Step-By-Step Instructions

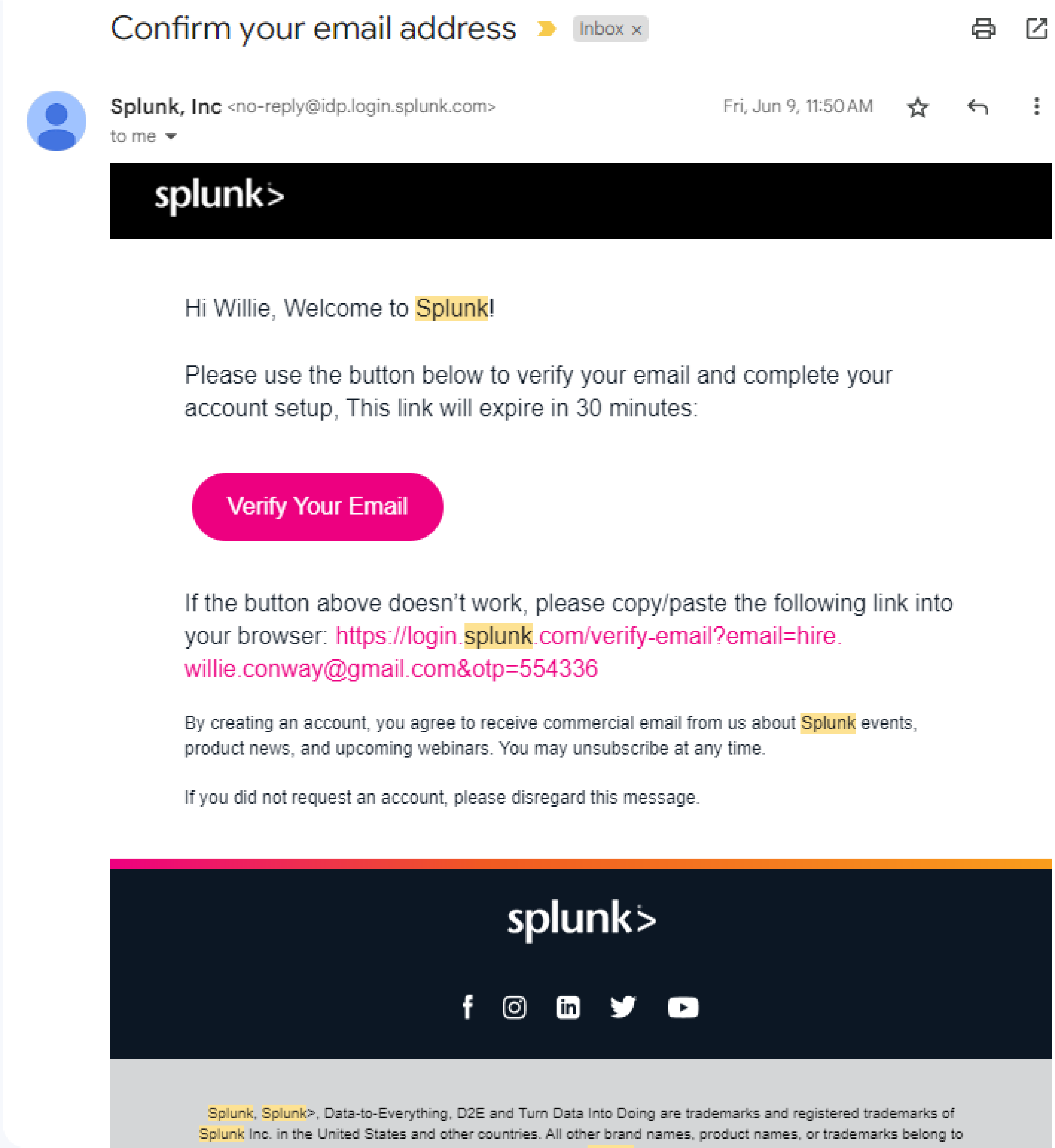
Follow the instructions and fill in the sections to complete the activity.

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. The data contains log and event information from Buttercup Games' mail servers and web accounts. This includes information like access and authentication logs, email logs, and more.

Navigate to supporting materials (tutorialdata.zip)

Step 2: Create a Splunk Cloud account



Confirm your email address

Splunk, Inc <no-reply@idp.login.splunk.com>

to me

Fri, Jun 9, 11:50 AM

Hi Willie, Welcome to Splunk!

Please use the button below to verify your email and complete your account setup, This link will expire in 30 minutes:

If the button above doesn't work, please copy/paste the following link into your browser: https://login.splunk.com/verify-email?email=hire.willie.conway@gmail.com&otp=554336

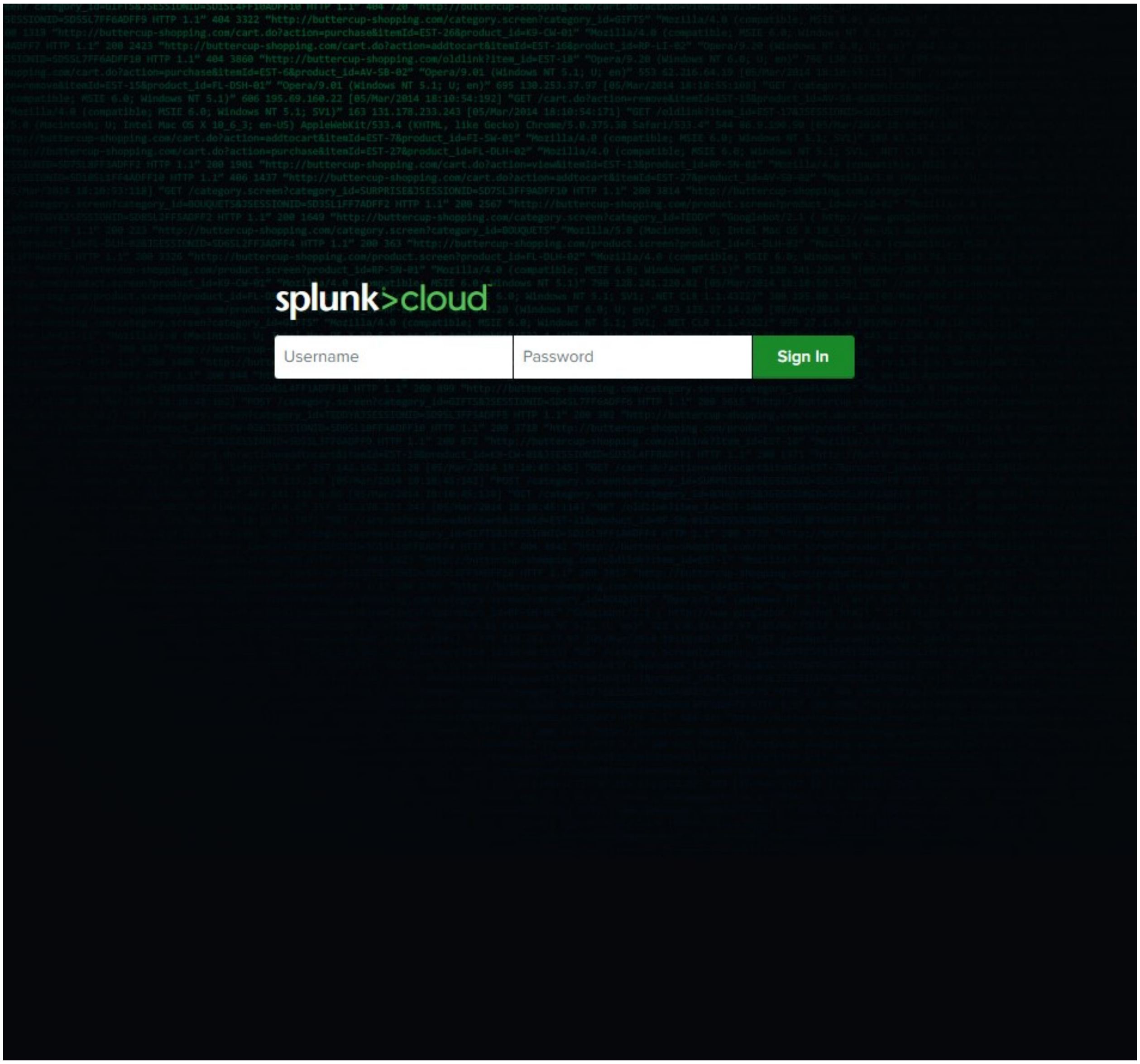
By creating an account, you agree to receive commercial email from us about Splunk events, product news, and upcoming webinars. You may unsubscribe at any time.

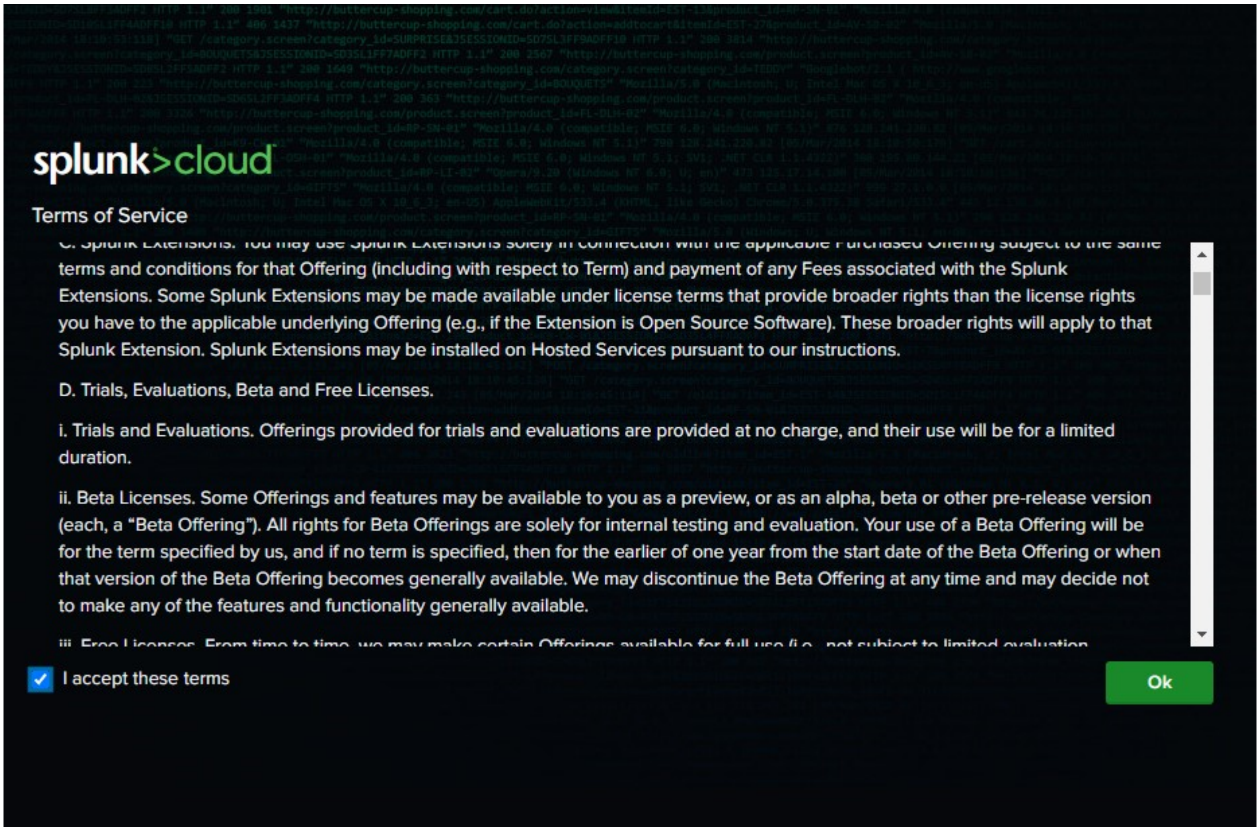
If you did not request an account, please disregard this message.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to

