

## Scenario

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.

## Steps

### **Step 1) Splunk cloud trial and account setup**

Use this reading for step-by-step instructions on how to create a Splunk Cloud account, activate a Splunk Cloud free trial, and upload data to a Splunk Cloud instance.

The following guide identifies parts of the video that may require adjustment. This reference guide can also serve as a usability reminder when using Splunk Cloud in the future.

## **Instructions**

### **Part 1 - Create a Splunk Cloud account**

1. Go to the [Splunk Cloud Platform Trial](#) page.
2. Fill in the fields in the **Start Your Cloud Platform Trial** sign-up form.
3. Click **Create Your Account**.

The screenshot shows the Splunk Cloud Platform Trial landing page. At the top, there's a navigation bar with links for Products, Solutions, Why Splunk?, and Resources. Below the navigation, a large heading says "TURN DATA INTO DOING" and "Splunk Cloud Platform Trial". A sub-headline reads "Try Splunk Cloud free for 14 days. No credit card required." To the right, there's a large, colorful graphic with red, orange, and yellow gradients. On the left, there are four icons with corresponding text: a cloud icon for "Keep it simple with SaaS — no installation required to start getting data in.", a laptop icon for "Ingest up to 5GB/day of your own data in a Splunk-hosted cloud environment.", a monitor icon for "Start searching, analyzing and visualizing your data on powerful, easy-to-understand dashboards.", and a lock icon for "Keep your data safe in a highly secure environment that is SOC 2 Type I Attestation, ISO 27001 certification, HIPAA and PCI DSS compliant." Below these, a section titled "Once you sign up for the Splunk Cloud Platform trial, you'll see how it helps you to:" lists five bullet points: "Tackle your hardest security and observability use cases.", "Stream, collect and index any data at any scale.", "Set up real-time alerts so you can act fast.", "Customize for your unique business needs with free, pre-built apps from Splunkbase.", and "Integrate with your existing systems and tools." At the bottom left, a link says "Prefer to install Splunk on your own hardware? Try out Splunk Enterprise for free, or explore the rest of our free trials and downloads." On the right side, a modal window titled "Start Your Cloud Platform Trial" is open. It contains fields for "Business Email" (marked as required), "Password", "First Name", "Last Name", "Job Title", "Phone Number", "Company", a dropdown for "Country" set to "United States", and a field for "Zip / Postal Code". There's also a checkbox for "I agree to the Splunk Website Terms & Conditions of Use, Splunk Privacy Policy and Splunk General Terms." At the bottom of the modal is a "Create Your Account" button.

PCI Attestation, ISO 27001 Certification, HIPAA and PCI DSS compliant.

**sign up for the Splunk Cloud Platform trial, you'll help you to:**

our hardest security and observability use cases.

collect and index any data at any scale.

real-time alerts so you can act fast.

ze for your unique business needs with free, pre-built apps from Splunkbase.

**Install Splunk on your own hardware?** Try out Splunk [Cloud Trial](#) or [free](#), or explore the rest of our [free trials and downloads](#).

Job Title	GOOD
Analyst	

Phone Number	GOOD
[REDACTED]	

Company	GOOD
NA	

United States	▼
---------------	---

Zip / Postal Code	GOOD
96707	

I agree to the [Splunk Website Terms & Conditions of Use](#), [Splunk Privacy Policy](#) and [Splunk General Terms](#).

**Create Your Account**

GET STARTED

## Splunk Cloud Trial

Search, analyze, and visualize 5 GB/day of your own data in a Splunk hosted cloud environment for fast insights. Didn't want a cloud trial? Review our [Free Trials and Downloads page](#) for other options.

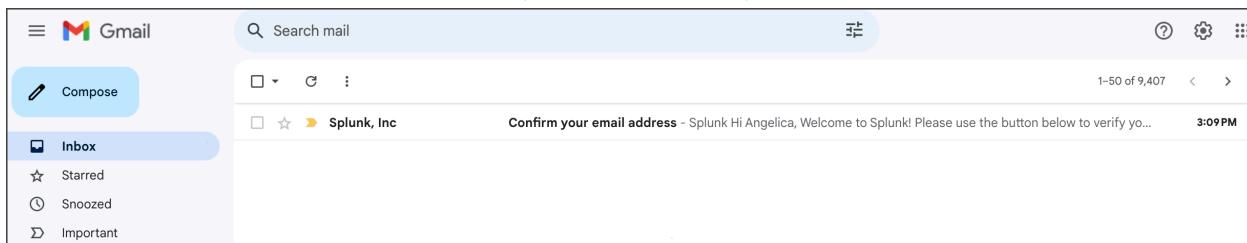
**Thank you for registering, your free trial is on its way!**

You will receive an email within 15 minutes. Check your spam folder if it doesn't arrive.

