to 'Default', and there is a 'Create a new index' link.

- 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.

splunk>enterprise Apps ▾

Add Data Progress: Select Source, Input Settings, Review, Done < Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic Select New

_json ▾

Index

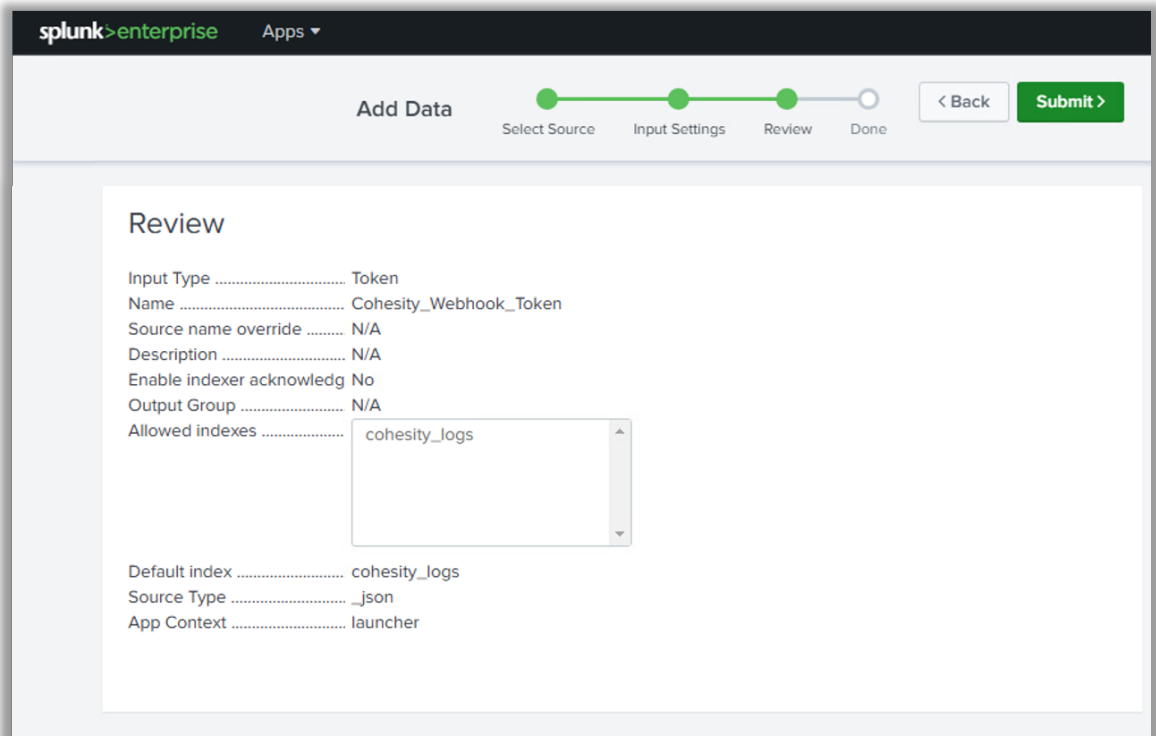
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Select Allowed Indexes	Available item(s)	add all >	Selected item(s) remove all
	<input checked="" type="checkbox"/> cohesity_logs		<input checked="" type="checkbox"/> cohesity_logs
	<input type="checkbox"/> history		
	<input type="checkbox"/> main		
	<input type="checkbox"/> summary		

Select indexes that clients will be able to select from.

Default Index: cohesity_logs ▾ [Create a new index](#)

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



splunk>enterprise Apps ▾

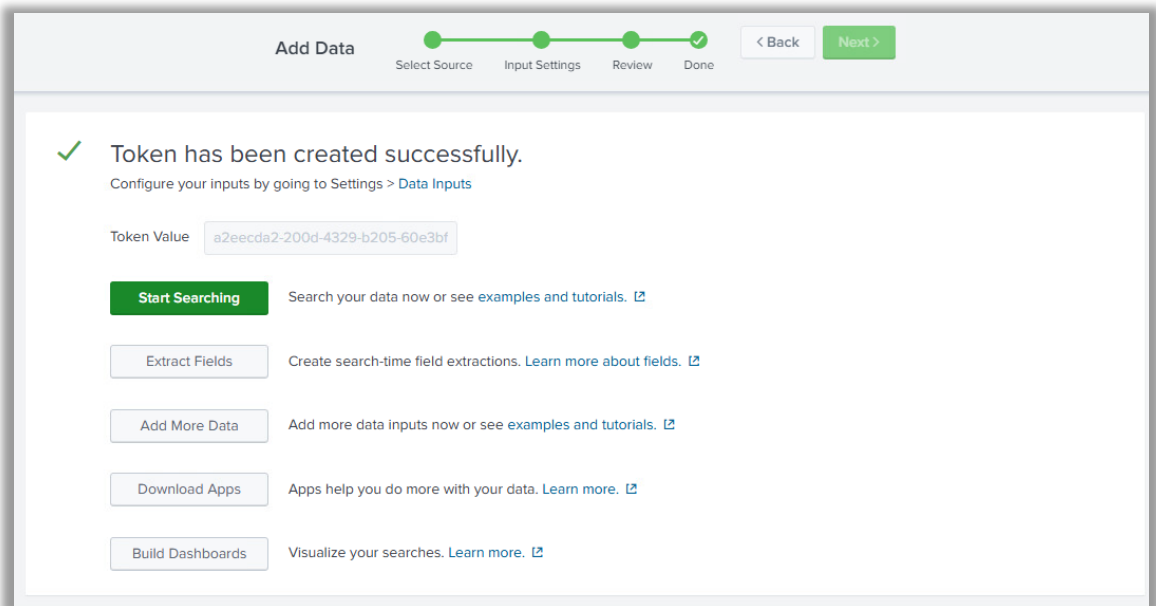
Add Data Select Source Input Settings **Review** Done < Back Submit >

Review

Input Type Token
 Name Cohesity_Webhook_Token
 Source name override N/A
 Description N/A
 Enable indexer acknowledg No
 Output Group N/A
 Allowed indexes

Default index cohesity_logs
 Source Type _json
 App Context launcher

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



Add Data Select Source Input Settings Review **Done** < Back Next >

✓ **Token has been created successfully.**
 Configure your inputs by going to Settings > [Data Inputs](#)

Token Value

Start Searching Search your data now or see [examples and tutorials](#). [↗](#)

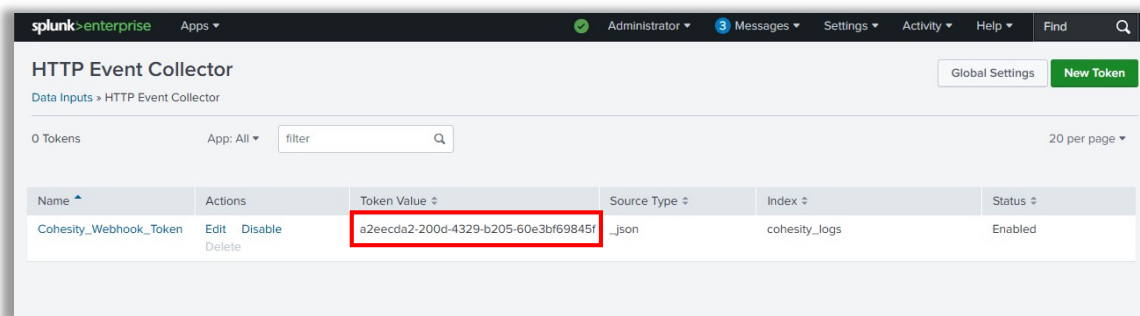
Extract Fields Create search-time field extractions. [Learn more about fields](#). [↗](#)

Add More Data Add more data inputs now or see [examples and tutorials](#). [↗](#)

Download Apps Apps help you do more with your data. [Learn more](#). [↗](#)

Build Dashboards Visualize your searches. [Learn more](#). [↗](#)

