Integrating Splunk as a Data Collector

Version 1.3

Overview

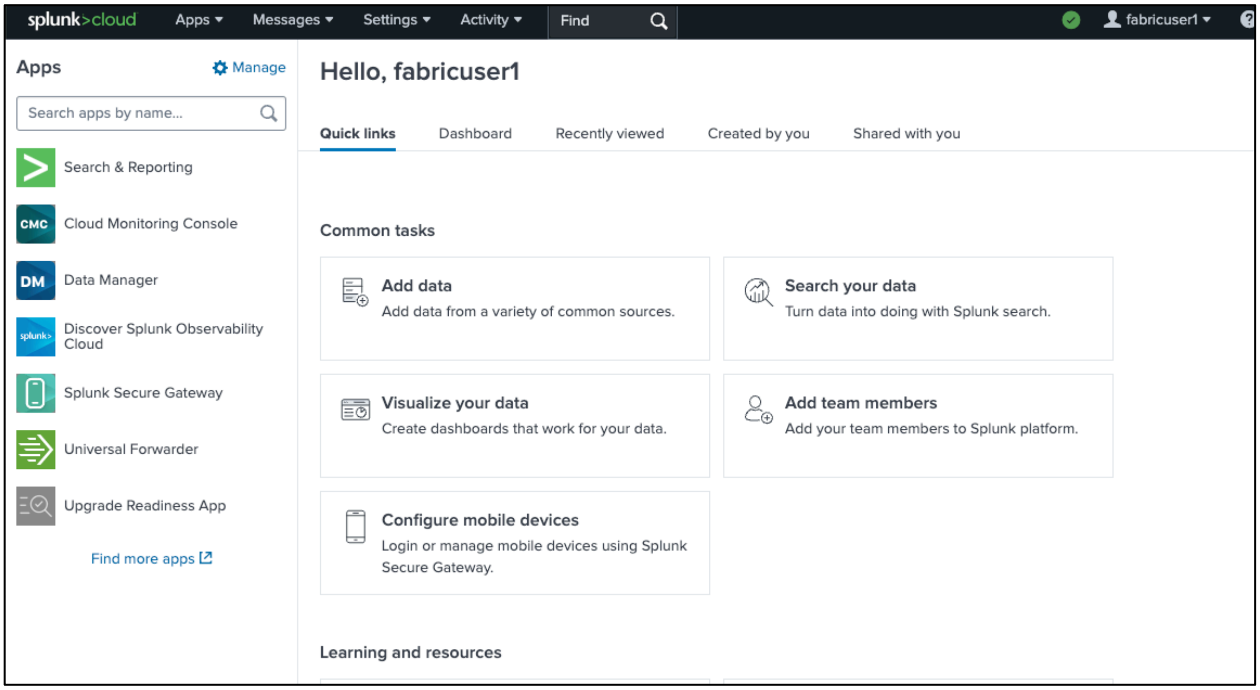
This guide will provide step-by-step instructions on how to set up Splunk Indexes and an HTTP Event Collector, enabling you to easily view Fabric Events and Metrics. You will create two Indexes—one for Metrics and one for Events—and configure the settings for data retention and storage. You can use the Index and HTTP Event Collector Token Details in the following POST /fabric/v4/streamSubscriptions request.

```
curl –X
POST 'https://api.equinix.com/fabric/v4/streamSubscriptions'
 -H 'Content-Type: application/json'
 -H ' Authorization: Bearer <Bearer Token>’
 -d '{
    "type": "STREAM_SUBSCRIPTION",
    "name": "<subscription_name>",
    "description": "subscription_desc",
    "stream": {
        "uuid": "<stream_id>"
    },
    "sink": {
        "uri": "<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>",
        "type": "SPLUNK_HEC",
        "settings": {
            "eventIndex": "<name_of_eventIndex>",
            "metricIndex": "<name_of_metricIndex>",
            "source": "<name_of_splunk_hec>"
        },
        "credential": {
            "type": "ACCESS_TOKEN",
            "accessToken": "Splunk <splunk_access_token>"
        }
    }
 }'
```

Step-by-Step Instructions

1. Log in and Navigate to the Home Page

- Start by logging in to your Splunk instance.
- Once logged in, go to the **Home** page.



Hello, fabricuser1

Common tasks

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

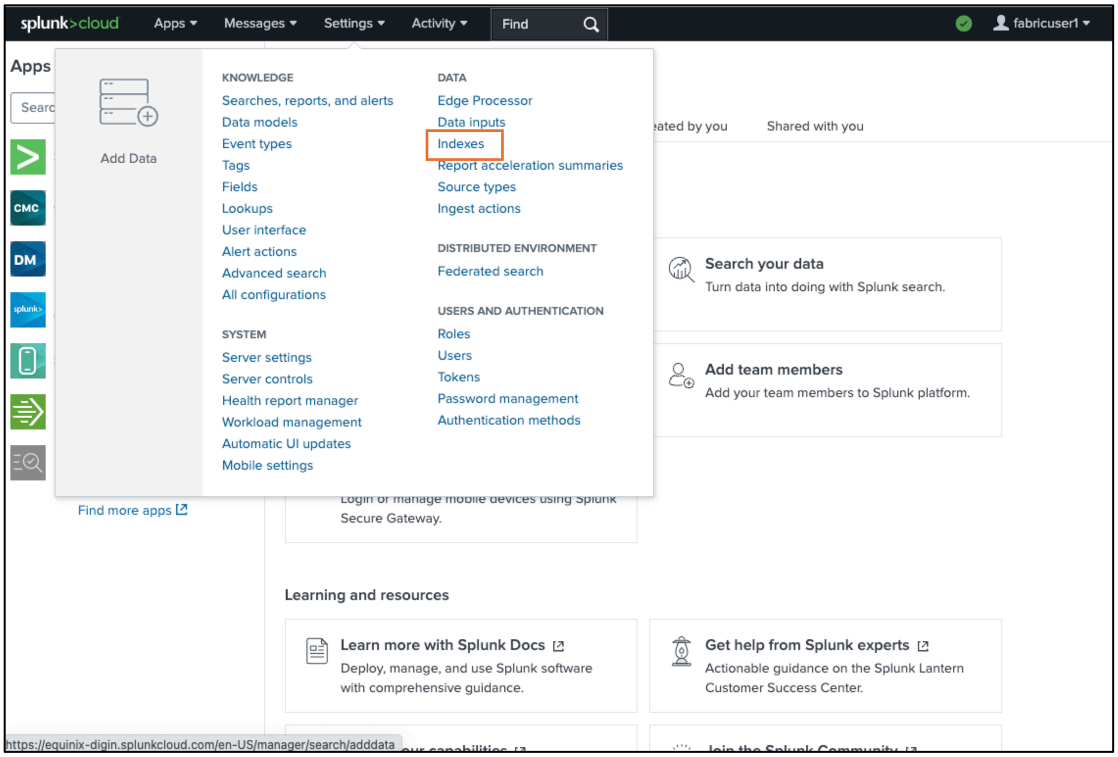
Add team members
Add your team members to Splunk platform.

Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

2. Access the Settings

- On the Home page, click on **Settings** in the top menu.
- In the Settings menu, navigate to **Indexes** under the "Data" section.



Turn data into doing with Splunk search.

Add your team members to Splunk platform.

Login or manage mobile devices using Splunk Secure Gateway.

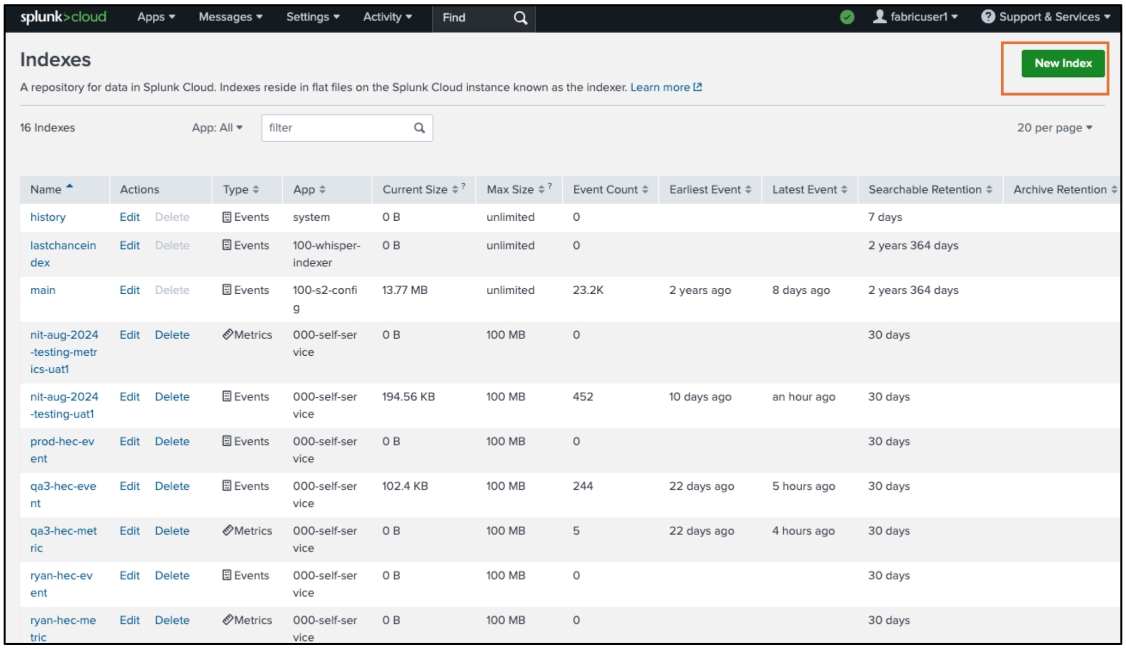
Deploy, manage, and use Splunk software with comprehensive guidance.

Actionable guidance on the Splunk Lantern Customer Success Center.

https://equinix-digin.splunkcloud.com/en-US/manager/search/adddata

3. Create an Event Index

- On the Indexes page, click on **New Index** to create a new index.



Indexes

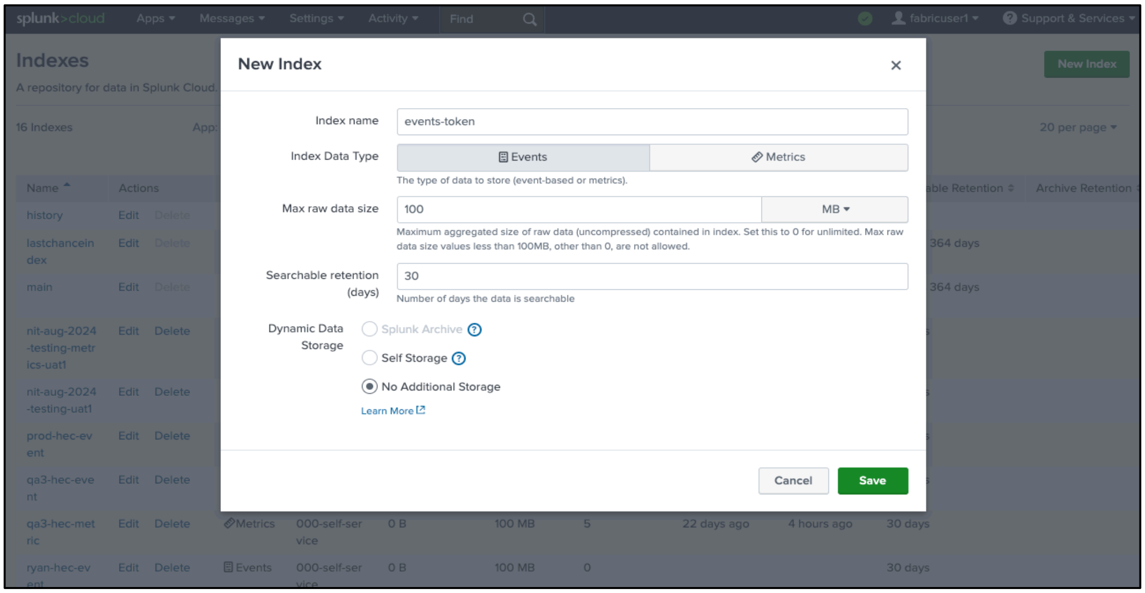
A repository for data in Splunk Cloud. Indexes reside in flat files on the Splunk Cloud instance known as the indexer. Learn more

