

## Splunk 基本 1 ラボ実習

ラボ表記規則:

[sourcetype=db\_audit] または [cs\_mime\_type] はソースタイプまたはフィールド名を指します。

**備考:** ラボ作業が個人のコンピュータまたはバーチャルマシンで実施された場合、ラボ環境は提供されません。 運用環境でのラボ作業は決して実施しないでください。

## ラボモジュール 4 - データの取り込み

### 説明

このラボ実習は 3 つのソースタイプから Splunk にデータを取り込みます。

**備考:** 30日におよぶ静的データソースを取り込みます。  
このデモではリアルタイムデータは扱いません。

### 手順

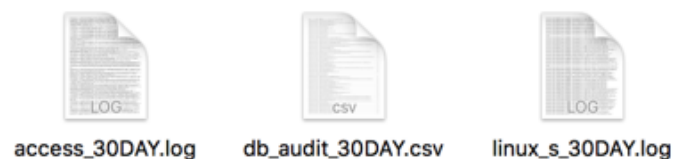
シナリオ: あなたは最近 Buttercup Games のチームに Splunk 管理者として加わりました。 あなたは Splunk Enterprise インスタンスにサーチのためのデータを取り込むよう依頼されます。

タスク 1: レポジトリからログファイルをダウンロードします。

1. 新しいブラウザウィンドウを開き、<http://splk.it/f1data> に移動します。
2. **Splunk\_f1\_Data.zip** ファイルがシステムにダウンロードされます。
3. アーカイブツールを使用してファイルを解凍します。
4. 解凍したら、**tmp** フォルダが確認できます。



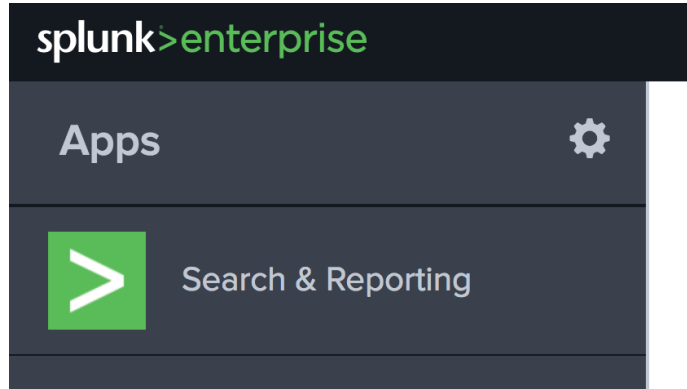
5. フォルダの中にはファイルが 3 つあります。



6. Splunk Web のインスタンスのブラウザウィンドウに戻るか、新しいウィンドウを開きます。

タスク 2: ウェブアプリケーションデータを Splunk Enterprise に取り込みます。

7. インターフェイスの左上にある Splunk Enterprise ロゴをクリックしてホーム App に移動します。



8. データ追加アイコンをクリックします。



## Add Data

Add or forward data to Splunk Enterprise. Afterwards, you may [extract fields](#).

**備考:** このアイコンを表示するためにはadminでログインしなければなりません。このアイコンが表示されない場合、一度ログアウトしてから管理者アカウントで再びログインしてください。

9. データ追加ページから、アップロードボタンをクリックします。



## Upload

files from my computer

Local log files  
Local structured files (e.g. CSV)  
[Tutorial for adding data](#) [↗](#)

10. ソース選択ステップに移ります。 **ファイル選択** ボタンをクリックし、前もってダウンロードし解凍した access\_30Day.log ファイルを選択します。

## 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. ファイルのアップロードが完了したら、**次へ**ボタンをクリックします。
12. ソースタイプ設定ステップで、Splunk が自動的にソースタイプを **access\_combined\_wcookie** として正しく設定しているか確認します。 **次へ**ボタンをクリックします。

Source type: access_combined_wcookie ▼	Save As	List ▼	Format	20 Per Page ▼
<ul style="list-style-type: none"> <li>Event Breaks</li> <li>Timestamp</li> <li>Advanced</li> </ul>				
			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 SL5FF10ADFF4E "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) Gec

13. 設定入力ステップから、ホストフィールド値として「web\_application」と入力し、**レビュー**ボタンをクリックします。

Host field value

web\_application

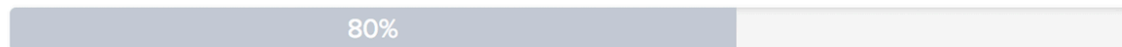
14. **レビュー**ステップに移ります。 設定が下に表示されるものと一致していることを確認し、**提出**ボタンをクリックします。

## Review

Input Type ..... Uploaded File  
File Name ..... access\_30DAY.log  
Source Type ..... access\_combined\_wcookie  
Host ..... web\_application  
Index ..... Default

15. Splunk がファイルを処理します。

### Uploading File



16. 完了すると、ダイアログが表示され、ファイルが正常にアップロードされたことを知らせます。

タスク 3: Web サーバーデータを Splunk Enterprise に取り込みます。

17. 他のデータを追加ボタンをクリックします。



**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. アップロードアイコンとファイル選択ボタンをクリックします。

19. 前もってダウンロードし解凍した linux\_s\_30Day.log ファイルを選択し、次へボタンをクリックします。

20. 今回は Splunk が自動的にデータ用のソースタイプを選択できないことに注意してください。

Source: **linux\_s\_30DAY.log**

Source type: default ▼
Save As
List ▼

> Event Breaks

> Timestamp

> Advanced

21. ソースタイプボタンを選択し、オペレーティングシステムメニューから **linux\_secure** を選択して、ソースタイプを手動で割り当てます。

Source type: default ▼
Save As
List ▼
Format

filter

- Default Settings
  - Splunk's default source type settings
- Application
- Database
- Email
- Metrics
- Miscellaneous
- Network & Security
- Operating System**
  - 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
- Structured
- Uncategorized
- Web

