
Lab Exercises

Lab typographical conventions:

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

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.

Open a new browser window and direct it to <http://splk.it/fldata>

The file **Splunk_fl_Data.zip** will be downloaded to your system.

Use an archive tool to unarchive the file.

- 1.
2. Once unarchived, you will see a folder labeled **tmp**.
- 3.
- 4.



Inside the folder you will see three files

- 5.

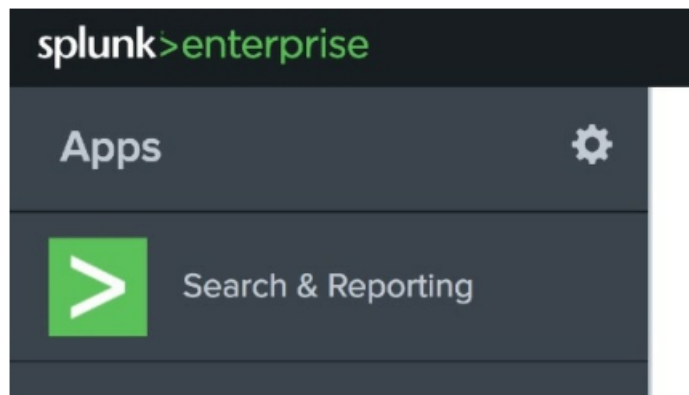


Return to the browser window for your instance of Splunk Web or open a new one

Task 2: Ingest web application data into Splunk Enterprise.

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

- 7.



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.

Select Source

Choose a file to upload to Splunk, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **access_30DAY.log**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

Done

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.

Source type: access_combined_wcookie

Save As

> Event Breaks

> Timestamp

> Advanced

List	Format	20 Per Page
	Time	Event
1	4/21/18 8:00:31.000 AM	92.46.53.223 0ADFF4953 HTTP en-US; rv:1.
2	4/21/18 8:00:55.000 AM	92.46.53.223 SL5FF10ADFF45 "Mozilla/5.0 T CLR 3.5.307
3	4/21/18 8:03:49.000 AM	212.58.253.71 ADFF4953 HTTP 1.9.2.28) Ge

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

Host field value

web_application

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



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**

Source type: default ▼
Save As
List ▼

> 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.

Source type: default ▼
Save As

filter

Default Settings
Splunk's default source type settings

Application
Database
Email
Metrics
Miscellaneous
Network & Security
Operating System
Structured
Uncategorized
Web

linux_messages_syslog

Format found within the Linux log file

/var/log/messages

linux_secure

Format for the /var/log/secure file containing

all security related messages on a Linux

machine

List ▼
Format

Time

14/21/1800:05.000

24/21/1800:29.000

34/21/1801:14.000

44/21/1803:04.000

54/21/1803:04.000

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