- 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_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"}'
```

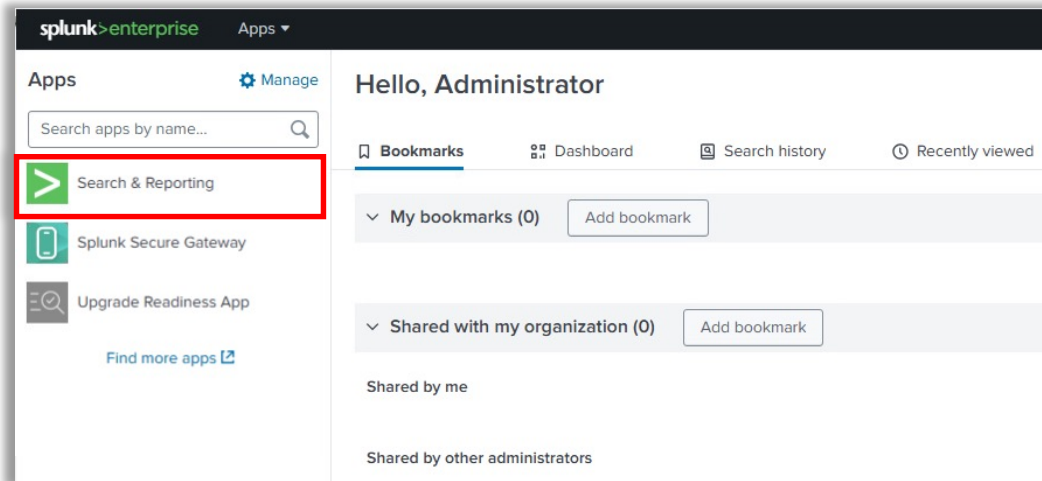
- Your Splunk IP – is the IP address of the system where your Splunk Enterprise is running.
- HEC Token – is the Token Value of the HTTP Event Collector Token you created in previous step

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

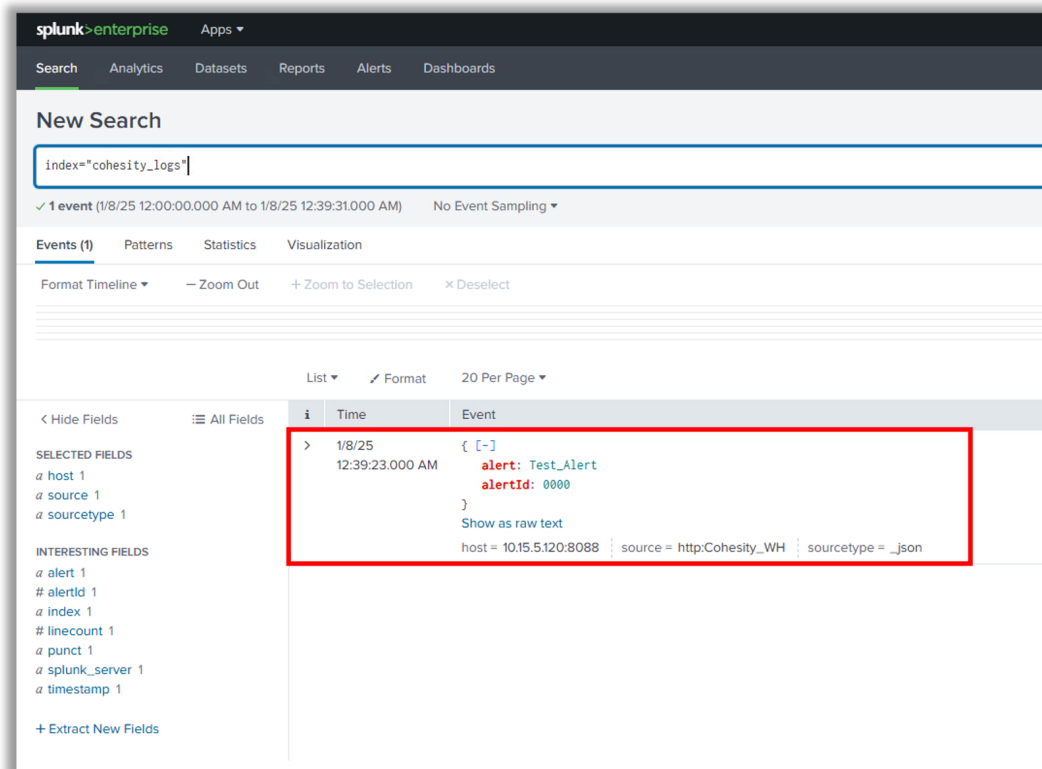
```
shashanka.sr@COH-J6CJPK74WG ~ % curl -k "https://10.15.5.120:8088/services/collector/raw" \
-H "Authorization: Splunk c37725f2-299e-4f03-929d-12f0d8f0254c" \
-H "Content-Type: application/json" \
-d '{"alert": "Test_Alert", "alertId": "0000"}'
{"text": "Success", "code": "0"}
shashanka.sr@COH-J6CJPK74WG ~ %
```

- 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.



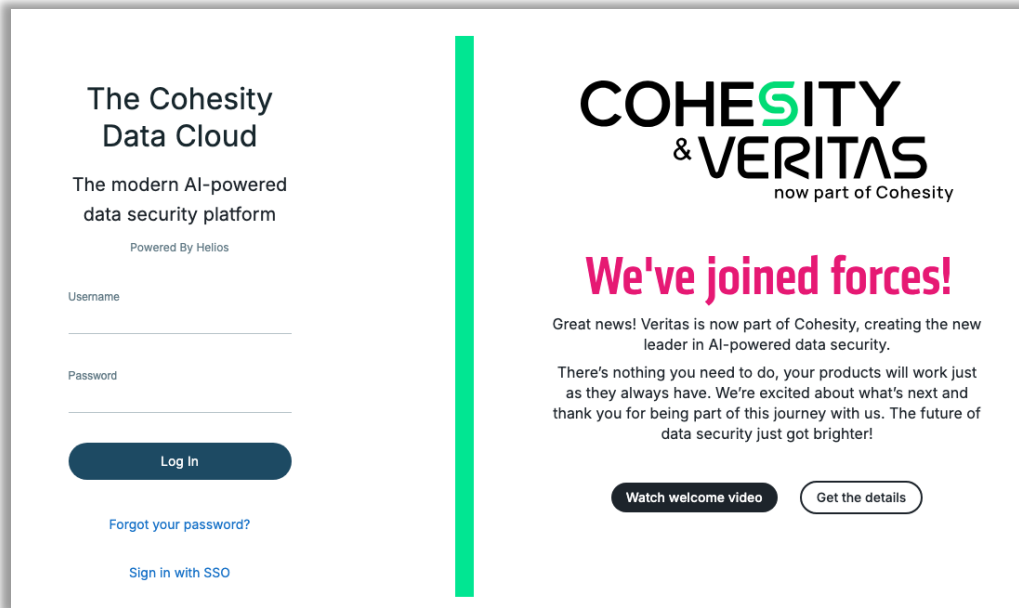
- ii. Run search query to filter logs. You must see the event sent by curl command in Splunk.



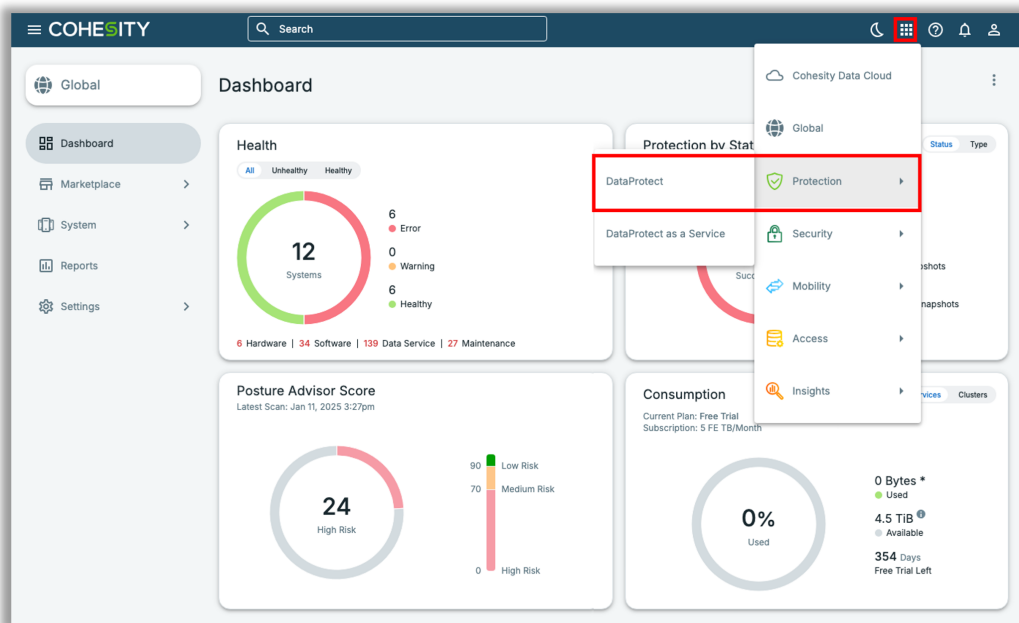
- If you are not receiving the message `{"text": "Success", "code": "0"}` or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

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

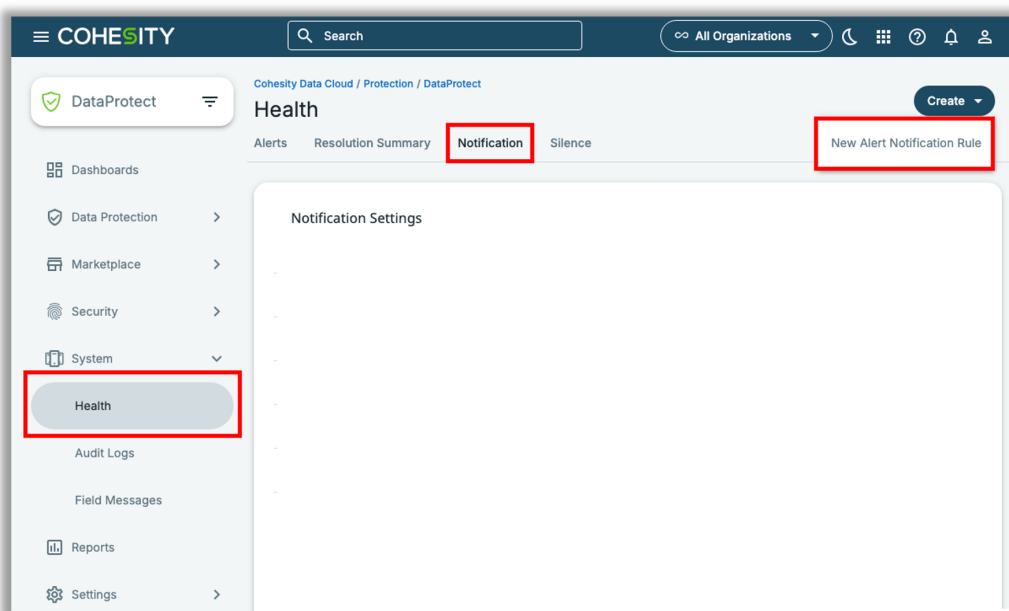
- a. Login to [Cohesity Data Cloud](#).



- 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.

Create Alert Notification Rule

Notification Name

Notification Filters

Notification Frequency
 Real-time Every 6 hours Every 24 hours

Notification Method
 Email
 Webhook
 +

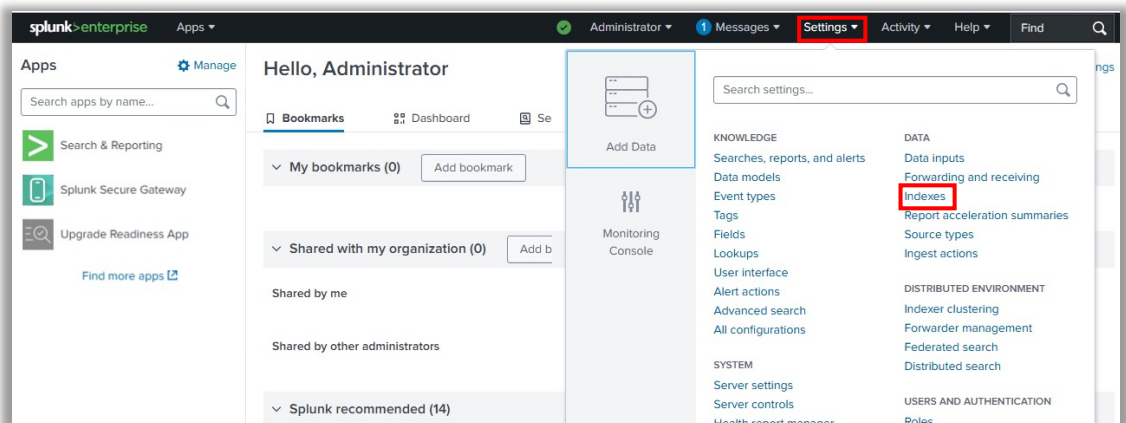
Cancel

NOTE:

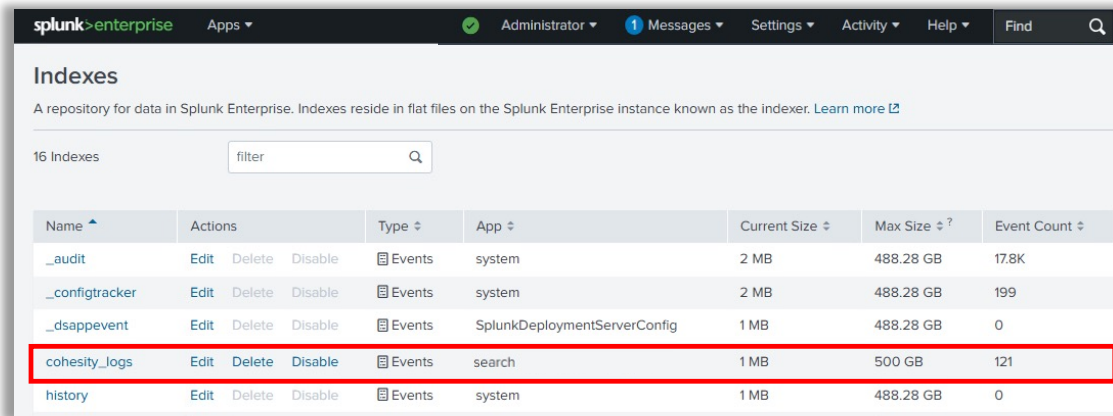
- Use Clusters, Organization, Alert Severity, Alert Type, Alert Category or Alert Name to filter out the selective alerts you want to send to Splunk.
- If you do not select any value for Clusters, Organization, Alert Severity, Alert Type, Alert Category or Alert Name, then all the alerts generated by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



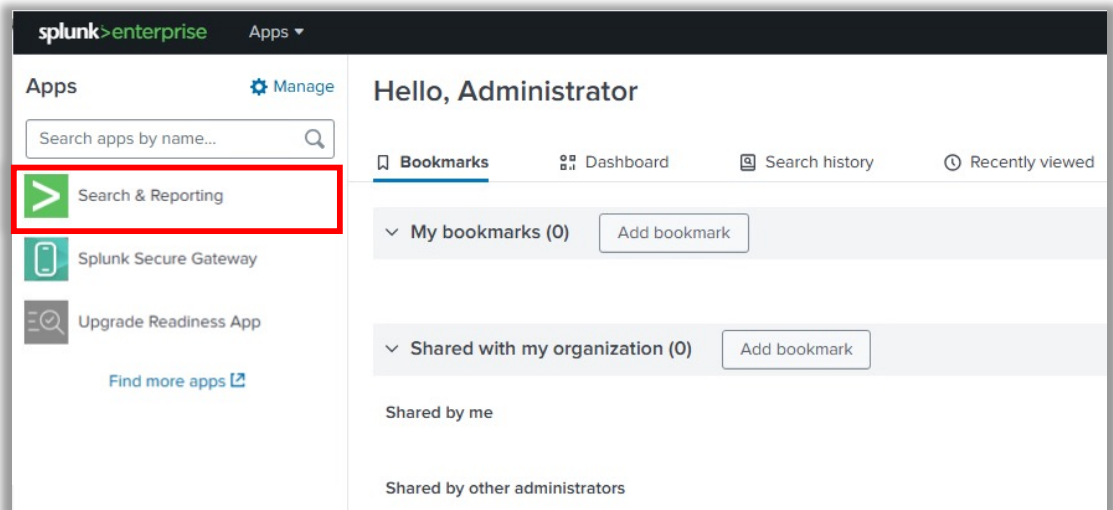
The screenshot shows the Splunk Enterprise 'Indexes' page. A table lists 16 indexes. The 'cohesity_logs' index is highlighted with a red border. The table columns are Name, Actions, Type, App, Current Size, Max Size, and Event Count.

Name	Actions	Type	App	Current Size	Max Size	Event Count
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	17.8K
_configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	199
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	Events	search	1 MB	500 GB	121
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0

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.

The screenshot shows the Splunk Enterprise interface. The search bar contains the query `index=*cohesity_logs`. Below the search bar, it indicates "1 of 1 event matched". The event details are as follows:

Time	Event
1/6/25 11:40:27.000 PM	<pre>{ [-] alertCategory: kNodeHealth alertCode: CE00411001 alertDocument: { [+] } alertState: kOpen alertType: 11001 alertTypeBucket: kSoftware clusterHost: 10.15.10.81 dedupCount: 1418 dedupTimestamps: [[+]] }</pre>

c. Filter search results based on time.

The screenshot shows the Splunk Enterprise interface with the search query `index=*cohesity_logs`. A dropdown menu is open, showing various time range presets. The "Last 24 hours" option is highlighted in red. The dropdown menu is organized into three columns: REAL-TIME, RELATIVE, and OTHER.

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

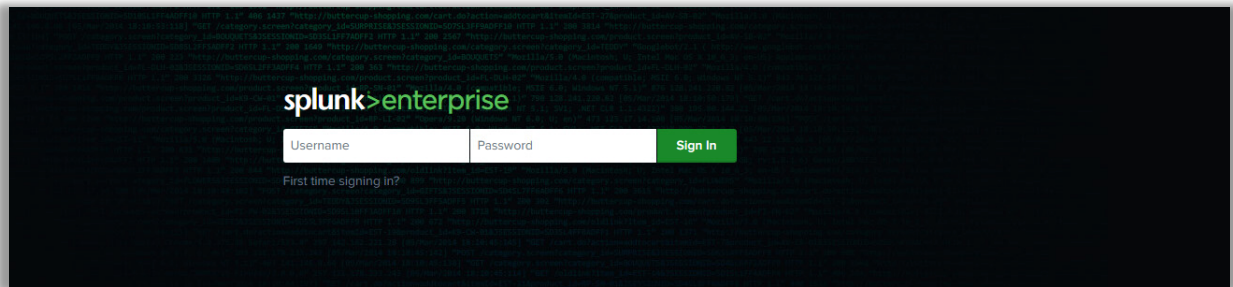
d. Alert and visualize.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a search bar with the query 'index='cohesity_logs''. The search results show '1 of 1 event matched'. A dropdown menu is open under 'Save As', listing options: 'Report', 'Alert', 'Existing Dashboard', 'New Dashboard', and 'Event Type'. The 'Alert' option is highlighted. Below the search results, there's a table with columns for 'Time' and 'Event'. The event details include fields like 'alertCategory', 'alertCode', 'alertDocument', 'alertState', 'alertType', 'alertTypeBucket', 'clusterHost', 'dedupCount', and 'dedupTimestamps'.

NOTE: For more details, refer to the [Search and Reporting](#) section.

DataProtect as a Service [Cohesity SaaS Service]

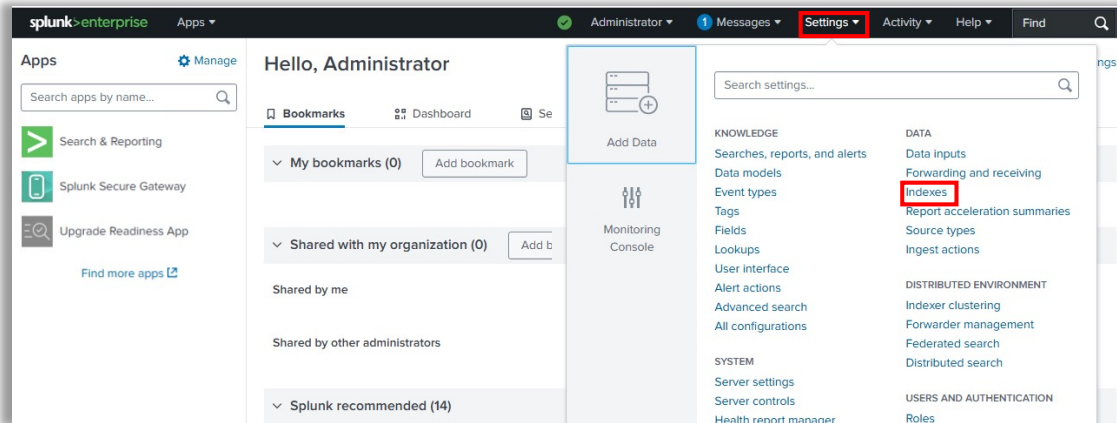
1. Login to your Splunk Enterprise Instance.



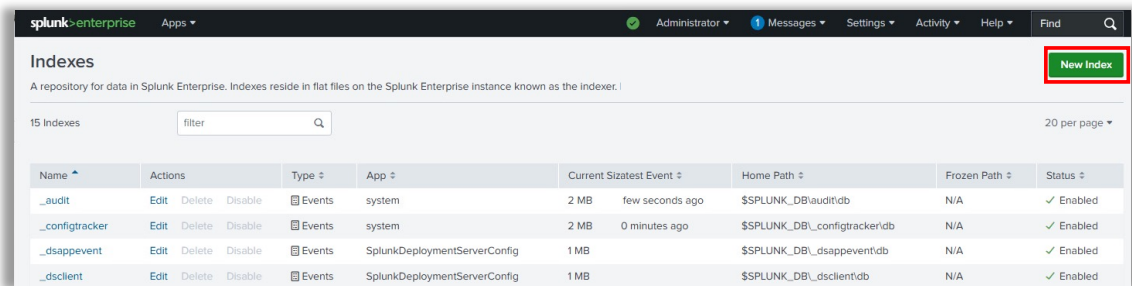
2. Create a new index to store Cohesity logs.

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**.



New Index ×

Index Data Type Events Metrics

The type of data to store (event-based or metrics).

Home Path

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path

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 GB ▾

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket GB ▾

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App

Save Cancel

b. You can see the newly created index under Indexes

splunk>enterprise Apps ▾

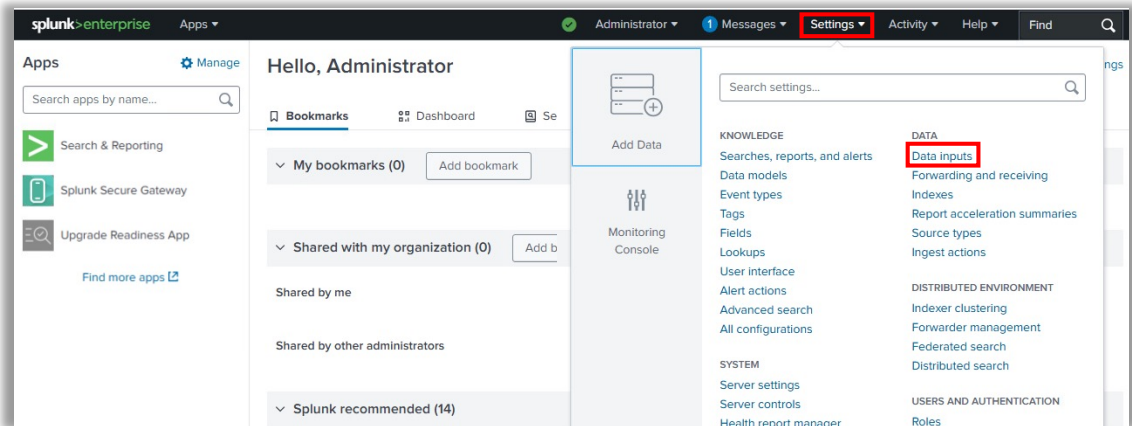
Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. [Learn more](#)

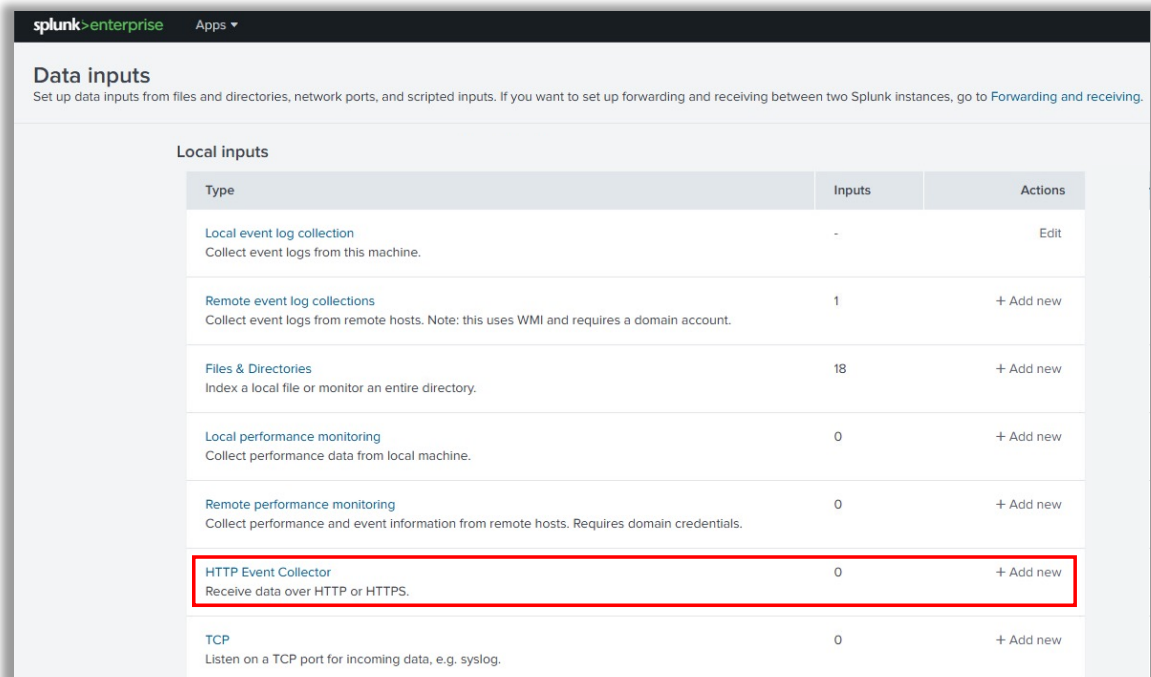
16 Indexes

Name ▲	Actions	Type ▾	App ▾	Current Size ▾	Max Size ▾ ?	Event Count ▾
._audit	Edit Delete Disable	<input checked="" type="radio"/> Events	system	2 MB	488.28 GB	117K
._configtracker	Edit Delete Disable	<input checked="" type="radio"/> Events	system	2 MB	488.28 GB	186
._dsappevent	Edit Delete Disable	<input checked="" type="radio"/> Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	<input checked="" type="radio"/> Events	search	1 MB	500 GB	0
history	Edit Delete Disable	<input checked="" type="radio"/> Events	system	1 MB	488.28 GB	0
main	Edit Delete Disable	<input checked="" type="radio"/> Events	system	1 MB	488.28 GB	0

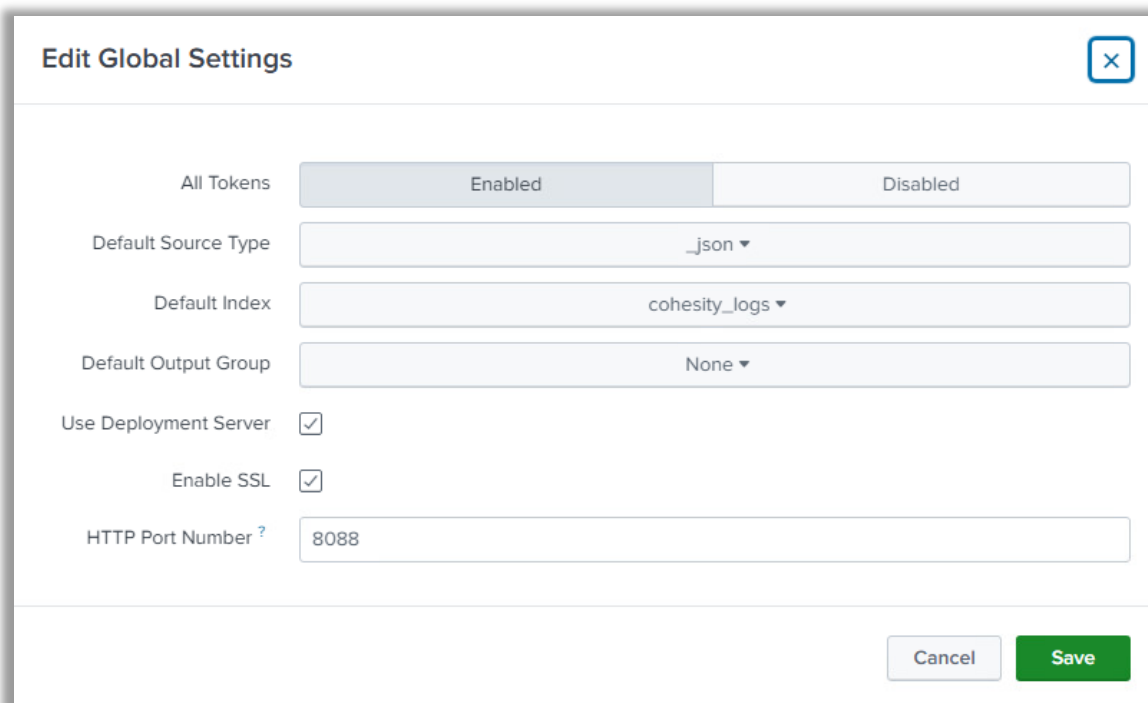
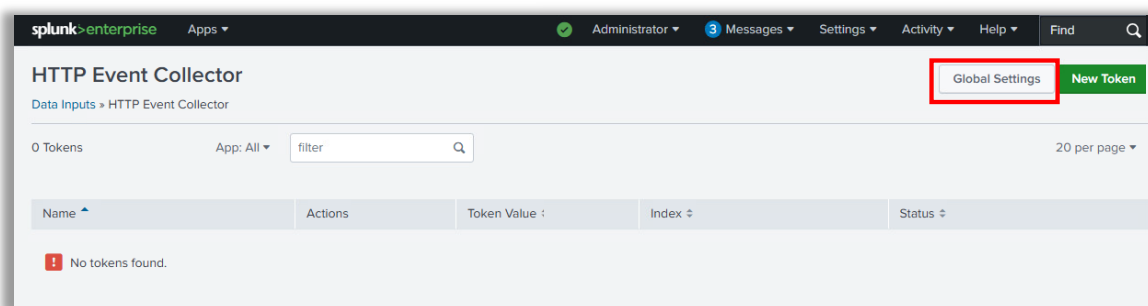
4. Configure HTTP Event Collector to receive data from Cohesity.
 - a. Click **Data Inputs** under **Data** in **Settings**.



- b. Click **HTTP Event Collector**.

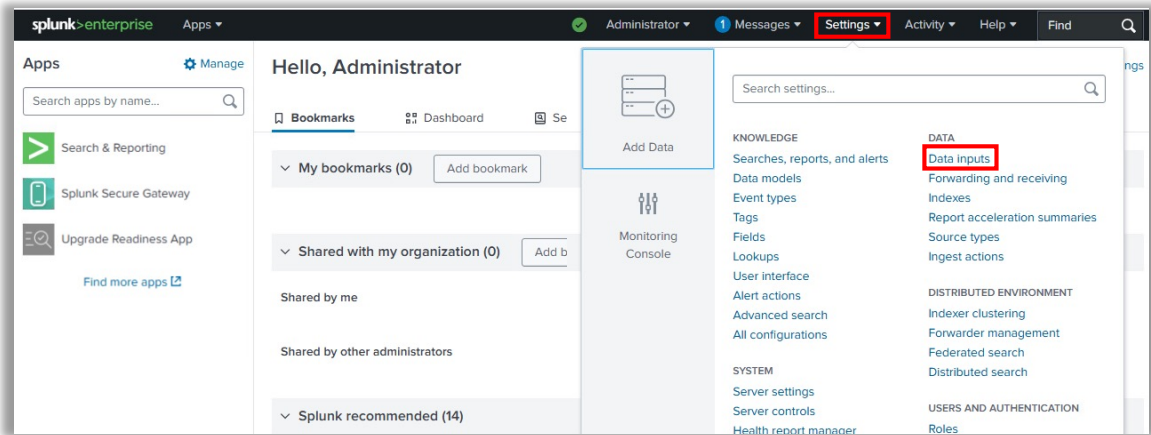


c. Click **Global Settings**.

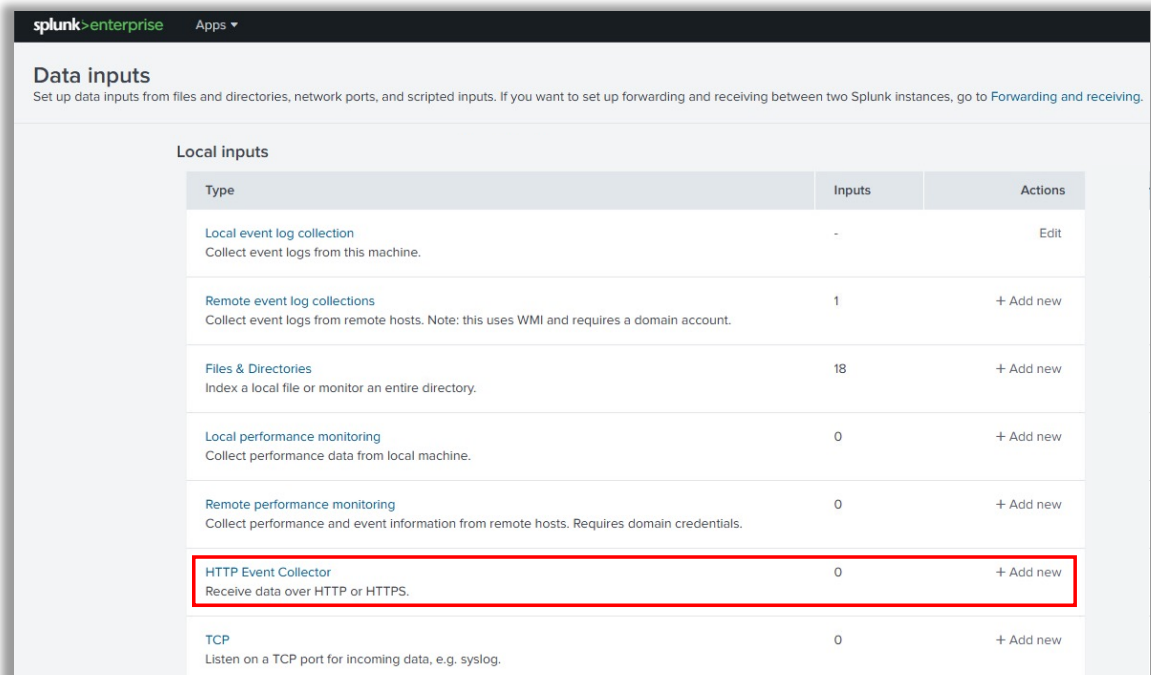


- Select **Enabled** for **All Tokens**.
- Select the **Default Source Type** as **_json** (If it is not shown under the dropdown, then type **_json** in search bar to bring it up).
- Select the **Default index** as the new index we created exclusively for Cohesity logs and alerts under step 1.
- By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

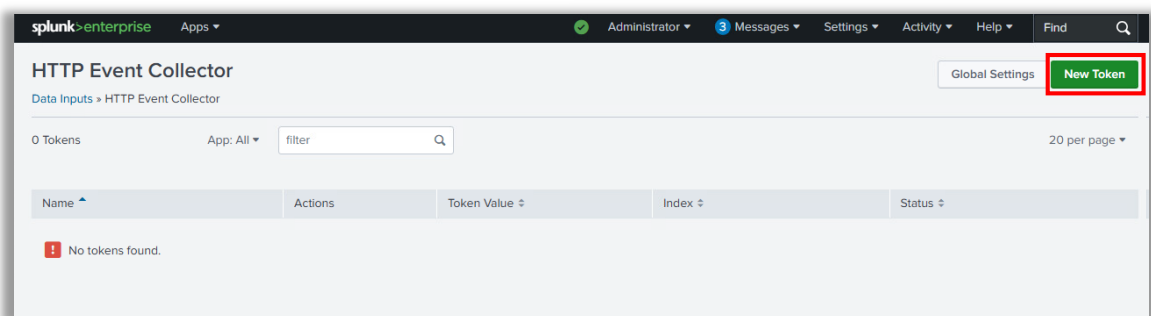
5. Create a new token to authenticate Cohesity.
 - a. Click **Data Inputs** under **Data** in **Settings**.



- b. Click **HTTP Event Collector**.



- c. Click **New Token**.



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

The screenshot shows the 'Add Data' configuration page in Splunk Enterprise. The 'Name' field is set to 'Cohesity_Webhook_Token' and is highlighted with a red box. The 'Next >' button is also highlighted with a red box. The page shows a progress bar with 'Select Source' completed and 'Input Settings' in progress. On the left, there is a sidebar with various data source options, and on the right, there are fields for 'Source name override', 'Description', and 'Output Group', along with an 'Enable indexer acknowledgement' checkbox and an FAQ section.

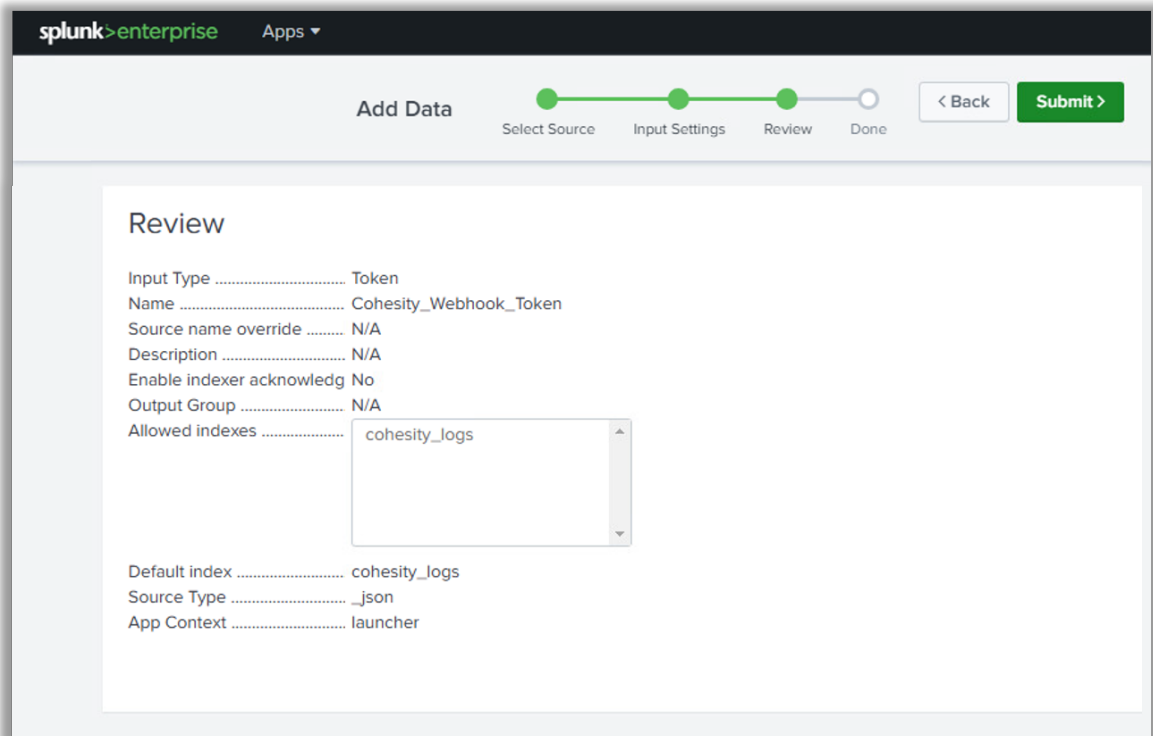
- e. Under **Input Settings**, For **Source Type**, choose **Select** and then click **Select Source Type**, Select **_json** from the dropdown. If it is not shown under the dropdown, then type **_json** in search bar to bring it up.

The screenshot shows the 'Input Settings' page in Splunk Enterprise. The 'Source type' is set to 'Select' and is highlighted with a red box. The 'Select Source Type' dropdown is open, showing '_json' selected and highlighted with a red box. The page shows a progress bar with 'Select Source' and 'Input Settings' completed and 'Review' in progress. On the left, there is a sidebar with various data source options, and on the right, there are fields for 'Index' and 'Default Index'.

- 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.

The screenshot shows the 'Input Settings' page in Splunk Enterprise. At the top, there's a progress bar with four steps: 'Select Source', 'Input Settings', 'Review', and 'Done'. The 'Input Settings' step is currently active. Below the progress bar, there are navigation buttons: '< Back' and 'Review >'. The main content area is titled 'Input Settings' and includes a sub-header: 'Optionally set additional input parameters for this data input as follows:'. There are two main sections: 'Source type' and 'Index'. The 'Source type' section has a description and buttons for 'Automatic', 'Select', and 'New', with a dropdown menu currently set to '_json'. The 'Index' section has a description and a 'Learn More' link. Below the description, there are three columns: 'Select Allowed Indexes', 'Available item(s)', and 'Selected item(s) remove all'. The 'Available item(s)' column lists 'cohesity_logs', 'history', 'main', and 'summary'. The 'Selected item(s)' column contains 'cohesity_logs'. The 'Default Index' dropdown is also set to 'cohesity_logs'. A 'Create a new index' link is visible at the bottom right of the index selection area.

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



splunk>enterprise Apps ▾

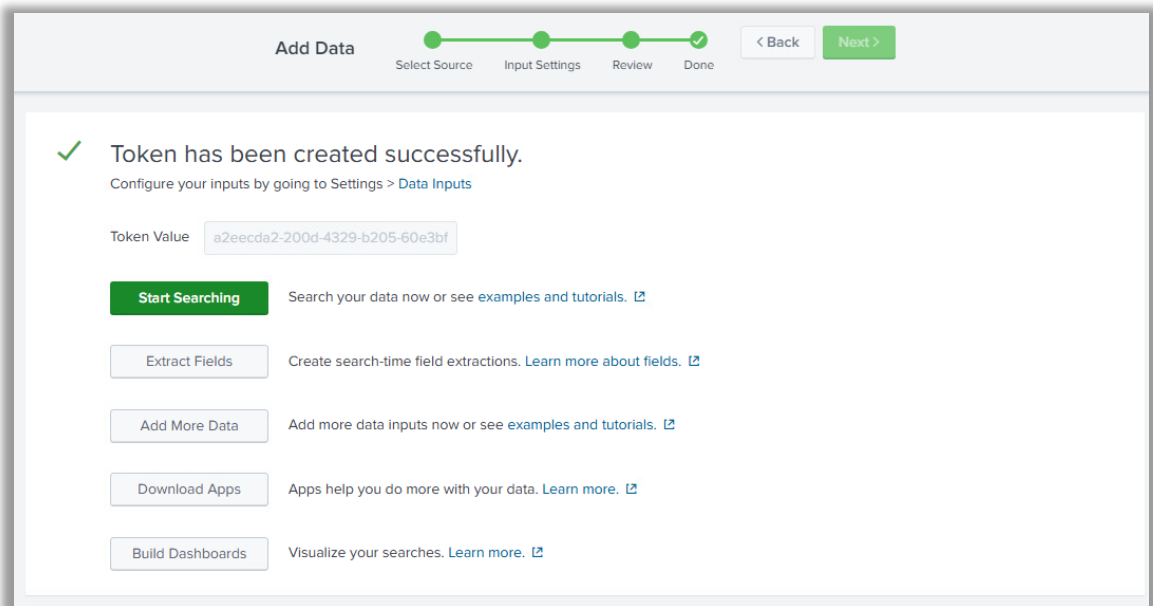