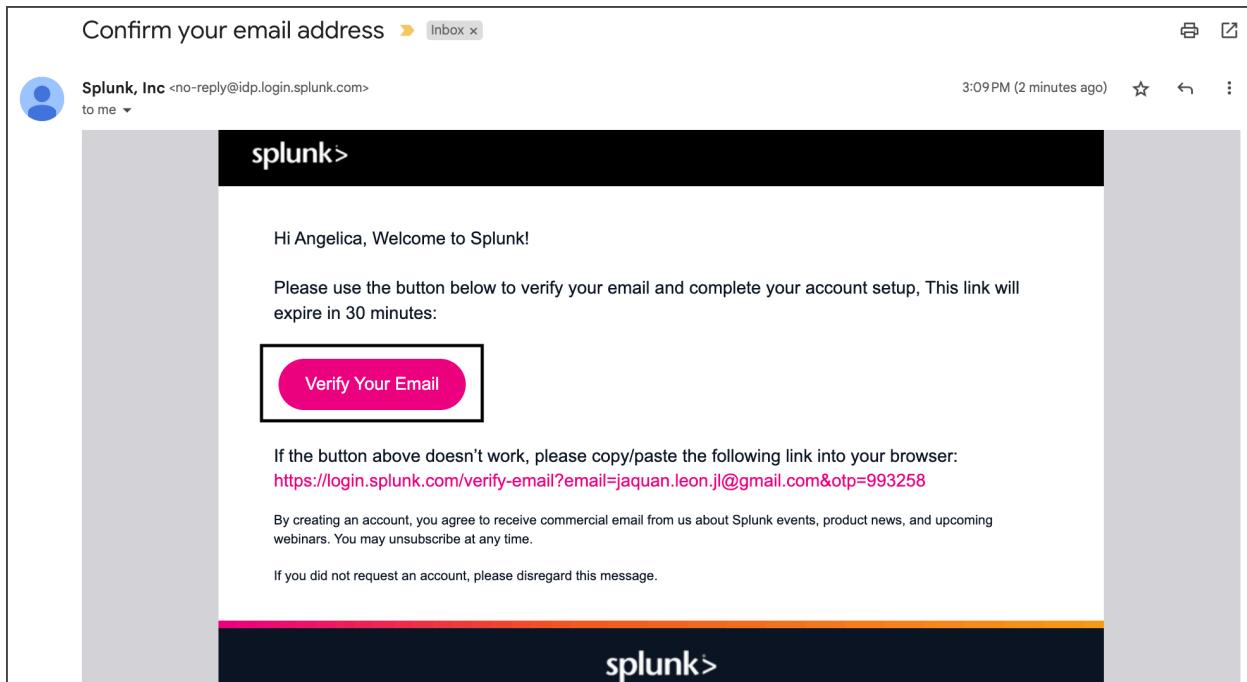
If you still need help, please reach out to Splunk support.

## Part 2 - Verify your email

1. Check the inbox for the email address that you used to sign up for the Splunk account. Find the verification email from Splunk with the subject line **Confirm your email address**.



2. Open the email and click the **Verify Your Email** button.



**Note:** Check your spam folder if you didn't receive the verification email.

## Part 3 - Activate a Splunk Cloud trial

After clicking the **Verify Your Email** button, you'll be redirected to the Splunk Cloud Trial page.

**Note:** You can activate one Splunk Cloud trial instance at a time, and you can use a maximum of three trials per Splunk account. The Splunk Cloud free trial expires after 14 days, so you may want to complete this activity before the free trial expires.

**Note:** Alternatively, you can also access the Splunk Cloud Trial page by visiting [Splunk Cloud Platform Trial](#) and logging into your account, then clicking **Start Trial**.

1. Click the **Start Trial** button.

GET STARTED

## Splunk Cloud Trial

Search, analyze, and visualize 5 GB/day of your own data in a Splunk hosted cloud environment for fast insights. Didn't want a cloud trial? Review our [Free Trials and Downloads page](#) for other options.

[Start Trial](#)

GET STARTED

## Splunk Cloud Trial

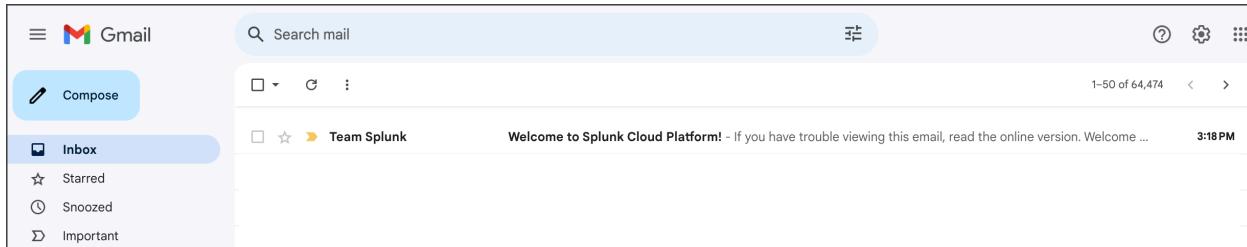
Search, analyze, and visualize 5 GB/day of your own data in a Splunk hosted cloud environment for fast insights. Didn't want a cloud trial? Review our [Free Trials and Downloads page](#) for other options.

**Thank you for registering, your free trial is on its way!**

You will receive an email within 15 minutes. Check your spam folder if it doesn't arrive.

If you still need help, please reach out to Splunk support.

2. Check your inbox for an email from Team Splunk with the subject line **Welcome to Splunk Cloud Platform!**



3. Open the email to access your Splunk Cloud login information.
4. Click the link beside **URL** to access the Splunk Cloud Platform.

