splunk>

Splunk Fundamentals 1 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.

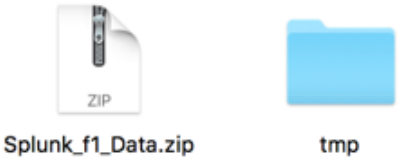
NOTE: We will be ingesting static data sources that cover 30 days. For this demo you will not see real-time data.

Steps

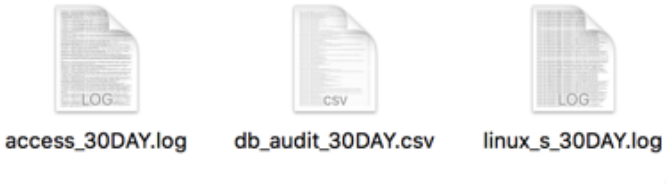
Scenario: You have recently joined the team at Buttercup Games as a Splunk Administrator. You have been asked to ingest data into your Splunk Enterprise instance for searching.

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.**



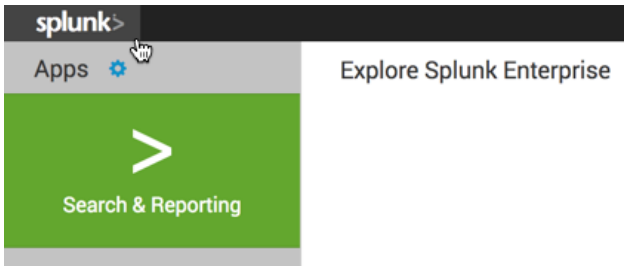
5. Inside the folder you will see three files.



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.

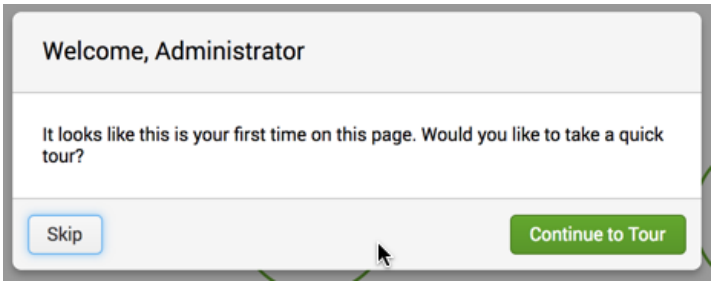
7. Go to the **Home** app by clicking the Splunk logo in the upper left hand of the interface.



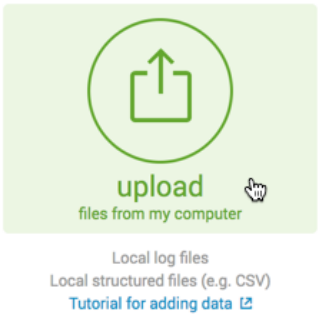
8. Click the **Add Data** icon.

NOTE: You must be logged in a admin to see this icon.

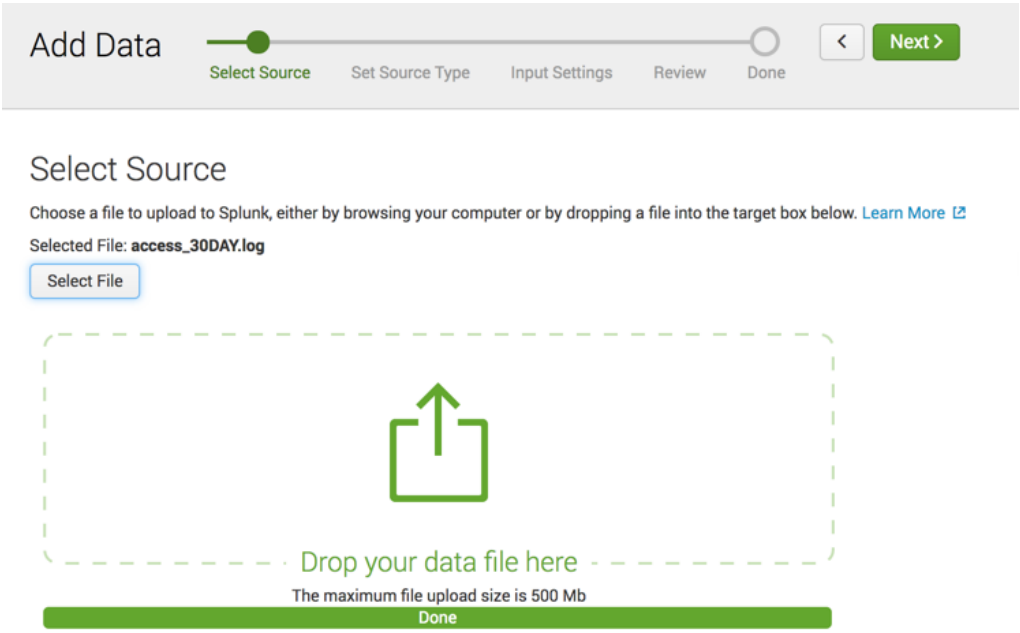
9. A modal window will open asking if you want to take a tour. Press the **skip** button.