Add Data Select Source Input Settings **Review** Done < Back Submit >

Review

Input Type Token
 Name Cohesity_Webhook_Token
 Source name override N/A
 Description N/A
 Enable indexer acknowledg No
 Output Group N/A
 Allowed indexes

Default index cohesity_logs
 Source Type _json
 App Context launcher

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



Add Data Select Source Input Settings Review **Done** < Back Next >

✓ **Token has been created successfully.**
 Configure your inputs by going to Settings > [Data Inputs](#)

Token Value

Start Searching Search your data now or see [examples and tutorials](#). [🔗](#)

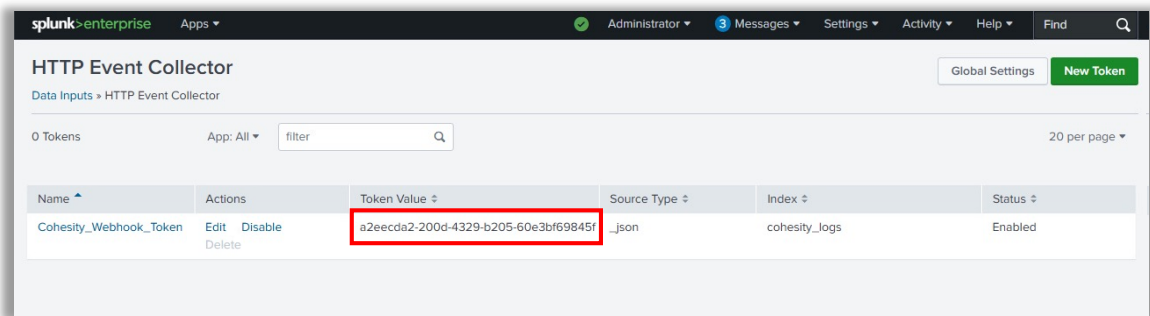
Extract Fields Create search-time field extractions. [Learn more about fields](#). [🔗](#)

Add More Data Add more data inputs now or see [examples and tutorials](#). [🔗](#)

Download Apps Apps help you do more with your data. [Learn more](#). [🔗](#)

Build Dashboards Visualize your searches. [Learn more](#). [🔗](#)

- 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.

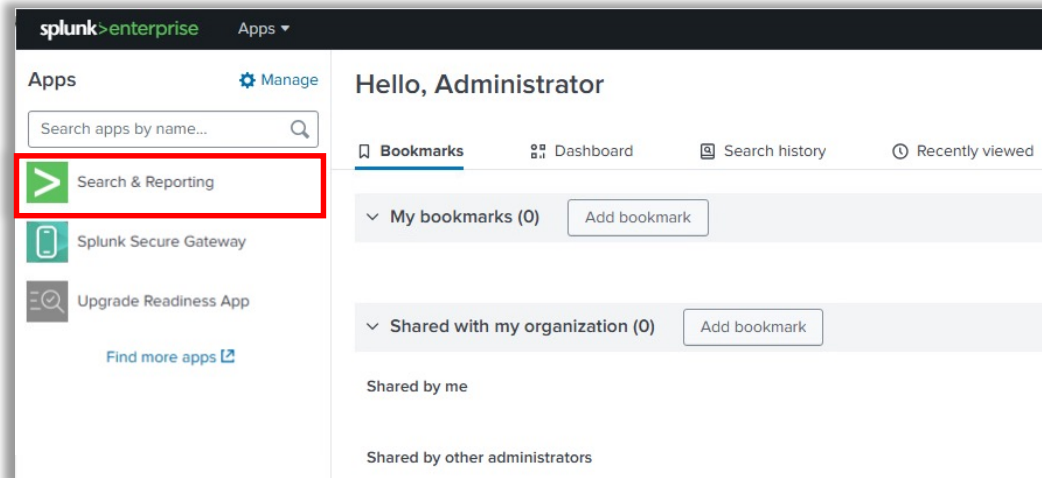
```
shashanka.sr@COH-J6CJPK74WG ~ % curl -k "https://10.15.5.120:8088/services/collector/raw" \
-H "Authorization: Splunk c37725f2-299e-4f03-929d-12f0d8f0254c" \
-H "Content-Type: application/json" \
-d '{"alert": "Test_Alert", "alertId": "0000"}'
{"text": "Success", "code": "0"}
shashanka.sr@COH-J6CJPK74WG ~ %
```

NOTE:

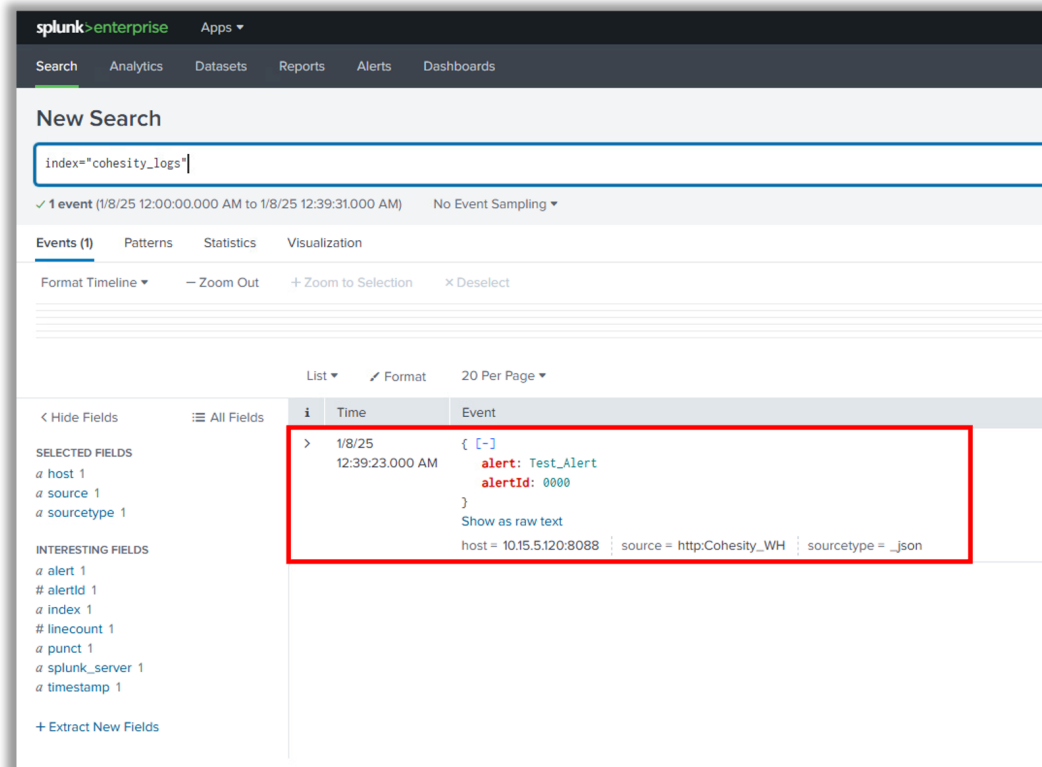
- If you are not receiving the message `{"text": "Success", "code": "0"}` or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

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

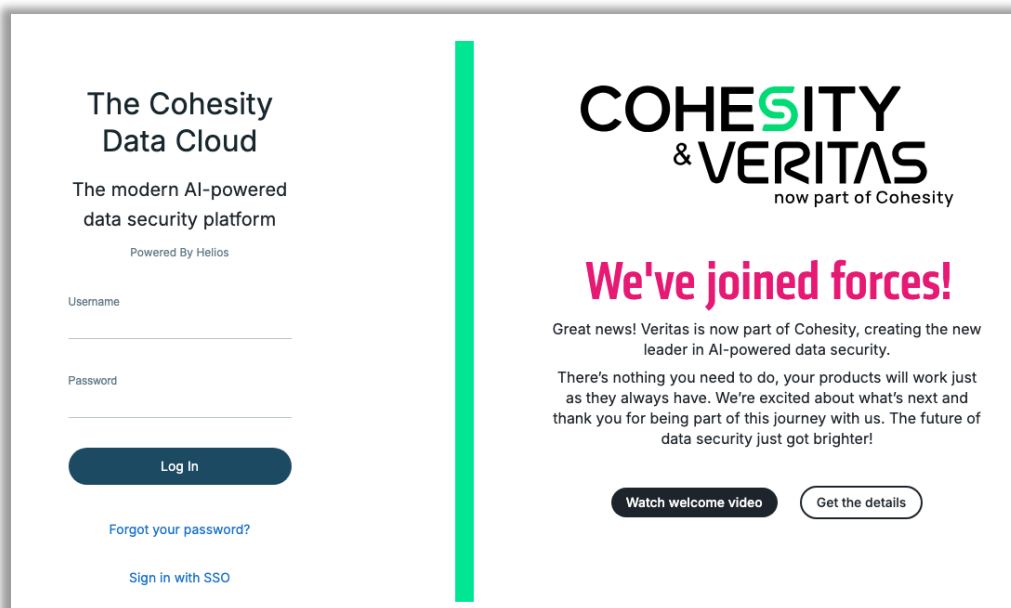


NOTE:

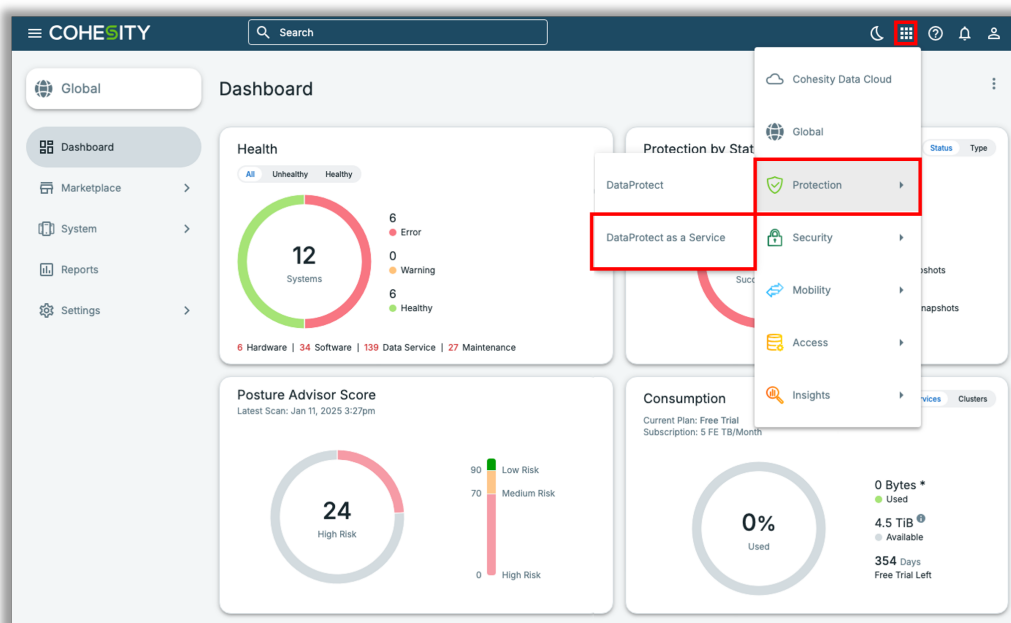
- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

8. Configure alert notification with webhook on Cohesity Data Cloud

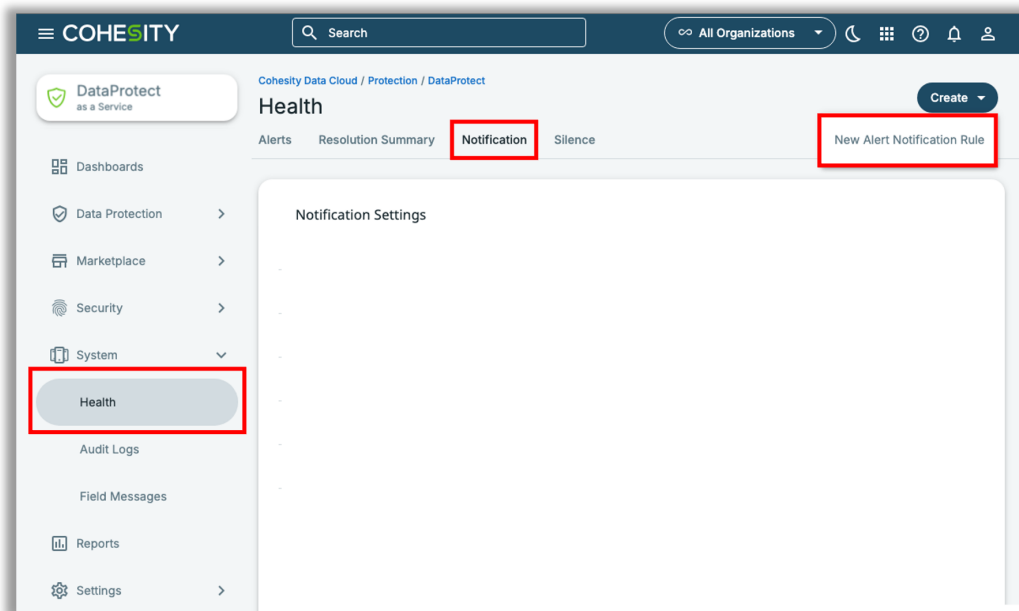
- Login to [Cohesity Data Cloud](#).



- 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.

Create Alert Notification Rule

Notification Name

Notification Filters

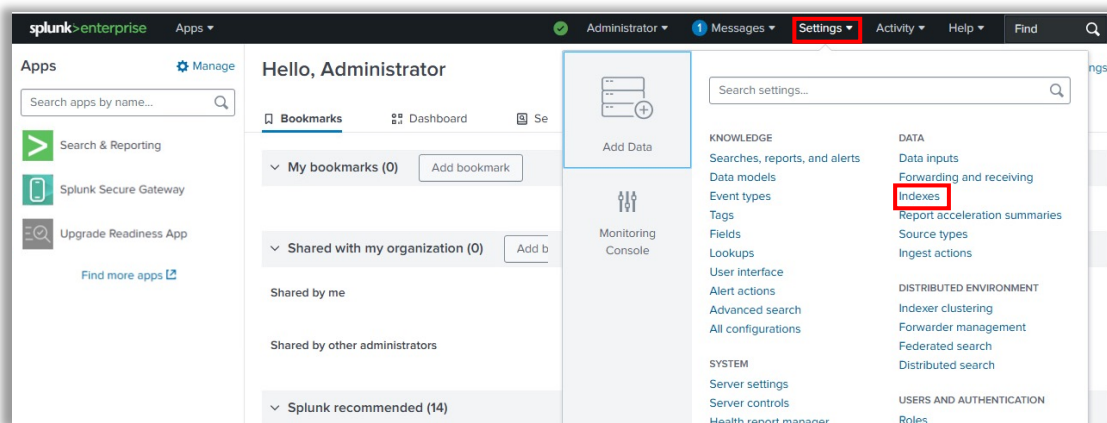
Notification Frequency
 Real-time Every 6 hours Every 24 hours

Notification Method
 Email
 Webhook

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.

The screenshot shows the Splunk Enterprise 'Indexes' page. A table lists 16 indexes. The 'cohesity_logs' index is highlighted with a red border. The table columns are Name, Actions, Type, App, Current Size, Max Size, and Event Count.

Name	Actions	Type	App	Current Size	Max Size	Event Count
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	17.8K
_configtracker	Edit Delete Disable	Events	system	2 MB	488.28 GB	199
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0
cohesity_logs	Edit Delete Disable	Events	search	1 MB	500 GB	121
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0

10. Search, alert and visualize.

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

The screenshot shows the Splunk Web Home interface. The left sidebar contains a list of apps. The 'Search & Reporting' app is highlighted with a red box. The main content area shows a 'Hello, Administrator' message and a 'Bookmarks' section.

b. Run search query to filter logs.

The screenshot shows the Splunk Enterprise interface. The search bar contains the query `index=*cohesity_logs`. Below the search bar, it indicates "1 of 1 event matched" and "No Event Sampling". The search results are displayed in a table format with columns for Time and Event. The event details are as follows:

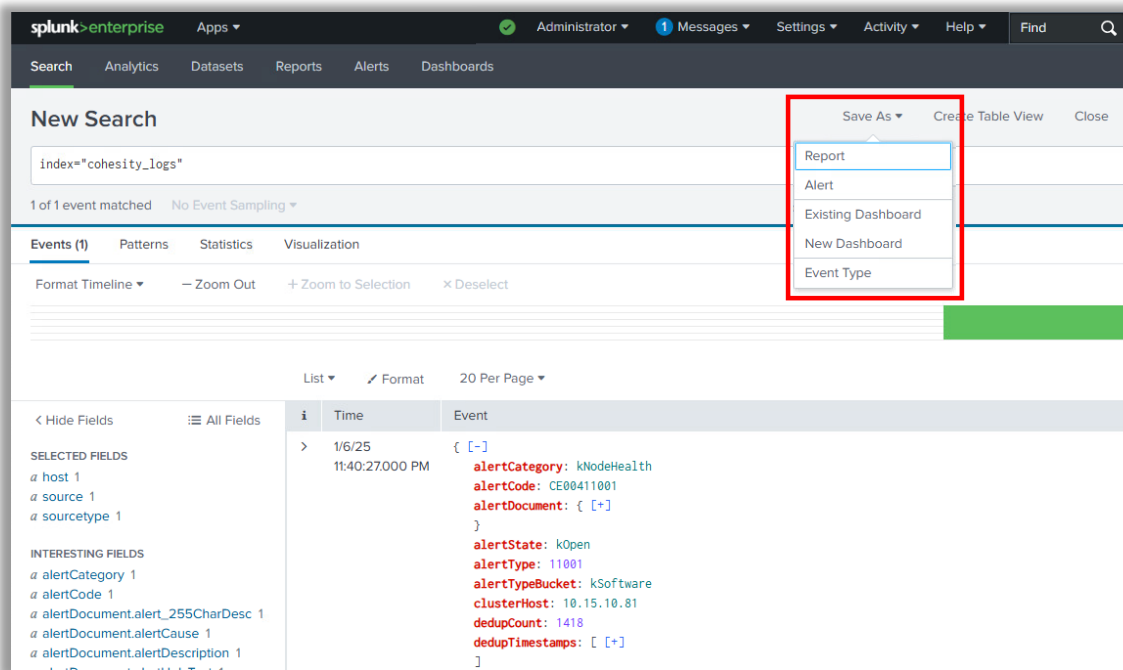
Time	Event
1/6/25 11:40:27.000 PM	<pre>{ [-] alertCategory: kNodeHealth alertCode: CE00411001 alertDocument: { [+] } alertState: kOpen alertType: 11001 alertTypeBucket: kSoftware clusterHost: 10.15.10.81 dedupCount: 1418 dedupTimestamps: [[+]] }</pre>

c. Filter search results based on time.

The screenshot shows the Splunk Enterprise interface with the search query `index=*cohesity_logs`. A dropdown menu is open, showing various time range options. The dropdown menu is titled "Presets" and is divided into three columns: REAL-TIME, RELATIVE, and OTHER. The options are as follows:

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

d. Alert and visualize.



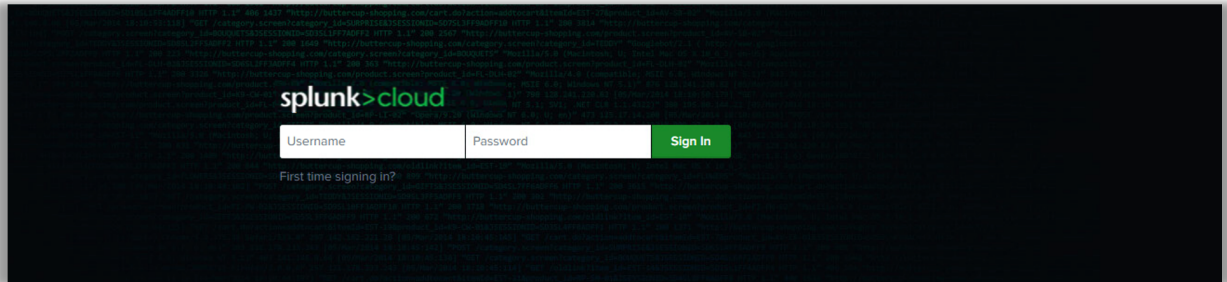
NOTE: For more details, refer to the [Search and Reporting](#) section.



Integrate Cohesity with Splunk Cloud

Self-managed Cohesity Clusters

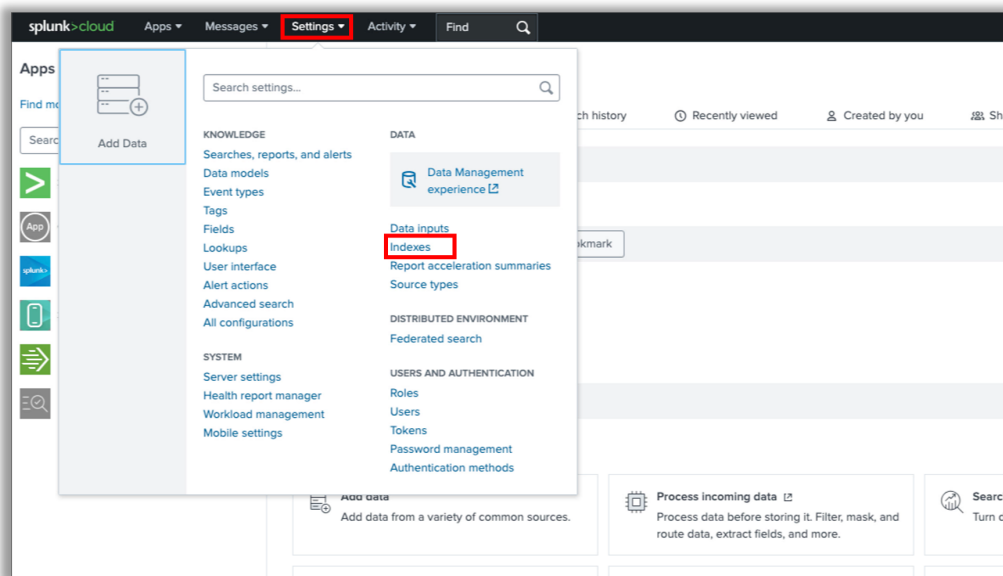
1. Login to your Splunk Cloud Instance.



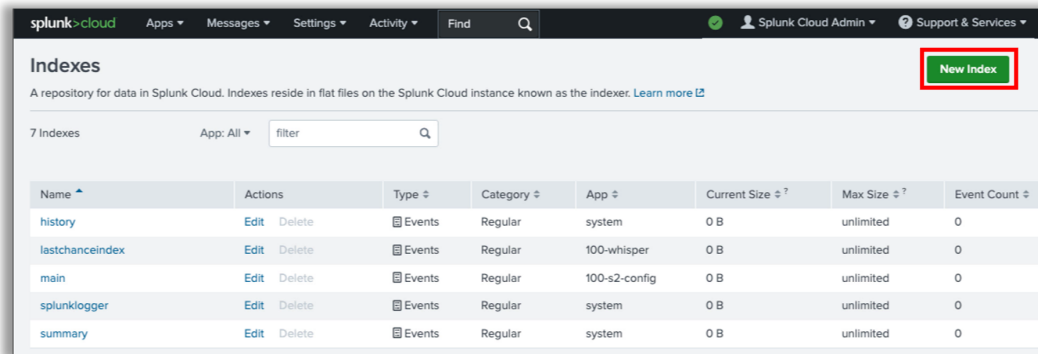
2. Create a new index to store Cohesity logs.

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**.

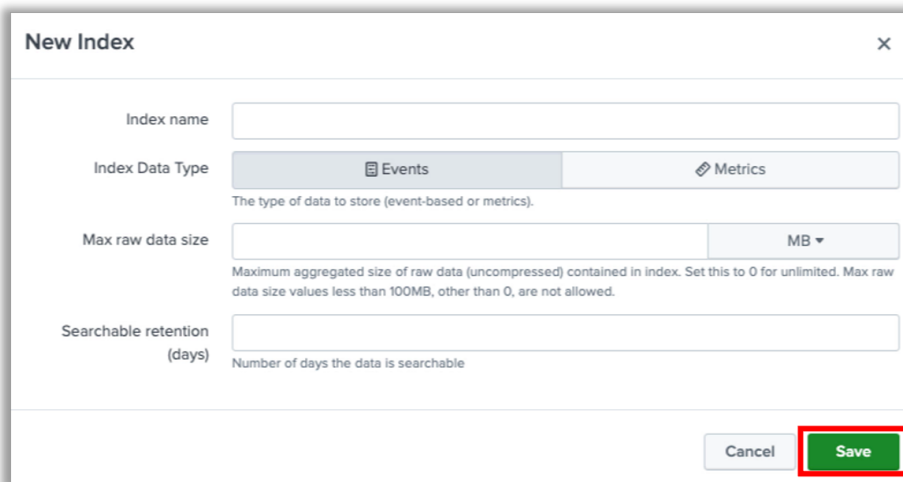


- b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type**. Define the maximum size and retention for data and click **Save**.



The screenshot shows the Splunk Cloud interface with the 'Indexes' page. A 'New Index' button is highlighted with a red box in the top right corner. Below the header, there is a table listing existing indexes:

Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0



The screenshot shows the 'New Index' configuration form. The 'Index Data Type' is set to 'Events'. The 'Max raw data size' is set to 500 MB. The 'Searchable retention (days)' is set to 0. The 'Save' button is highlighted with a red box.

Index name:

Index Data Type: Events Metrics

The type of data to store (event-based or metrics).

Max raw data size: MB

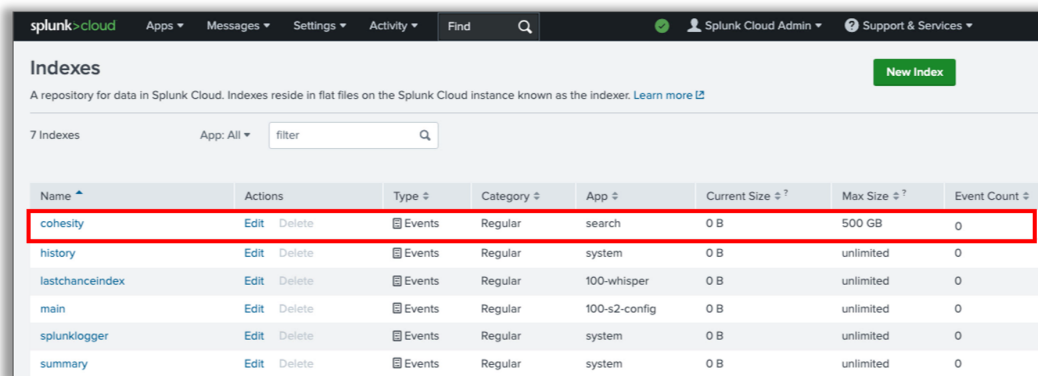
Maximum aggregated size of raw data (uncompressed) contained in index. Set this to 0 for unlimited. Max raw data size values less than 100MB, other than 0, are not allowed.

Searchable retention (days):

Number of days the data is searchable

Buttons: Cancel, Save

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

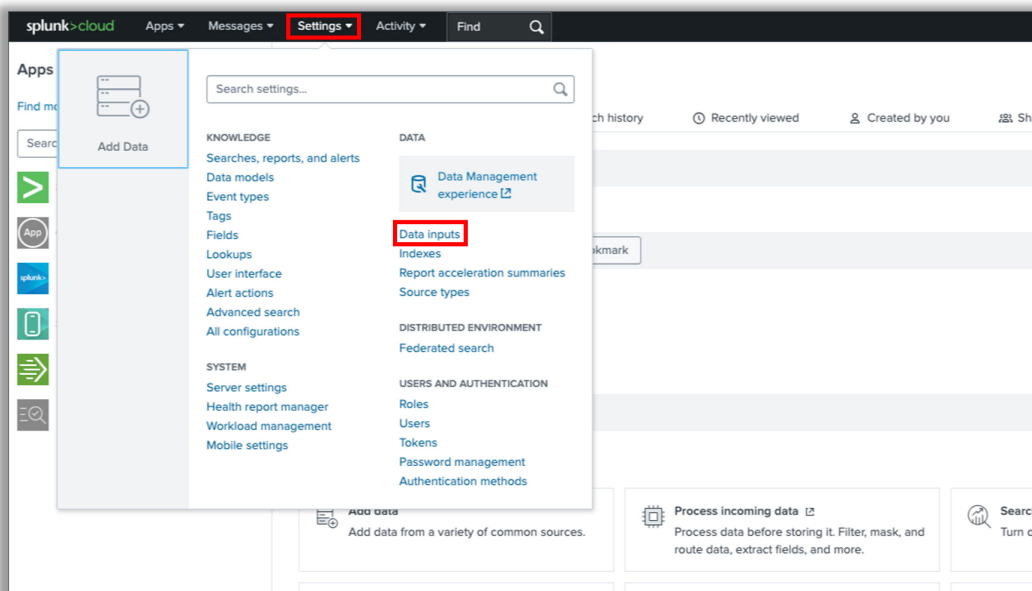


The screenshot shows the Splunk Cloud interface with the 'Indexes' page. The newly created 'cohesity' index is highlighted with a red box in the table below:

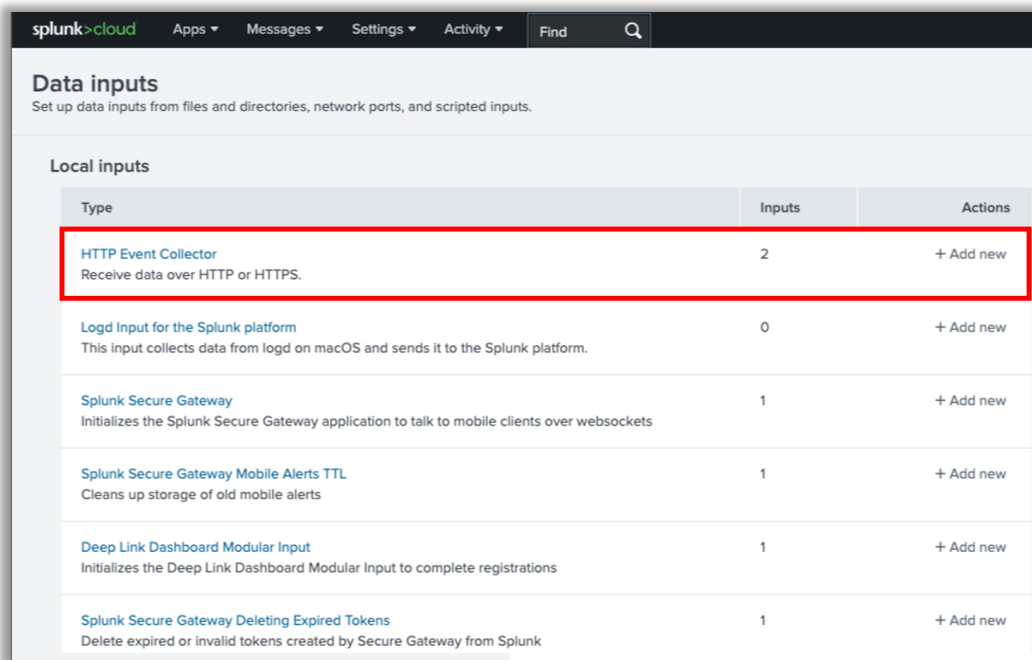
Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
cohesity	Edit Delete	Events	Regular	search	0 B	500 GB	0
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0

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

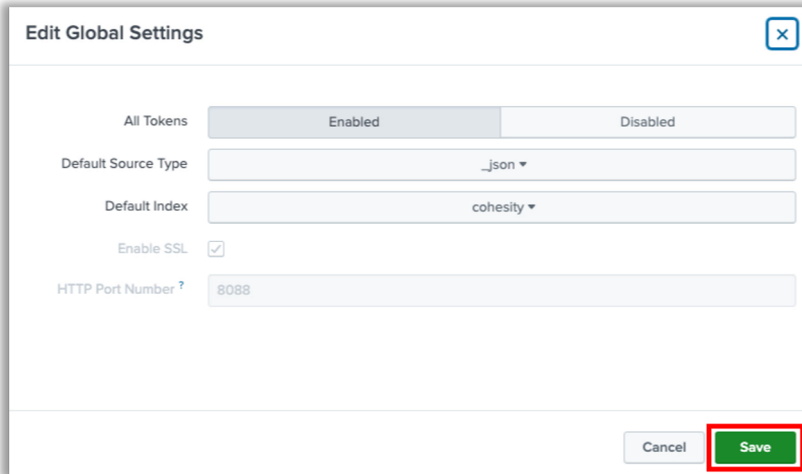
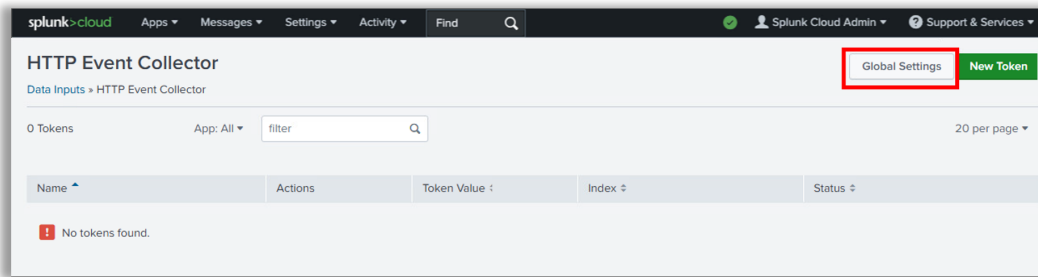
- a. Click **Data Inputs** under **Data** in **Settings**.



- b. Click **HTTP Event Collector**.

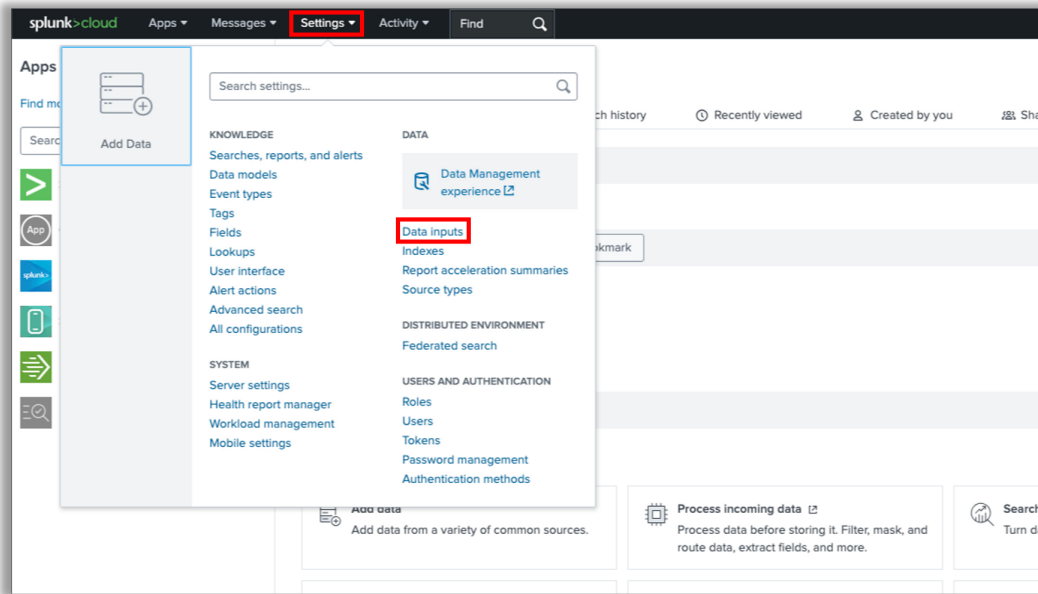


- c. Click **Global Settings** and fill in all requested details and click **Save**.

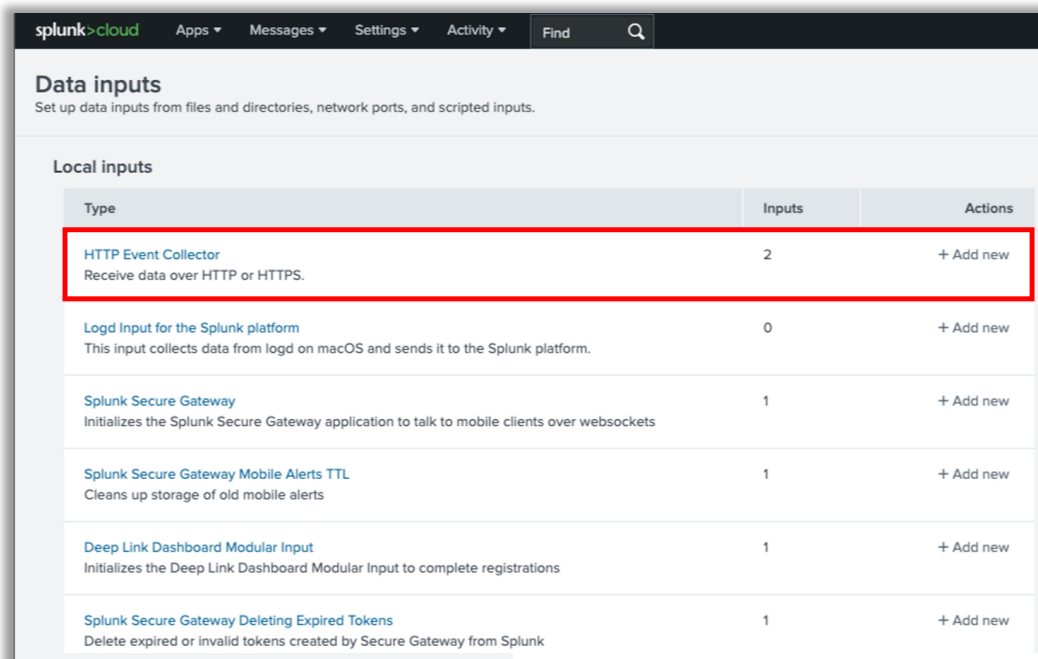


- Select Enabled for All Tokens.
 - Select the Default Source Type as _json (If it is not shown under the dropdown, then type _json in search bar to bring it up).
 - Select the Default index as the new index we created exclusively for Cohesity logs and alerts under step 1.
 - By default, SSL is enabled 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.

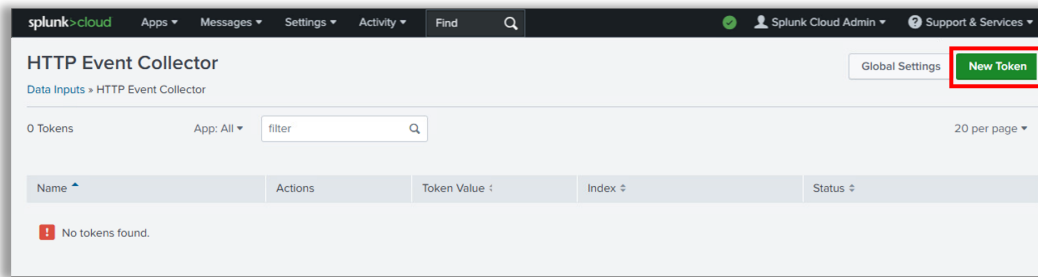
- a. Click **Data Inputs** under **Data** in **Settings**.



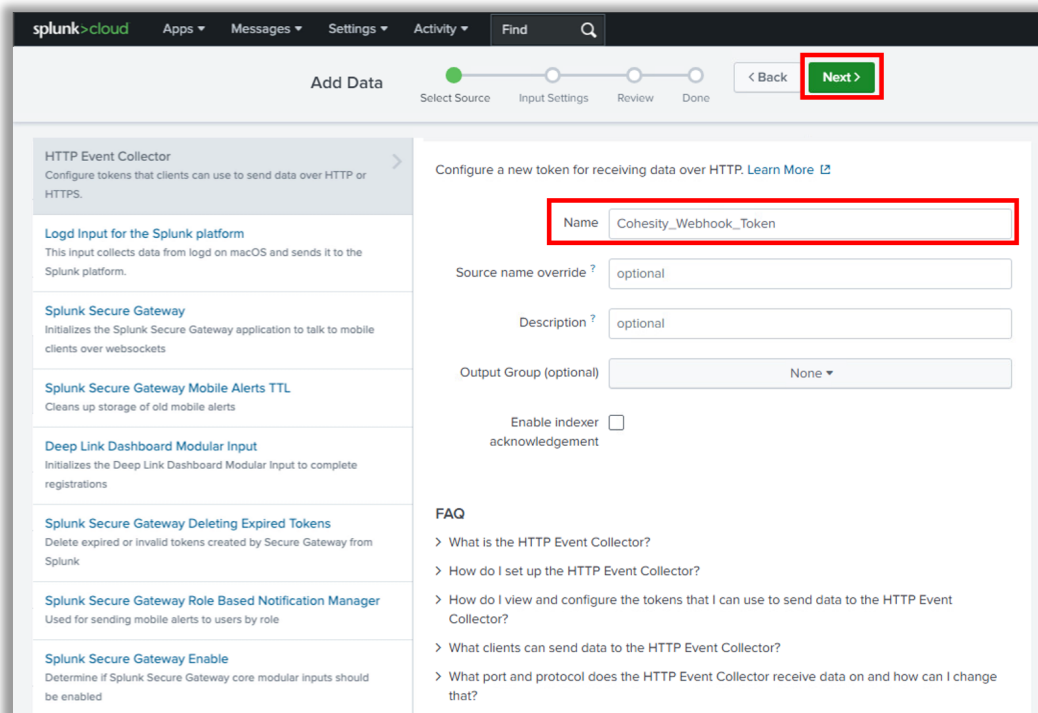
- b. Click **HTTP Event Collector**.



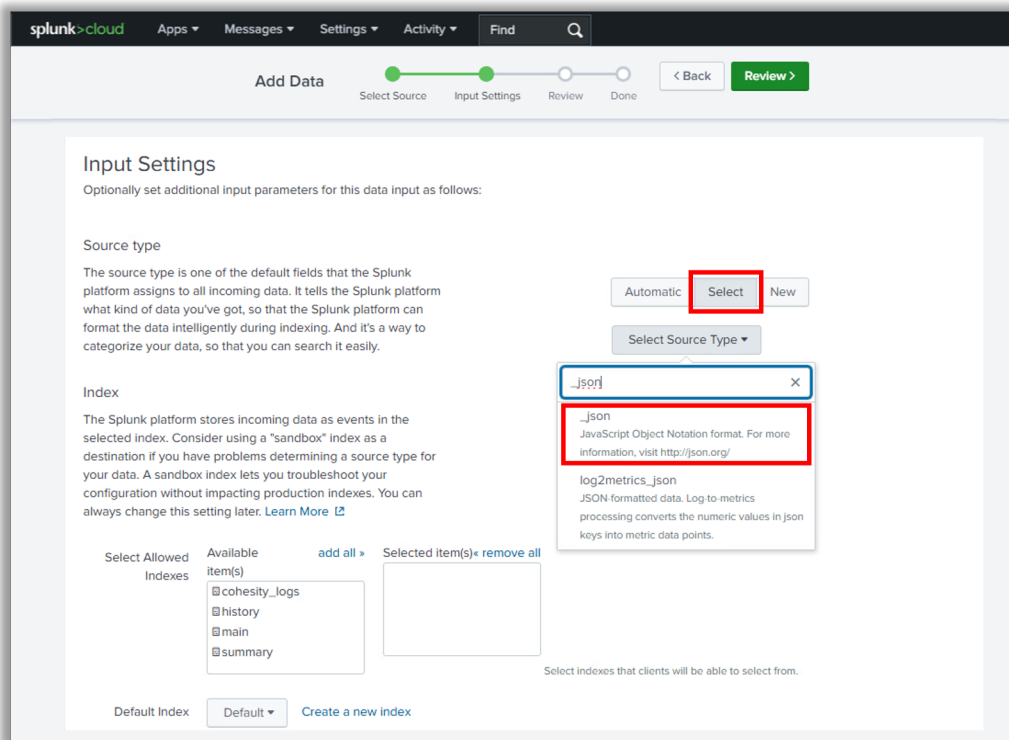
c. Click **New Token**.



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.

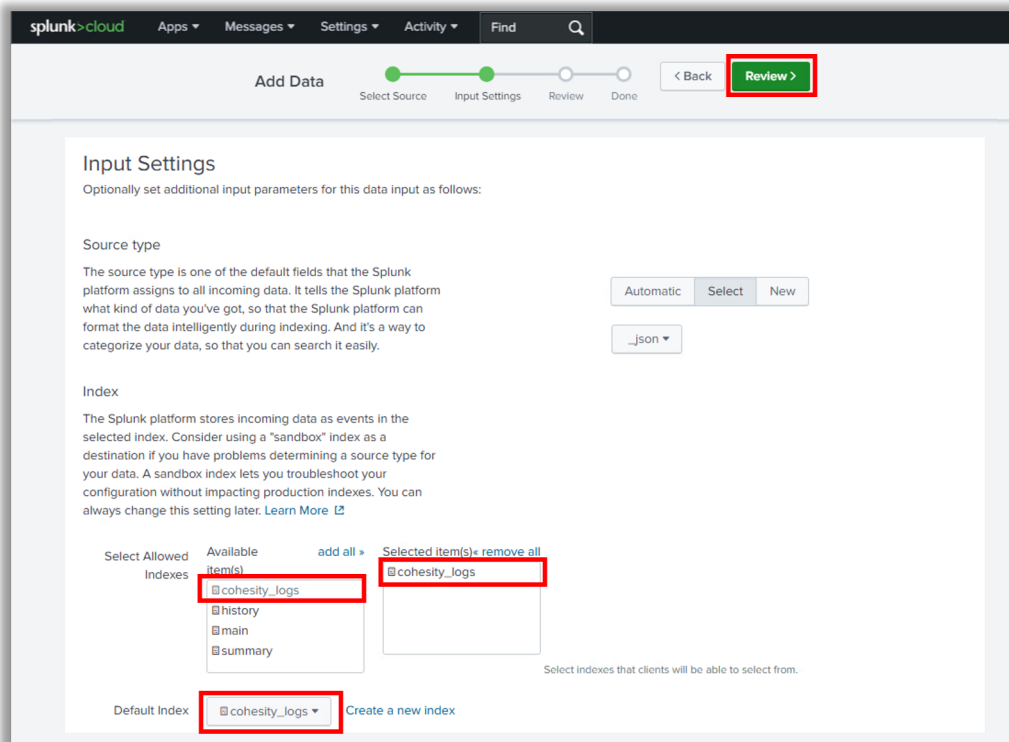


The screenshot shows the Splunk Cloud interface for configuring data input. At the top, there's a navigation bar with 'splunk > cloud' and menu items for 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. Below this is a progress bar for 'Add Data' with steps: 'Select Source', 'Input Settings' (current), 'Review', and 'Done'. A '< Back' button and a 'Review >' button are also present.

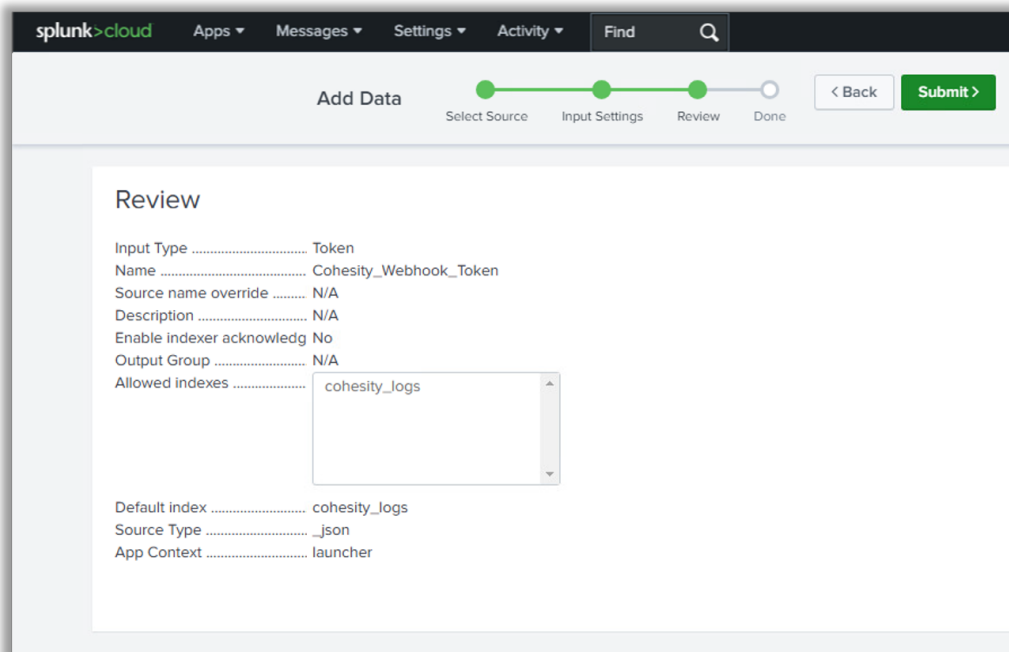
The main content area is titled 'Input Settings' and includes the instruction: 'Optionally set additional input parameters for this data input as follows:'. Under the 'Source type' section, it explains that the source type tells Splunk what kind of data is being ingested. There are three buttons: 'Automatic', 'Select' (highlighted with a red box), and 'New'. Below these is a 'Select Source Type' dropdown menu. The dropdown is open, showing a search bar with '_json' entered and a list of results. The first result, '_json', is highlighted with a red box. Its description is: 'JavaScript Object Notation format. For more information, visit <http://json.org/>'. Below it is another result, 'log2metrics_json', described as 'JSON formatted data. Log to metrics processing converts the numeric values in json keys into metric data points.'

The 'Index' section explains that data is stored as events in a selected index. It suggests using a 'sandbox' index for troubleshooting. Below this is a section for 'Select Allowed Indexes' with a list of available indexes: 'cohesity_logs', 'history', 'main', and 'summary'. There are 'add all >' and 'remove all' buttons. At the bottom, there's a 'Default Index' dropdown set to 'Default' and a 'Create a new index' button.

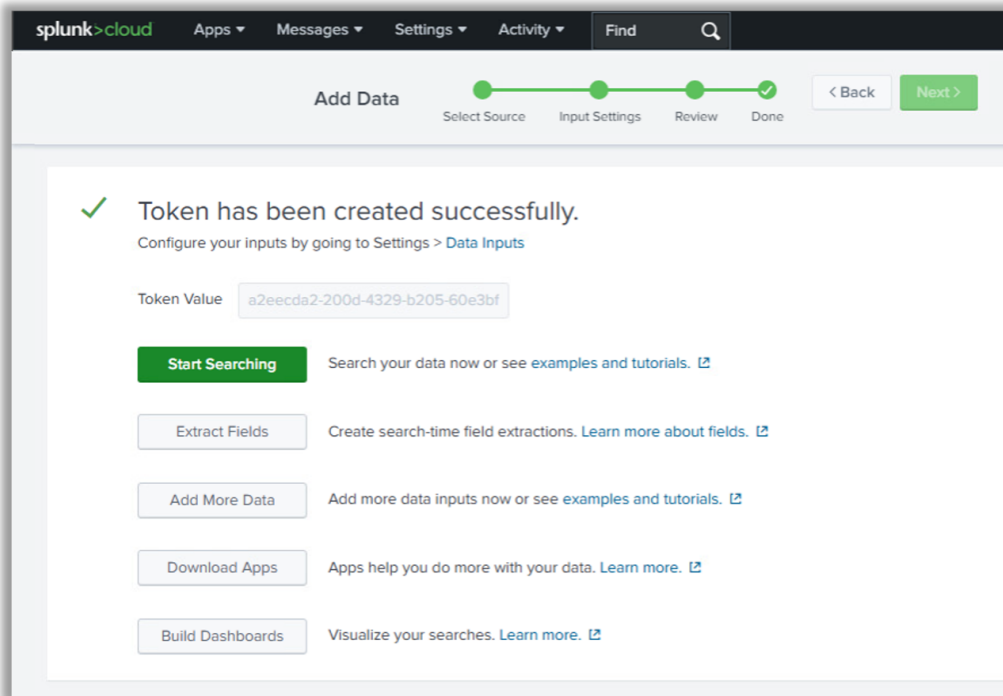
- f. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.



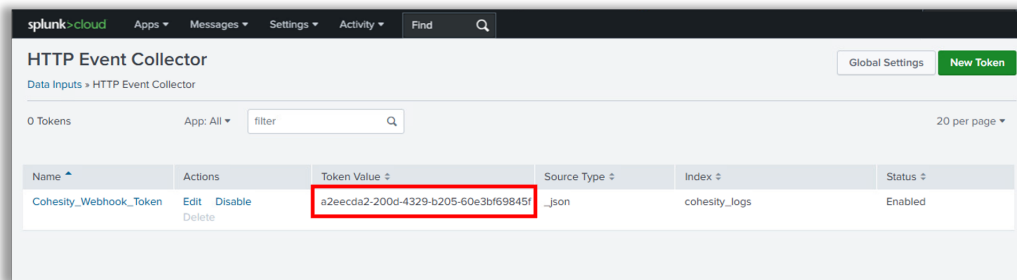
- g. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.



- 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}
```

