

Scenario

Review the following scenario. Then complete the step-by-step instructions.

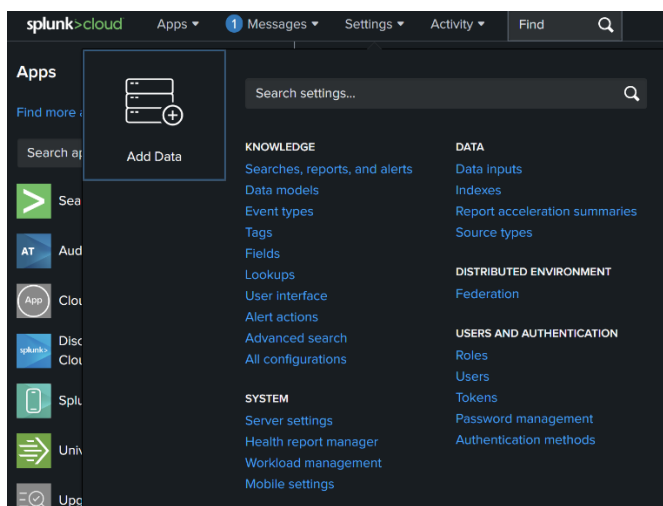
You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

Step 1: 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:

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.
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**.
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.
9. Click the **Review** button and review the details of the upload before you submit.
The details should be as follows: Input Type: Uploaded File File Name: tutorialdata.zip Source Type: Automatic Host: Source path segment number: 1 Index: Default

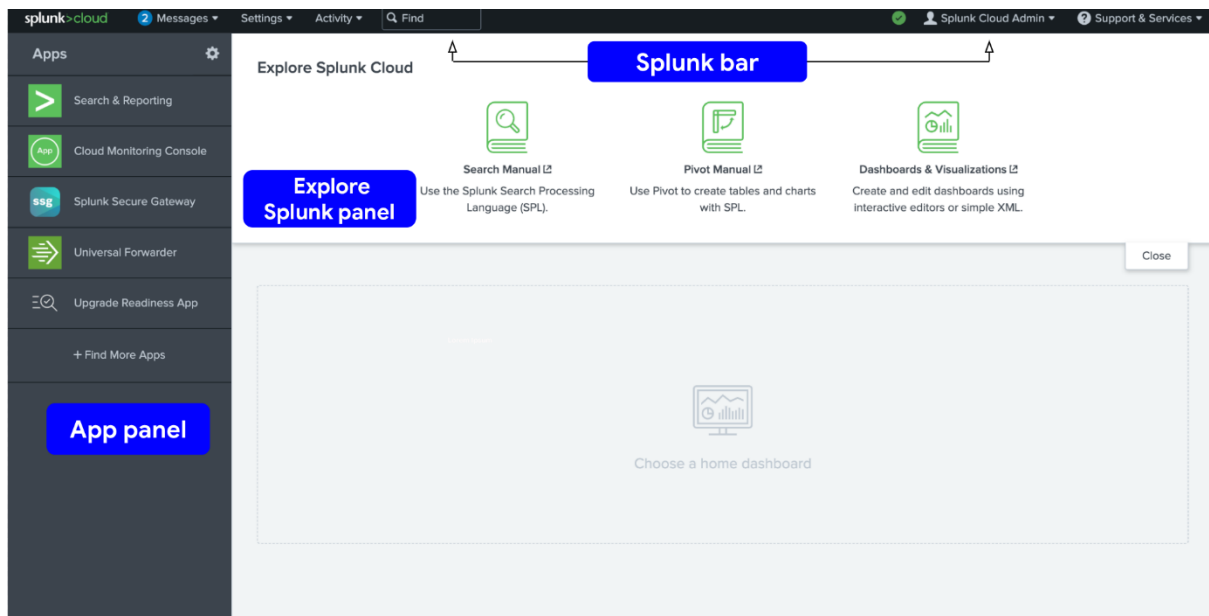
The screenshot shows the 'Add Data' workflow in Splunk Cloud. The top navigation bar includes 'splunk>cloud', 'Apps', '1 Messages', 'Settings', 'Activity', and a 'Find' search bar. Below the navigation bar is a progress indicator with four steps: 'Select Source', 'Input Settings', 'Review', and 'Done'. The 'Review' step is currently active, indicated by a green dot and a green line connecting the first three steps. To the right of the progress indicator are two buttons: '< Back' and 'Submit >'. The main content area is titled 'Review' and displays the following details:

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.

Step 2: 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.



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.
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.

splunk>cloud

AppsMessagesSettingsActivityFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

Index="main"Time range: All time

109,864 events (before 4/17/25 7:27:23.000 AM)No Event SamplingJobPauseRefreshDownloadPolicy-Based PoolSmart Mode

Events (109,864)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect1 hour per column

FormatShow: 20 Per PageView: List

< Hide Fields

All 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

https://prd-p-no64w.splunkcloud.com/en-US

TimeEvent

> 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

splunk>cloud

AppsMessagesSettingsActivityFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

Search

enter search here...Last 24 hours

No Event Samplingstandard_perf (search default)Smart Mode

> Search History

How to Search

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.

DocumentationTutorial

Analyze Your Data with Table Views

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!

Create Table View

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

Step 3: 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.

The screenshot shows the Splunk Search interface. At the top, there's a navigation bar with 'splunk>cloud' and various menu items. Below that, a 'New Search' section shows a search query 'index=*' and '109,864 events (before 12/7/22 8:24:04.000 PM)'. The main results area displays a table of search results. On the left, under 'SELECTED FIELDS', there are three fields listed: 'host', 'source', and 'sourcetype'. The first event in the table shows the following values: 'host = www1', 'source = tutorialdata (1).zip:/www1/access.log', and 'sourcetype = access_combined_wcookie'. These values are highlighted with red boxes in the original image.

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 4: 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.

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.

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query `index=main host=mailsv`. Below the search bar, it indicates **9,829 events** (before 4/17/25 8:13:57.000 AM). The interface includes a timeline visualization and a table of search results.

Time	Event
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv 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 mailsv 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 mailsv 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 mailsv sshd[21881]: pam_unix(sshd:session): session closed for user nsharp (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 mailsv 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 mailsv 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
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2

Step 5: 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.

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**.

The screenshot shows the Splunk Search interface. The search bar contains the query `index=main host=mailsv fail* root`. Below the search bar, it indicates 346 events were found. The results are displayed in a table view with columns for Time and Event. The events show failed password attempts for the root user from various IP addresses on the mailsv host.

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
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
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
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
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
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
3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1151]: Failed password for root from 175.44.1.122 port 1202 ssh2

Step 6: 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.

- **Over 100,000** events are contained in main index across all time
- **Host** field identifies the name of a network device/system from which event originates
- **Vendor_sales** contains log information relevant to financial transactions
- **346 Failed SSH logins** are found in the root account on mail server