16 Indexes App: All filter 20 per page

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Searchable Retention	Archive Retention
history	Edit Delete	Events	system	0 B	unlimited	0			7 days	
lastchanceindex	Edit Delete	Events	100-whisper-indexer	0 B	unlimited	0			2 years 364 days	
main	Edit Delete	Events	100-s2-config	13.77 MB	unlimited	23.2K	2 years ago	8 days ago	2 years 364 days	
nit-aug-2024-testing-metrics-uat1	Edit Delete	Metrics	000-self-service	0 B	100 MB	0			30 days	
nit-aug-2024-testing-uat1	Edit Delete	Events	000-self-service	194.56 KB	100 MB	452	10 days ago	an hour ago	30 days	
prod-hec-event	Edit Delete	Events	000-self-service	0 B	100 MB	0			30 days	
qa3-hec-event	Edit Delete	Events	000-self-service	102.4 KB	100 MB	244	22 days ago	5 hours ago	30 days	
qa3-hec-metric	Edit Delete	Metrics	000-self-service	0 B	100 MB	5	22 days ago	4 hours ago	30 days	
ryan-hec-event	Edit Delete	Events	000-self-service	0 B	100 MB	0			30 days	
ryan-hec-metric	Edit Delete	Metrics	000-self-service	0 B	100 MB	0			30 days	

3.1 Select Event Index Data Type

- **Index Data Type: Events Index Data Type** is selected by default.



New Index

Index name: events-token

Index Data Type: [✓ Events] Metrics

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

Max raw data size: 100 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): 30

Number of days the data is searchable

Dynamic Data Storage:
○ Splunk Archive
○ Self Storage
● No Additional Storage

Learn More

3.2 Name the Event Index

- **Name:** Enter a name for your Event Index.

3.3 Set Data Size Limit

- **Data Size:** Set the data size limit for the Index. For example, you can set it to **100 MB**.

3.4 Configure Retention Policy

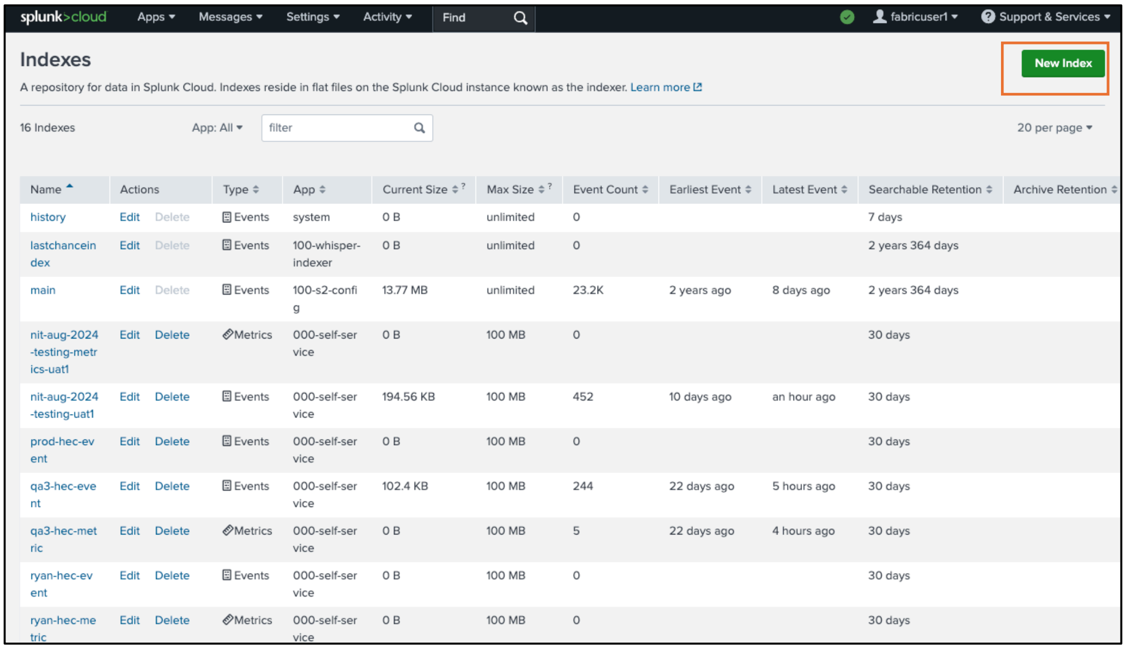
- **Retention Policy:** Set the retention policy, i.e. **30 days**. This means that data older than 30 days will be automatically deleted from the Index.

3.5 Set Dynamic Data Storage

- **Dynamic Data Storage:** Leave the settings as default for dynamic data storage. This ensures that your data is stored efficiently based on Splunk's default storage configuration.
- You will use above Event Index Name later in the POST /fabric/v4/streamSubscriptions request.

4. Create a Metric Index

- On the Indexes page, click on **New Index** to create a new index.



Indexes

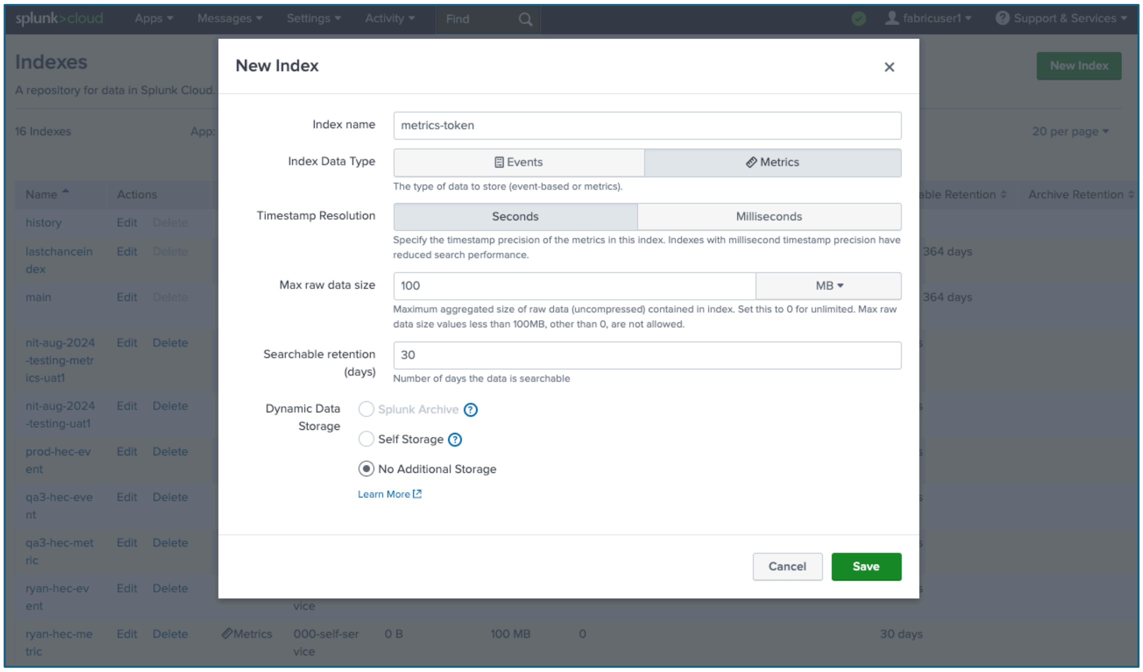
A repository for data in Splunk Cloud. Indexes reside in flat files on the Splunk Cloud instance known as the indexer. Learn more