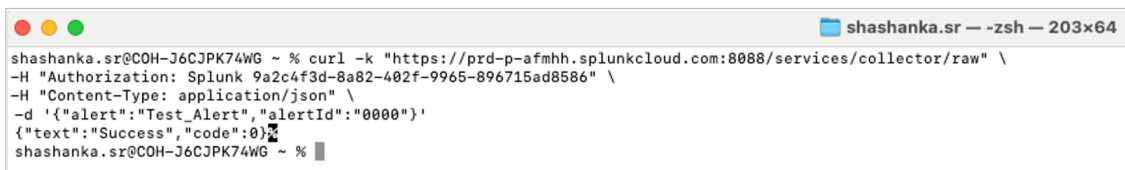
- c. If you get a **404 Not Found** or similar error, it indicates an issue with the URL or HEC configuration. Revisit previous steps to configure the HEC properly.

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:



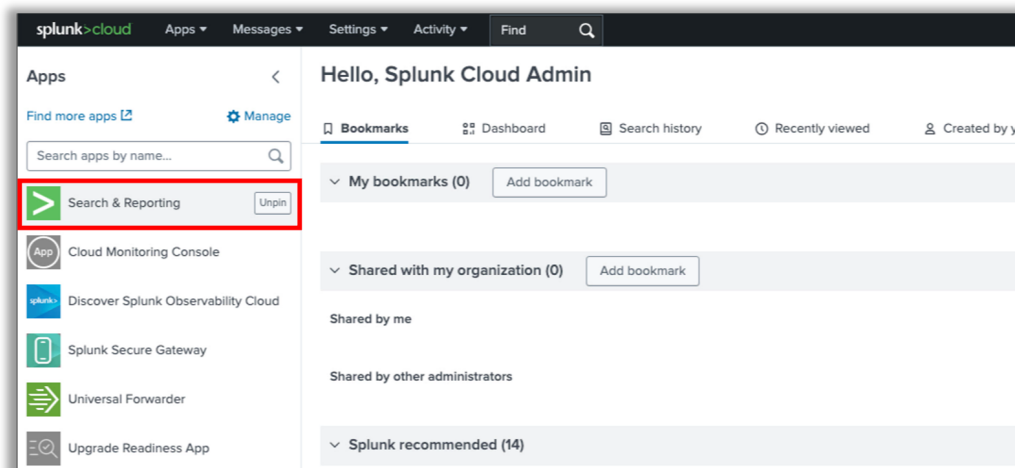
```
shashanka.sr@C0H-J6CJPK74WG ~ % curl -k "https://prd-p-afmh.splunkcloud.com:8088/services/collector/raw" \
-H "Authorization: Splunk 9a2c4f3d-8a82-402f-9965-896715ad8586" \
-H "Content-Type: application/json" \
-d '{"alert": "Test_Alert", "alertId": "0000"}'
{"text": "Success", "code": "0"}
shashanka.sr@C0H-J6CJPK74WG ~ %
```

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.

The screenshot shows the Splunk Search interface. The search query is `index=cohesity_logs`. The results show 1 event from 1/8/25 12:00:00.000 AM to 1/8/25 12:39:31.000 AM. The event is highlighted with a red box and contains the following JSON data:

```
{
  "alert": "Test_Alert",
  "alertId": "0000"
}
```

The interface also shows a list of fields on the left, including 'SELECTED FIELDS' (host, source, sourcetype) and 'INTERESTING FIELDS' (alert, alertId, index, linecount, punct, splunk_server, timestamp).

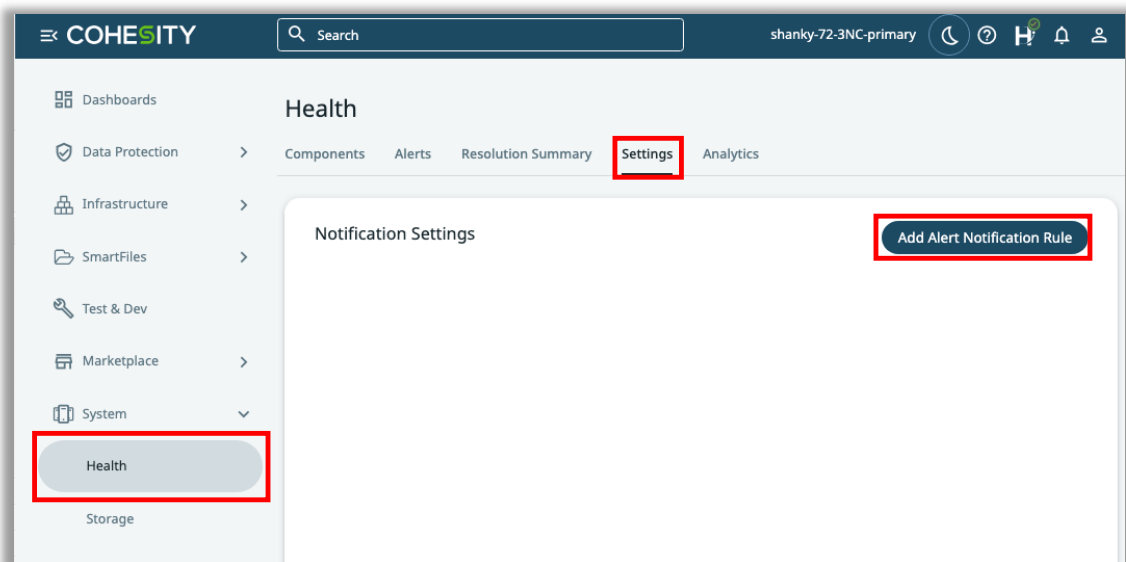
NOTE:

- 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.

The screenshot shows the Cohesity Cluster UI login page. The page is titled "Welcome To Cohesity Data Cloud". Below the title, it displays the cluster name: "Cluster: shanky-72-3NC-primary". There are input fields for "Username" and "Password", and a "Sign In" button. The background features a stylized cloud graphic with various icons, including a checkmark, a padlock, a gear, and a magnifying glass.

- 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.

Edit Alert Notification Rule ✕

Rule Name

When

Alert Category	Alert Severities	Alert Name
All applies by default	All applies by default	All applies by default

Send Alert Notification via *

Email

Add email addresses of users to receive alert email notifications

[+ Add](#)

SNMP

Syslog

Webhook

URL ⓘ
 https://prd-p-afmhh.splunkcloud.com:8088/services/collector.