To use Splunk Cloud, you must create an account. Follow *Part 1 - Create a Splunk Cloud account* and *Part 2 - Verify your email* in the Follow-along guide for Splunk sign-up to create an account.

Step 3: Sign up for free Splunk Cloud trial





Terms of Service

C. Splunk Extensions. You may use Splunk Extensions solely in connection with the applicable Purchased Offering subject to the same terms and conditions for that Offering (including with respect to Term) and payment of any Fees associated with the Splunk Extensions. Some Splunk Extensions may be made available under license terms that provide broader rights than the license rights you have to the applicable underlying Offering (e.g., if the Extension is Open Source Software). These broader rights will apply to that Splunk Extension. Splunk Extensions may be installed on Hosted Services pursuant to our instructions.

D. Trials, Evaluations, Beta and Free Licenses.

i. Trials and Evaluations. Offerings provided for trials and evaluations are provided at no charge, and their use will be for a limited duration.

ii. Beta Licenses. Some Offerings and features may be available to you as a preview, or as an alpha, beta or other pre-release version (each, a "Beta Offering"). All rights for Beta Offerings are solely for internal testing and evaluation. Your use of a Beta Offering will be for the term specified by us, and if no term is specified, then for the earlier of one year from the start date of the Beta Offering or when that version of the Beta Offering becomes generally available. We may discontinue the Beta Offering at any time and may decide not to make any of the features and functionality generally available.

iii. Free Licenses. From time to time, we may make certain Offerings available for full use (i.e., not subject to limited evaluation

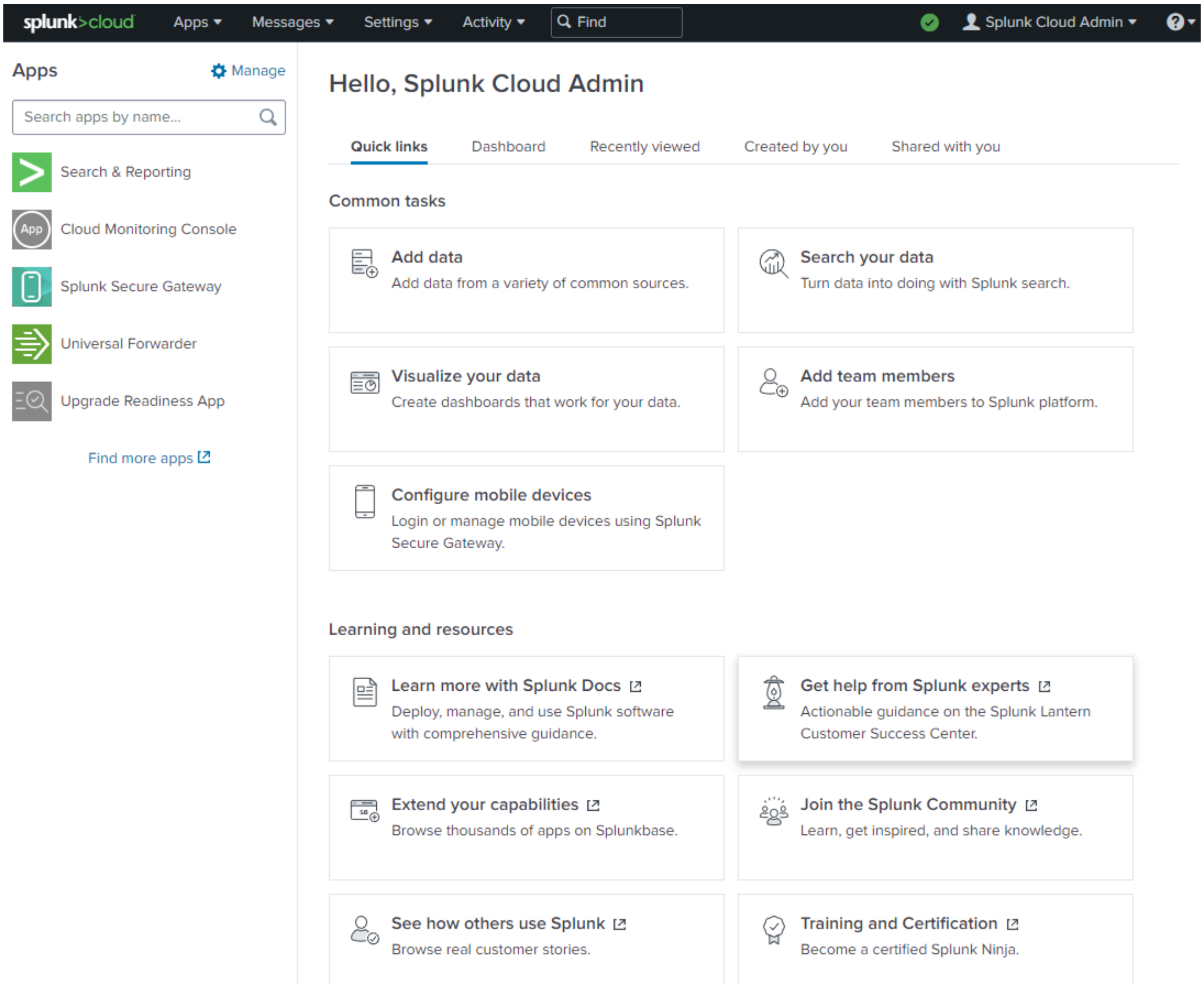
☑ I accept these terms

After you've created your Splunk account, you'll need to sign up for a free Splunk Cloud trial. Follow *Part 3 - Activate a Splunk Cloud trial* in the [Follow-along guide for Splunk sign-up]().
Note: If you experience any issues activating your Splunk Cloud trial please check out the [Splunk cloud tutorial video]().

Step 4: Upload data into Splunk

To operate effectively, it's essential that SIEM tools ingest and index data. SIEM tools collect and process data so that it becomes searchable events that can be queried, viewed, and analyzed.

So far, you've created a Splunk account and activated and accessed the Splunk Cloud free trial, but your Splunk Cloud instance does not contain any data. Next, you'll need to upload data into Splunk to start querying. Complete the following steps to upload data into Splunk:



Hello, Splunk Cloud Admin

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

Learn more with Splunk Docs
Deploy, manage, and use Splunk software with comprehensive guidance.

Get help from Splunk experts
Actionable guidance on the Splunk Lantern Customer Success Center.

Extend your capabilities
Browse thousands of apps on Splunkbase.

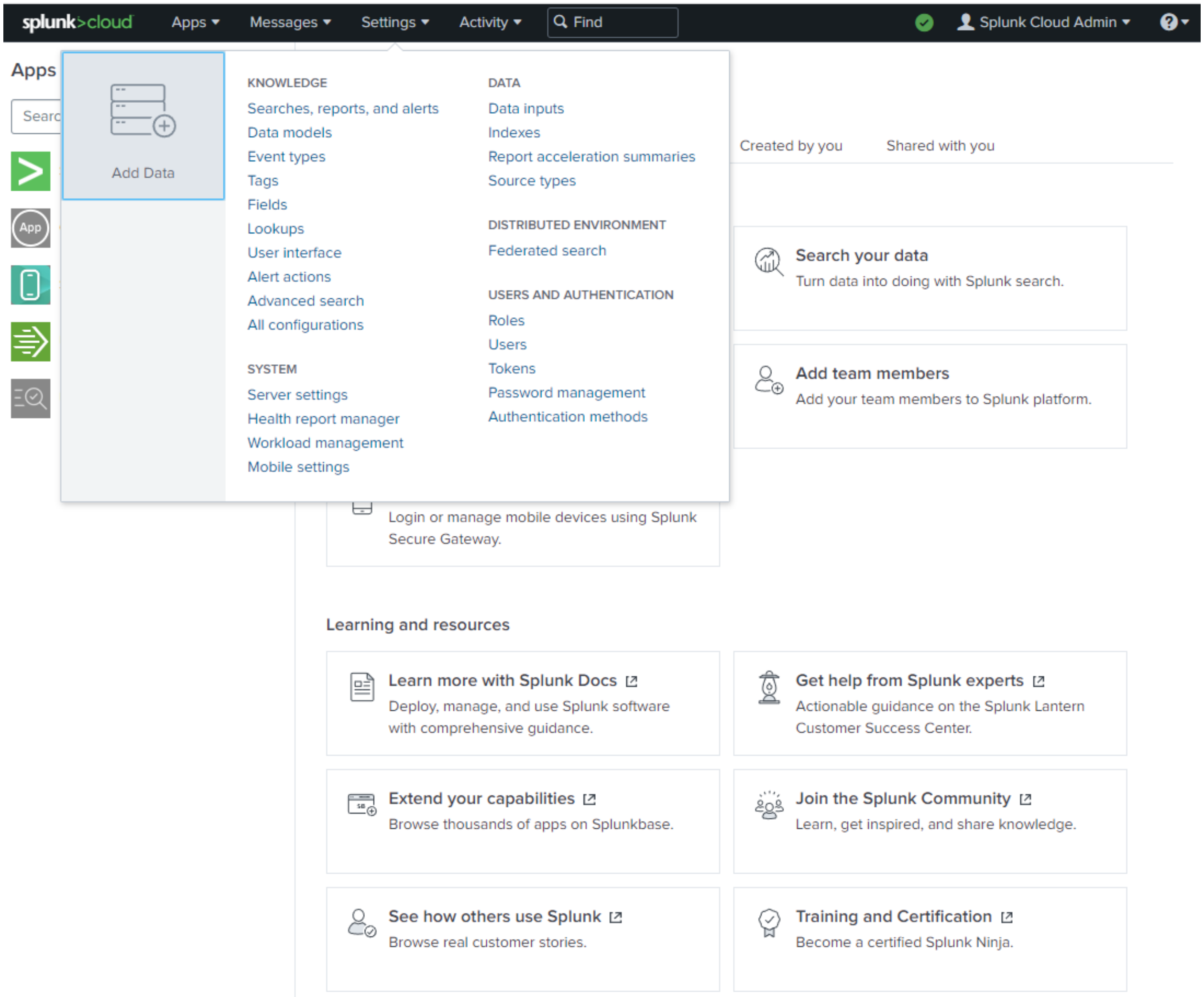
Join the Splunk Community
Learn, get inspired, and share knowledge.