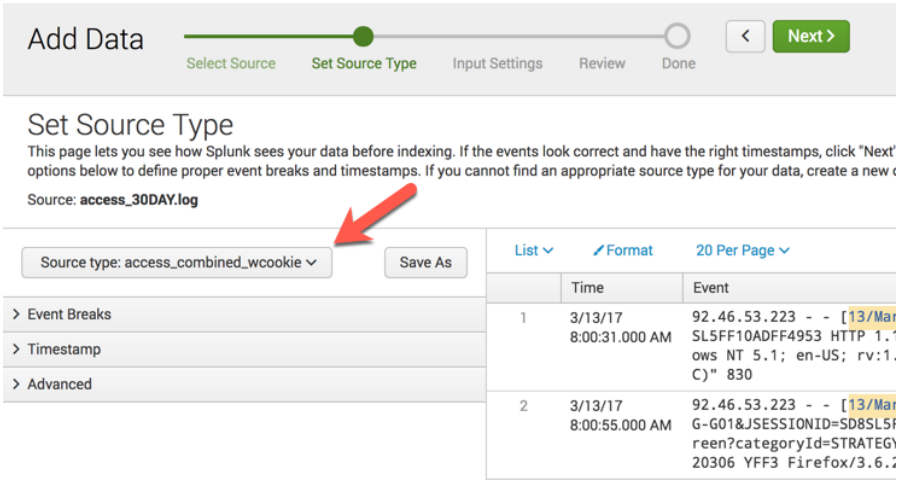
10. From the **Add Data** page, click the **upload** button.



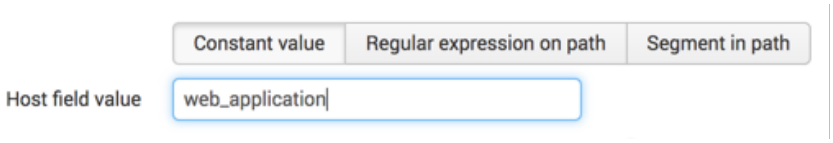
11. You will be taken to the **Select Source** step. Click the **Select File** button and choose the access_30Day.log file that you downloaded and unarchived earlier.



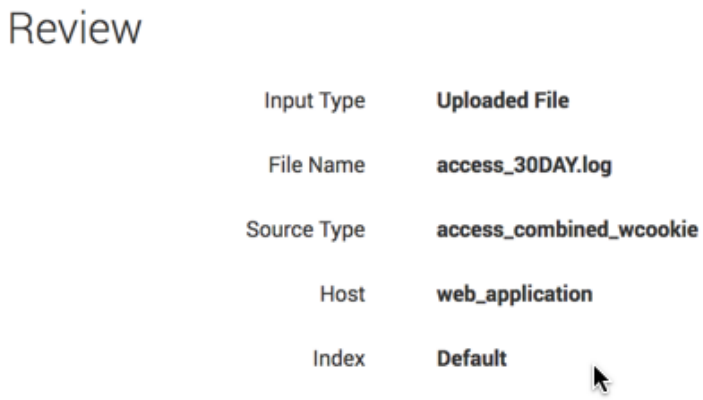
12. Once the file is uploaded, click the **Next** button.
13. On the **Set Source Type** step, you will see that Splunk automatically set the source type correctly as **access_combined_wcookie**. Click the **Next** button.