Options ⓘ
 -H "Authorization: Splunk 355abee2-f248-46f6-bff6-b1f679072"

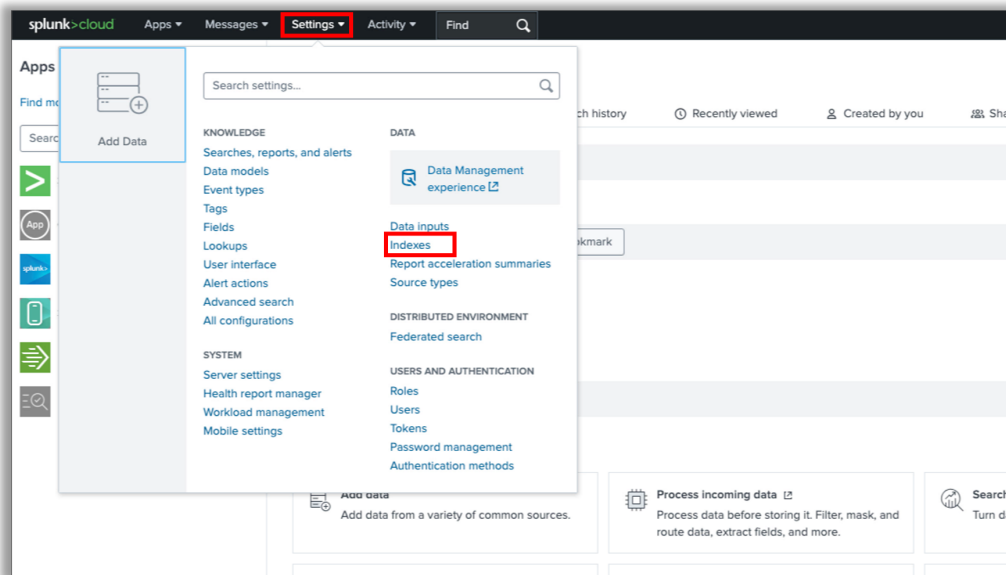
curl -H "Authorization: Splunk 355abee2-f248-46f6-bff6-b1f679072a0" -H "Content-Type: application/json" -XPOST https://prd-p-afmhh.splunkcloud.com:8088/services/collector/raw:8088/services/collector/raw

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.

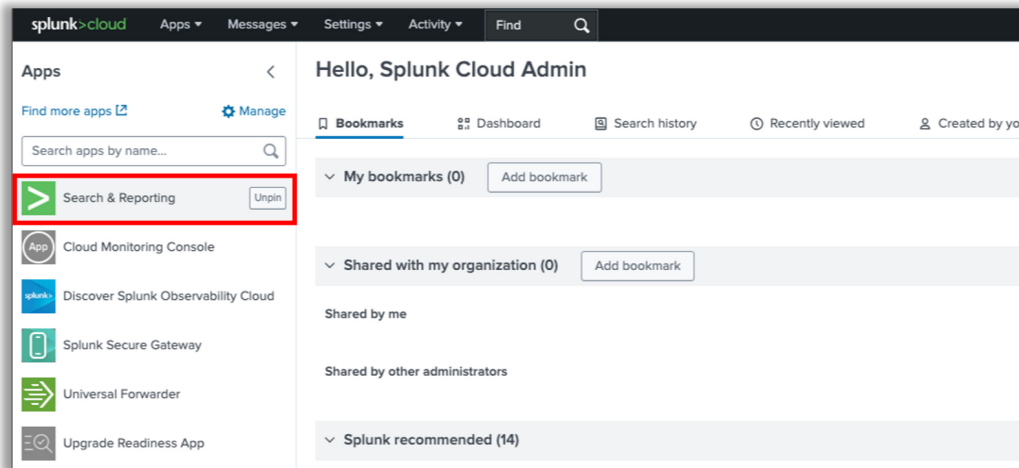
The screenshot shows the Splunk Cloud 'Indexes' page. A table lists several indexes, with the 'cohesity' index highlighted by a red box. The table has columns for Name, Actions, Type, Category, App, Current Size, Max Size, and Event Count.

Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
cohesity	Edit Delete	Events	Regular	search	0 B	500 GB	48
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0

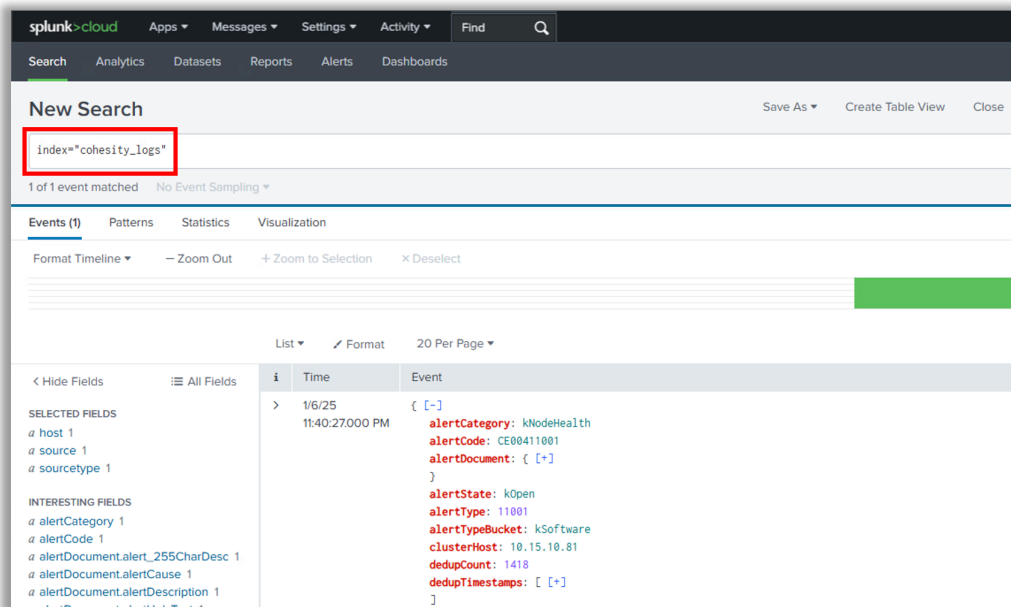
NOTE:

- 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.

The screenshot shows the Splunk Cloud 'New Search' interface. The search query is `index=*cohesity_logs*`. A dropdown menu for time filtering is open, showing various options. The 'Last 24 hours' option is highlighted with a red box. The interface also shows a table with one event matched, and a list of fields including `host`, `source`, and `sourcetype`.

- f. Alert and visualize.

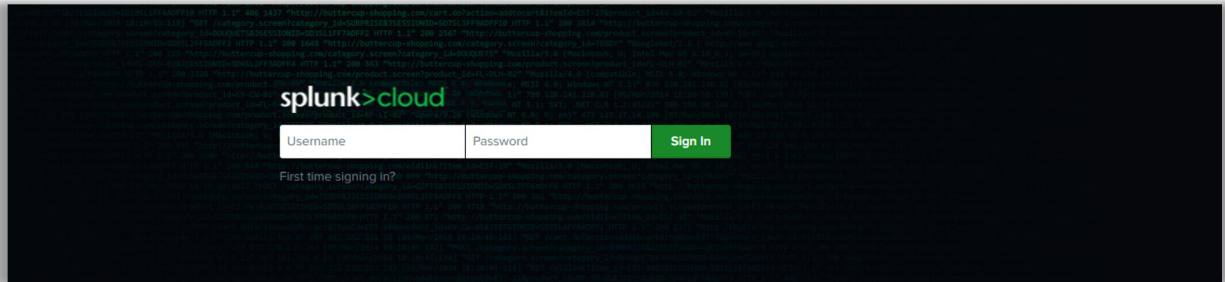
The screenshot shows the Splunk Cloud 'New Search' interface. The search query is `index=*cohesity_logs*`. A dropdown menu for actions is open, showing options like 'Report', 'Alert', 'Existing Dashboard', 'New Dashboard', and 'Event Type'. The 'Report' option is highlighted with a red box. The interface also shows a table with one event matched, and a list of fields including `host`, `source`, and `sourcetype`.

NOTE: For more details, refer to the [Search and Reporting](#) section.

Cohesity Data Cloud

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

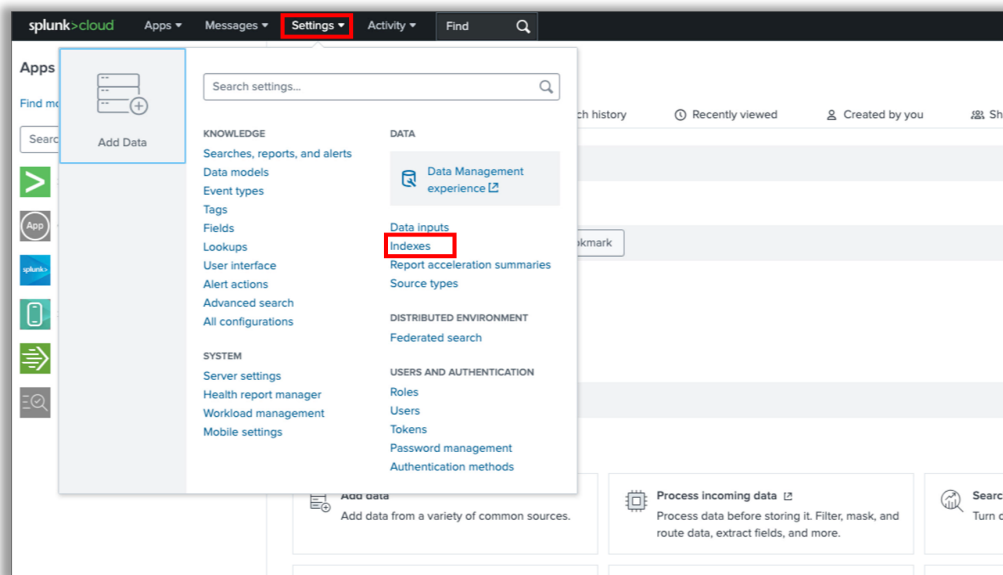
1. Login to your Splunk Cloud Instance.



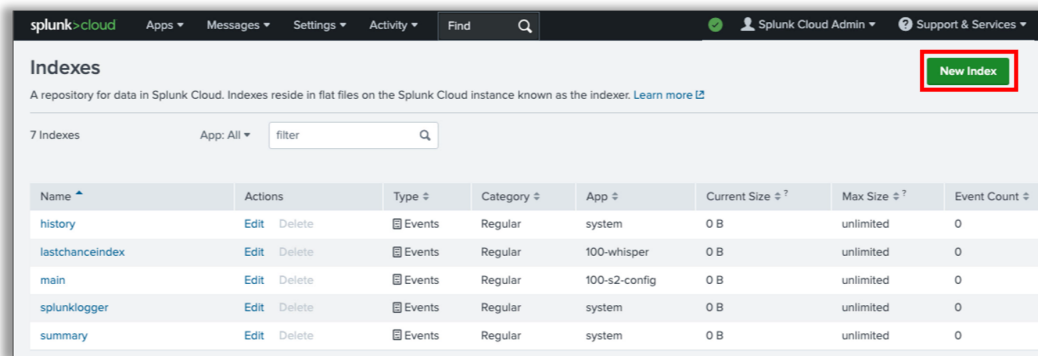
2. Create a new index to store Cohesity logs.

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**.

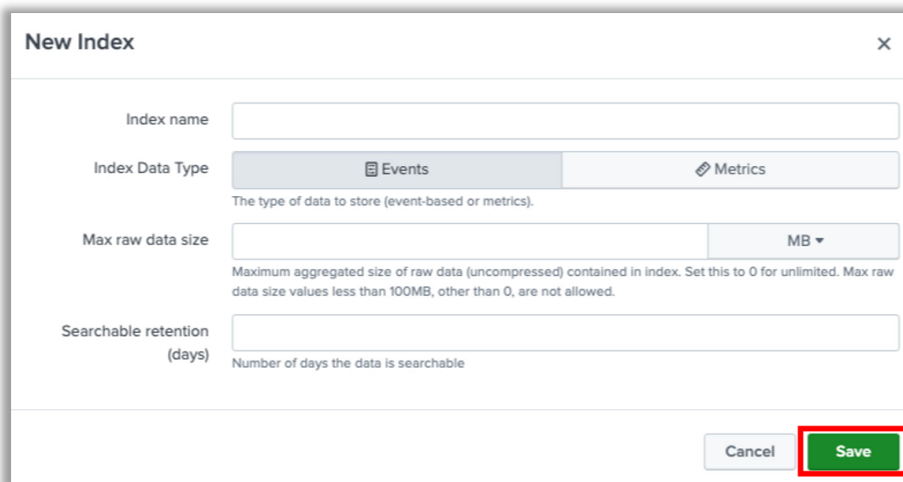


- b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save**.



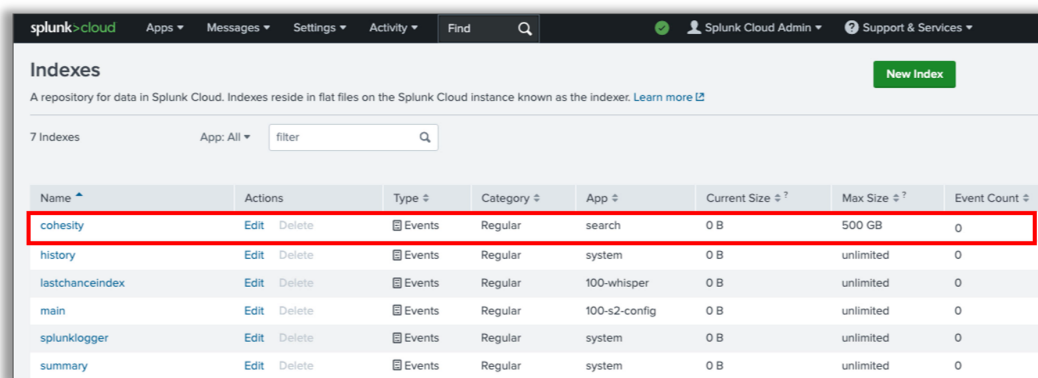
The screenshot shows the Splunk Cloud interface with the 'Indexes' page. A 'New Index' button is highlighted with a red box in the top right corner. Below the header, there is a table listing existing indexes:

Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0



The screenshot shows the 'New Index' configuration form. The 'Index name' field is empty. The 'Index Data Type' is set to 'Events'. The 'Max raw data size' is set to 'MB'. The 'Searchable retention (days)' field is empty. The 'Save' button is highlighted with a red box.

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

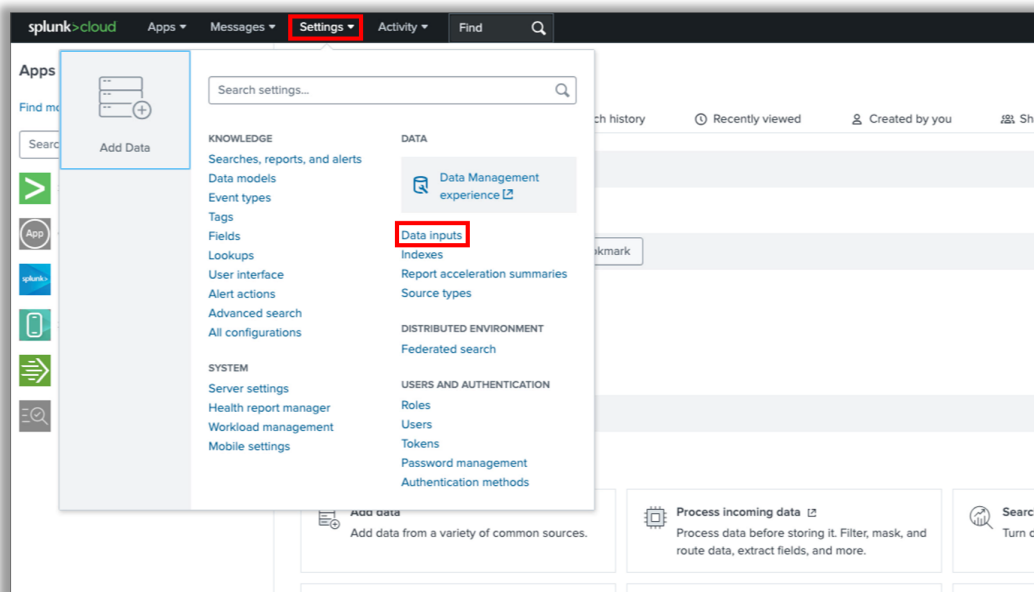


The screenshot shows the Splunk Cloud interface with the 'Indexes' page. The 'cohesity' index is highlighted with a red box in the table below:

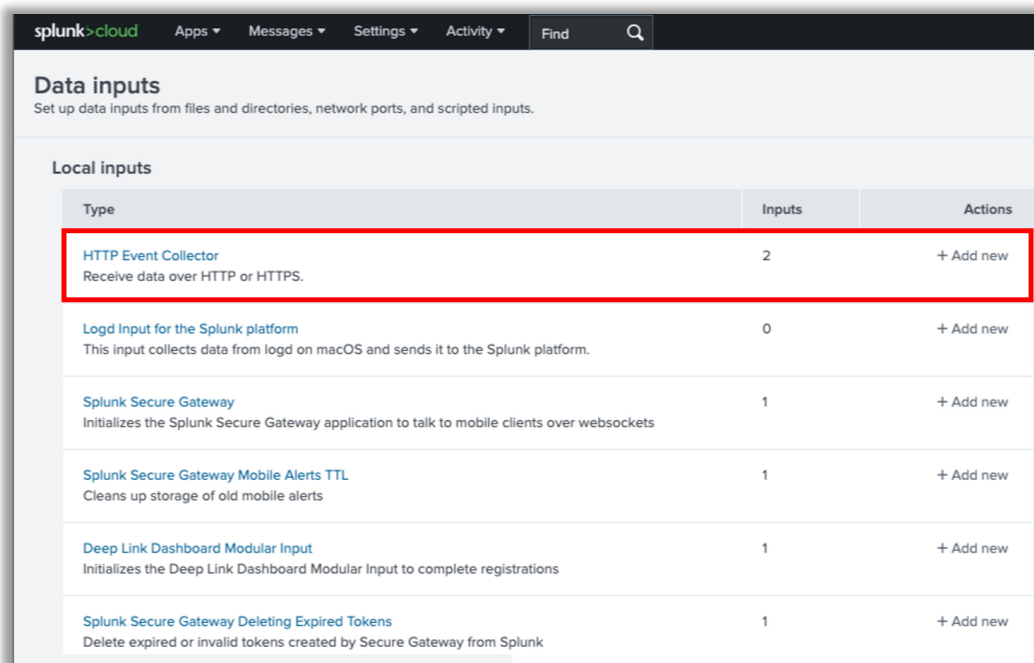
Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
cohesity	Edit Delete	Events	Regular	search	0 B	500 GB	0
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0

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

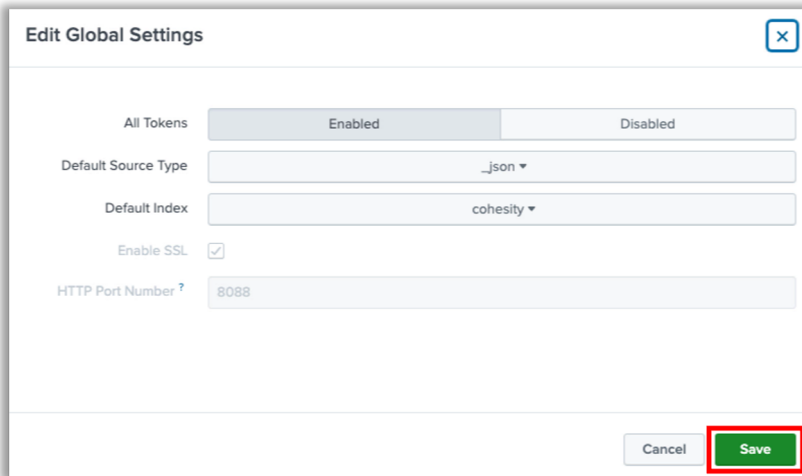
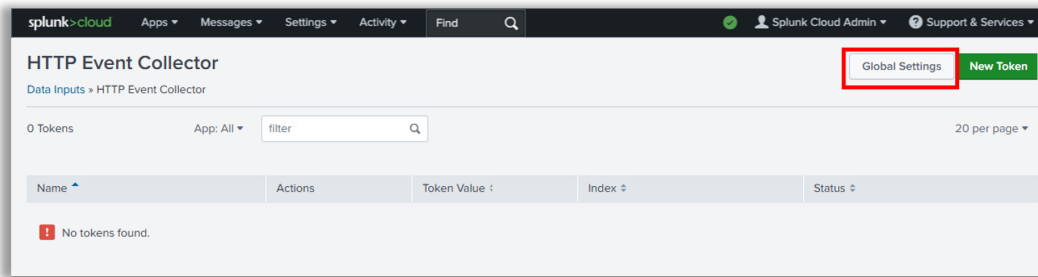
a. Click **Data Inputs** under **Data** in **Settings**.



b. Click **HTTP Event Collector**.



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

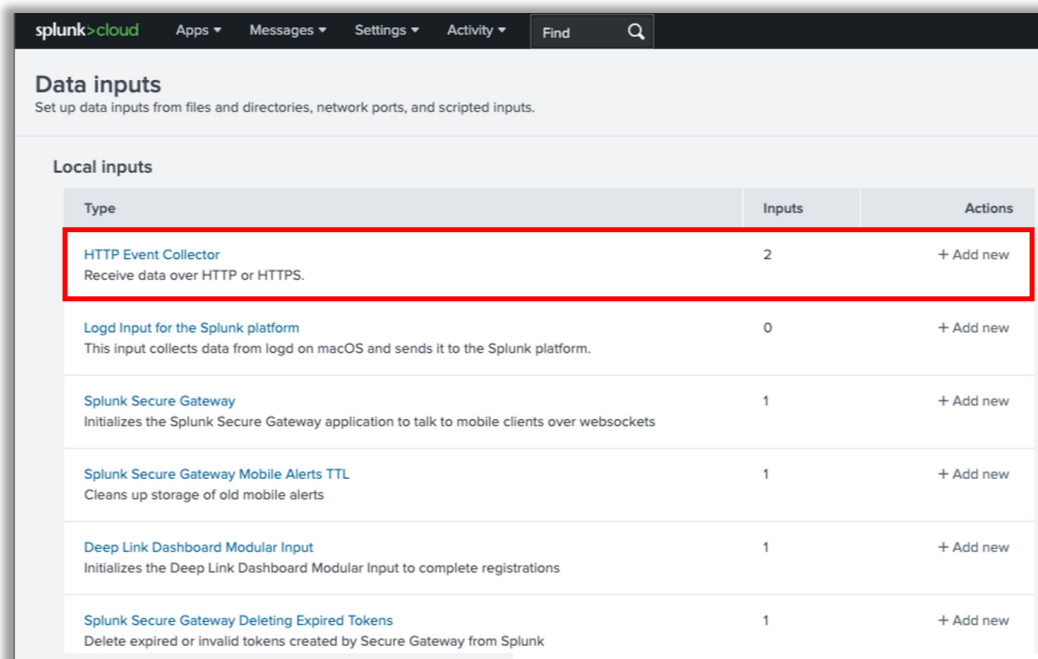


- Select Enabled for All Tokens.
 - Select the Default Source Type as _json (If it is not shown under the dropdown, then type _json in search bar to bring it up).
 - Select the Default index as the new index we created exclusively for Cohesity logs and alerts under step 1.
 - By default, SSL is enabled 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.

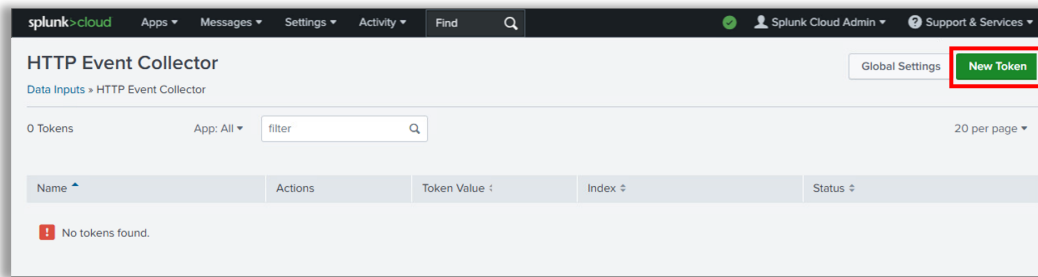
- a. Click **Data Inputs** under **Data** in **Settings**.



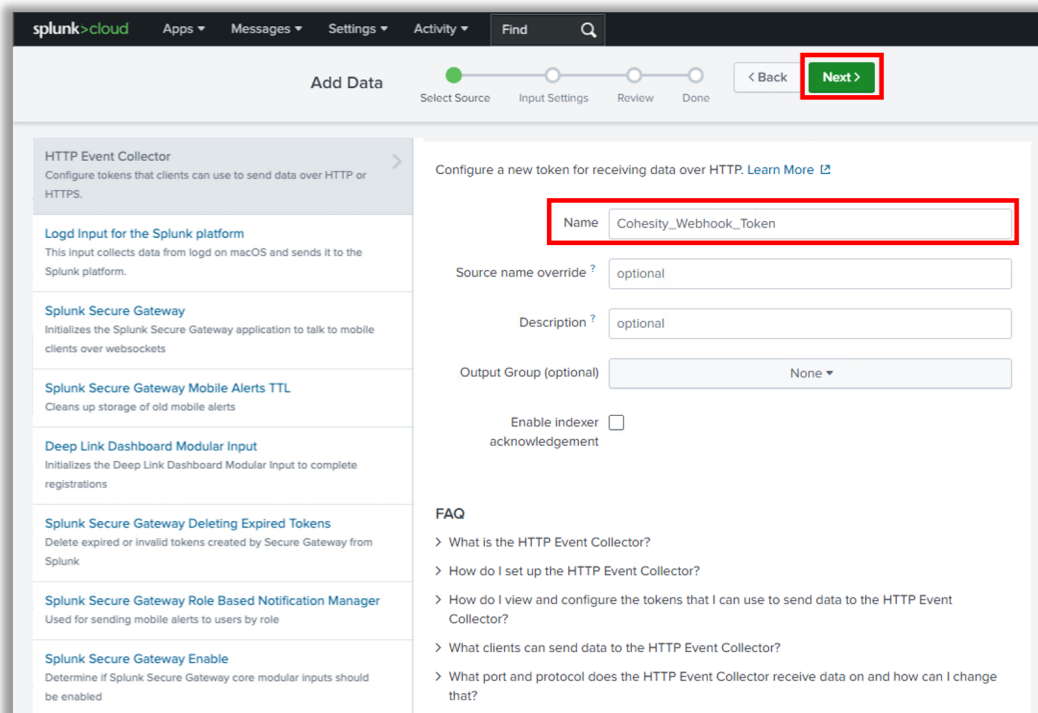
- b. Click **HTTP Event Collector**.



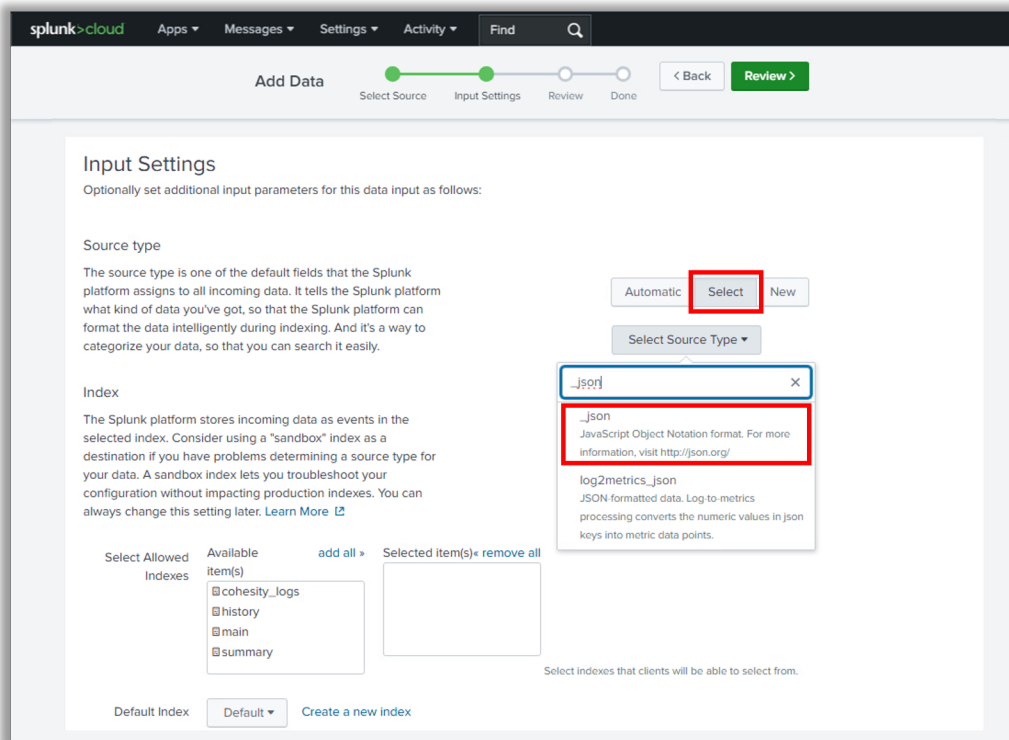
c. Click **New Token**.



