Lab Exercises

Lab typographical conventions:

[`sourcetype=db_audit`] OR [`cs_mime_type`] indicates either a source type or the name of a field.

> **NOTE:** Lab work will be done on your personal computer or virtual machine, no lab environment is provided. We suggest you **DO NOT** do the lab work on your production environment.

Lab Module 4 – Ingesting Data

Description

This lab exercise will get data ingested into Splunk from three source types.

> **NOTE:** We will be ingesting static data sources that cover 30 days. For this demo you will not see real-time data.

Steps

Scenario: You have recently joined the team at Buttercup Games as a Splunk Administrator. You have been asked to ingest data into your Splunk Enterprise instance for searching.

Task 1:   Download log files from the repository.

1. Open a new browser window and direct it to http://splk.it/f1data
2. The file **Splunk_f1_Data.zip** will be downloaded to your system.
3. Use an archive tool to unarchive the file.
4. Once unarchived, you will see a folder labeled **tmp.**

Splunk_f1_Data.zip   tmp

5. Inside the folder you will see three files.

access_30DAY.log   db_audit_30DAY.csv   linux_s_30DAY.log
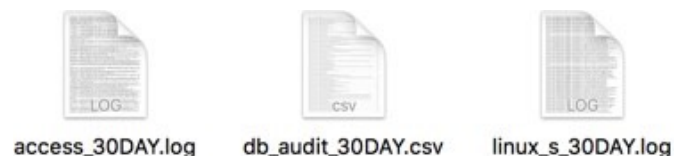
6. Return to the browser window for your instance of Splunk Web or open a new one.

Task 2:   Ingest web application data into Splunk Enterprise.

7. Go to the **Home** app by clicking the Splunk Enterprise logo in the upper left hand of the interface.
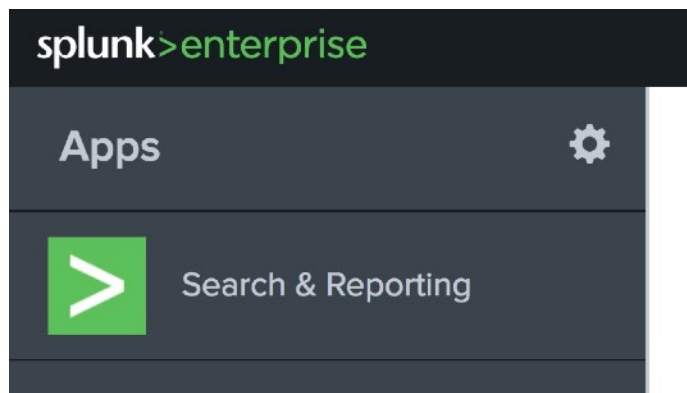
8. Click the **Add Data** icon.

Add Data

Add or forward data to Splunk
Enterprise. Afterwards, you may
extract fields.

NOTE: You must be logged in as admin to see this icon. If you do not see the icon, log out and back in
with your administrator account.

9. From the **Add Data** page, click the **upload** button.

Upload
files from my computer

Local log files
Local structured files (e.g. CSV)
Tutorial for adding data ⤴

10. You will be taken to the **Select Source** step**.** Click the **Select File** button and choose the
access_30Day.log file that you downloaded and unarchived earlier.

11. Once the file is uploaded, click the **Next** button.

12. On the **Set Source Type** step, you will see that Splunk automatically set the source type correctly as **access_combined_wcookie**. Click the **Next** button.

13. From the **Input Settings** step, enter `web_application` as the **Host field value** and click the **Review** button.

14. You will be taken to the **Review** step. Make sure your settings match what is shown below and click the **Submit** button.

Review

```
Input Type ................................ Uploaded File
File Name ................................ access_30DAY.log
Source Type ........................... access_combined_wcookie
Host ......................................... web_application
Index ....................................... Default
```

15. Splunk will process the file.

Uploading File

```
                              80%
```

16. When completed, a dialog will appear telling you the file has been successfully uploaded.

Task 3:   Ingest web server data into Splunk Enterprise.

17. Click the **Add More Data** button.

✓ File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

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. ⬀

18. Click the **upload** icon and the **Select File** button.
19. Select the linux_s_30Day.log file that you downloaded and unarchived earlier and click the **Next** button.
20. Notice that this time Splunk was not able to automatically select a source type for the data.

Source: **linux_s_30DAY.log**

			List ▼
Source type: default ▼		Save As	
> Event Breaks			1
> Timestamp			
> Advanced			2

21. Manually assign the source type by selecting the **Source type** button and selecting **linux_secure** from the **Operating System** menu.