16 Indexes

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Searchable Retention	Archive Retention
history	Edit Delete	Events	system	0 B	unlimited	0			7 days	
lastchanceindex	Edit Delete	Events	100-whisper-indexer	0 B	unlimited	0			2 years 364 days	
main	Edit Delete	Events	100-s2-config	13.77 MB	unlimited	23.2K	2 years ago	8 days ago	2 years 364 days	
nit-aug-2024-testing-metrics-uat1	Edit Delete	Metrics	000-self-service	0 B	100 MB	0			30 days	
nit-aug-2024-testing-uat1	Edit Delete	Events	000-self-service	194.56 KB	100 MB	452	10 days ago	an hour ago	30 days	
prod-hec-event	Edit Delete	Events	000-self-service	0 B	100 MB	0			30 days	
qa3-hec-event	Edit Delete	Events	000-self-service	102.4 KB	100 MB	244	22 days ago	5 hours ago	30 days	
qa3-hec-metric	Edit Delete	Metrics	000-self-service	0 B	100 MB	5	22 days ago	4 hours ago	30 days	
ryan-hec-event	Edit Delete	Events	000-self-service	0 B	100 MB	0			30 days	
ryan-hec-metric	Edit Delete	Metrics	000-self-service	0 B	100 MB	0			30 days	

4.1 Select Metrics Index Data Type

- **Index Data Type:** Select **Metrics Index Data Type**.



New Index

Index name: metrics-token

Index Data Type: Events | [✓ Metrics]

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

Timestamp Resolution: [✓ Seconds] | Milliseconds

Specify the timestamp precision of the metrics in this index. Indexes with millisecond timestamp precision have reduced search performance.

Max raw data size: 100 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): 30

Number of days the data is searchable

Dynamic Data Storage:
○ Splunk Archive
○ Self Storage
● No Additional Storage

Learn More

Cancel Save

4.2 Name the Metric Index

- **Name:** Enter a name for your Metric Index.

4.3 Set Data Size Limit

- **Data Size:** Set the data size limit for the Index. For example, you can set it to **100 MB**.

4.4 Configure Retention Policy

- **Retention Policy:** Set the retention policy, i.e. **30 days**. This means that data older than 30 days will be automatically deleted from the Index.

4.5 Set Dynamic Data Storage

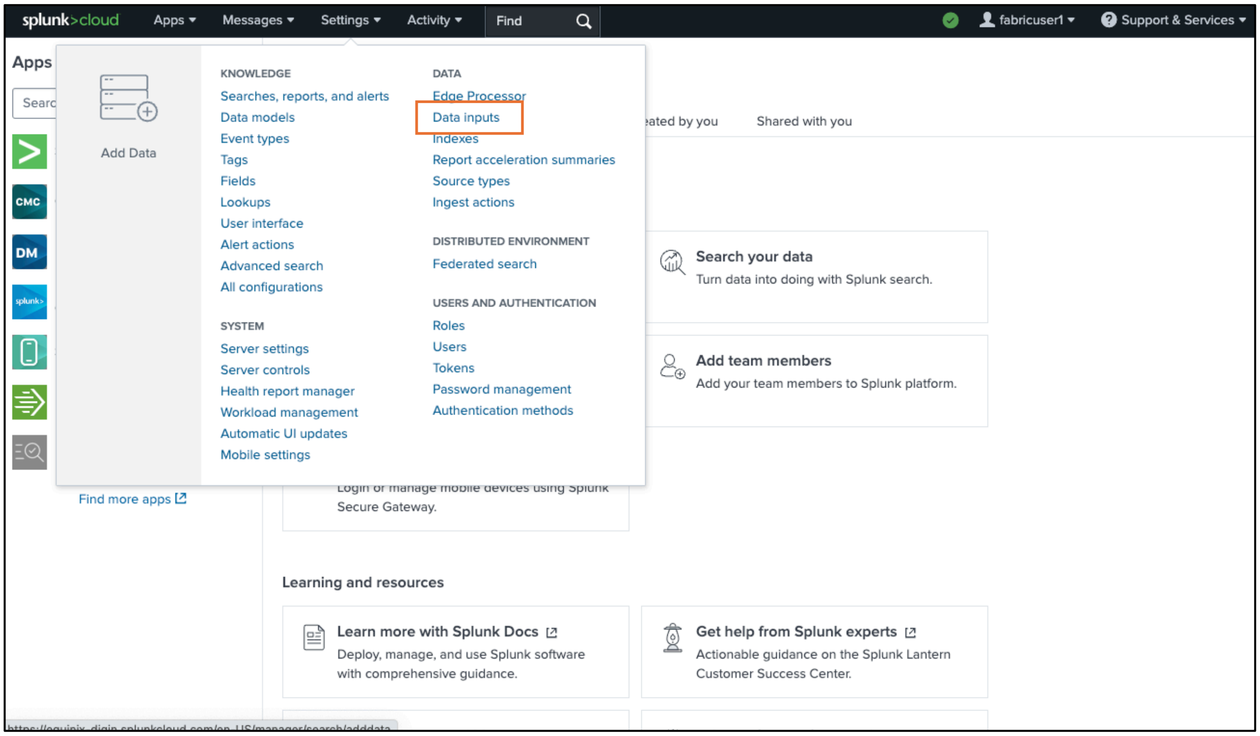
- **Dynamic Data Storage:** Leave the settings as default for dynamic data storage. This ensures that your data is stored efficiently based on Splunk's default storage configuration.
- You will use above Metric Index Name later in the POST /fabric/v4/streamSubscriptions request.