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.



The screenshot shows the Splunk Cloud interface for the 'Add Data' process, specifically the 'Input Settings' step. The page title is 'Input Settings' and it includes a progress bar with steps: Select Source, Input Settings, Review, and Done. The 'Input Settings' section is active. Under 'Source type', there are buttons for 'Automatic', 'Select', and 'New'. The 'Select' button is highlighted with a red box. Below it is a 'Select Source Type' dropdown menu. The dropdown is open, showing a search bar with '_json' entered. The search results list several options, with '_json' highlighted by a red box. The description for '_json' is 'JavaScript Object Notation format. For more information, visit http://json.org/'. Other options include 'log2metrics_json' and 'JSON formatted data. Log to metrics processing converts the numeric values in json keys into metric data points.' At the bottom, there is a 'Select Allowed Indexes' section with a list of available indexes: cohesity_logs, history, main, and summary. The 'Default Index' is set to 'Default'.

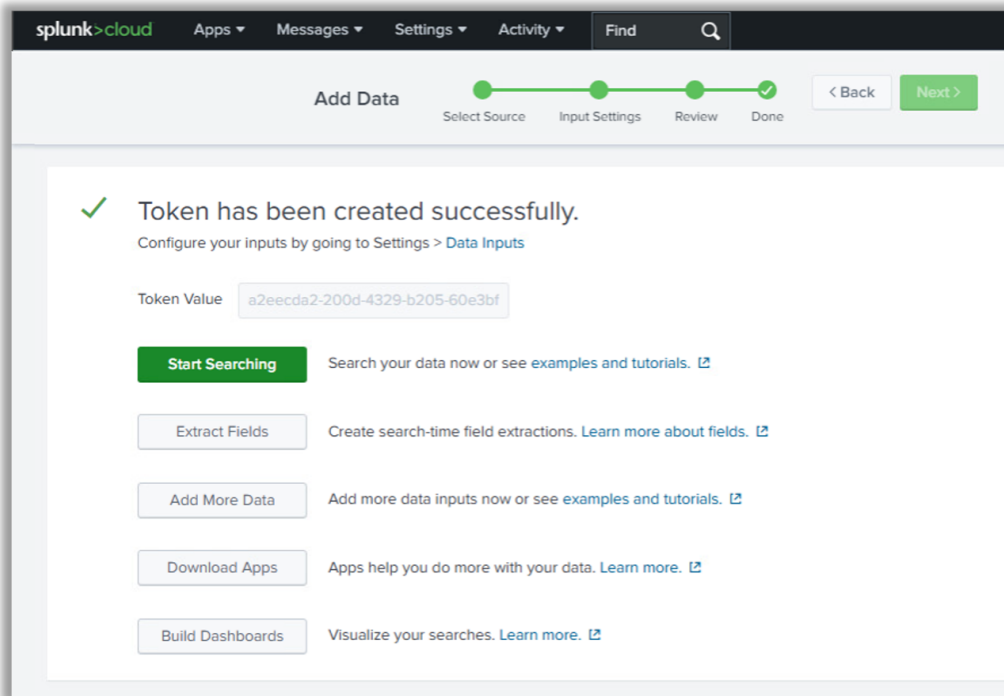
- f. Select the **Index** where you want the Cohesity logs and alerts need to be stored. Select the new index we created exclusively for Cohesity logs and alerts under step 1. Also make sure the **Default Index** is set to the same index as chosen.

The screenshot shows the 'Input Settings' page in Splunk. The 'Index' section is highlighted, showing a list of available indexes: 'cohesity_logs', 'history', 'main', and 'summary'. The 'cohesity_logs' index is selected and moved to the 'Selected item(s)' list. The 'Default Index' dropdown is also set to 'cohesity_logs'. A 'Review >' button is highlighted in the top right corner.

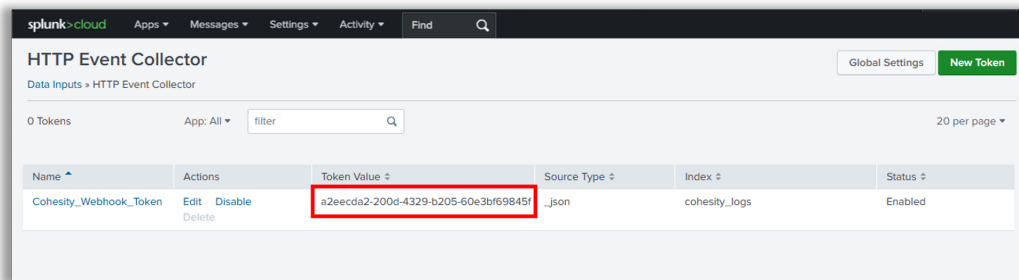
- g. Click **Review** to review the details of the token. If you want to make any changes, you can go back and modify.

The screenshot shows the 'Review' page for the 'Cohesity_Webhook_Token'. The 'Allowed indexes' field is set to 'cohesity_logs' and the 'Default index' is also 'cohesity_logs'. A 'Submit >' button is highlighted in the top right corner.

- 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:



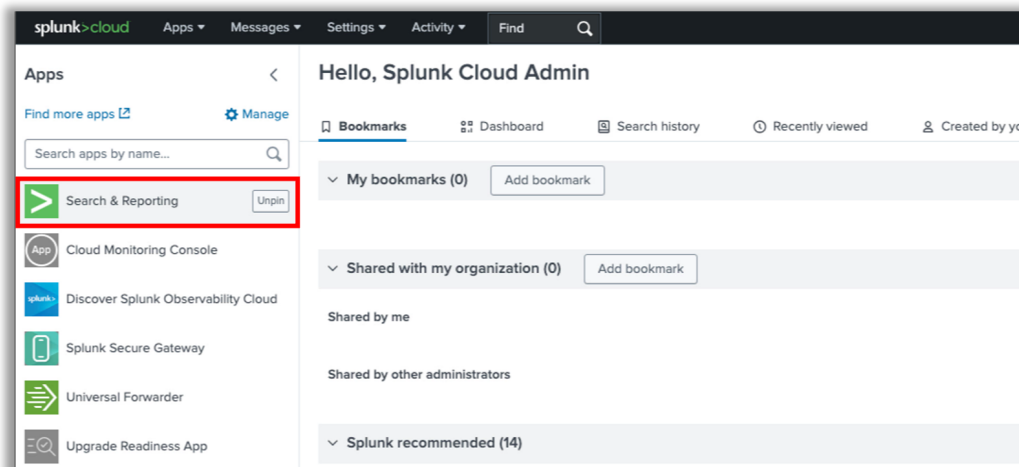
```
shashanka.sr@COH-J6CJPK74WG ~ % curl -k "https://prd-p-afmhh.splunkcloud.com:8088/services/collector/raw" \
-H "Authorization: Splunk 9a2c4f3d-8a82-402f-9965-896715ad8586" \
-H "Content-Type: application/json" \
-d '{"alert": "Test_Alert", "alertId": "0000"}'
{"text": "Success", "code": "0"}
shashanka.sr@COH-J6CJPK74WG ~ % █
```

NOTE:

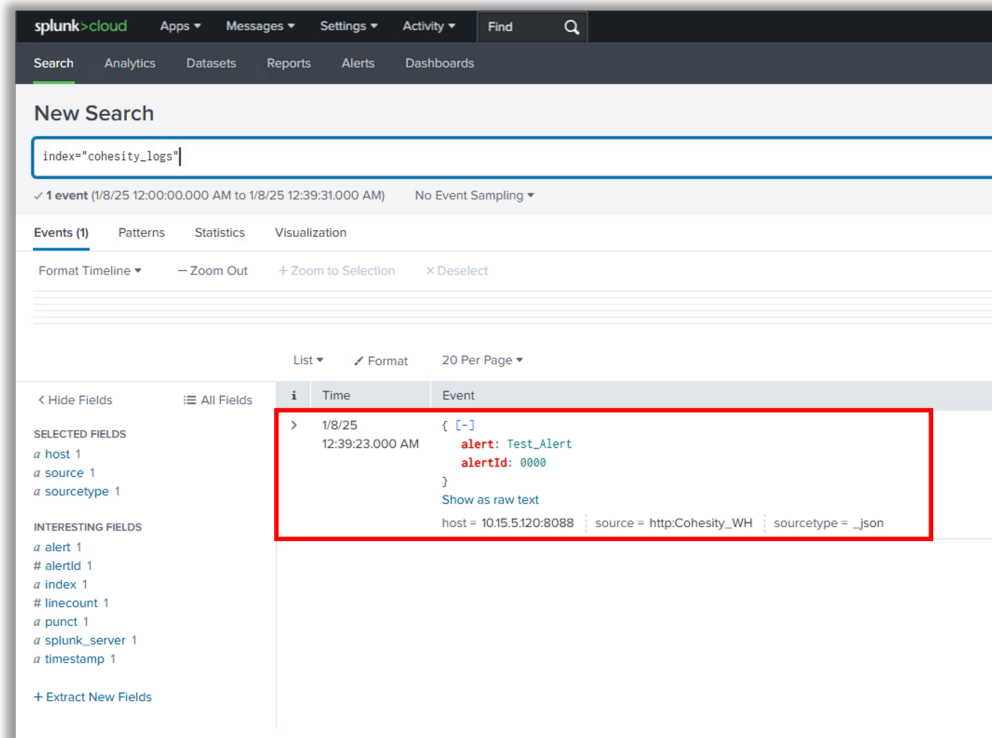
- If you are not receiving the message `{"text": "Success", "code": "0"}` or receiving some other message, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

- 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.



The screenshot shows the Splunk Cloud interface with a search query `index=cohesity_logs` entered in the search bar. The search results show 1 event from 1/8/25 12:00:00.000 AM to 1/8/25 12:39:31.000 AM. The event is displayed in a table with columns for Time and Event. The event data is as follows:

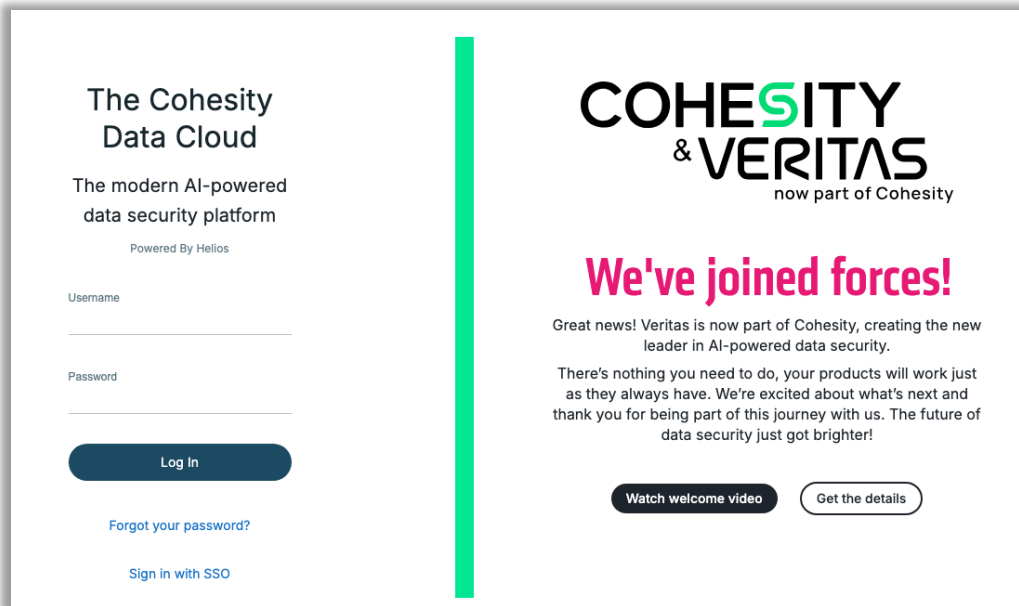
Time	Event
1/8/25 12:39:23.000 AM	<pre>{ [-] alert: Test_Alert alertId: 0000 }</pre> <p>host = 10.15.5.120:8088 source = http:Cohesity_WH sourcetype = _json</p>

NOTE:

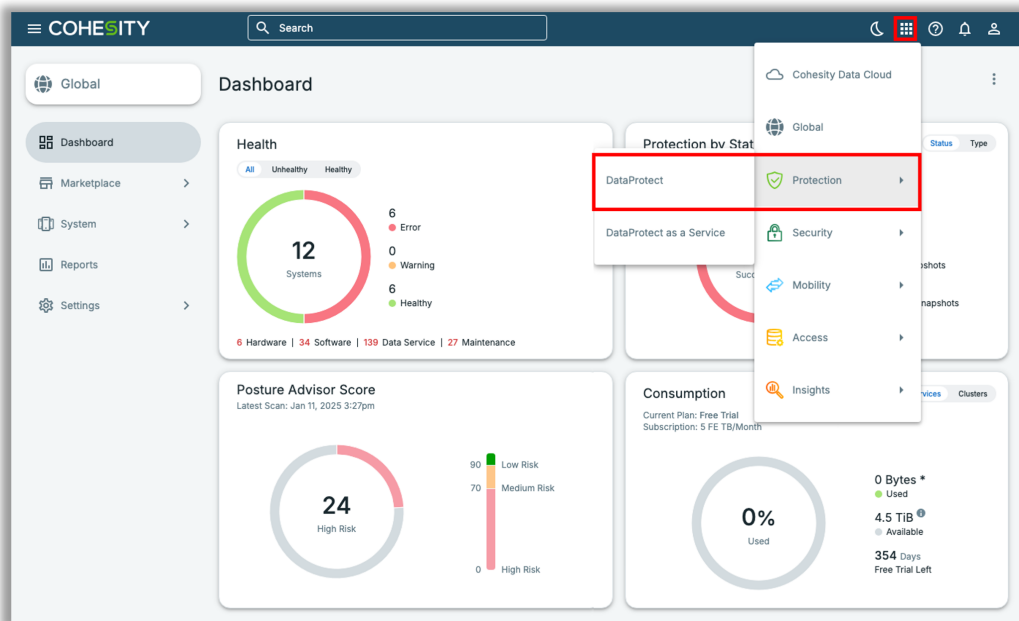
- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

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

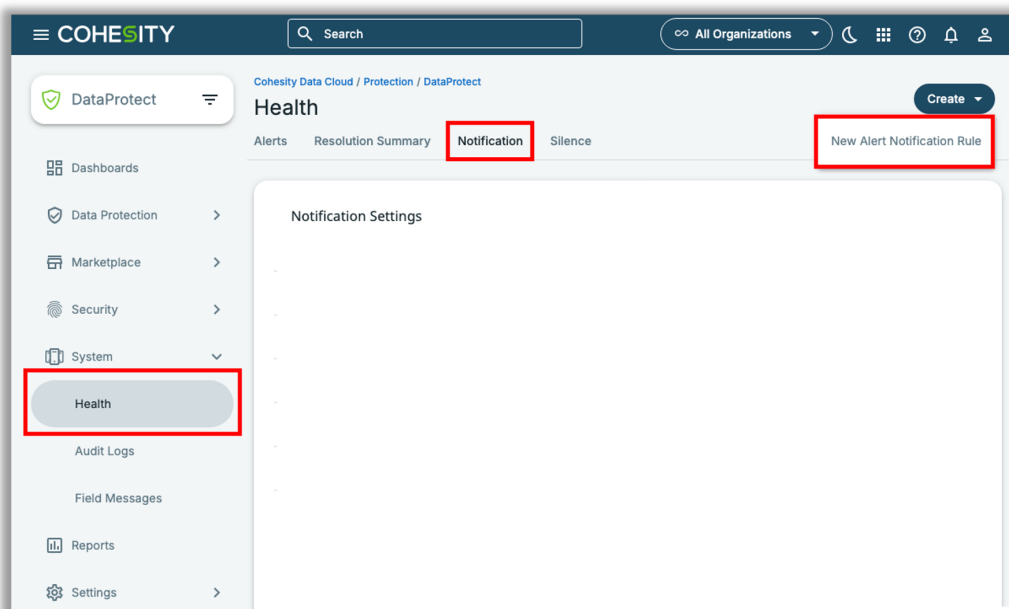
- a. Login to [Cohesity Data Cloud](#).



- 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.

Create Alert Notification Rule

Notification Name
Splunk

Notification Filters
Clusters Organization Alert Severity Alert Type Alert Category
Alert Name

Notification Frequency
 Real-time Every 6 hours Every 24 hours

Notification Method
 Email
 Webhook

`https://13.52.181.193:8088/services/c {"authorization": {"type": "Sp`

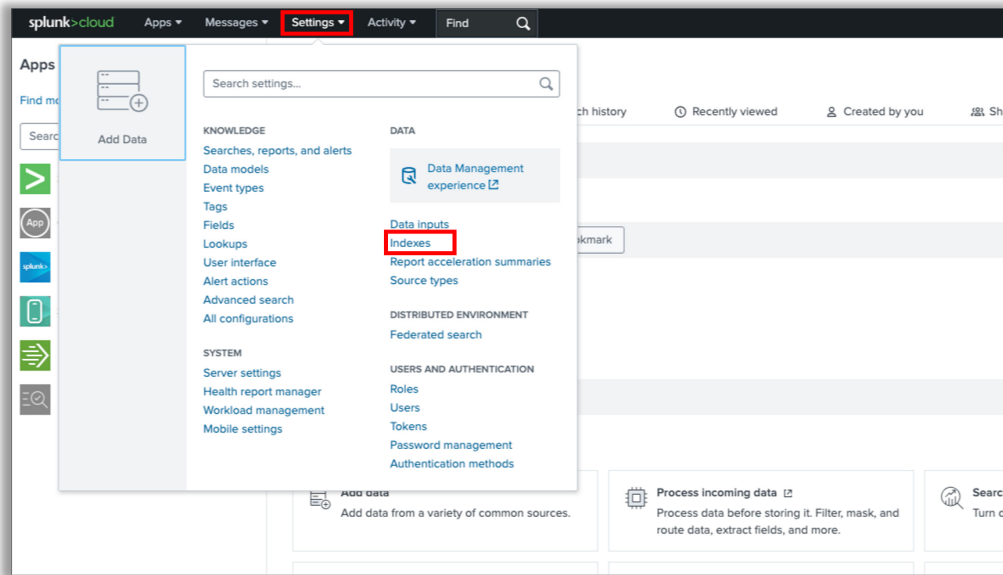
Cancel Create

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.

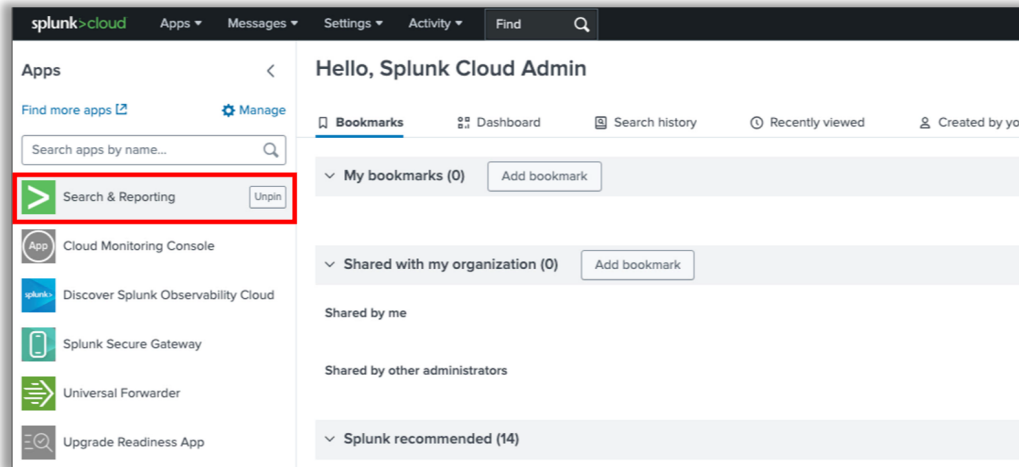
 A screenshot of the Splunk Cloud 'Indexes' page. The page shows a list of 7 indexes. The 'cohesity' index is highlighted with a red box. The table columns are Name, Actions, Type, Category, App, Current Size, Max Size, and Event Count.

Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
cohesity	Edit Delete	Events	Regular	search	0 B	500 GB	48
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0

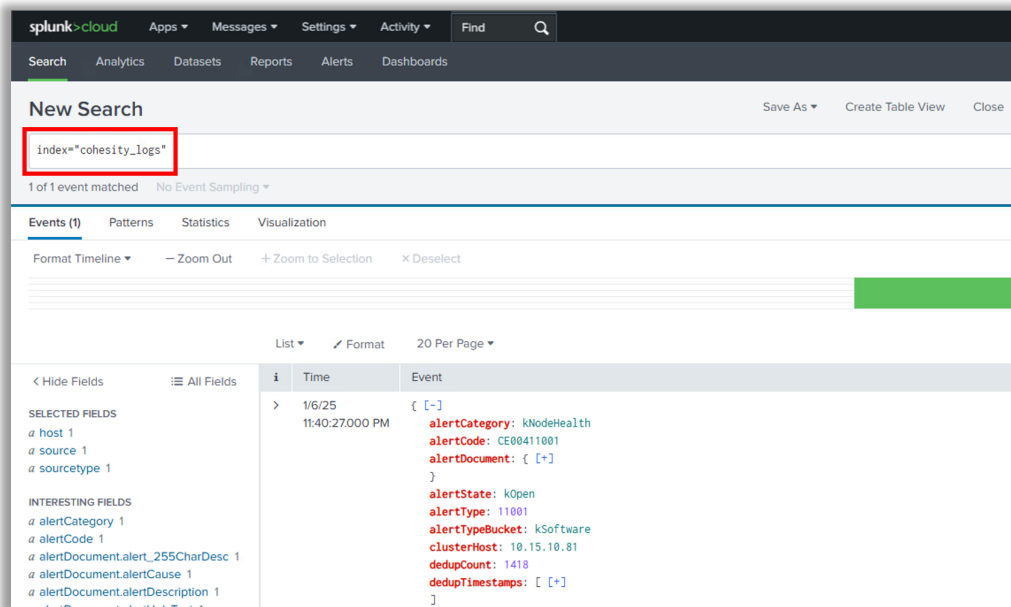
NOTE: Alerts and logs will be pushed from Cohesity to Splunk in real time. However, it is not immediate. Sometimes it takes more time for the data to be transmitted to Splunk. If you are not seeing the events after significant amount of time, then there could be an issue in HEC configuration. Edit your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

The screenshot shows the Splunk Cloud interface with a search query `index=*cohesity_logs*` entered in the search bar. The time filter is set to "Last 24 hours". The search results show 1 event matched. The interface includes a navigation bar with "Search", "Analytics", "Datasets", "Reports", "Alerts", and "Dashboards". A "Presets" dropdown menu is open, showing various time range options like "30 second window", "1 minute window", "5 minute window", "30 minute window", "1 hour window", "All time (real-time)", "Today", "Week to date", "Business week to date", "Month to date", "Year to date", "Yesterday", "Previous week", "Previous business week", "Previous month", "Previous year", "Last 15 minutes", "Last 60 minutes", "Last 4 hours", "Last 24 hours", "Last 7 days", and "Last 30 days".

10. Alert and visualize.

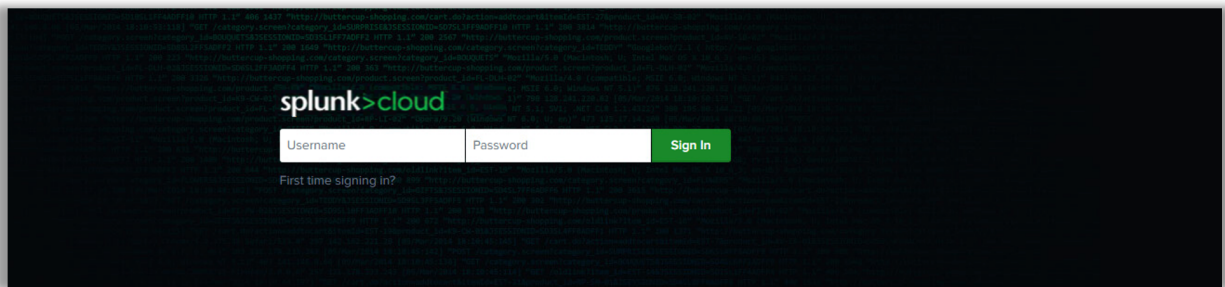
The screenshot shows the Splunk Cloud interface with a search query `index=*cohesity_logs*` entered in the search bar. The search results show 1 event matched. The interface includes a navigation bar with "Search", "Analytics", "Datasets", "Reports", "Alerts", and "Dashboards". A "Save As" dropdown menu is open, showing options: "Report", "Alert", "Existing Dashboard", "New Dashboard", and "Event Type". The search results table shows the following event:

i	Time	Event
>	1/6/25 11:40:27.000 PM	{ [-] <code>alertCategory: kNodeHealth</code> <code>alertCode: CE00411001</code> <code>alertDocument: [[+]</code> <code>]</code> <code>alertState: kOpen</code> <code>alertType: 11001</code> <code>alertTypeBucket: kSoftware</code> <code>clusterHost: 10.15.10.81</code> <code>dedupCount: 1418</code> <code>dedupTimestamps: [[+]</code> <code>]</code>

NOTE: For more details, refer to the [Search and Reporting](#) section.

DataProtect as a Service [Cohesity SaaS Service]

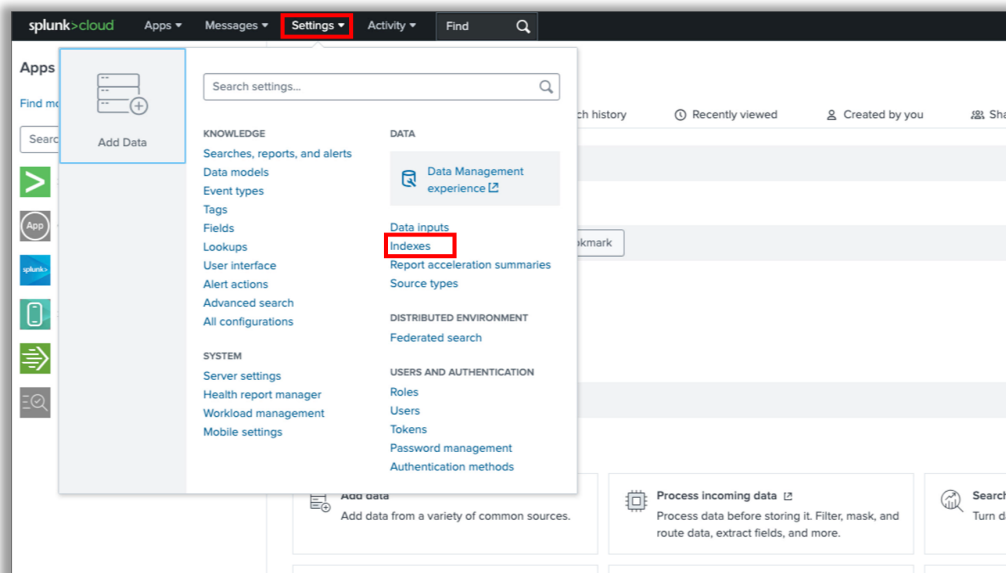
1. Login to your Splunk Cloud Instance.



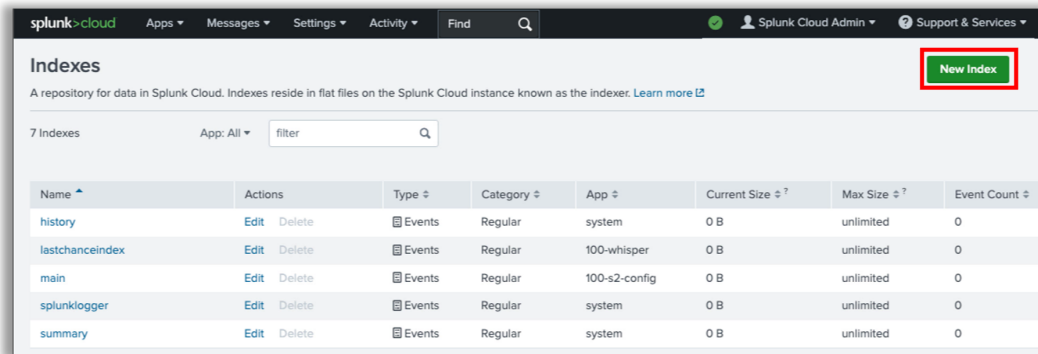
2. Create a new index to store Cohesity logs.