See how others use Splunk
Browse real customer stories.

Training and Certification
Become a certified Splunk Ninja.

1. If you haven't already, download the data file from Step 1: tutorialdata.zip. Click the link then click the download icon. Do not uncompress the file.

2. Navigate to Splunk Home from your Splunk Cloud free trial instance. You might need to log in again using your credentials from Step 3.



Search your data
Turn data into doing with Splunk search.

Add team members
Add your team members to Splunk platform.

Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

Learn more with Splunk Docs
Deploy, manage, and use Splunk software with comprehensive guidance.

Get help from Splunk experts
Actionable guidance on the Splunk Lantern Customer Success Center.

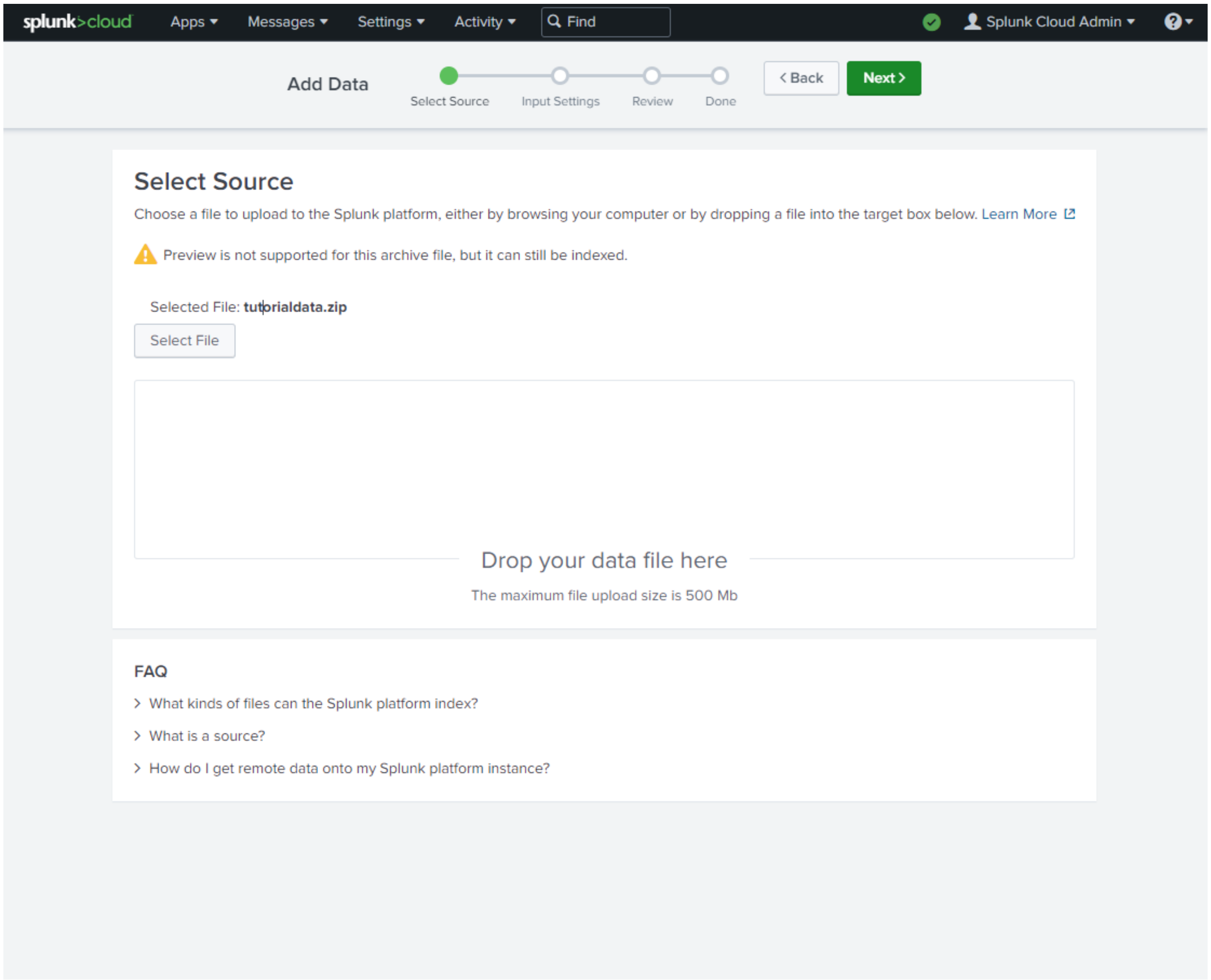
Extend your capabilities
Browse thousands of apps on Splunkbase.

Join the Splunk Community
Learn, get inspired, and share knowledge.

See how others use Splunk
Browse real customer stories.

Training and Certification
Become a certified Splunk Ninja.

3. On the Splunk bar, click **Settings**. Then click the **Add Data** icon.
4. Click **Upload**.
5. Click the **Select File** button.
6. Upload the `tutorialdata.zip` file, and click **Open**.



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Preview is not supported for this archive file, but it can still be indexed.

Selected File: **tutorialdata.zip**

Drop your data file here

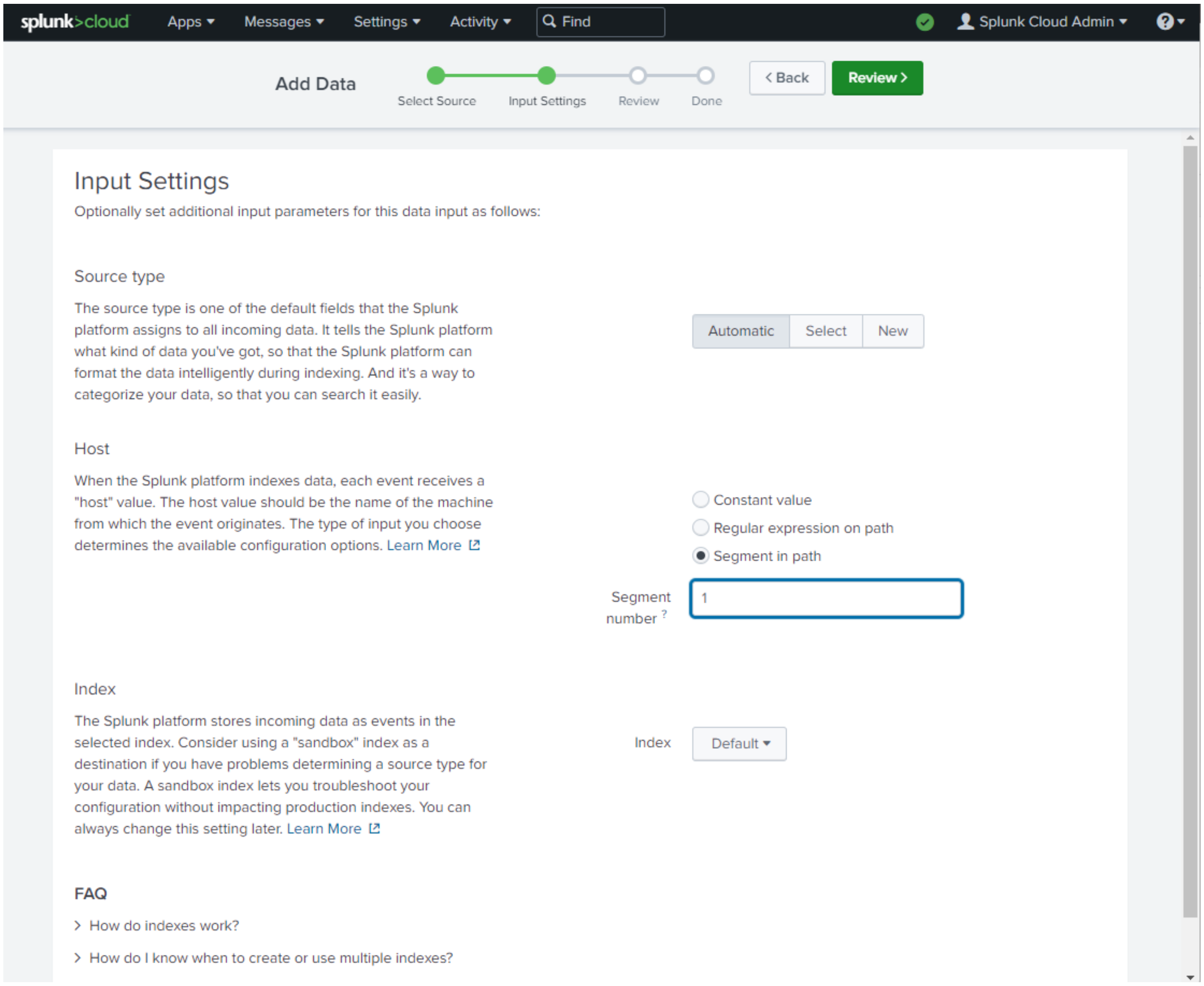
The maximum file upload size is 500 Mb

FAQ

- What kinds of files can the Splunk platform index?
- What is a source?
- How do I get remote data onto my Splunk platform instance?