5. Generate an HTTP Event Collector Token Value

- Ensure that the token values generated during this process are saved securely. These tokens may be required for further integration or for data ingestion processes.

5.1. Navigate to the Splunk Home Page

- On the Home page, go to **Settings** in the top menu.
- Under the "Data" section, click on **Data inputs**.



Turn data into doing with Splunk search.

Add your team members to Splunk platform.

Login or manage mobile devices using Splunk Secure Gateway.

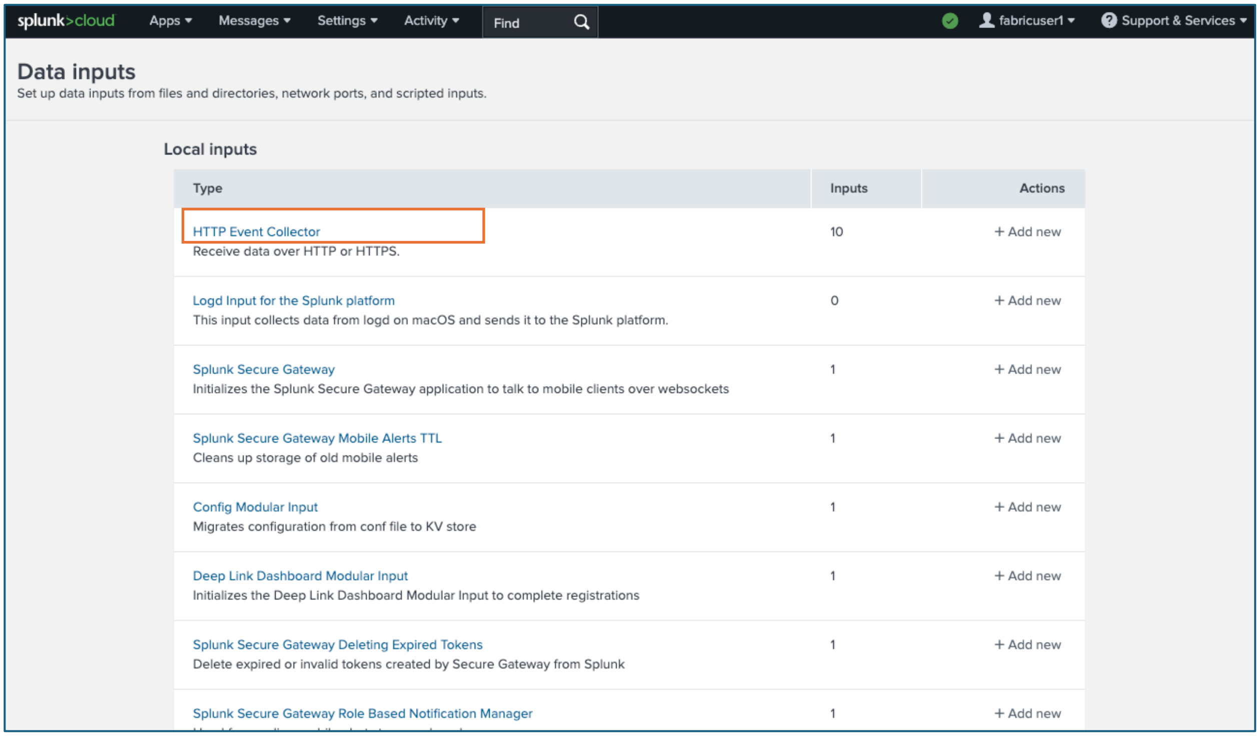
Deploy, manage, and use Splunk software with comprehensive guidance.

Actionable guidance on the Splunk Lantern Customer Success Center.

https://equinix-digin.splunkcloud.com/en-US/manager/search/adddata

5.2. Select HTTP Event Collector

- In the Data Inputs section, select **HTTP Event Collector**.



Data inputs

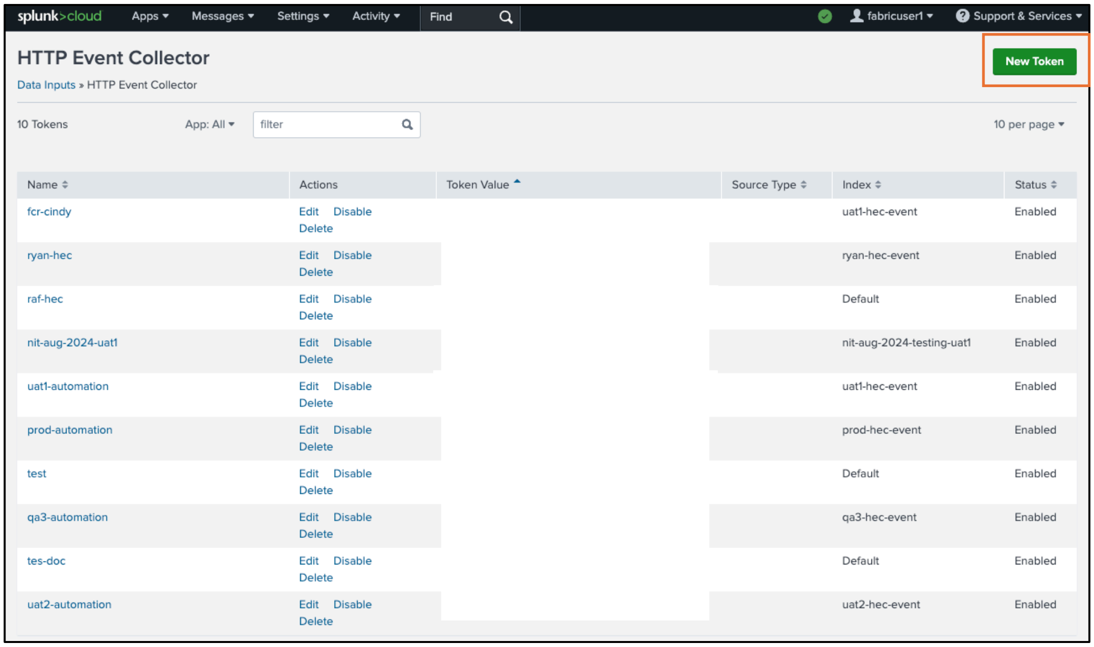
Set up data inputs from files and directories, network ports, and scripted inputs.