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**.

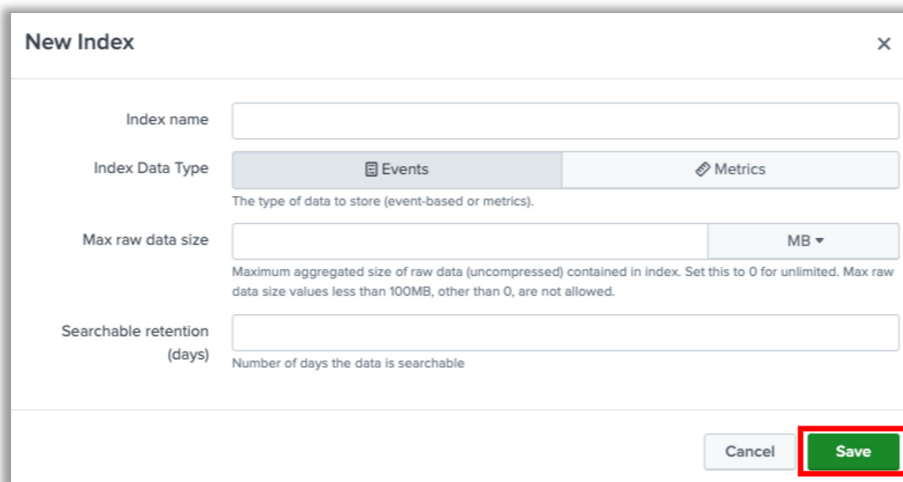


- b. Click **New Index** and fill in all requested details. Select **Events** for **Index Data Type** and **Search & Reporting** in **App** details. Define the maximum size for the index and click **Save**.



The screenshot shows the Splunk Cloud interface with the 'Indexes' page. A 'New Index' button is highlighted with a red box in the top right corner. Below the header, there is a table listing existing indexes:

Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0



The screenshot shows the 'New Index' configuration form. The 'Index Data Type' is set to 'Events'. The 'Max raw data size' is set to 500 MB. The 'Searchable retention (days)' is set to 0. The 'Save' button is highlighted with a red box.

Index name:

Index Data Type: Events Metrics

The type of data to store (event-based or metrics).

Max raw data size: MB

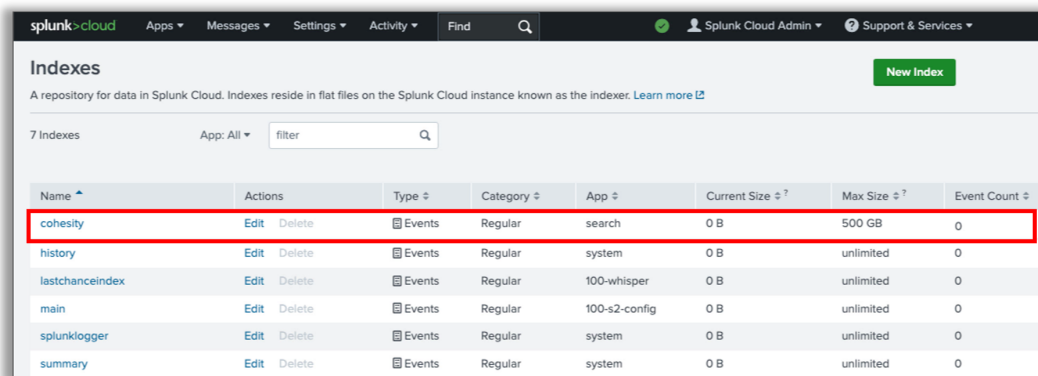
Maximum aggregated size of raw data (uncompressed) contained in index. Set this to 0 for unlimited. Max raw data size values less than 100MB, other than 0, are not allowed.

Searchable retention (days):

Number of days the data is searchable

Buttons: Cancel, Save

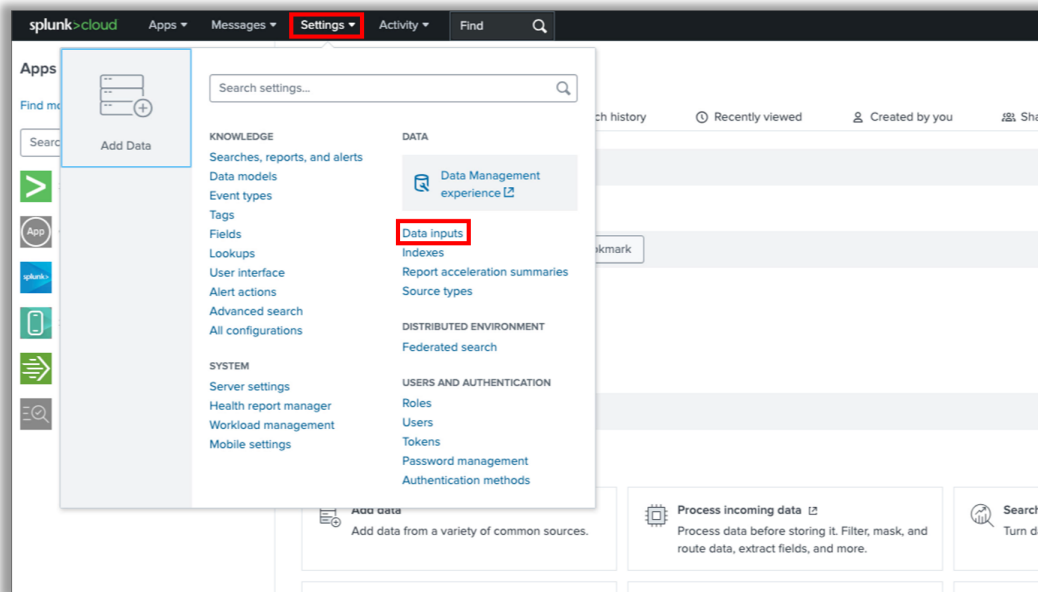
- c. You can see the newly created index under Indexes.



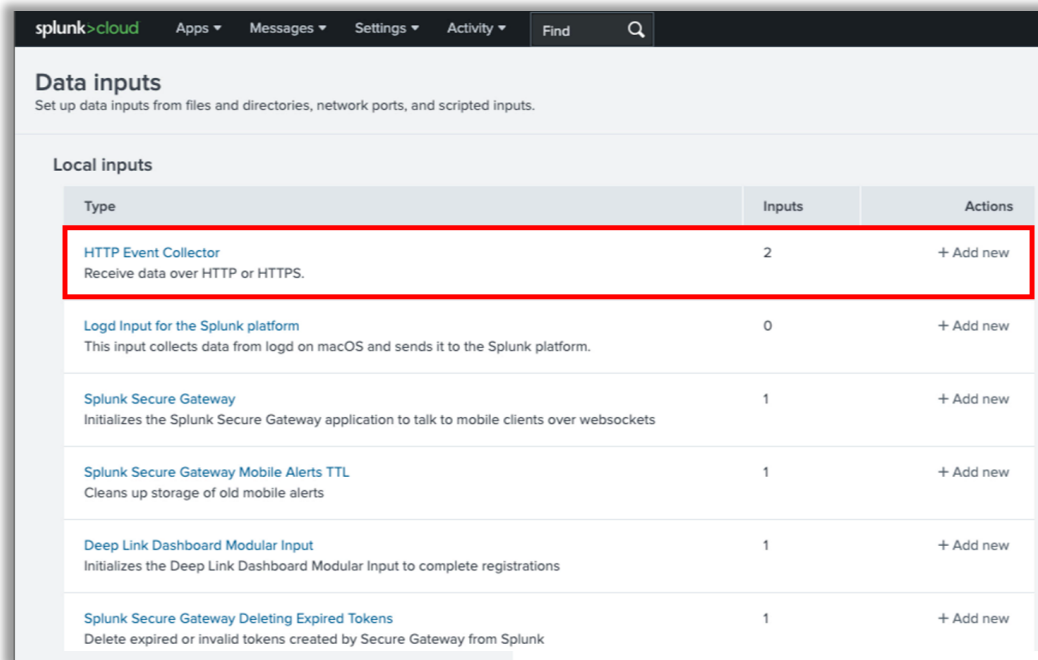
The screenshot shows the Splunk Cloud interface with the 'Indexes' page. The newly created 'cohesity' index is highlighted with a red box in the table below:

Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
cohesity	Edit Delete	Events	Regular	search	0 B	500 GB	0
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0

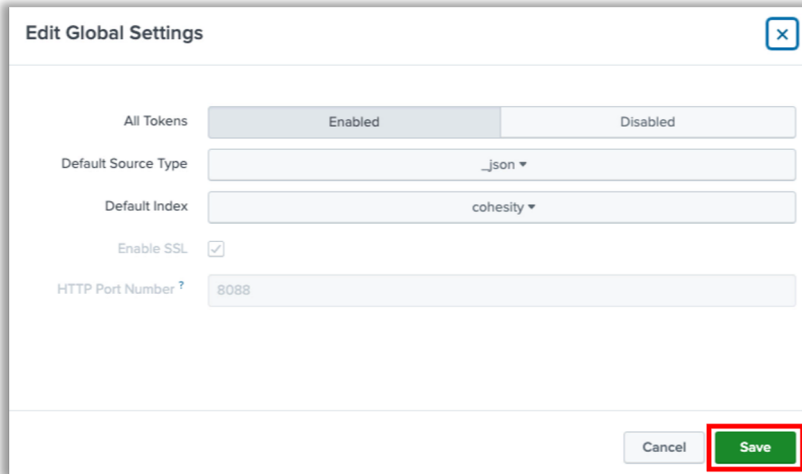
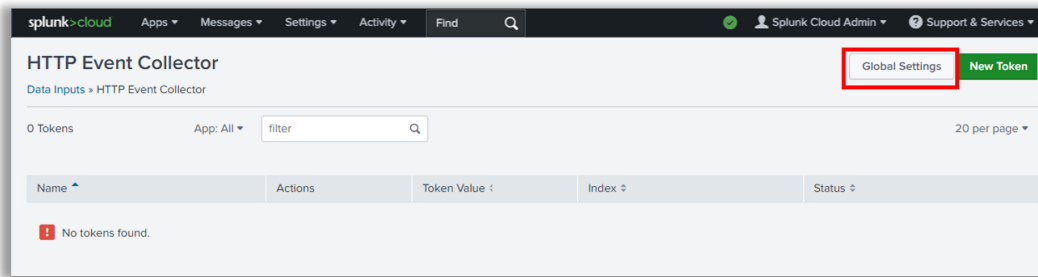
3. Configure HTTP Event Collector to receive data from Cohesity.
 - a. Click **Data Inputs** under **Data** in **Settings**.



- b. Click **HTTP Event Collector**.

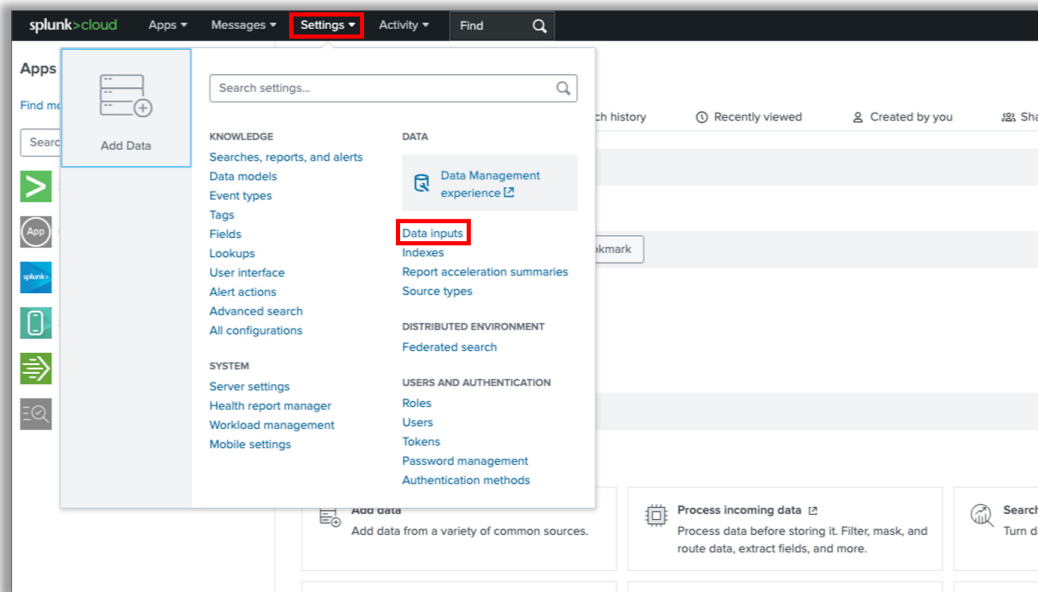


- c. Click **Global Settings** and fill in all requested details and click **Save**.

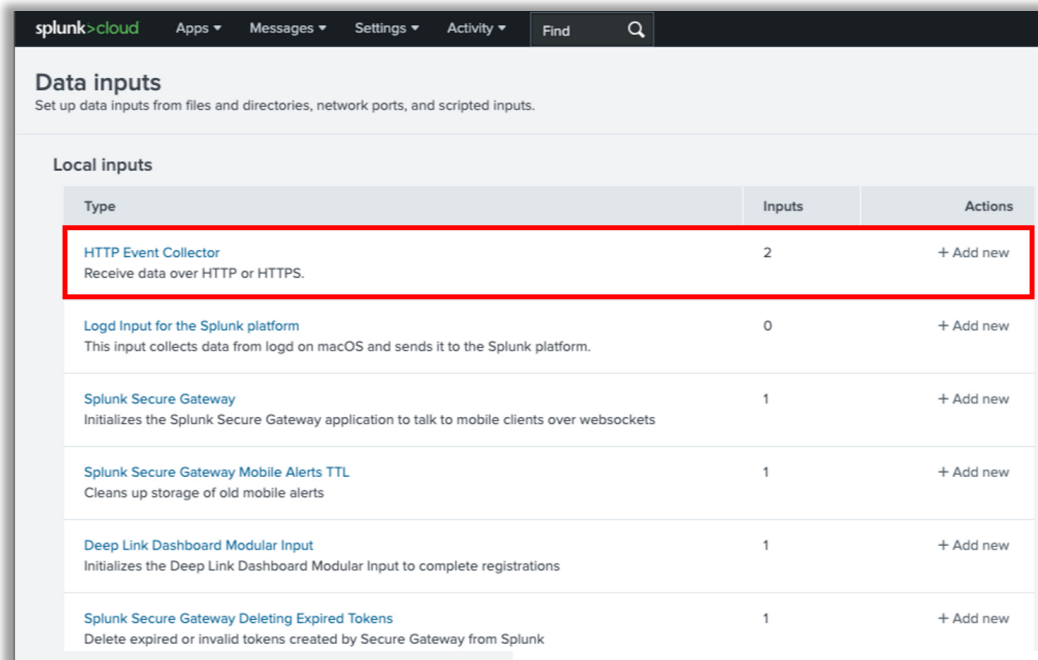


- Select **Enabled** for **All Tokens**.
- Select the **Default Source Type** as **_json** (If it is not shown under the dropdown, then type **_json** in search bar to bring it up).
- Select the **Default index** as the new index we created exclusively for Cohesity logs and alerts under step 1.
- By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

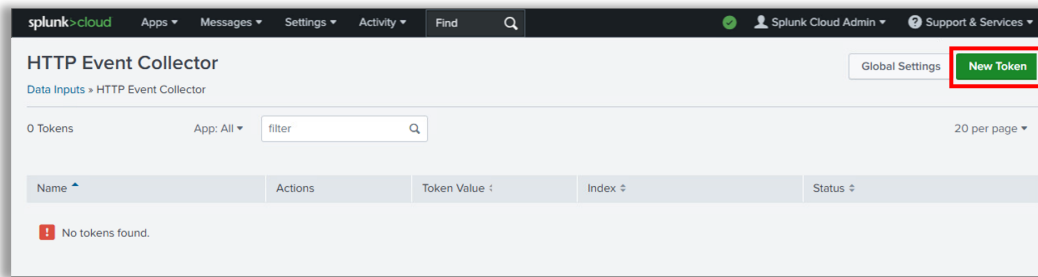
4. Create a new token to authenticate Cohesity.
 - a. Click **Data Inputs** under **Data** in **Settings**.



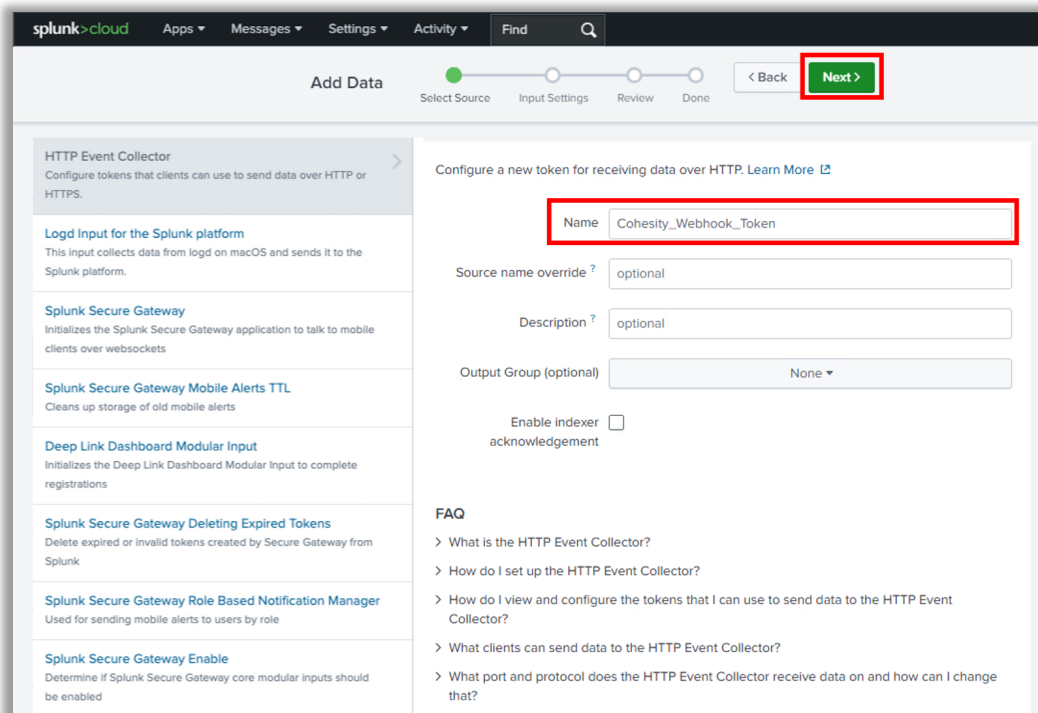
- b. Click **HTTP Event Collector**.



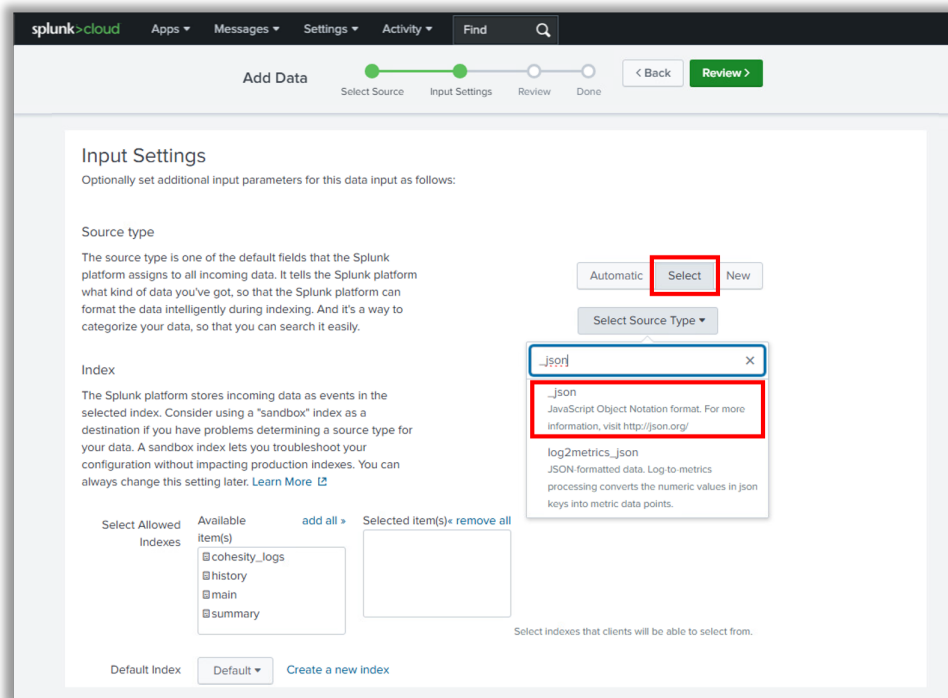
c. Click **New Token**.



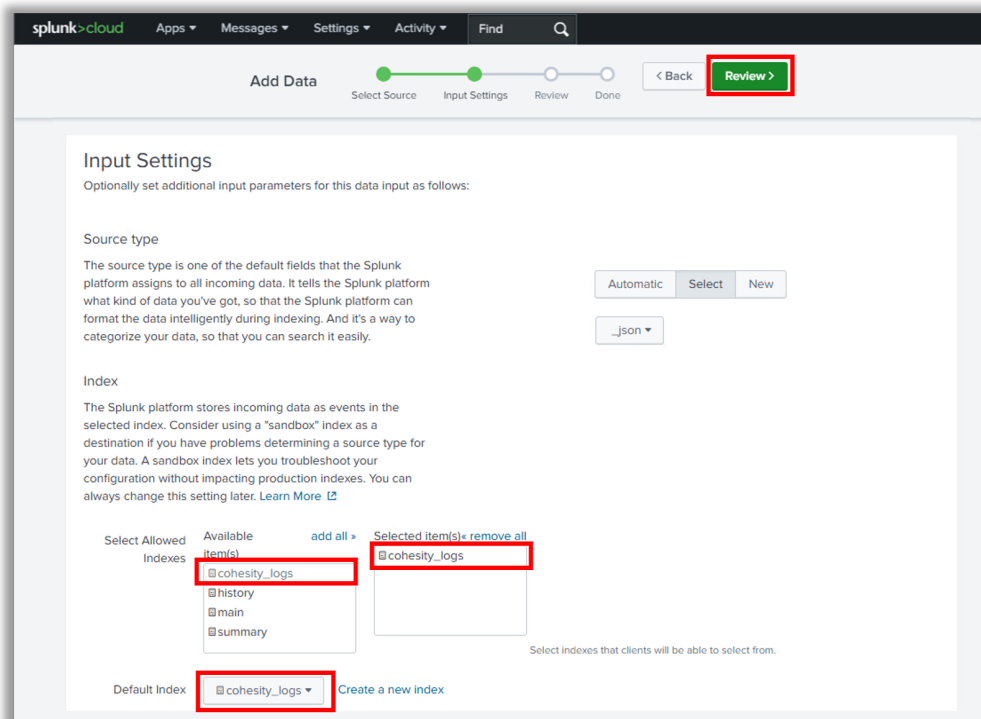
d. Provide a unique **Name** for your token and click **Next**.



- 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.

The screenshot shows the 'Add Data' configuration page in Splunk Cloud, specifically the 'Review' step. The progress bar at the top indicates the current step is 'Review', with 'Select Source' and 'Input Settings' completed and 'Done' pending. The 'Submit' button is visible in the top right corner.

Review

Input Type Token
 Name Cohesity_Webhook_Token
 Source name override N/A
 Description N/A
 Enable indexer acknowledg No
 Output Group N/A
 Allowed indexes cohesity_logs
 Default index cohesity_logs
 Source Type _json
 App Context launcher

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

The screenshot shows the 'Add Data' configuration page in Splunk Cloud, displaying a success message. The progress bar at the top indicates the 'Review' step is completed, and the 'Done' step is active. The 'Next >' button is visible in the top right corner.

Token has been created successfully.