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



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

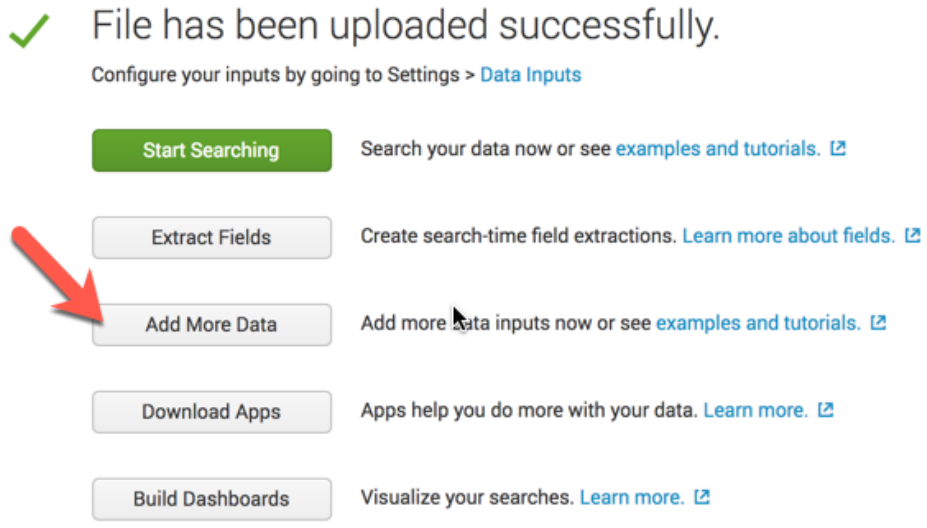


16. Splunk will process the file.

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

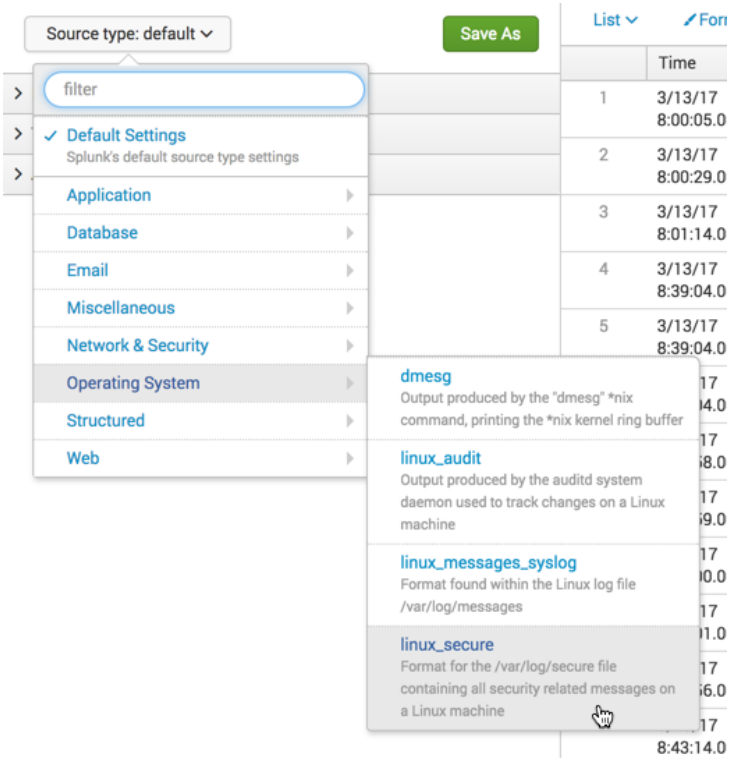
Task 3: Ingest web server data into Splunk Enterprise.

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

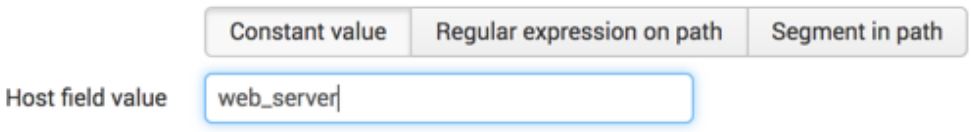


19. Click the **upload** icon and the **Select File** button.
20. Select the linux_s_30Day.log file that you downloaded and unarchived earlier and click the **Next** button.
21. Notice that this time Splunk was not able to automatically select a source type for the data.