Welcome to Splunk Cloud Platform!   

 Team Splunk <teamsplunk@splunk.com>  
to me

If you have trouble viewing this email, [read the online version](#).

**splunk>cloud**

## Welcome to Splunk Cloud Platform!

Thanks for signing up for Splunk Cloud Platform! Here is your login information:

<b>Splunk Cloud Platform</b>	<a href="https://prd-p-nyzxg.splunkcloud.com">https://prd-p-nyzxg.splunkcloud.com</a>
<b>URL:</b>	
<b>User Name:</b>	sc_admin
<b>Temporary Password:</b>	4wy5kus20d0t8p26

\* You'll be asked to create a permanent password on first login.

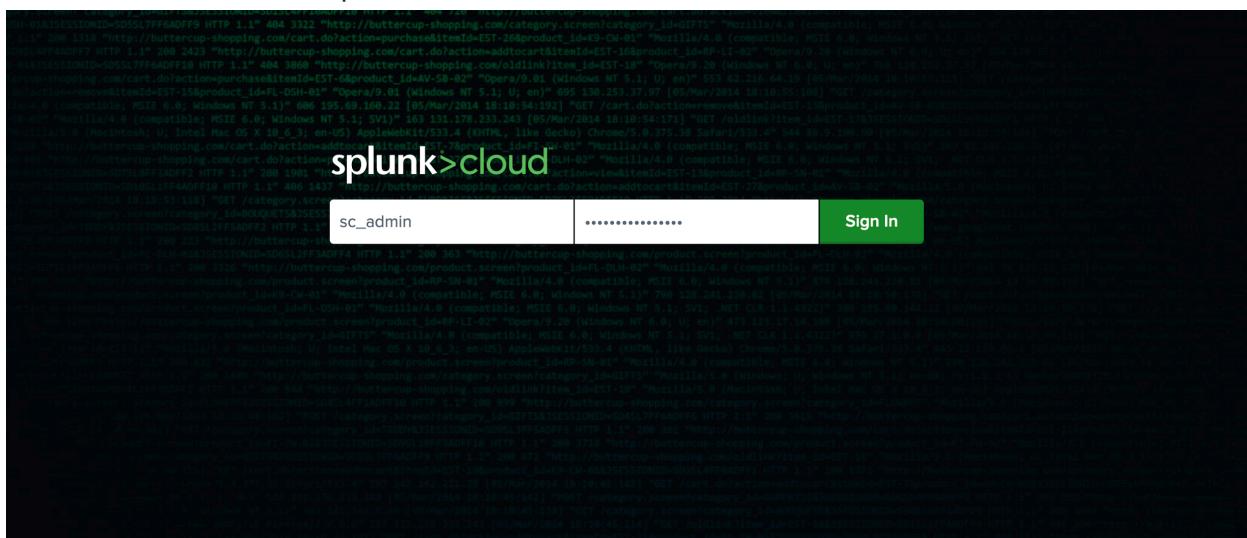
**Let the adventure begin**

All data journeys start at the same place: getting data in. But we've got some you can start with, if that helps.

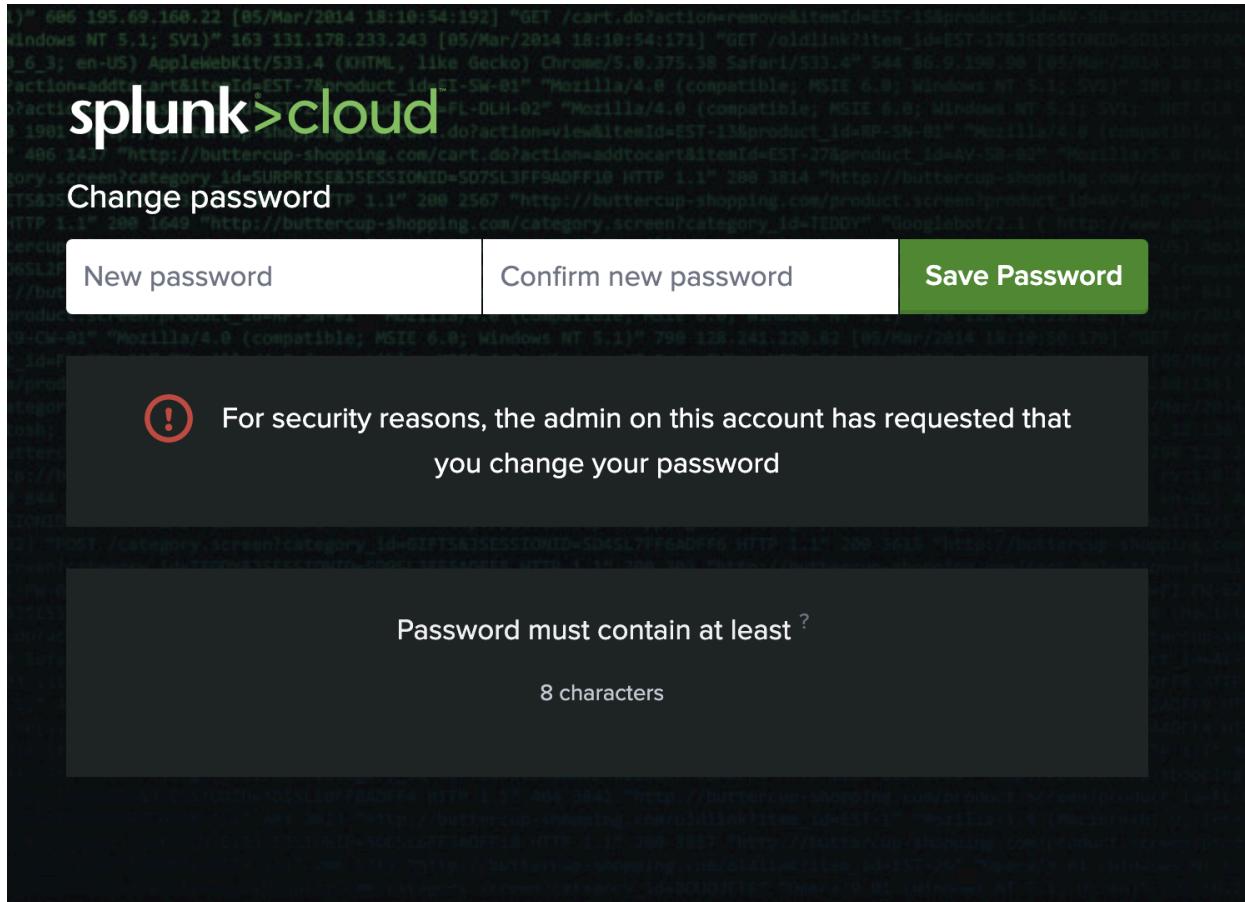
[Get Started](#)