7. Click the **Next** button to continue to **Input Settings**.

8. By the **Host** section, select **Segment in path** and enter **1** as the segment number.



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

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

○ Constant value
○ Regular expression on path
● Segment in path

Segment number ?: 1

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

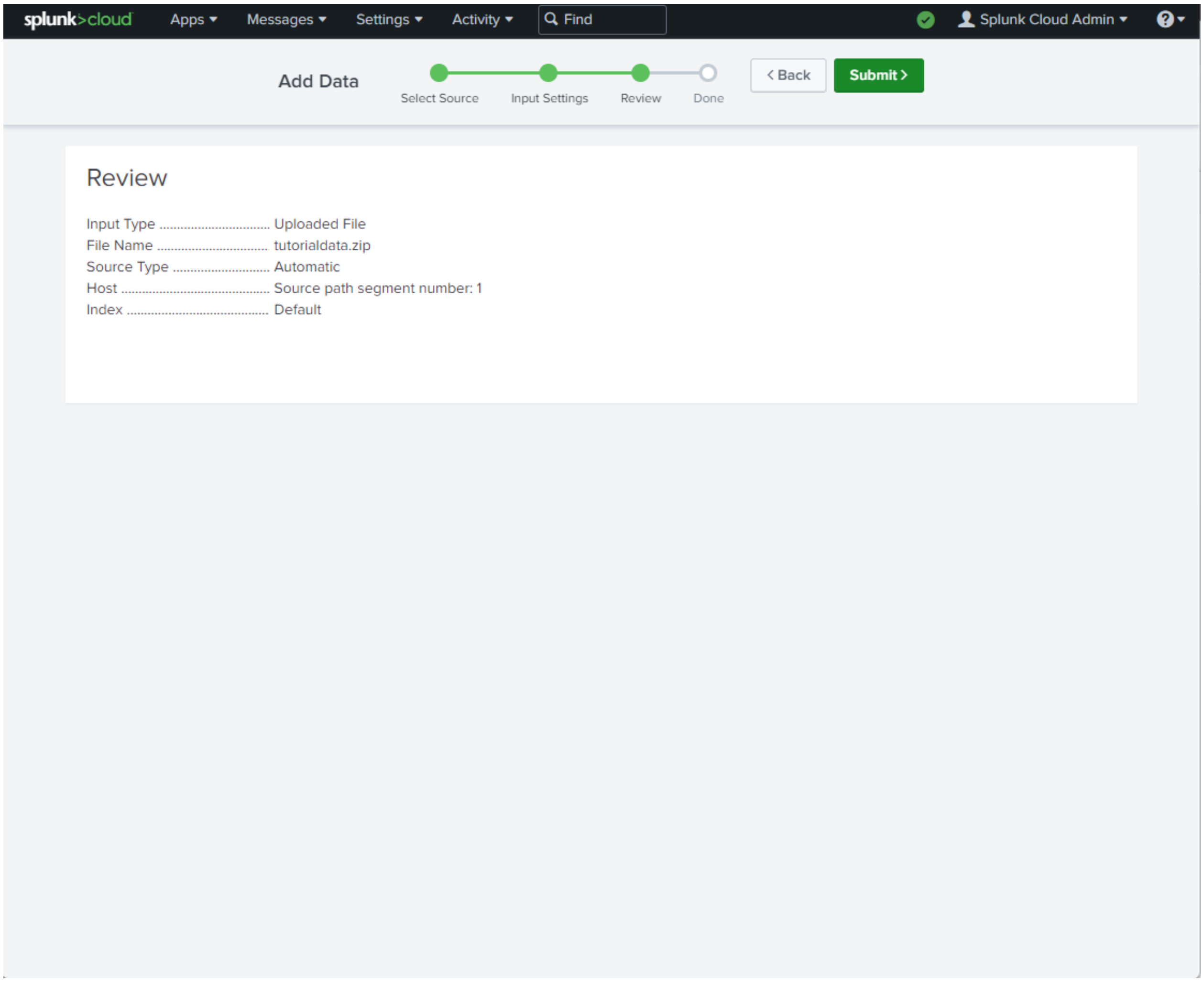
Index: Default ▾

FAQ

> How do indexes work?

> How do I know when to create or use multiple indexes?

9. Click the **Review** button and review the details of the upload before you submit. The details should be as follows:



Review

Input Type .... Uploaded File
File Name .... tutorialdata.zip
Source Type .... Automatic
Host .... Source path segment number: 1
Index .... Default

Input Type: Uploaded File

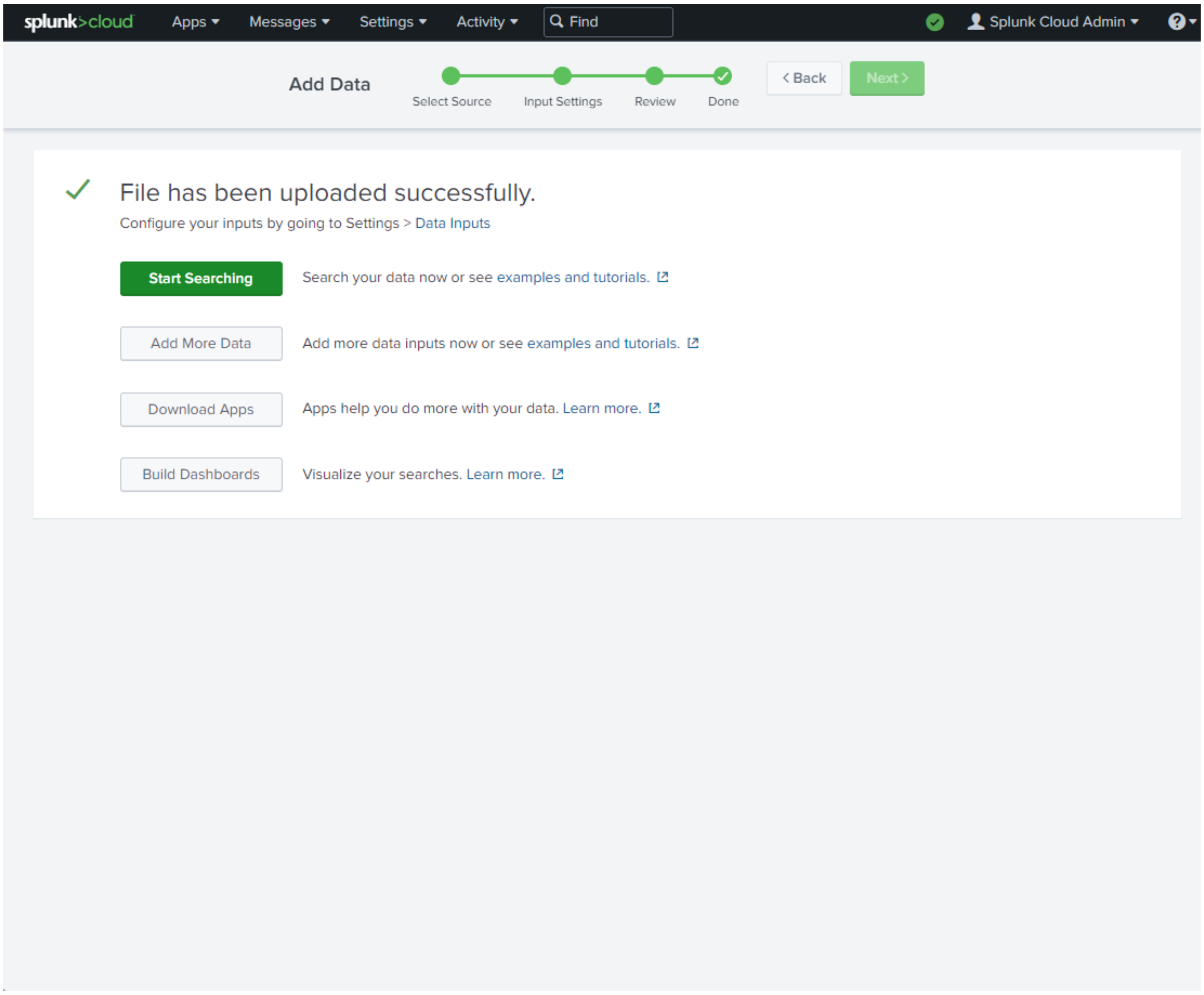
File Name: tutorialdata.zip

Source Type: Automatic

Host: Source path segment number: 1

Index: Default

10. Click **Submit**. Once Splunk has ingested the data, you will receive confirmation that the file was successfully uploaded.



File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

Add more data inputs now or see examples and tutorials.