Local inputs

Type	Inputs	Actions
HTTP Event Collector Receive data over HTTP or HTTPS.	10	+ Add new
Logd Input for the Splunk platform This input collects data from logd on macOS and sends it to the Splunk platform.	0	+ Add new
Splunk Secure Gateway Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets	1	+ Add new
Splunk Secure Gateway Mobile Alerts TTL Cleans up storage of old mobile alerts	1	+ Add new
Config Modular Input Migrates configuration from conf file to KV store	1	+ Add new
Deep Link Dashboard Modular Input Initializes the Deep Link Dashboard Modular Input to complete registrations	1	+ Add new
Splunk Secure Gateway Deleting Expired Tokens Delete expired or invalid tokens created by Secure Gateway from Splunk	1	+ Add new
Splunk Secure Gateway Role Based Notification Manager	1	+ Add new

5.3 Create an HTTP Event Collector Token

- Click the **New Token** button to start the setup process for the HTTP Event Collector.



HTTP Event Collector

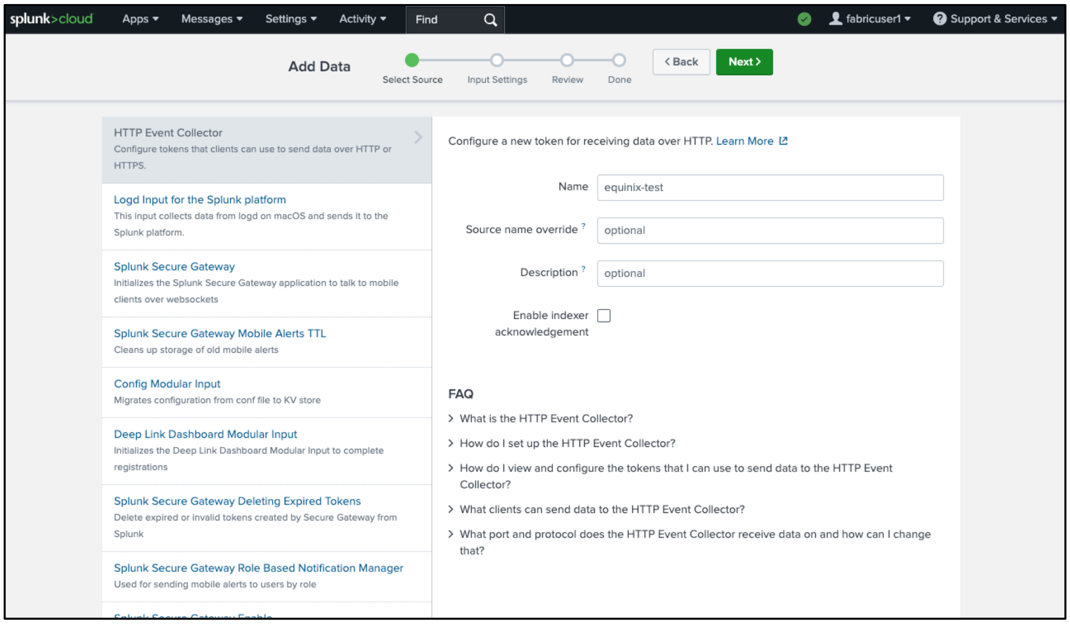
Data Inputs » HTTP Event Collector

10 Tokens

Name	Actions	Token Value	Source Type	Index	Status
fcr-cindy	Edit Disable Delete			uat1-hec-event	Enabled
ryan-hec	Edit Disable Delete			ryan-hec-event	Enabled
raf-hec	Edit Disable Delete			Default	Enabled
nit-aug-2024-uat1	Edit Disable Delete			nit-aug-2024-testing-uat1	Enabled
uat1-automation	Edit Disable Delete			uat1-hec-event	Enabled
prod-automation	Edit Disable Delete			prod-hec-event	Enabled
test	Edit Disable Delete			Default	Enabled
qa3-automation	Edit Disable Delete			qa3-hec-event	Enabled
tes-doc	Edit Disable Delete			Default	Enabled
uat2-automation	Edit Disable Delete			uat2-hec-event	Enabled

5.4. Name the HTTP Event Collector

- On the **Add Data** page, the only required input is the name.
- **Name:** Enter a name for your HTTP Event Collector.



Add Data

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

Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.

Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

Splunk Secure Gateway Mobile Alerts TTL
Cleans up storage of old mobile alerts

Config Modular Input
Migrates configuration from conf file to KV store

Deep Link Dashboard Modular Input
Initializes the Deep Link Dashboard Modular Input to complete registrations

Splunk Secure Gateway Deleting Expired Tokens
Delete expired or invalid tokens created by Secure Gateway from Splunk

Splunk Secure Gateway Role Based Notification Manager
Used for sending mobile alerts to users by role

Configure a new token for receiving data over HTTP. Learn More

Name: equinix-test

Source name override ?: optional

Description ?: optional

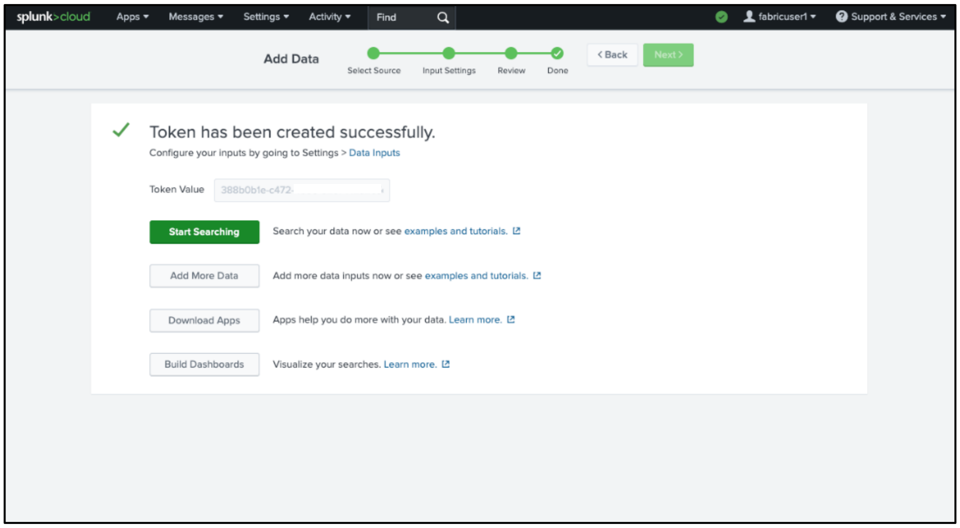
Enable indexer acknowledgement □

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?