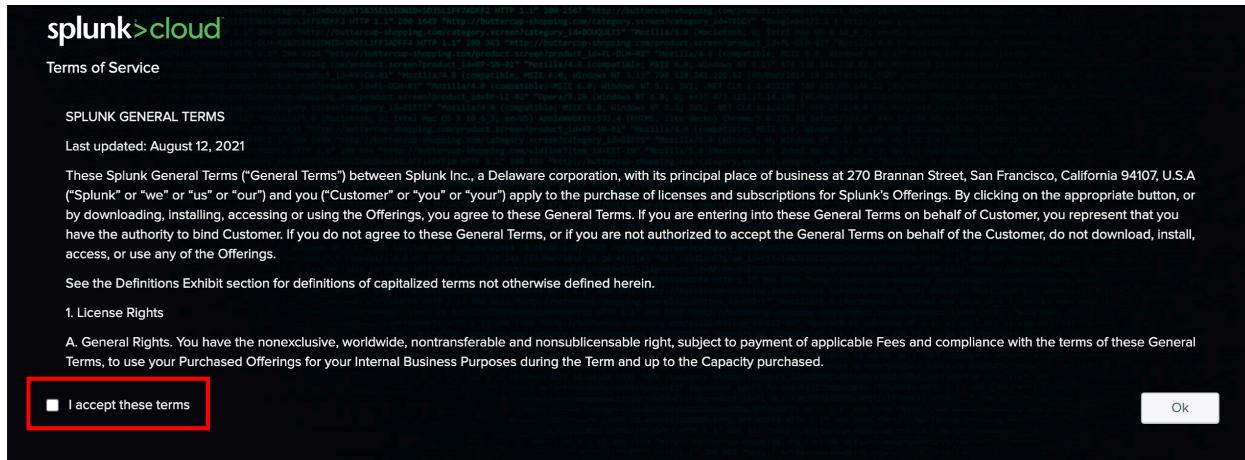
5. Enter the username and password credentials that were included in the email.



6. You will be prompted to change the password of the Splunk Cloud Platform account. Enter a new password and click **Save Password**.



7. Check the box next to **I accept these terms** and click **Ok**.



## Part 4 - Download and upload Splunk data

After you've accepted the Terms of Service, you'll automatically be redirected to the Splunk Home dashboard.

1. Go to [Activity: Perform a query with Splunk](#).
2. Go to **Step 1: Access supporting materials**.

✓ 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.



To download this data, click the link then click the download icon.

Link to supporting materials: [tutorialdata.zip](#)