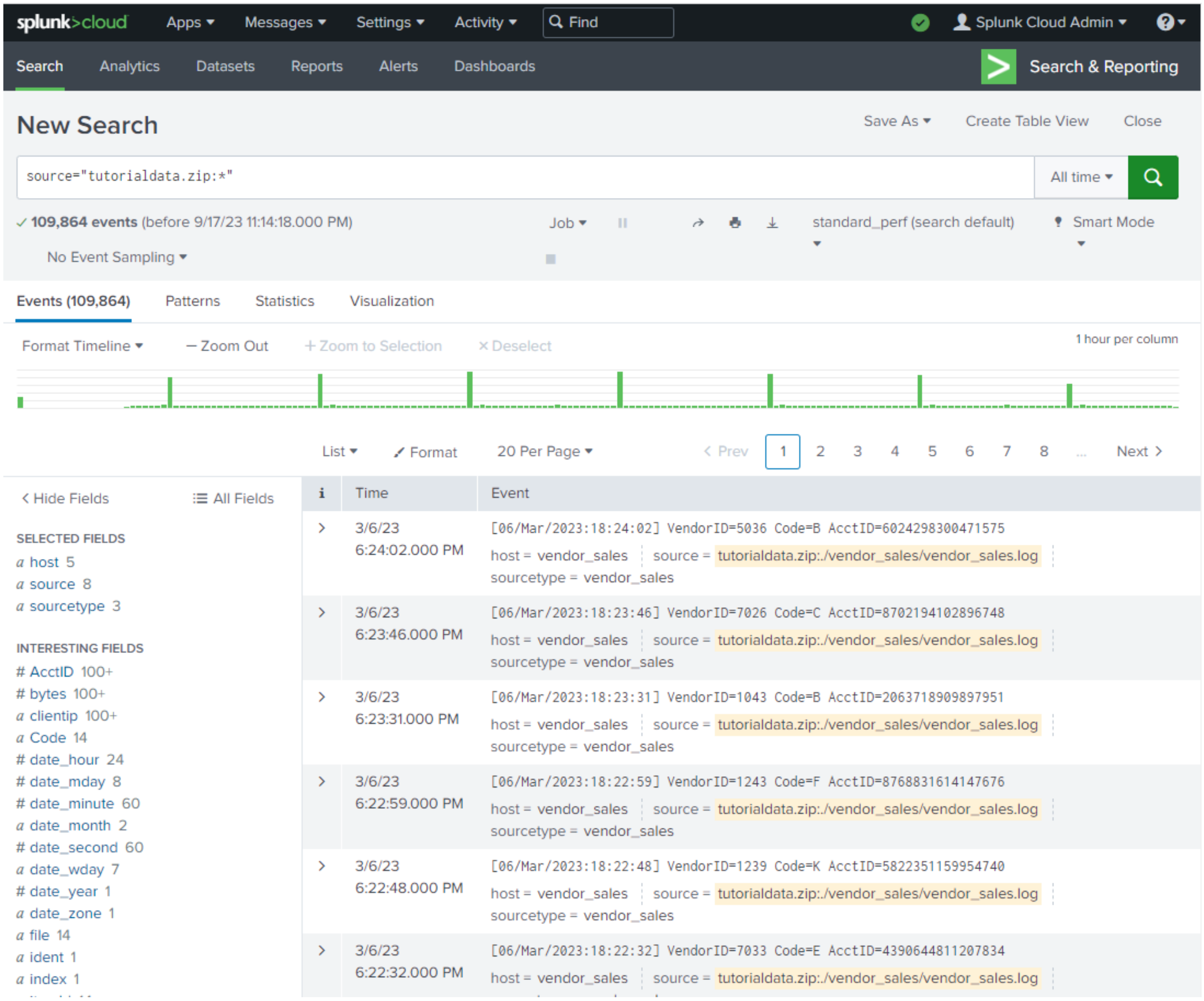
Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

Note: *If you are experiencing issues uploading data into Splunk, refer to the Splunk Search Tutorial guide for help.*

Step 5: Perform a basic search

Take a moment to examine the Splunk Cloud interface by locating the app panel, the Explore Splunk panel, and the Splunk bar.



New Search

```
source="tutorialdata.zip:*"
```

✓ **109,864 events** (before 9/17/23 11:14:18.000 PM)

standard_perf (search default)

SELECTED FIELDS

a	host	5
a	source	8
a	sourcetype	3

INTERESTING FIELDS

#	AcctID	100+
#	bytes	100+
a	clientip	100+
a	Code	14
#	date_hour	24
#	date_mday	8
#	date_minute	60
a	date_month	2
#	date_second	60
a	date_wday	7
#	date_year	1
a	date_zone	1
a	file	14
a	ident	1
a	index	1

i	Time	Event

›	3/6/23
	6:24:02.000 PM
		[06/Mar/2023:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

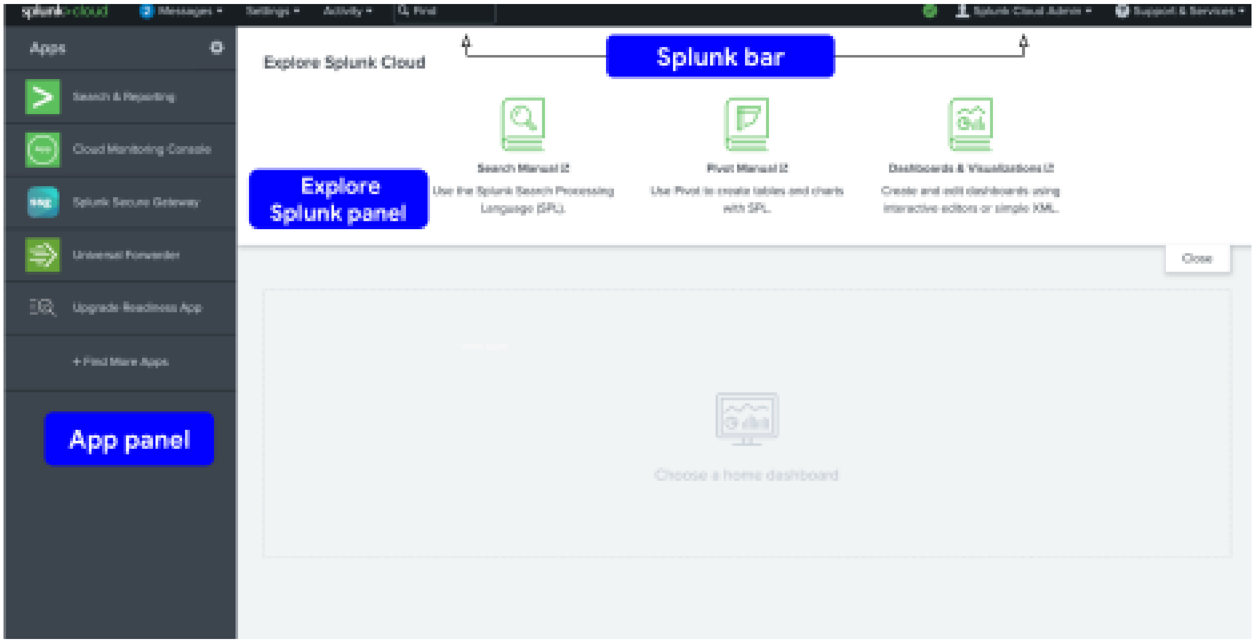
›	3/6/23
	6:23:46.000 PM
		[06/Mar/2023:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

›	3/6/23
	6:23:31.000 PM
		[06/Mar/2023:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

›	3/6/23
	6:22:59.000 PM
		[06/Mar/2023:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

›	3/6/23
	6:22:48.000 PM
		[06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

›	3/6/23 6:22:32.000 PM	[06/Mar/2023:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log



Use the Splunk Search Processing Language (SPL).

Use Pivot to create tables and charts with SPL.

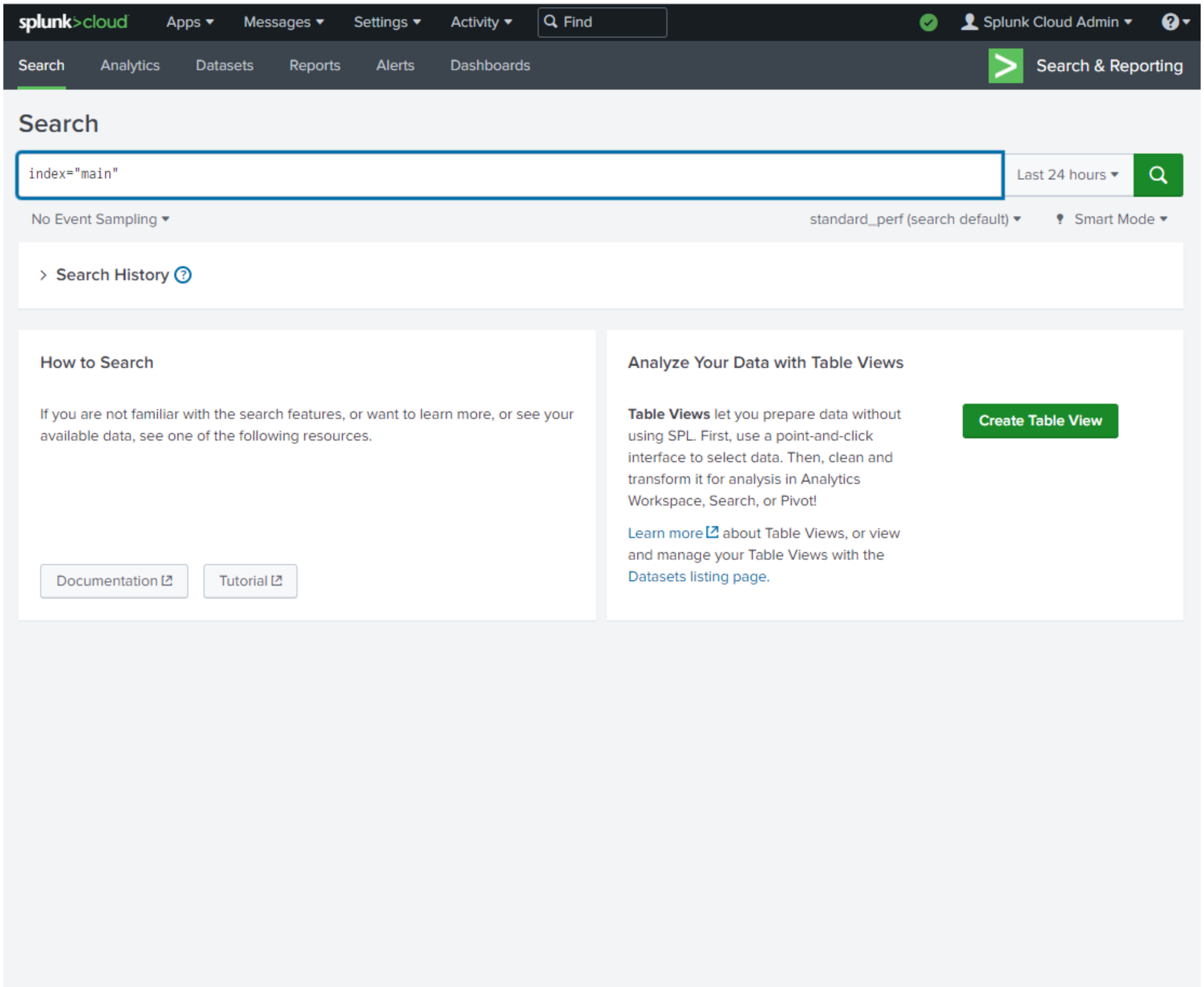
Create and edit dashboards using interactive editors or simple XML.

Now that you've uploaded the data into Splunk, perform your first query to confirm that the data has been ingested, indexed, and is searchable. Follow these steps to perform a query:

1. Navigate to Splunk Home. (To return to Splunk Home, click the Splunk Cloud logo on the Splunk Cloud page.)

2. Click **Search & Reporting**. You may close any pop ups that appear.

3. In the search bar, enter your search query: `index=main` This search term specifies the index. An **index** is a repository for data. Here, the index is a single dataset containing events from an index named main.