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



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



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

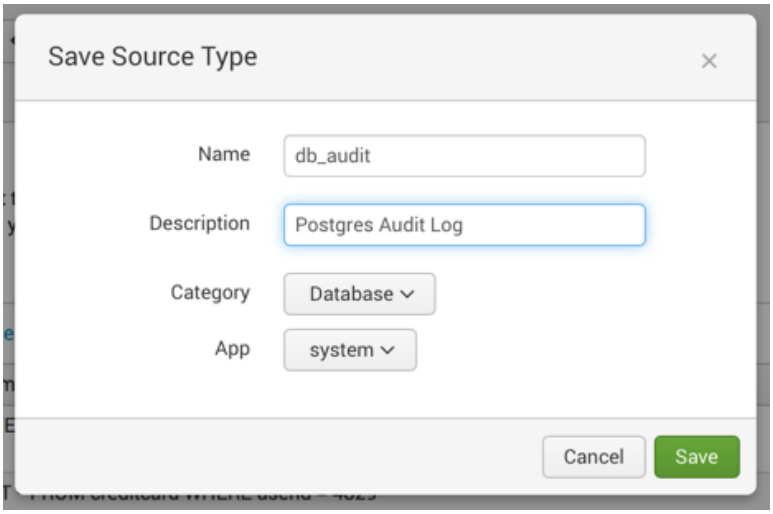
Input Type	**Uploaded File**
File Name	**linux_s_30DAY.log**
Source Type	**linux_secure**
Host	**web_server**
Index	**Default**

Task 4: Ingest database server data into Splunk Enterprise.

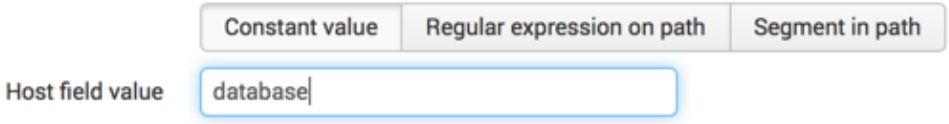
26. Click the **Add More Data** button.

27. Click the **upload** icon and the **Select File** button.
28. Select the db_audit_30DAY.csv file that you downloaded and unarchived earlier and click the **Next** button.
29. 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.

30. 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**.



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

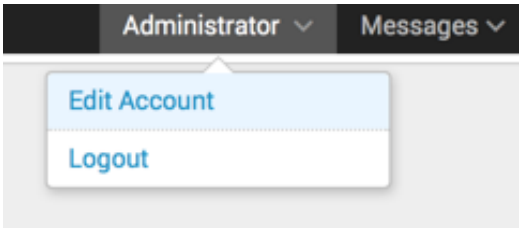


33. Make sure your settings match what is shown below and click the **Submit** button.

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

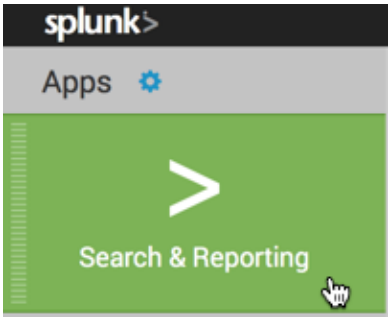
Task 5: Log in to Splunk Enterprise as a Power User.

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

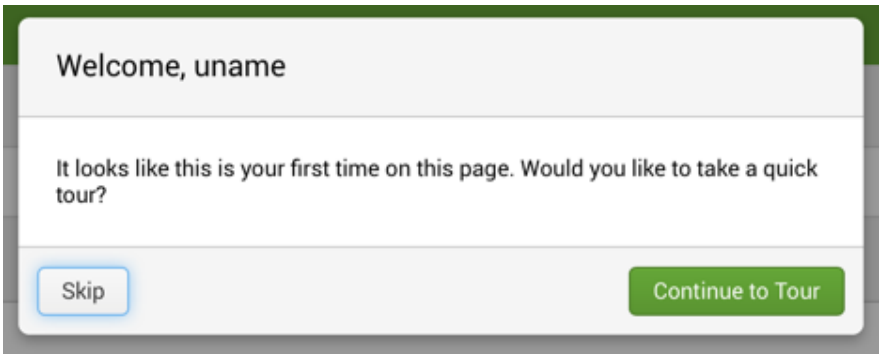


35. Log back in using the Power User account you created earlier. If you followed the suggested credentials, use `uname` in the **Username** field and `5p1unkbcup` for the **Password** field.

36. Select the **Search & Reporting** app from the sidebar.



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



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