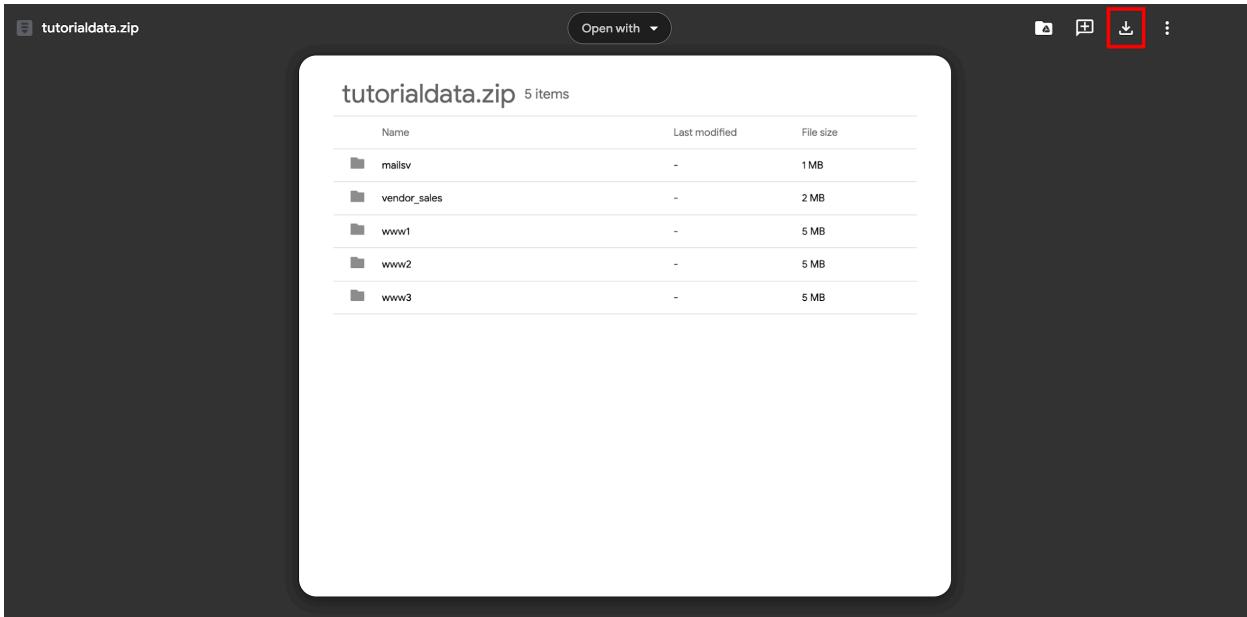
OR

If you don't have a Google account, you can download the supporting materials directly from the following attachment.

**tutorialdata**  
ZIP File

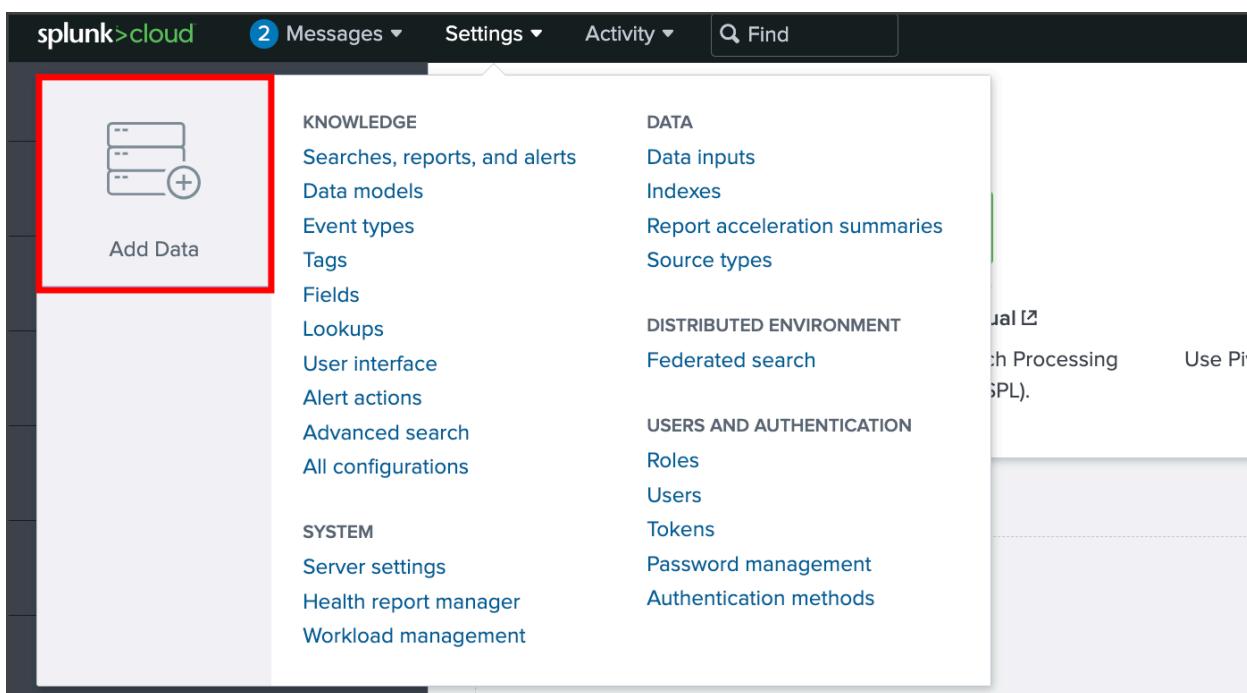
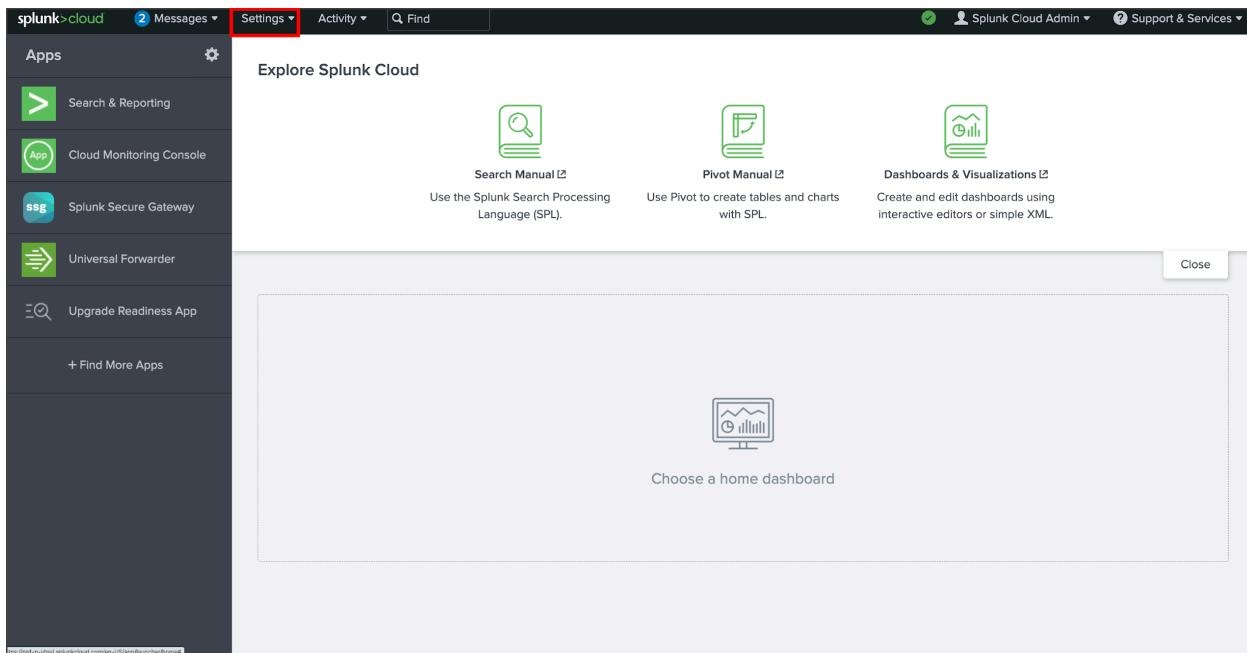
3. Beside **Link to supporting materials** click [tutorialdata.zip](#).