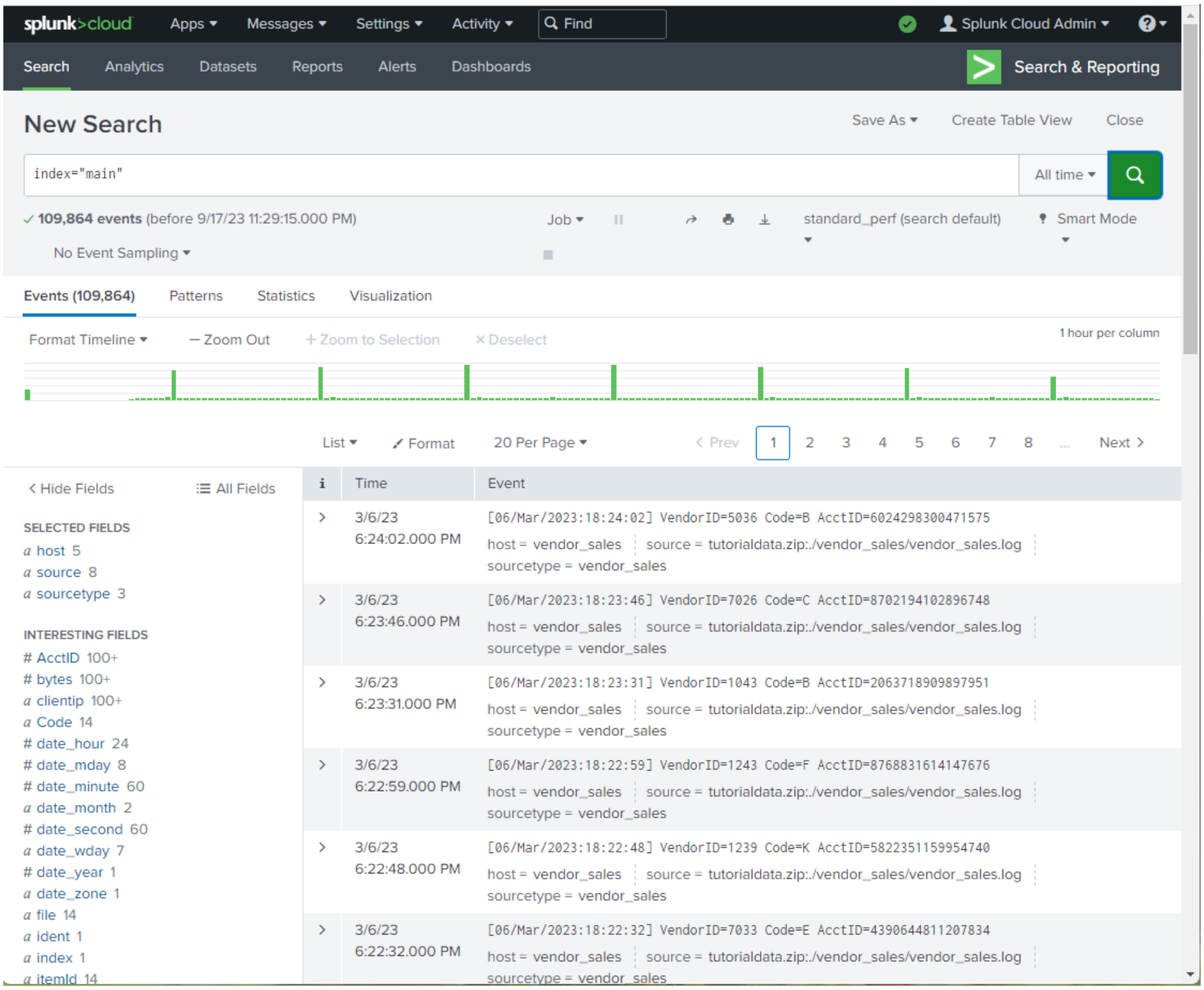
```
index="main"
```

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

4. Select **All Time** from the time range dropdown to search for all the events across all time.
5. Click the search button. Note that the search button is represented by the magnifying glass icon. Your search should retrieve thousands of events.



```
index="main"
```

✓ 109,864 events (before 9/17/23 11:29:15.000 PM)

standard_perf (search default)

Smart Mode

No Event Sampling

SELECTED FIELDS

- a host 5
- a source 8
- a sourcetype 3

INTERESTING FIELDS

- # AcctID 100+
- # bytes 100+
- a clientip 100+
- a Code 14
- # date_hour 24
- # date_mday 8
- # date_minute 60
- a date_month 2
- # date_second 60
- a date_wday 7
- # date_year 1
- a date_zone 1
- a file 14
- a ident 1
- a index 1
- a itemId 14

i	Time	Event

>	3/6/23
	6:24:02.000 PM
		[06/Mar/2023:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

>	3/6/23
	6:23:46.000 PM
		[06/Mar/2023:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

>	3/6/23
	6:23:31.000 PM
		[06/Mar/2023:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

>	3/6/23
	6:22:59.000 PM
		[06/Mar/2023:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

>	3/6/23
	6:22:48.000 PM
		[06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

>	3/6/23
	6:22:32.000 PM
		[06/Mar/2023:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834
		host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log
		sourcetype = vendor_sales

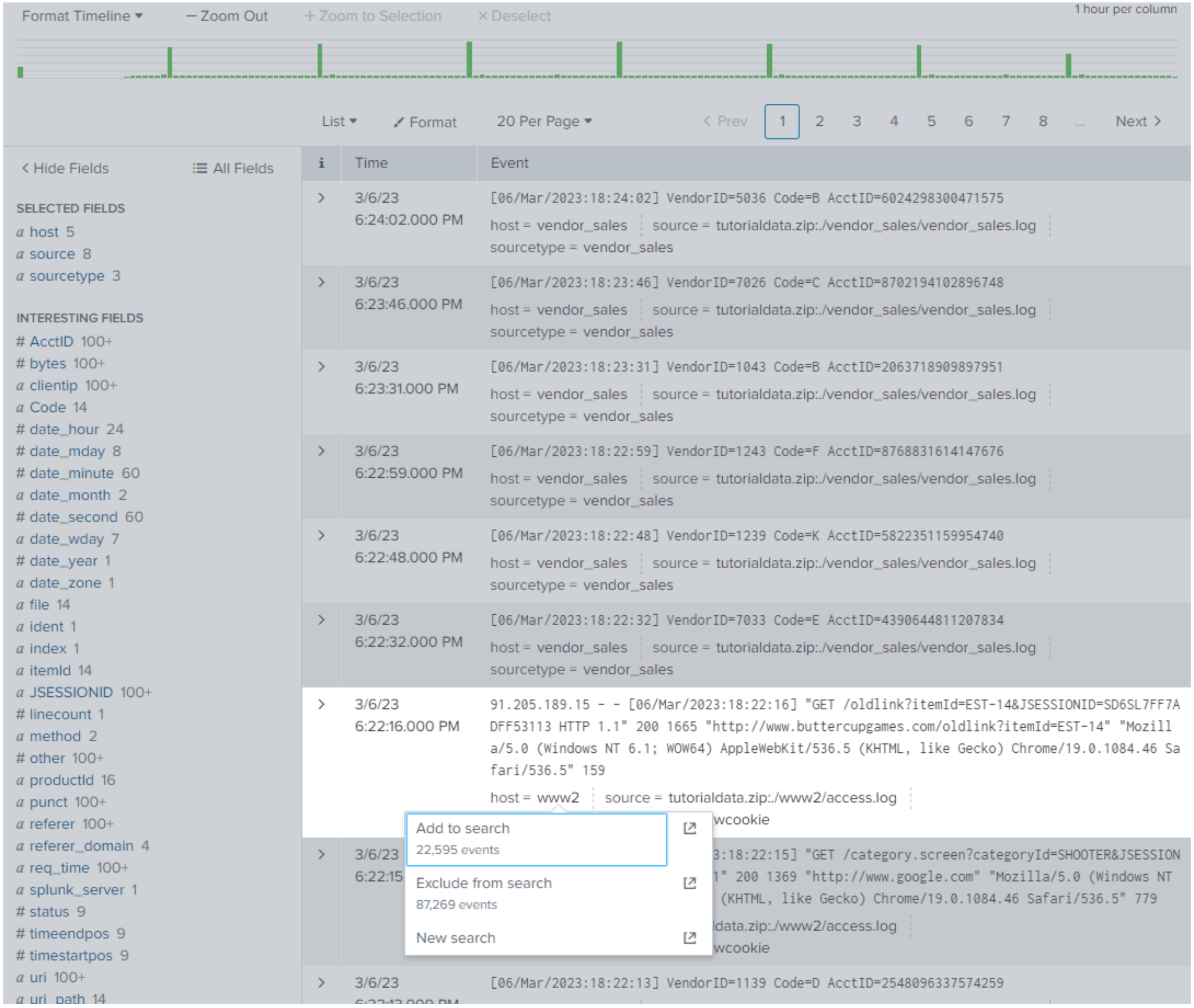
Pro tip*: It's a best practice to use short time ranges in your searches because a shorter time range returns results faster and uses fewer resources. Adjust the time using the time range dropdown or by using time modifiers in your search.*

Step 6: Evaluate the fields

When Splunk indexes data, it attaches fields to each event. These fields become part of the searchable index event data. This helps security analysts easily search for and find the specific data they need. Now that you've run your first query, examine the search results and the fields.

For each event the fields are `host`, `source`, and `sourcetype`. Under **SELECTED**

FIELDS, examine the same fields.