5.5. Complete the Setup

- After naming your HTTP Event Collector, click **Next** on the **Select Source** Step.
- Click **Next** on the **Input Settings** Step to review your configurations.
- Finally, click **Submit** on the **Review** Step to complete the setup.



✓ Token has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Token Value: 388b0b1e-c472-

Start Searching — Search your data now or see examples and tutorials.

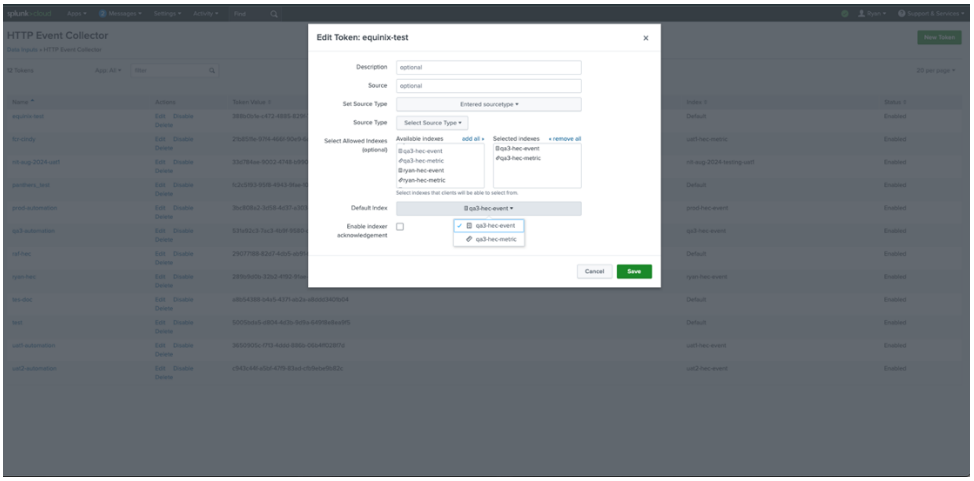
Add More Data — Add more data inputs now or see examples and tutorials.

Download Apps — Apps help you do more with your data. Learn more.

Build Dashboards — Visualize your searches. Learn more.

5.6. Add the Event and Metric Indexes to the HTTP Event Collector

- In HTTP Event Collector, click "Edit" on your HTTP Event Collector.
- Select your event and metric indexes that you have created.
- Set the event index as your Default Index.



Edit Token: equinix-test

Description: optional

Source: optional

Set Source Type: Entered sourcetype ▾

Source Type: Select Source Type ▾

Select Allowed Indexes (optional)

Available indexes: qa3-hec-event, qa3-hec-metric, ryan-hec-event, ryan-hec-metric

Selected indexes: qa3-hec-event, qa3-hec-metric

Select indexes that clients will be able to select from.

Default Index: qa3-hec-event ▾ (✓ qa3-hec-event, qa3-hec-metric)

Enable indexer acknowledgement: □

5.7. Copy the Token Value

- Once the setup is complete, a Token value will be generated.
- **Copy this Token value** to your clipboard, as it will be needed later for the POST streamSubscription API.

6. Create a Splunk Subscription

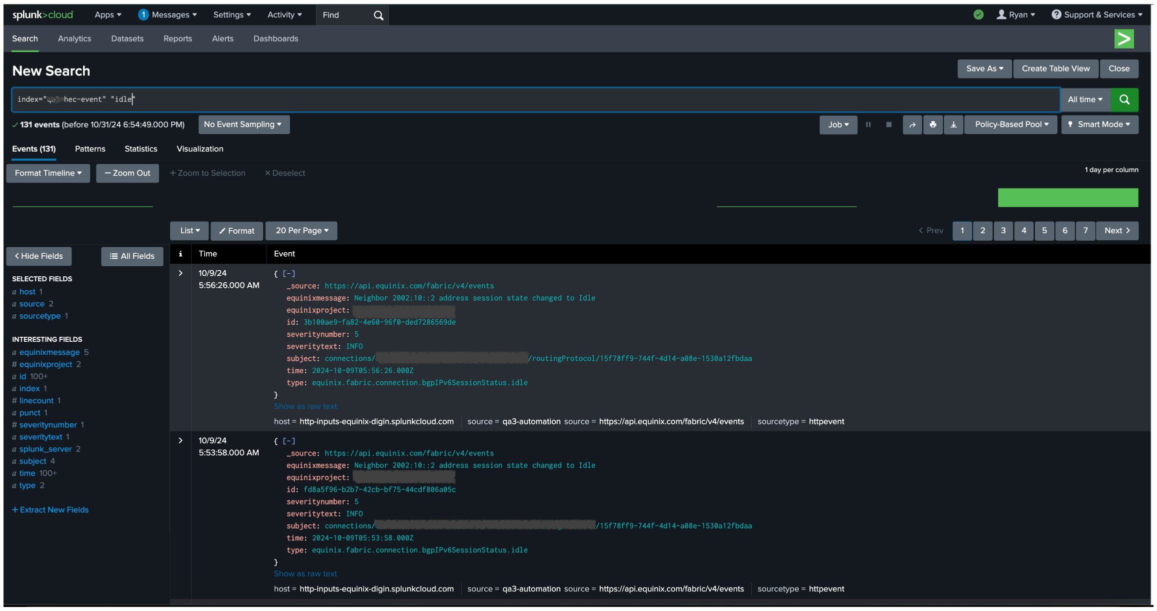
- Now that the Indexes and HTTP Event Collector are set up, call the POST fabric/v4/streamSubscriptions request.