4. Click the **download icon** to download the zip file.



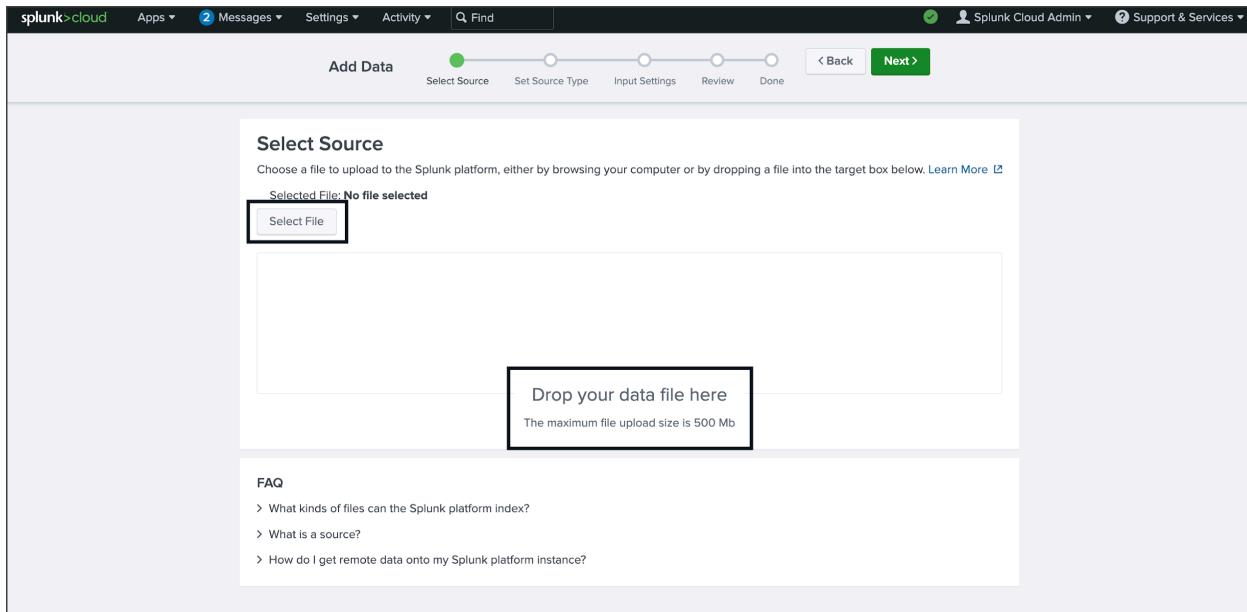
5. Go to the Splunk Home dashboard.