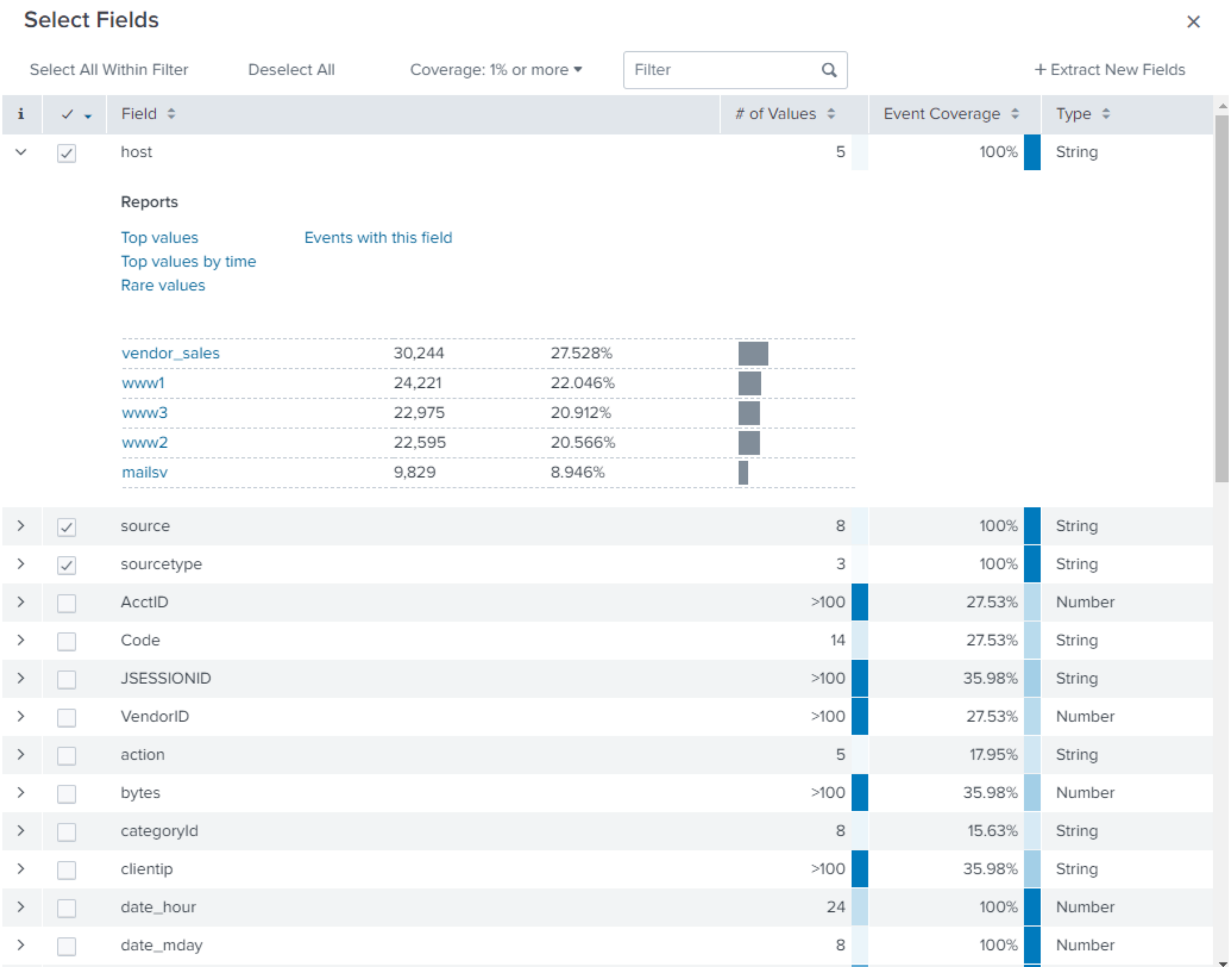
SELECTED FIELDS

- a host 5
- a source 8
- a sourcetype 3

INTERESTING FIELDS

- # AcctID 100+
- # bytes 100+
- a clientip 100+
- a Code 14
- # date_hour 24
- # date_mday 8
- # date_minute 60
- a date_month 2
- # date_second 60
- a date_wday 7
- # date_year 1
- a date_zone 1
- a file 14
- a ident 1
- a index 1
- a itemId 14
- a JSESSIONID 100+
- # linecount 1
- a method 2
- # other 100+
- a productId 16
- a punct 100+
- a referer 100+
- a referer_domain 4
- a req_time 100+
- a splunk_server 1
- # status 9
- # timeendpos 9
- # timestartpos 9
- a uri 100+
- a uri_path 14

```
> 3/6/23            [06/Mar/2023:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575
  6:24:02.000 PM    host = vendor_sales   source = tutorialdata.zip:./vendor_sales/vendor_sales.log
                    sourcetype = vendor_sales

> 3/6/23            [06/Mar/2023:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748
  6:23:46.000 PM    host = vendor_sales   source = tutorialdata.zip:./vendor_sales/vendor_sales.log
                    sourcetype = vendor_sales

> 3/6/23            [06/Mar/2023:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951
  6:23:31.000 PM    host = vendor_sales   source = tutorialdata.zip:./vendor_sales/vendor_sales.log
                    sourcetype = vendor_sales

> 3/6/23            [06/Mar/2023:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676
  6:22:59.000 PM    host = vendor_sales   source = tutorialdata.zip:./vendor_sales/vendor_sales.log
                    sourcetype = vendor_sales

> 3/6/23            [06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740
  6:22:48.000 PM    host = vendor_sales   source = tutorialdata.zip:./vendor_sales/vendor_sales.log
                    sourcetype = vendor_sales

> 3/6/23            [06/Mar/2023:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834
  6:22:32.000 PM    host = vendor_sales   source = tutorialdata.zip:./vendor_sales/vendor_sales.log
                    sourcetype = vendor_sales

> 3/6/23            91.205.189.15 - - [06/Mar/2023:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7A
  6:22:16.000 PM    DFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozill
                    a/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Sa
                    fari/536.5" 159
                    host = www2   source = tutorialdata.zip:./www2/access.log
                    wcookie

> 3/6/23            3:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSION
  6:22:15           1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT
                    (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779
                    ldata.zip:./www2/access.log
                    wcookie

> 3/6/23            [06/Mar/2023:18:22:13] VendorID=1139 Code=D AcctID=2548096337574259
```



Select Fields ×

Select All Within Filter   Deselect All   Coverage: 1% or more ▾   Filter   + Extract New Fields

i	✓	Field	# of Values	Event Coverage	Type
⌄	☑	host	5	100%	String

Reports

Top values   Events with this field
Top values by time
Rare values

vendor_sales	30,244	27.528%
www1	24,221	22.046%
www3	22,975	20.912%
www2	22,595	20.566%
mailsv	9,829	8.946%

i	✓	Field	# of Values	Event Coverage	Type
›	☑	source	8	100%	String
›	☑	sourcetype	3	100%	String
›	□	AcctID	>100	27.53%	Number
›	□	Code	14	27.53%	String
›	□	JSESSIONID	>100	35.98%	String
›	□	VendorID	>100	27.53%	Number
›	□	action	5	17.95%	String
›	□	bytes	>100	35.98%	Number
›	□	categoryId	8	15.63%	String
›	□	clientip	>100	35.98%	String
›	□	date_hour	24	100%	Number
›	□	date_mday	8	100%	Number

Examine the field values by clicking on the field under **SELECTED FIELDS**. You should observe the following:

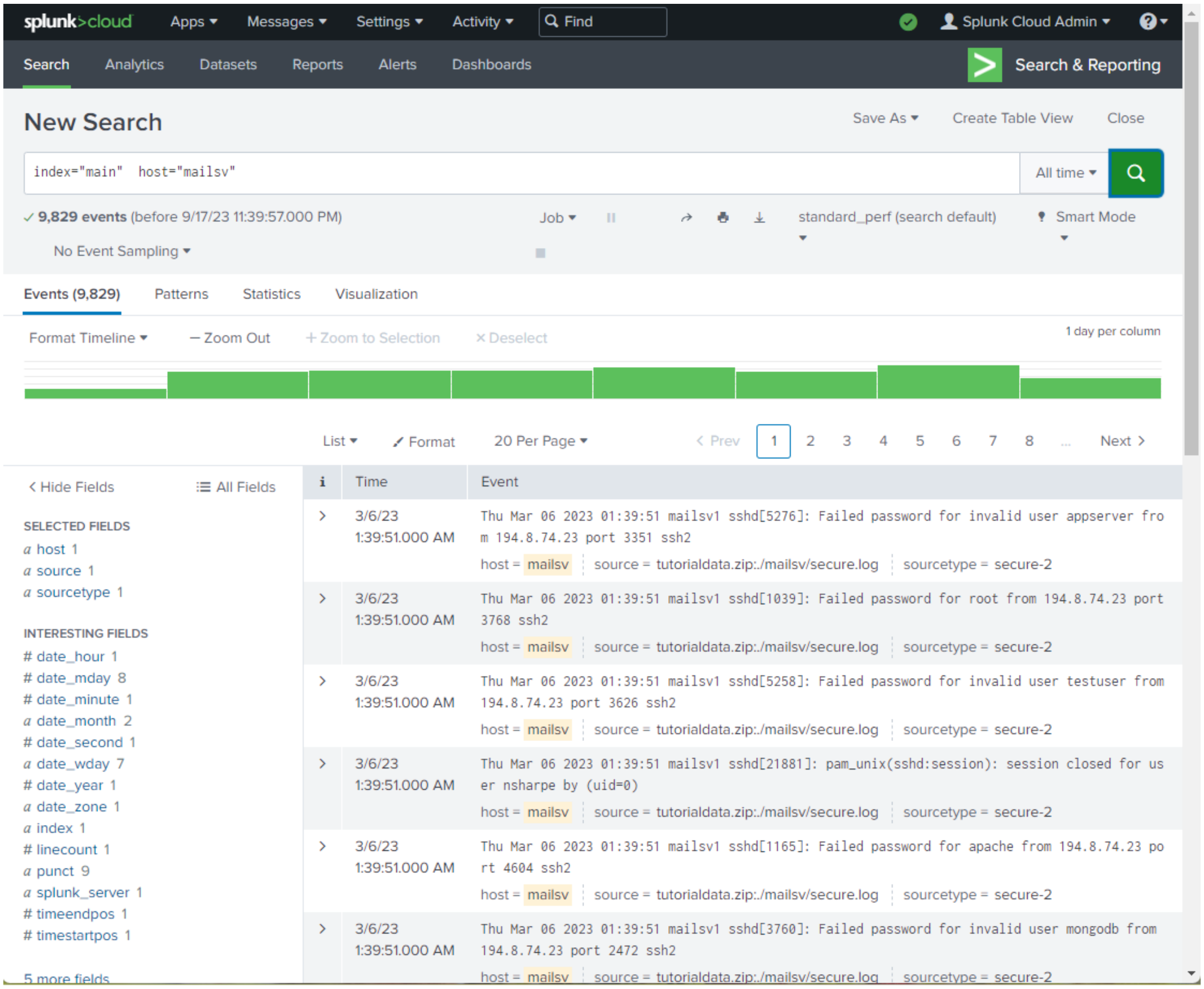
- **host**: The host field specifies the name of the network host from which the event originated. In this search there are five hosts:
  - `mailsv` - Buttercup Games' mail server. Examine events generated from this host.
  - `www1` - This is one of Buttercup Games' web applications.
  - `www2` - This is one of Buttercup Games' web applications.
  - `www3` - This is one of Buttercup Games' web applications.
  - `vendor_sales` - Information about Buttercup Games' retail sales.
- **source**: The source field indicates the file name from which the event originates. You should identify eight sources. Notice `/mailsv/secure.log`, which is a log

file that contains information related to authentication and authorization attempts on the mail server.