22. Click the **Next** button.
23. For the **Input Settings** step, enter `web_server` as the **Host field value** and click the **Review** button.

Host field value   web_server|

24. On the **Review** step, make sure your settings match what is shown below and click the **Submit** button.

Review

Input Type .... Uploaded File
File Name .... linux_s_30DAY.log
Source Type .... linux_secure
Host .... web_server
Index .... Default

Task 4:   Ingest database server data into Splunk Enterprise.

25. Click the **Add More Data** button.

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

26. Click the **upload** icon and the **Select File** button.
27. Select the db_audit_30DAY.csv file that you downloaded and unarchived earlier and click the **Next** button.
28. Notice that Splunk automatically selected a source type of csv for the data. We want to create a new source type for this data so we click the **Save As** button.

Source type: csv ▾   Save As

29. In the modal window, give the source type a name of db_audit and a description. Using the **Category** menu, select **Database** and click **Save**.

Save Source Type   ✕

Name	db_audit
Description	Postgres Audit Log
Category	Database ▾
App	system ▾

Cancel   **Save**

30. Click the **Next** button to continue to the **Input Settings** step.
31. Enter database as the **Host field value** and click the **Review** button.
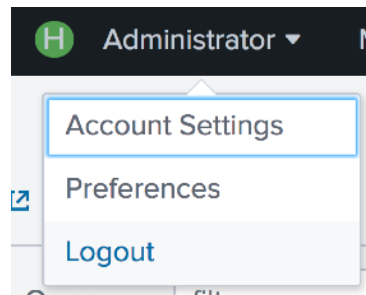
Host field value	database

32. Make sure your settings match what is shown below and click the **Submit** button.

Review

Input Type .... Uploaded File
File Name .... db_audit_30DAY.csv
Source Type .... db_audit
Host .... database
Index .... Default

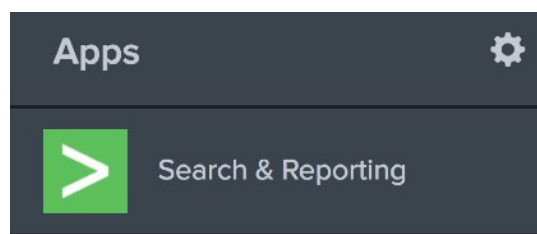**Task 5:   Log in to Splunk Enterprise as a Power User.**

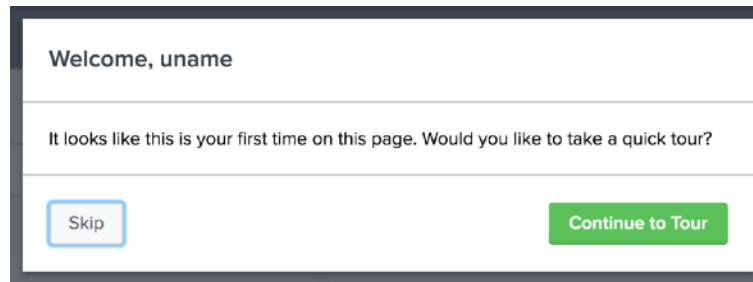33. Log out of your instance using the **Logout** link in the **User** menu.

34. Log back in using the Power User account you created earlier. If you followed the suggested credentials, use `uname` in the **Username** field and `5p1unkbcup` for the **Password** field.
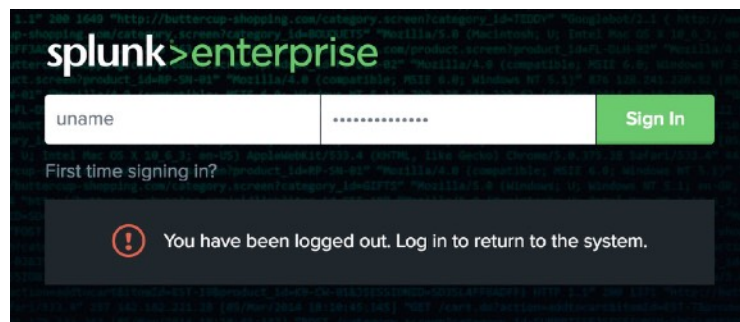
35. Select the **Search & Reporting** app from the sidebar.

36. You will be asked if you would like to take a tour. Click the **Skip** button.

Welcome, uname

It looks like this is your first time on this page. Would you like to take a quick tour?

Skip

Continue to Tour

37. You should now see the number of events indexed in your system.

What to Search

239,625 Events

a month ago

12 hours ago

INDEXED

EARLIEST EVENT

LATEST EVENT

Data Summary