Example:

```
curl –X
POST 'https://api.equinix.com/fabric/v4/streamSubscriptions'
 -H 'Content-Type: application/json'
 -H ' Authorization: Bearer <Bearer Token>’
 -d '{
     "type": "STREAM_SUBSCRIPTION",
     "name": "<subscription_name>",
     "description": "subscription_desc",
     "stream": {
         "uuid": "<stream_id>"
     },
     "sink": {
         "uri": "<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>",
         "type": "SPLUNK_HEC",
         "settings": {
             "eventIndex": "<name_of_eventIndex>",
             "metricIndex": "<name_of_metricIndex>",
             "source": "<name_of_splunk_hec>"
         },
         "credential": {
             "type": "ACCESS_TOKEN",
             "accessToken": "Splunk <splunk_access_token>"
         }
     }
 }'
```

7. Search Events and Metrics

- Go to Home Page. Click on **Search & Reporting**. This will take you to a Splunk search page and search with your Event Index. E.g. index="<name_of_event_index>".
- Refer to the "Fabric Observability with Client Sink Integration" document for detailed instructions on how to receive Events using a specific Sink Type.



New Search

```
index="[redacted]hec-event" "idle"
```

✓ 131 events (before 10/31/24 6:54:49.000 PM) No Event Sampling

Events (131) Patterns Statistics Visualization

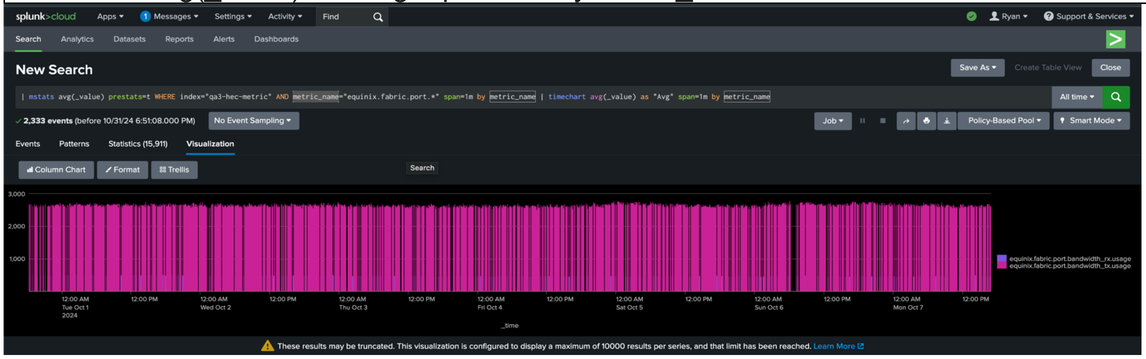
```
10/9/24
5:56:26.000 AM
{ [-]
   _source: https://api.equinix.com/fabric/v4/events
   equinixmessage: Neighbor 2002:10::2 address session state changed to Idle
   equinixproject: [redacted]
   id: 3b100ae9-fa82-4e60-96f0-ded7286569de
   severitynumber: 5
   severitytext: INFO
   subject: connections/[redacted]/routingProtocol/15f78ff9-744f-4d14-a08e-1530a12fbdaa
   time: 2024-10-09T05:56:26.000Z
   type: equinix.fabric.connection.bgpIPv6SessionStatus.idle
}
host = http-inputs-equinix-digin.splunkcloud.com   source = qa3-automation source = https://api.equinix.com/fabric/v4/events   sourcetype = httpevent

10/9/24
5:53:58.000 AM
{ [-]
   _source: https://api.equinix.com/fabric/v4/events
   equinixmessage: Neighbor 2002:10::2 address session state changed to Idle
   equinixproject: [redacted]
   id: fd8a5f96-b2b7-42cb-bf75-44cdf806a05c
   severitynumber: 5
   severitytext: INFO
   subject: connections/[redacted]/15f78ff9-744f-4d14-a08e-1530a12fbdaa
   time: 2024-10-09T05:53:58.000Z
   type: equinix.fabric.connection.bgpIPv6SessionStatus.idle
}
host = http-inputs-equinix-digin.splunkcloud.com   source = qa3-automation source = https://api.equinix.com/fabric/v4/events   sourcetype = httpevent
```

- Additionally, refer to Splunk Documentation to Search and Query for Metrics.

  Example:

```
| mstats avg(_value) prestats=t WHERE index="<name_of_metric_index>" AND
metric_name="equinix.fabric.[port | connection | metro].*" span=1m by metric_name |
timechart avg(_value) as "Avg" span=1m by metric_name
```



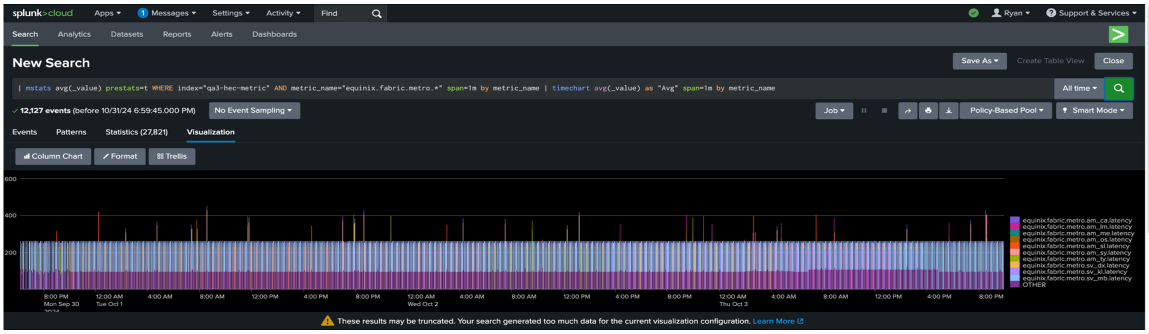
New Search

```
| mstats avg(_value) prestats=t WHERE index="qa3-hec-metric" AND metric_name="equinix.fabric.port.*" span=1m by metric_name | timechart avg(_value) as "Avg" span=1m by metric_name
```

✓ 2,333 events (before 10/31/24 6:51:08.000 PM) No Event Sampling

Events Patterns Statistics (15,911) Visualization

⚠ These results may be truncated. This visualization is configured to display a maximum of 10000 results per series, and that limit has been reached.



New Search

```
| mstats avg(_value) prestats=t WHERE index="qa3-hec-metric" AND metric_name="equinix.fabric.metro.*" span=1m by metric_name | timechart avg(_value) as "Avg" span=1m by metric_name
```

✓ **12,127 events** (before 10/31/24 6:59:45.000 PM) No Event Sampling

These results may be truncated. Your search generated too much data for the current visualization configuration. Learn More