- **sourcetype**: The sourcetype determines how data is formatted. You should observe three sourcetypes. Examine `secure-2`.

Step 7: Narrow your search

Because you've been tasked with exploring any failed SSH logins for the root account on the mail server, you'll need to narrow the search results for events from the mail server.



splunk>cloud
Apps ▾ Messages ▾ Settings ▾ Activity ▾ Find
Splunk Cloud Admin ▾
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As ▾ Create Table View Close
All time ▾
Job ▾
standard_perf (search default)
Smart Mode
No Event Sampling ▾
Events (9,829) Patterns Statistics Visualization
Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect
1 day per column
List ▾ Format 20 Per Page ▾
< Prev 1 2 3 4 5 6 7 8 ... Next >
< Hide Fields
All Fields

```
index="main"  host="mailsv"
```

✓ 9,829 events (before 9/17/23 11:39:57.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 1
- # date_mday 8
- # date_minute 1
- a date_month 2
- # date_second 1
- a date_wday 7
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 9
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1

5 more fields

i	Time	Event

>	3/6/23
	1:39:51.000 AM
		`Thu Mar 06 2023 01:39:51 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2`
		host = mailsv ⋮ source = tutorialdata.zip:./mailsv/secure.log ⋮ sourcetype = secure-2

>	3/6/23
	1:39:51.000 AM
		`Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2`
		host = mailsv ⋮ source = tutorialdata.zip:./mailsv/secure.log ⋮ sourcetype = secure-2

>	3/6/23
	1:39:51.000 AM
		`Thu Mar 06 2023 01:39:51 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2`
		host = mailsv ⋮ source = tutorialdata.zip:./mailsv/secure.log ⋮ sourcetype = secure-2

>	3/6/23
	1:39:51.000 AM
		`Thu Mar 06 2023 01:39:51 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharpe by (uid=0)`
		host = mailsv ⋮ source = tutorialdata.zip:./mailsv/secure.log ⋮ sourcetype = secure-2

>	3/6/23
	1:39:51.000 AM
		`Thu Mar 06 2023 01:39:51 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2`
		host = mailsv ⋮ source = tutorialdata.zip:./mailsv/secure.log ⋮ sourcetype = secure-2

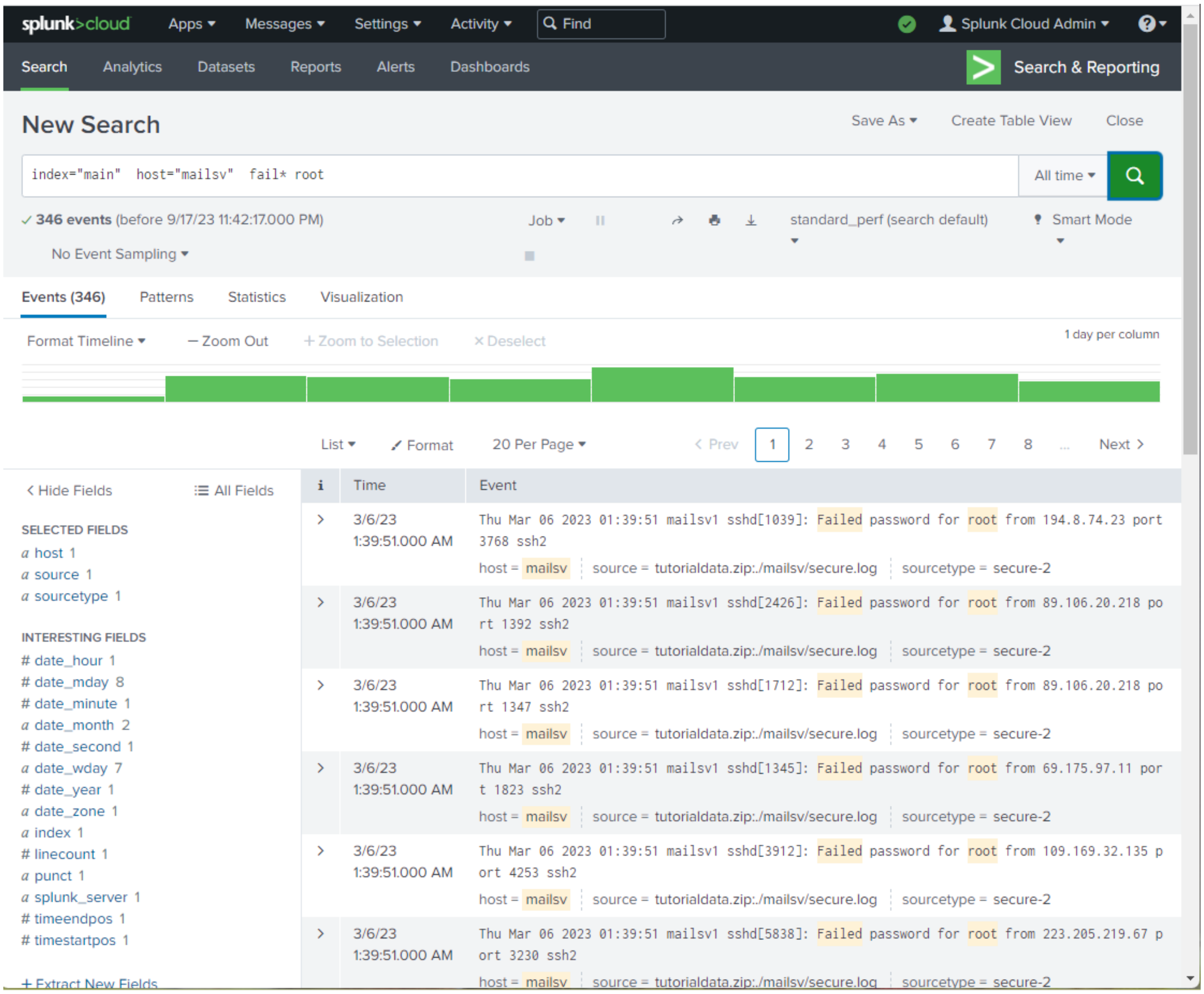
>	3/6/23
	1:39:51.000 AM
		`Thu Mar 06 2023 01:39:51 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2`
		host = mailsv ⋮ source = tutorialdata.zip:./mailsv/secure.log ⋮ sourcetype = secure-2

Under **SELECTED FIELDS**, click **host** and click **mailsv**.

Notice that a new term has been added to the search bar: **`index=main host=mailsv`**. The search results have narrowed to over 9000 events that are generated by the mail server.

Step 8: Search for a failed login for root

Now that you've narrowed your search results to events generated by the mail server, continue to narrow the search to locate any failed SSH logins for the root account.



New Search

```
index="main"  host="mailsv"  fail* root
```

✓ 346 events (before 9/17/23 11:42:17.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 8
# date_minute 1
a date_month 2
# date_second 1
a date_wday 7
# date_year 1
a date_zone 1
a index 1
# linecount 1
a punct 1
a splunk_server 1
# timeendpos 1
# timestartpos 1

i	Time	Event

>	3/6/23 1:39:51.000 AM	`Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2`
		host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

>	3/6/23 1:39:51.000 AM	`Thu Mar 06 2023 01:39:51 mailsv1 sshd[2426]: Failed password for root from 89.106.20.218 port 1392 ssh2`
		host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

>	3/6/23 1:39:51.000 AM	`Thu Mar 06 2023 01:39:51 mailsv1 sshd[1712]: Failed password for root from 89.106.20.218 port 1347 ssh2`
		host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

>	3/6/23 1:39:51.000 AM	`Thu Mar 06 2023 01:39:51 mailsv1 sshd[1345]: Failed password for root from 69.175.97.11 port 1823 ssh2`
		host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

>	3/6/23 1:39:51.000 AM	`Thu Mar 06 2023 01:39:51 mailsv1 sshd[3912]: Failed password for root from 109.169.32.135 port 4253 ssh2`
		host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

>	3/6/23 1:39:51.000 AM	`Thu Mar 06 2023 01:39:51 mailsv1 sshd[5838]: Failed password for root from 223.205.219.67 port 3230 ssh2`
		host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

1. Clear the search bar.
2. Enter **`index=main host=mailsv fail* root`** into the search bar. This search

expands on the search from the previous task and searches for the keyword `fail*`. The wildcard tells Splunk to expand the search term to find other terms that contain the word *fail* such as *failure*, *failed*, etc. Lastly, the keyword `root` searches for any event that contains the term root.

3. Click **search**.

Step 9: Evaluate the Search results

Your search from the previous task should have retrieved search results for over 300 events. Navigate to other pages of the search results to observe the events not listed on the first page of results.

Pro tip: *Splunk highlights search terms in search results to make it easier to identify where the search terms appear in the data.*

Step 10: Answer questions about the search results

1. How many events are contained in the main index across all time?

   a. 10-99
   b. 10,000
   c. Over 100,000
   d. 100 -1,000

2. Which field identifies the name of a network device or system from which an event originates?

   a. `index`
   b. `host`
   c. `source`
   d. `sourcetype`

3. Which of the following hosts used by Buttercup Games contains log information relevant to final transactions?

   a. `www2`

b. `www1`
c. `www3`
d. `vendor_sales`

4. How many failed SSH logins are there for root account on the mail server?

    a. More than 100
    b. None
    c. One
    d. 100

Key takeaways

In this activity, you used Splunk Cloud to perform a search and investigation. Using Splunk Cloud, you were able to:

- Upload sample log data
- Search through indexed data
- Evaluate search results
- Identify different data sources
- Locate failed SSH login(s) for the root account

If you would like to challenge yourself and explore more simulated incident investigations using Splunk, log in to Splunk and visit Splunk Boss of the SOC.