6. On the Splunk bar, click **Settings** and then click **Add Data**.

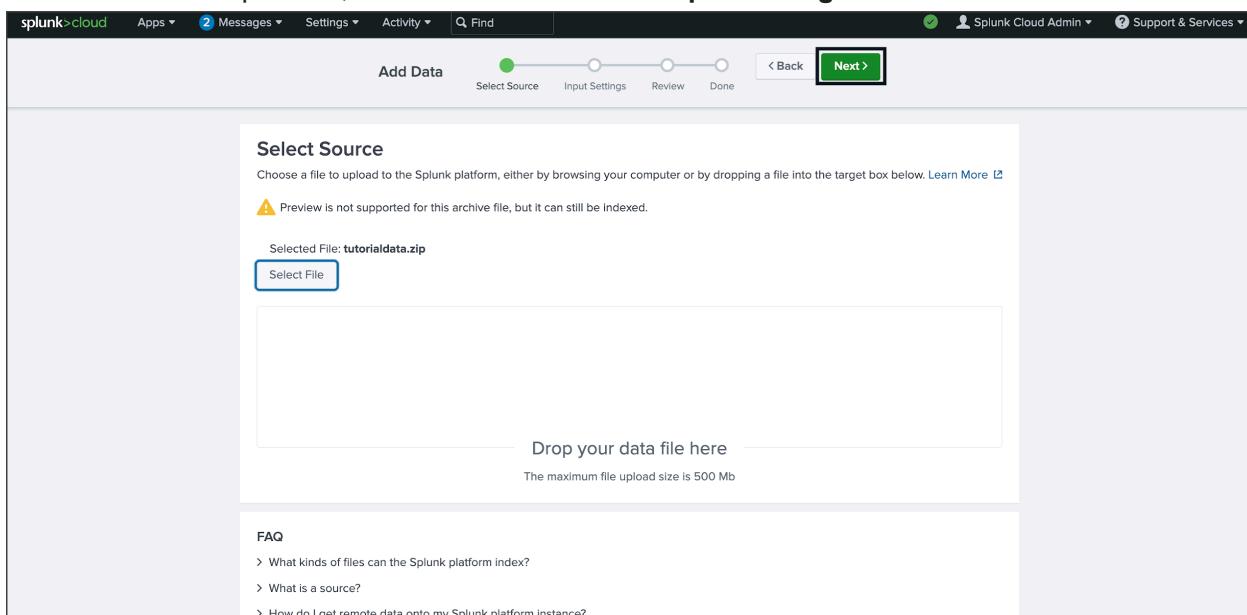


7. Click **Upload**.

8. Click **Select File** to upload the **tutorialdata.zip** file. Alternatively, you can also drag and drop your file in the **Drop your data file here** box.



9. Once the file is uploaded, click **Next** to continue to **Input Settings**.



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

**Input Settings**  
Optional 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.

**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:

**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

Index:

11. Click **Review** and check the details of the upload before you submit. The details should be as follows:

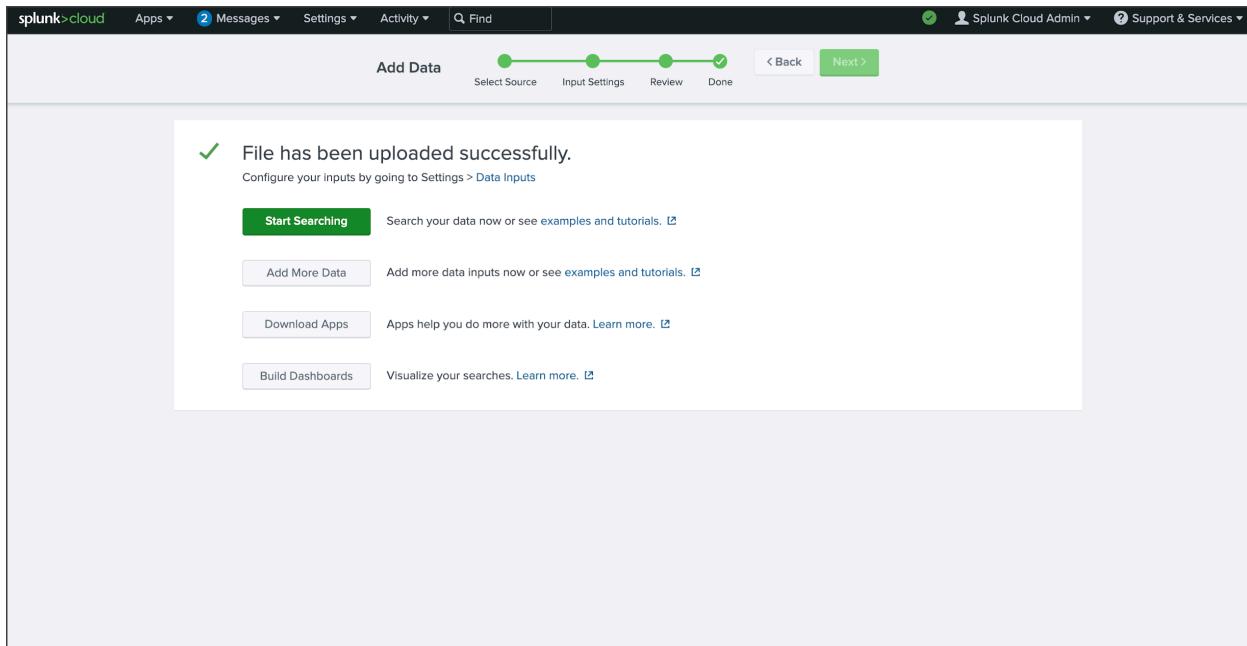
- Input Type: Uploaded File
- File Name: tutorialdata.zip
- Source Type: Automatic
- Host: Source path segment number: 1
- Index: Default