	Time
1	4/21/18 8:00:05.000
2	4/21/18 8:00:29.000
3	4/21/18 8:01:14.000
4	4/21/18 8:39:04.000
5	4/21/18 8:39:04.000

22. 次へボタンをクリックします。
23. 設定入力ステップから、ホストフィールド値として「web\_server」と入力し、レビューボタンをクリックします。

Host field value

web\_server

24. レビューステップで、設定が下に表示されるものと一致していることを確認し、提出ボタンをクリックします。

## Review

Input Type ..... Uploaded File  
 File Name ..... linux\_s\_30DAY.log  
 Source Type ..... linux\_secure  
 Host ..... web\_server  
 Index ..... Default

タスク 4: データベースサーバーデータを **Splunk Enterprise** に取り込みます。

25. 他のデータを追加ボタンをクリックします。

Add More Data

Add more data inputs now or see [examples and tutorials](#). [🔗](#)

26. アップロードアイコンとファイル選択ボタンをクリックします。

27. 前もってダウンロードし解凍した db\_audit\_30DAY.csv ファイルを選択し、次へボタンをクリックします。

28. Splunk が自動的にデータ用の csv ソースタイプを選択していることに注意してください。 このデータ用に新しいソースタイプを作成したいので、名前をつけて保存ボタンをクリックします。

Source type: csv ▼

Save As

29. モーダルウィンドウで、ソースタイプに「db\_audit」と名前を付け、説明を加えます。 カテゴリーメニューを使用し、データベースを選択して保存をクリックします。

### Save Source Type

×

Name db\_audit

Description Postgres Audit Log

Category Database ▼

App system ▼

Cancel

Save

30. 次へボタンをクリックし、設定入力ステップを続けます。

31. ホストフィールド値として「database」と入力し、レビューボタンをクリックします。

Host field value

database

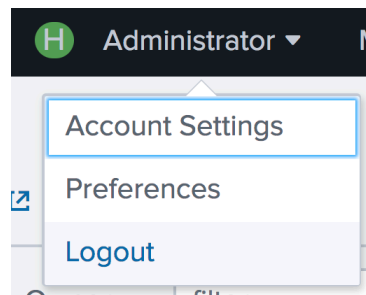
32. 設定が下に示されるものと一致していることを確認し、**提出**ボタンをクリックします。

## Review

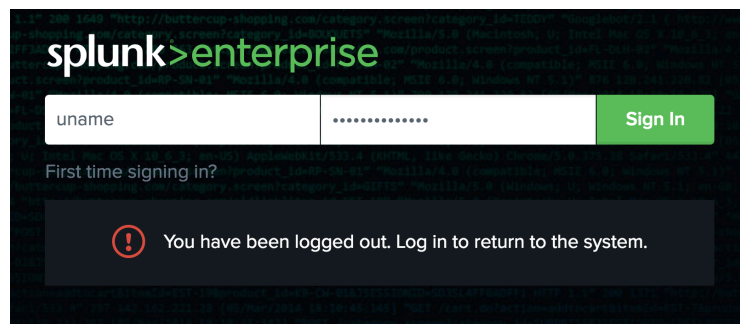
Input Type ..... Uploaded File  
 File Name ..... db\_audit\_30DAY.csv  
 Source Type ..... db\_audit  
 Host ..... database  
 Index ..... Default

**タスク 5: Splunk Enterprise** にパワーユーザーとしてログインします。

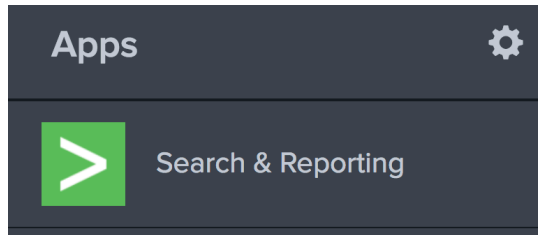
33. ユーザーメニューのログアウトリンクを使用し、インスタンスをログアウトします。



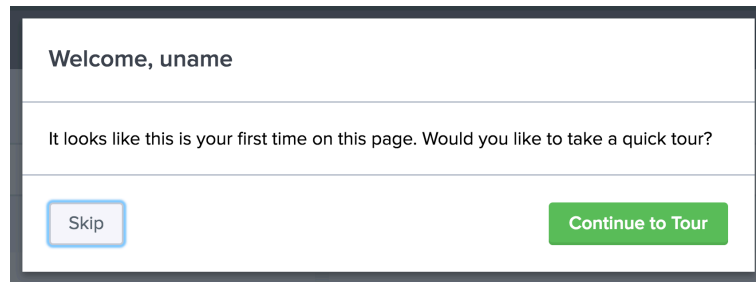
34. 前もって作成したパワーユーザーアカウントを使用してログインしなおします。 提案された認証情報に従った場合は、**ユーザー名**欄に「uname」を、**パスワード**欄に「5p1unkbcup」を使用してください。



35. サイドバーの**検索 & レポート App** を選択します。



36. ツアーに参加するか尋ねられます。 **スキップ**ボタンをクリックします。



37. ここで、システムにインデックスが作成されたイベント数を確認できます。