Configure your inputs by going to [Settings > Data Inputs](#)

Token Value

Start Searching Search your data now or see [examples and tutorials](#). [🔗](#)

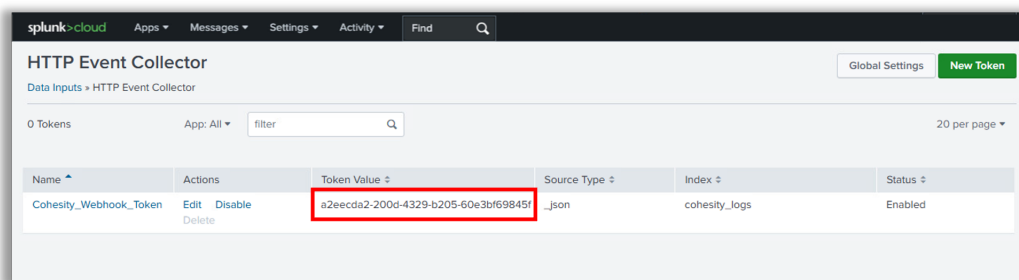
Extract Fields Create search-time field extractions. [Learn more about fields](#). [🔗](#)

Add More Data Add more data inputs now or see [examples and tutorials](#). [🔗](#)

Download Apps Apps help you do more with your data. [Learn more](#). [🔗](#)

Build Dashboards Visualize your searches. [Learn more](#). [🔗](#)

- 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"}'
```

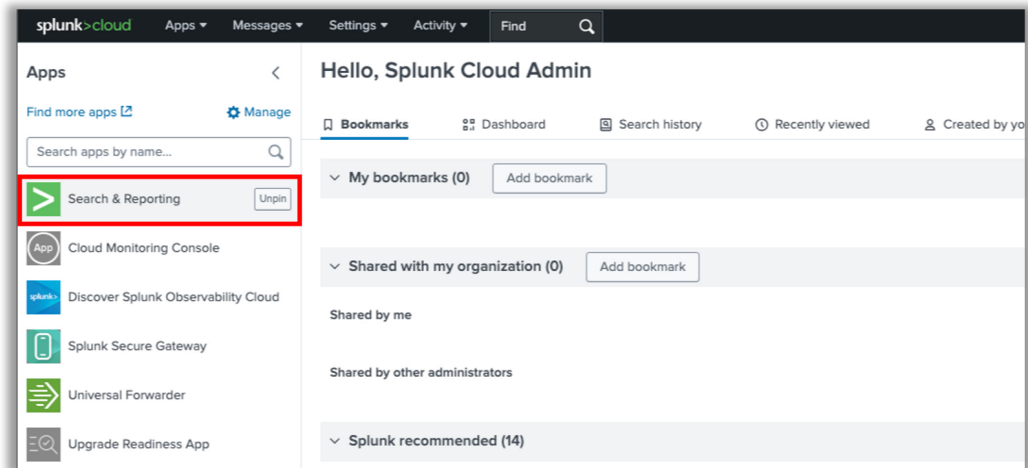
- Your domain – is your unique domain in your Splunk cloud. The link is same as your Splunk cloud access URL.
- HEC Token – is the Token Value of the HTTP Event Collector Token you created in previous step.
- Once the curl command executes successfully, it must return the message `{"text": "Success",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

```
shashanka.sr@COH-J6CJPK74WG ~ % curl -k "https://prd-p-afmhh.splunkcloud.com:8088/services/collector/raw" \
-H "Authorization: Splunk 9a2c4f3d-8a82-402f-9965-896715ad8586" \
-H "Content-Type: application/json" \
-d '{"alert": "Test_Alert", "alertId": "0000"}'
{"text": "Success", "code": 0}
shashanka.sr@COH-J6CJPK74WG ~ %
```

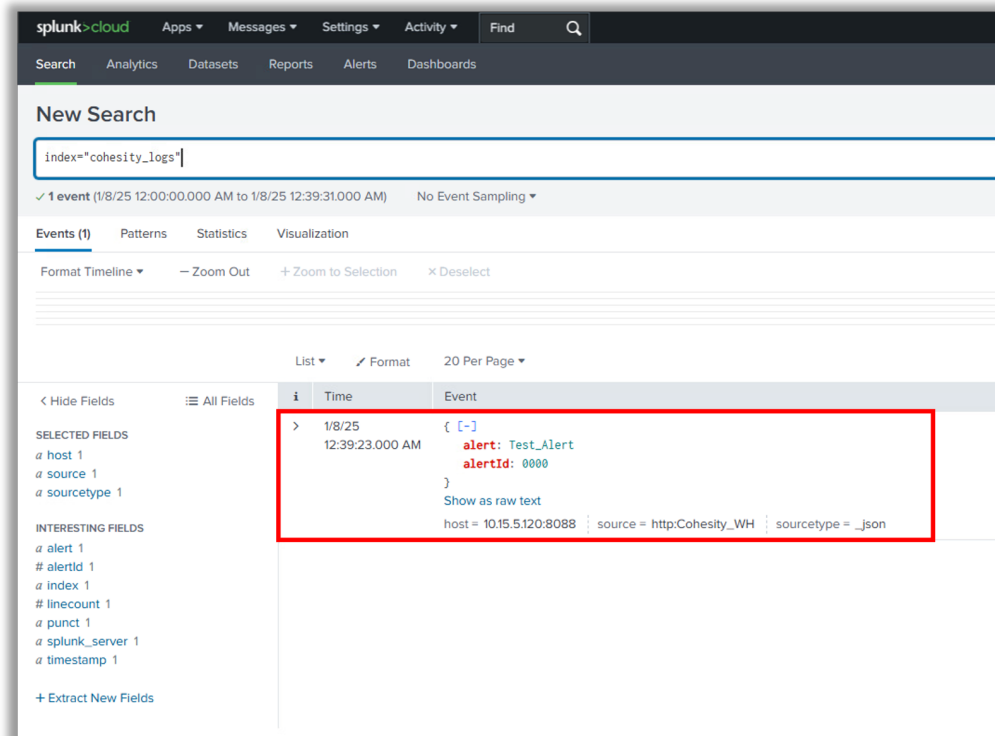
NOTE:

- 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.

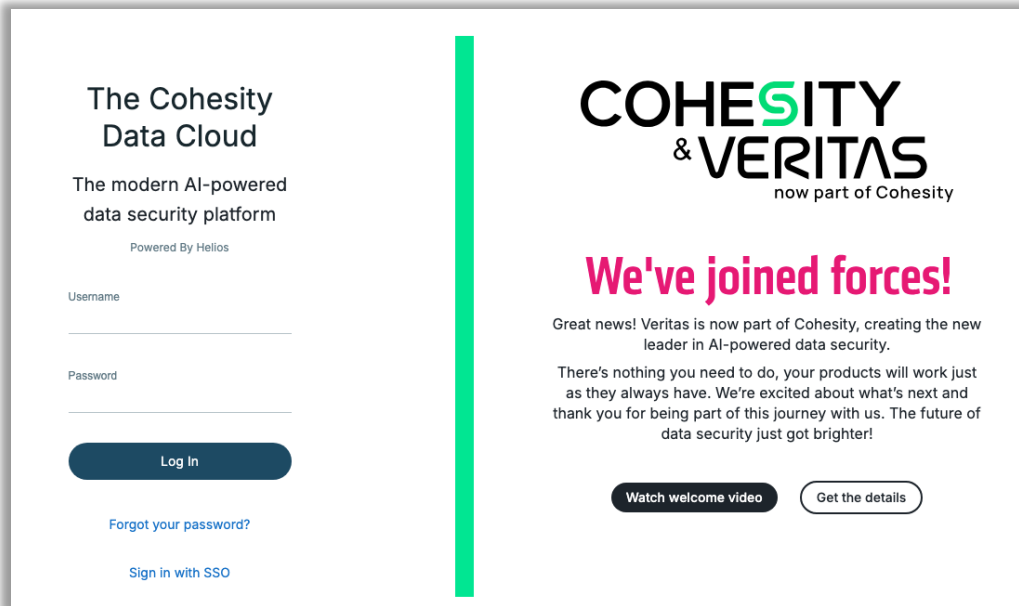


NOTE:

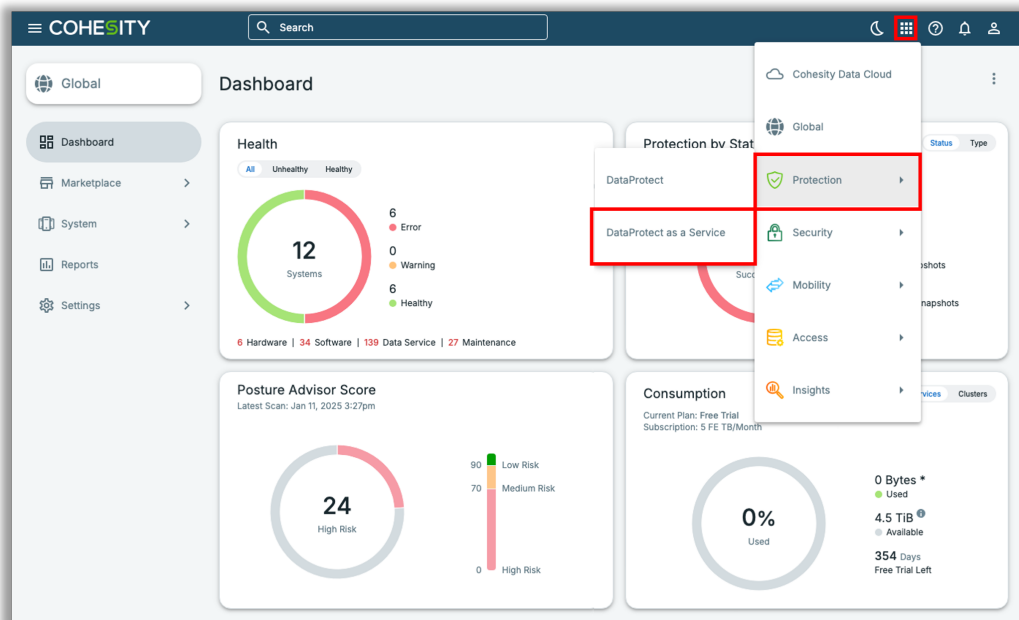
- If you are not receiving the event sent through curl command in Splunk, then there is some issue with the HTTP Event Collector configuration. Revisit steps 2 & 3 for proper configuration.
- Visit [Troubleshooting](#) for more details.

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

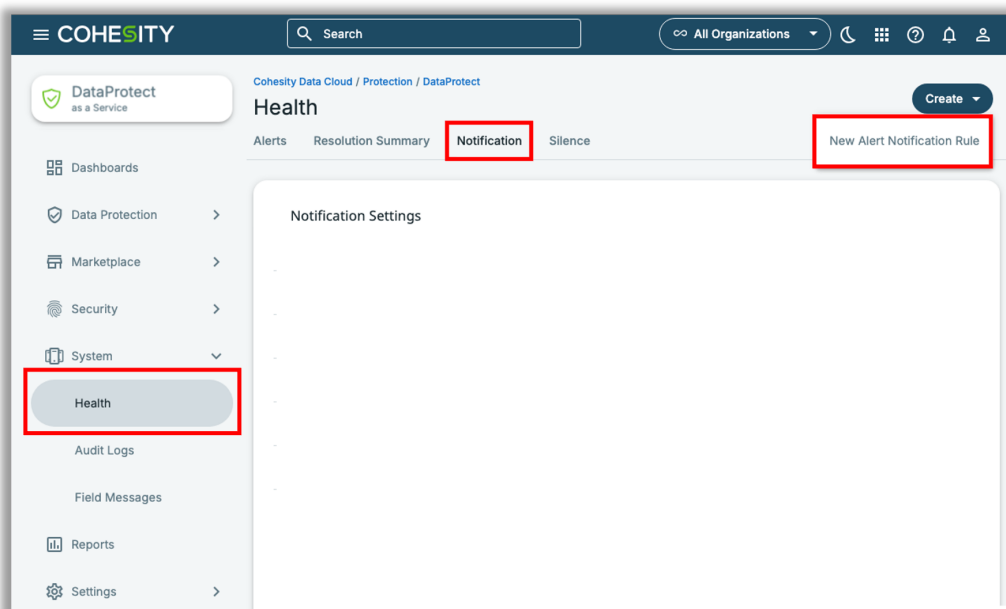
- a. Login to [Cohesity Data Cloud](#).



- 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.

Create Alert Notification Rule

Notification Name

Notification Filters

Notification Frequency
 Real-time Every 6 hours Every 24 hours

Notification Method
 Email
 Webhook

+

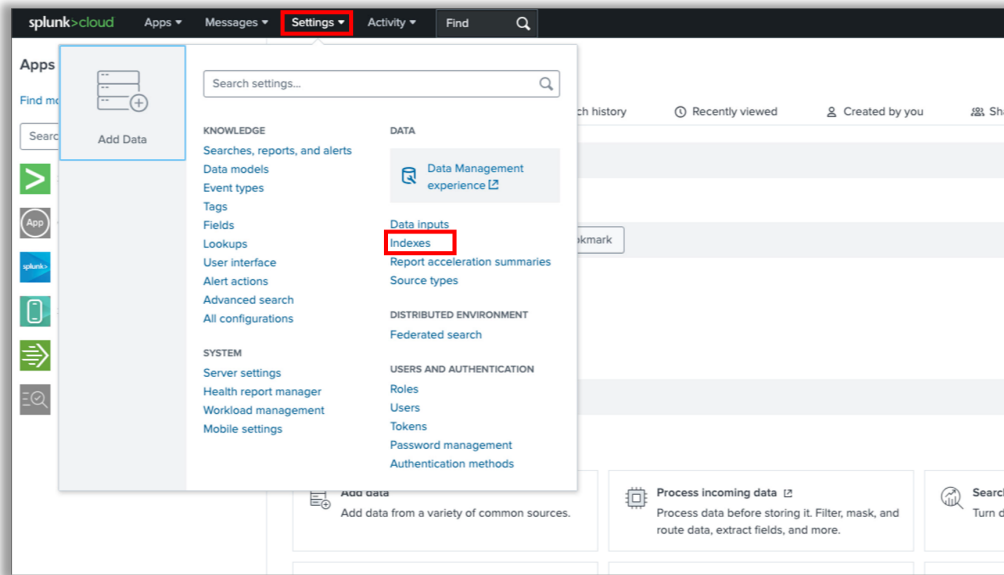
Cancel

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**.



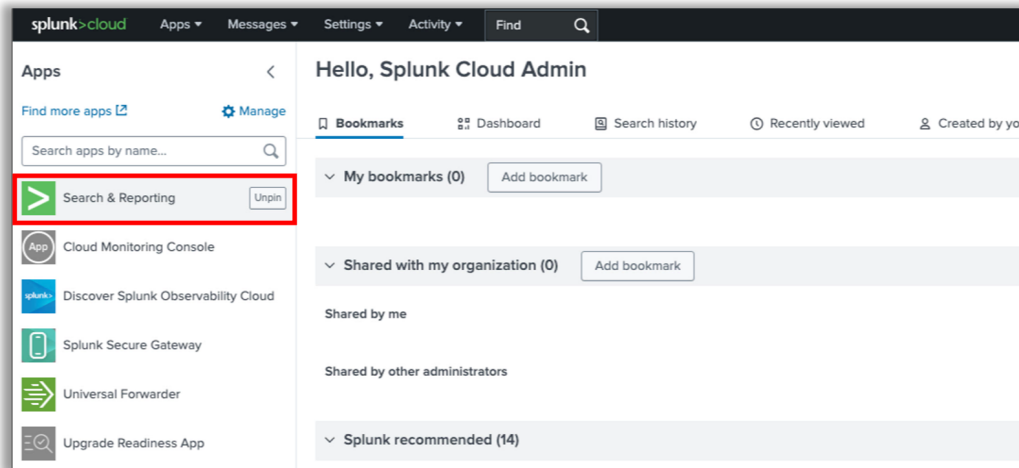
- b. Verify logs are being pushed to your index by checking the Event Count.

 A screenshot of the Splunk Cloud Indexes page. The page shows a list of 7 indexes. The 'cohesity' index is highlighted with a red box. The table columns are Name, Actions, Type, Category, App, Current Size, Max Size, and Event Count.

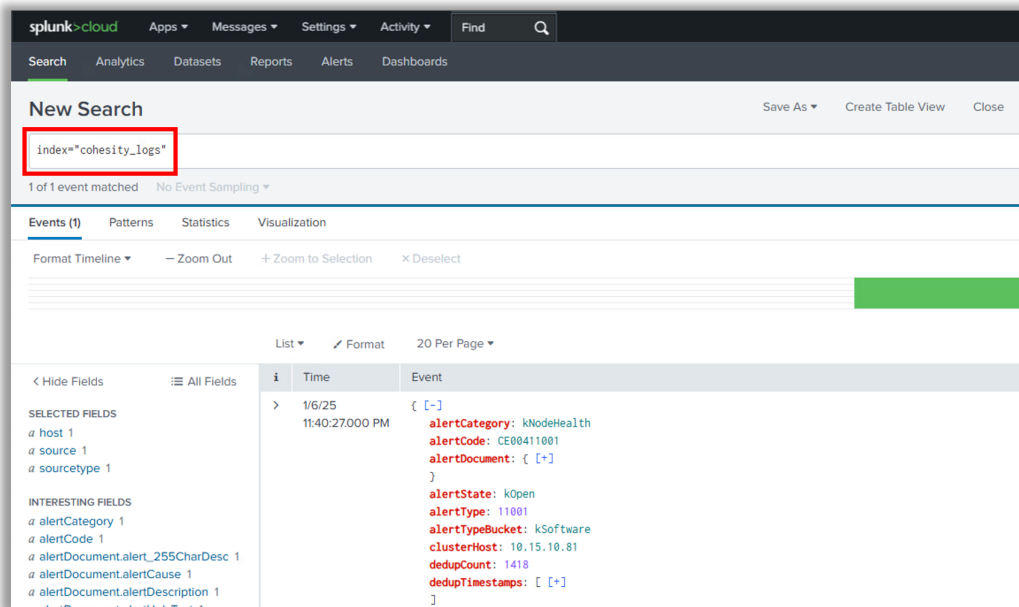
Name	Actions	Type	Category	App	Current Size	Max Size	Event Count
cohesity	Edit Delete	Events	Regular	search	0 B	500 GB	48
history	Edit Delete	Events	Regular	system	0 B	unlimited	0
lastchanceindex	Edit Delete	Events	Regular	100-whisper	0 B	unlimited	0
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0
splunklogger	Edit Delete	Events	Regular	system	0 B	unlimited	0
summary	Edit Delete	Events	Regular	system	0 B	unlimited	0

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.

The screenshot shows the Splunk Cloud interface with a search query `index=*cohesity_logs*` in the search bar. A dropdown menu is open, showing various time range options. The option **Last 24 hours** is highlighted with a red box. The interface also shows a table with one event matched, and a list of fields including `host`, `source`, and `sourcetype`.

- d. Alert and visualize.

The screenshot shows the Splunk Cloud interface with the same search query `index=*cohesity_logs*`. A dropdown menu is open under the **Save As** button, showing options: **Report**, **Alert**, **Existing Dashboard**, **New Dashboard**, and **Event Type**. The **Report** option is highlighted with a red box. The interface also shows a table with one event matched, and a list of fields including `host`, `source`, and `sourcetype`.

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"

The screenshot shows the Splunk Cloud Admin interface. At the top, there's a navigation bar with 'Search & Reporting' selected. Below that, the 'New Search' section shows the query 'index=cohesity' entered in the search bar. The search results are displayed in a table format, showing event details for 23/10/2024. The table has columns for 'Time' and 'Event'. The first event is at 12:07:37.000 and the second is at 12:05:46.000. The event details are shown in a JSON format, including fields like 'alerts', 'commonAnnotations', 'commonLabels', 'externalURL', 'groupKey', 'groupLabels', 'receiver', 'status', 'truncatedAlerts', and 'version'.

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**.

The screenshot shows a Splunk search interface. A modal window titled "alerts.labels.alert_category" is open, displaying a "Top 10 Values" table. The table lists various alert categories and their counts and percentages. The "BackupRestore" category is highlighted with a red box.

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	58	5.112%
Metadata	46	4.783%
Indexing	35	3.579%
Security	29	2.965%
ArchivalRestore	27	2.761%

The screenshot shows a Splunk search interface with a search query: `index=cohesity "alerts().labels.alert_category"=BackupRestore`. The search results show 352 events. The event list is displayed below, showing two events with their respective timestamps and alert details.

Search Query: `index=cohesity "alerts().labels.alert_category"=BackupRestore`

352 events (before 23/10/2024 12:20:47:000) No Event Sampling

Events (352) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection x Deselect 1 day per column

Time	Event
23/10/2024 12:07:37:000	alerts: [(+)] commonAnnotations: { (+) } commonLabels: { (+) } externalURL: https://helios-production-internal.cohesity.com/alertmanager-d1 groupKey: {}(account_id="0812380802e11qTQAS",hidden_from_user="false");(account_id="0812380802e11qTQAS", alertname="ProtectionGroupFailed", severity="Critical") groupLabels: { (+) } receiver: 0812380802e11qTQAS_Splunk Final status: firing truncatedAlerts: 0 version: 4 Show as raw text host = prd-p-afmh.splunkcloud.com:8088 source = http:Cohesity_WH sourcetype = _json
23/10/2024 11:27:37:000	alerts: [(+)] commonAnnotations: { (+) } commonLabels: { (+) } externalURL: https://helios-production-internal.cohesity.com/alertmanager-d1



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

The screenshot shows a Splunk search interface. The main panel displays a list of search results with columns for Time and Event. A field summary for 'alerts.labels.alertname' is overlaid on the results. The summary table shows the following data:

Values	Count	%
ProtectionGroupFailed	1,053	299.148%
ProtectionGroupSucceeded	20	5.682%
ProtectionPolicyModified	7	1.989%
ProtectionGroupDeleted	5	1.42%
ProtectionGroupModified	3	0.852%
RestoreTaskFailed	1	0.284%
VMMigrationIdentified	1	0.284%

The screenshot shows a Splunk search interface with a search query: `index=cohesity "alerts{}.labels.alert_category"="BackupRestore" "alerts{}.labels.alertname"="ProtectionPolicyModified"`. The search results show 6 events. The first event is highlighted, showing the following details:

- Time: 21/10/2024 09:34:28.000
- Alerts: [{"externalURL": "https://helios-production-internal.cohesity.com/alertmanager-d1", "groupKey": "(/(account_id='0012300002e1jqTQAS'.hidden_from_user='false')):(account_id='0012300002e1jqTQAS', alertname='ProtectionPolicyModified', severity='Info')", "receiver": "0012300002e1jqTQAS_Splunk Final", "status": "firing", "truncatedAlerts": 0, "version": 4}]]



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

The screenshot shows a Splunk search interface. The search bar contains the query: `index="cohesity" "alerts{}.labels.alert_category"=Security`. The results are displayed in a list view. A field picker overlay is open, showing the field `alerts.labels.alert_category` with 19 values and 98.888% of events. The field picker includes a table of top values:

Top Values	Count	%
BackupRestore	1,893	111.759%
RemoteReplication	212	21.677%
DataPath	184	18.634%
StorageUsage	67	6.851%
Networking	65	6.646%
ClusterManagement	58	5.112%
Metadata	46	4.781%
Indexing	35	3.579%
Security	29	2.955%
ArchivalRestore	27	2.761%

The screenshot shows a Splunk search interface with the search bar containing the query: `index="cohesity" "alerts{}.labels.alert_category"=Security`. The results are displayed in a list view. The search results show 28 events. The first event is from 23/10/2024 06:38:02.000 and the second is from 22/10/2024 12:58:17.000. The event details for the first event are:

```
{
  "alerts": [
    {
      "commonAnnotations": {
        "externalURL": "https://helios-production-internal.cohesity.com/alertmanager-d1",
      },
      "commonLabels": {
        "groupKey": "(/(account_id='0012700002e1jqTQAS',hidden_from_user='false')):(account_id='0012700002e1jqTQAS', alertname='AVServerConnectionFailed', severity='Warning')",
      },
      "receiver": "0012700002e1jqTQAS_Splunk Final",
      "status": "firing",
      "truncatedAlerts": 0,
      "version": 4
    }
  ]
}
```



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
```

The screenshot shows a Splunk search interface with the following details:

- Search Query:** `index=cohesity "alerts{}.labels.alert_category"=Security`
- Results:** 28 events (before 23/10/2024 12:21:36.000). No Event Sampling.
- Event Details:**

```

{
  "time": "2024-10-23T06:38:02.000Z",
  "alerts": [
    {
      "alertname": "DataIngestAnomalyAlert",
      "severity": "Warning",
      "status": "firing",
      "receiver": "0012f00002eJlqTQAS_Splunk_Final",
      "truncatedAlerts": 0
    }
  ],
  "commonAnnotations": {},
  "externalURL": "https://helios-production-internal.cohesity.com/alertmanager-d1",
  "groupKey": "({account_id='0012f00002eJlqTQAS', hidden_from_user='false'});({account_id='0012f00002eJlqTQAS', alertname='AVServerConnectionFailed', severity='Warning'})",
  "groupLabels": {}
}

```
- Summary Table:**

Values	Count	%
KMSUnreachable	13	46.428%
AVServerConnectionFailed	11	39.286%
DataClassificationAlert	2	7.143%
DataIngestAnomalyAlert	2	7.143%
AuditLogFailure	1	3.571%
- Selected Fields:**
 - host 1
 - source 1
 - sourcetype 1
- Interesting Fields:**
 - alerts().annotations.alert_details 1
 - alerts().annotations.alertedapter_plus_h_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_unit 1
 - alerts().annotations.timeline 24
 - alerts().endsAt 1
 - alerts().fingerprint 27
 - alerts().generatorURL 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
 - alerts().labels.hidden_from_user 1

New Search

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

2 events (before 23/10/2024 12:21:56.000) No Event Sampling

Time	Event
16/10/2024 07:03:04.000	<pre> alerts: [{}] commonAnnotations: { {} } commonLabels: { {} } externalURL: https://helios-production-internal.cohesity.com/alertmanager-d1 groupKey: {}/(account_id="001270002e71qTQAS",hidden_from_user="false");(account_id="001270002e71qTQAS", alertname="DataIngestAnomalyAlert", severity="Critical") groupLabels: { {} } receiver: 001270002e71qTQAS_Splunk_Final status: firing truncatedAlerts: 0 version: 4 } Show as raw text host = prd-p-afmth.splunkcloud.com:8088 source = http:Cohesity_WH sourcetype = _json </pre>
16/10/2024 02:13:04.000	<pre> alerts: [{}] commonAnnotations: { {} } commonLabels: { {} } externalURL: https://helios-production-internal.cohesity.com/alertmanager-d1 </pre>

New Search

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

2 events (before 23/10/2024 12:21:56.000) No Event Sampling

Time	Event
16/10/2024 07:03:04.000	<pre> alerts: [{}] commonAnnotations: { {} } cause: "The recent protection run of Protection Group testSlnJobMVM3M with job id 7858555 has dramatic changes in the composition of files, which is a significant deviation from the previously observed protection runs" description: Anomalous change in file system detected on Shanky-Win19-Ransomare-Test, a symptom of potential ransomware attack on your primary environment. help: Use the latest clean snapshot taken at 16, Oct 2024 06:11 AM to perform Instant Recovery. occurrence: Start at 2024-10-16 06:38:23.464757 +0800 UTC, total 1 time. summary: Anomalous activity detected in file system. variables: ("es_event_alert_id": "9989902973338497:172960789464787", "entity_id": "88847", "object": "Shanky-Win19-Ransomare-Test", "parent_id": "88834", "source": "sac01-pm-vc70-02.pn.cohesity.com", "cid": "3821361864608156", "cluster_incarnation_id": "1684863644625", "cluster": "hasew117-pl", "job_id": "7058555", "job_name": "testSlnJobMVM3M", "environment": "KWWare", "job_instance_id": "7071487", "job_start_time_usec": "1729659868713117", "anomalous_job_instance_id": "7074873", "anomalous_job_start_time_usec": "172966709464787", "anomaly_strength": "98", "cluster_partition_id": "23", "source_name": "Shanky-Win19-Ransomare-Test", "anomaly_cause": "The recent protection run of Protection Group testSlnJobMVM3M with job id 7858555 has dramatic changes in the composition of files, which is a significant deviation from the previously observed protection runs", "timestamp": "16, Oct 2024 06:11 AM", "tenant_account_id": "", "inline_snapshot_diff": "True", "additional_properties": "" "is_suppressed": "False", "suppressed_time_usec": "", "is_rpaa": "False", "rpaa_region_id": "", "vaults": "", "is_baas": "False", "baas_region_id": "", "protection_env_type": "KWWare") commonLabels: { {} } account_id: 001270002e71qTQAS alert_category: Security alert_id: -1080228877864643417 alert_type_bucket: Maintenance alertname: DataIngestAnomalyAlert cluster_id: 3821361864608156 entity_id: 88847 first_occurrence_usec: 172960789464787 hidden_from_user: false job_id: 7858555 severity: Critical </pre>

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



The screenshot shows a Splunk search interface with the following search query: `index=cohesity *alerts().labels.alert_category=Security`. The search results show 28 events. A modal window titled "alerts().labels.alertname" is open, displaying a report with the following data:

Values	Count	%
KMSUnreachable	13	46.4285
AVServerConnectionFailed	11	39.2857
DataClassificationAlert	2	7.1429
DataIngestAnomalyAlert	2	7.1429
AuditLogFailure	1	3.5714

The screenshot shows a Splunk search interface with the following search query: `index=cohesity *alerts().labels.alert_category=Security *alerts().labels.alertname=DataClassificationAlert`. The search results show 2 events. The first event is from 16/10/2024 at 08:46:37.000, and the second is from 16/10/2024 at 04:06:37.000. The event details for the first event are as follows:

```
{
  "alerts": [
    {
      "externalURL": "https://helios-production-internal.cohesity.com/alertmanager-d1",
      "groupKey": "({account_id='0012700002e11q7QAS', hidden_from_user='false'}):(account_id='0012700002e11q7QAS', alertname='DataClassificationAlert', severity='Info')",
      "groupLabels": {
        "receiver": "0012700002e11q7QAS_Splunk_Final",
        "status": "firing",
        "truncatedAlerts": 0,
        "version": 4
      },
      "host": "prp-p-afmth.splunkcloud.com:8088",
      "source": "http:Cohesity_WH",
      "sourcetype": "_json"
    }
  ]
}
```



The screenshot displays the Splunk Cloud interface for a search. The search query is `index=cohesity *alerts().labels.alert_category=Security *alerts().labels.alertname=DataClassificationAlert`. The search results show 2 events. The first event is expanded, showing a detailed JSON alert structure:

```
{
  "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: Sensitive 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_usec": "172969868171317",
          "scan_trigger": "Anomaly",
          "fl": ""
        }
      },
      "commonLabels": {
        "externalURL": "https://helios-production-internal.cohesity.com/alertmanager-dl",
        "groupKey": "(account_id='0012700002eJlqTQAS',hidden_from_user='false');(account_id='0012700002eJlqTQAS', alertname='DataClassificationAlert', severity='Info')",
        "groupLabels": {
          "receiver": "0012700002eJlqTQAS.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.

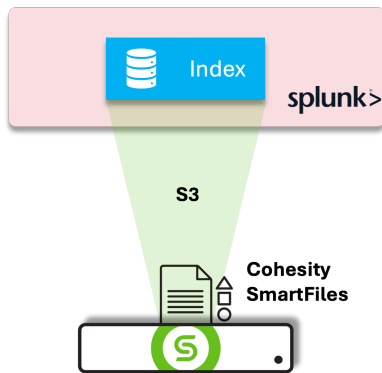
Q: Does Cohesity send Security alerts to Splunk?

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](#).

© 2025. Cohesity, Inc. All Rights Reserved. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.