12. After you've verified that the details are correct, click **Submit**.

**Review**

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

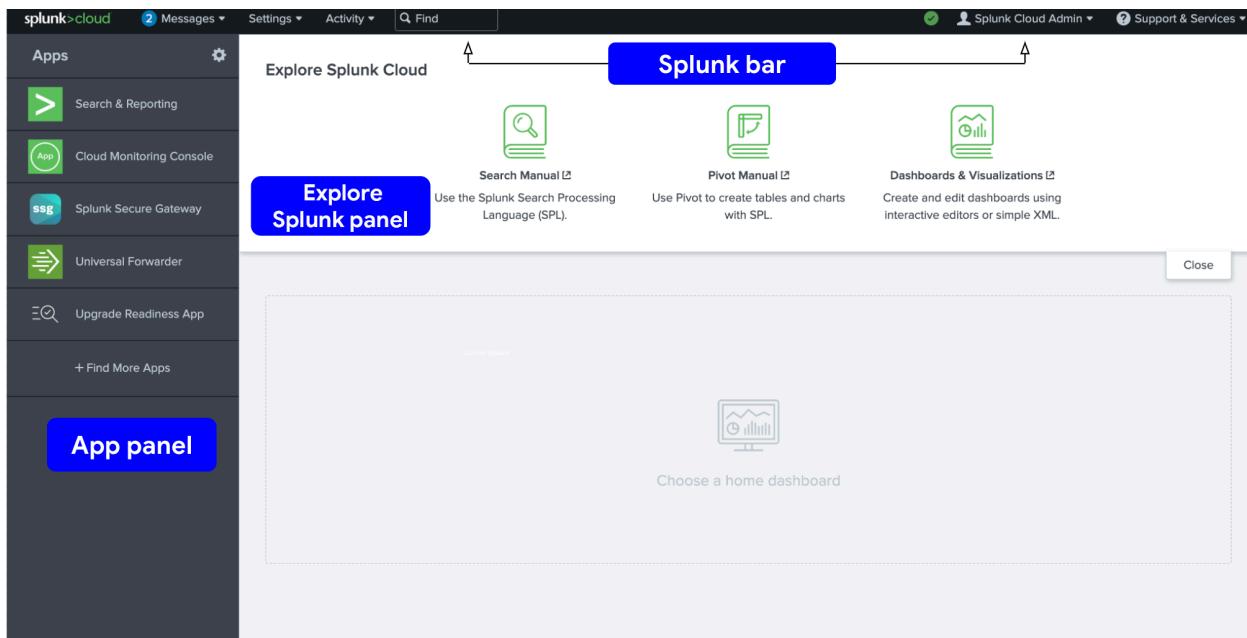
13. Once Splunk has ingested the data, you will receive a confirmation message stating that the file has been uploaded successfully.



14. Click the **Splunk Cloud** logo to return to the home page.

## 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.

In the search bar, enter your search query:

`index=main`

3. 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.

The screenshot shows the Splunk Cloud interface. At the top, there's a navigation bar with links for 'splunk>cloud', 'Apps', 'Messages' (with 2 notifications), 'Settings', 'Activity', and a search bar. On the right of the nav bar are icons for user profile, 'Splunk Cloud Admin', and help. Below the nav bar is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. To the right of this is a 'Search & Reporting' button with a magnifying glass icon. The main content area is titled 'Search' and contains a search bar with placeholder 'enter search here...', a time range dropdown set to 'Last 24 hours', and a green search button. Below the search bar are buttons for 'No Event Sampling', 'standard\_perf (search default)', and 'Smart Mode'. A 'Search History' link is also present. To the left, a 'How to Search' section provides links to 'Documentation' and 'Tutorial'. To the right, a 'Analyze Your Data with Table Views' section includes a 'Create Table View' button and a link to learn more about Table Views.

*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 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.

Time	Event
9/8/22 6:13:34.000 PM	91.205.189.15 - - [08/Sep/2022:18:13:34] "POST /cart/success.do?JSESSIONID=SD10SL4FF1ADFF53066 HTTP/1.1" 200 3129 "h 19.0.1084.46 Safari/536.5" 591 host = www1   source = tutorialdata (1).zip.:www1/access.log   sourcetype = access_combined_wcookie
9/8/22 6:13:33.000 PM	91.205.189.15 - - [08/Sep/2022:18:13:33] "GET /cart.do?action=view&itemId=EST-26&productId=DB-SG-G01&JSESSIONID=SD10SL4FF1ADFF53066 HTTP/1.1" 200 286 "h 0.7.4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 286

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.

## 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.

Enter `index=main host=mailsv fail* root` into the search bar.

2. 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 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.

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

## **Step 7) Answer the following**

1. How many events are contained in the main index across all time?
  - a. Over 100,000
2. Which field identifies the name of a network device or system from which an event originates?
  - a. host
3. Which of the following hosts used by Buttercup Games contains log information relevant to financial transactions?
  - a. vendor\_sales
4. How many failed SSH logins are there for the root account on the mail server?
  - a. More than 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