# 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。

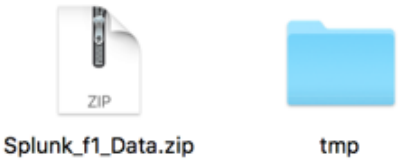
**備考:** 30日におよぶ静的データソースを取り込みます。
このデモではリアルタイムデータは扱いません。

### 手順

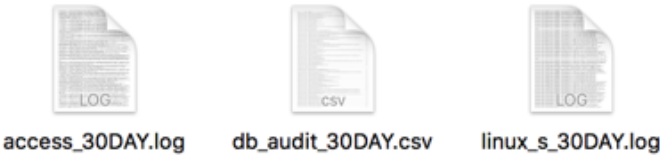
**シナリオ**: あなたは最近 Buttercup Games のチームに Splunk 管理者として加わりました。 あなたは Splunk Enterprise インスタンスにサーチのためのデータを取り込むよう依頼されます。

**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。



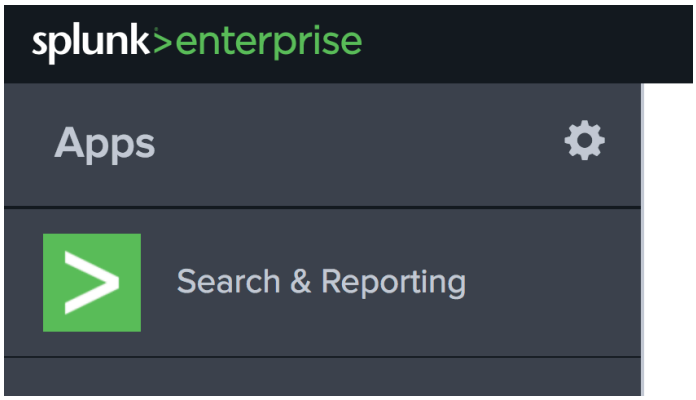

5. フォルダの中にはファイルが 3 つあります。




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。

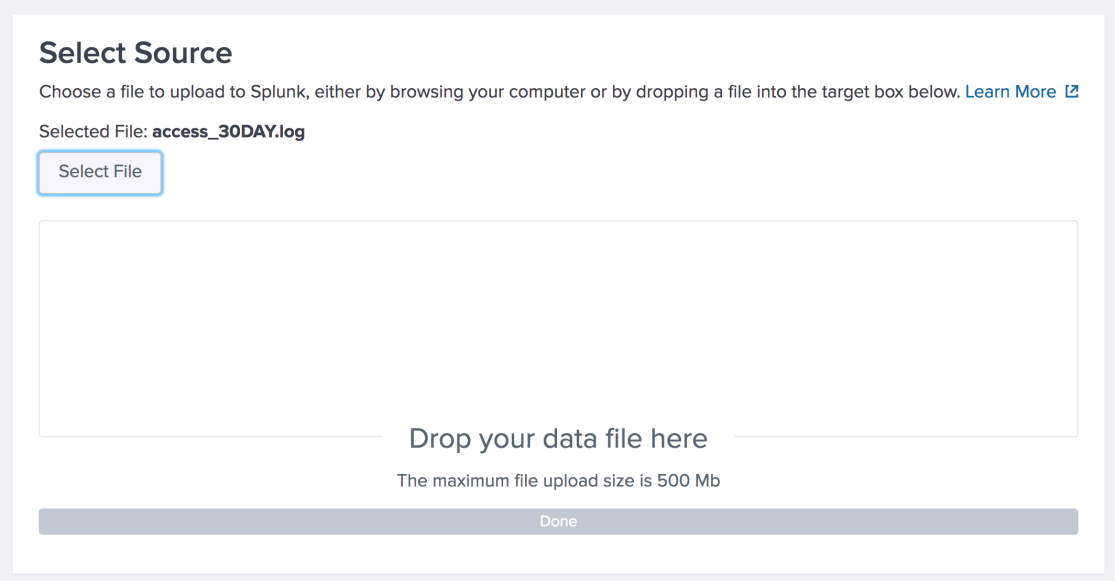
9. **データ追加**ページから、**アップロード**ボタンをクリックします。

**Upload**

files from my computer

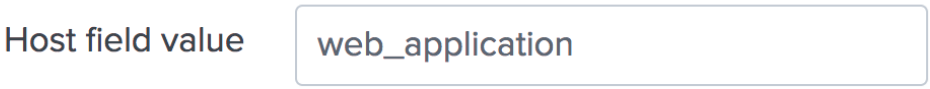
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

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。

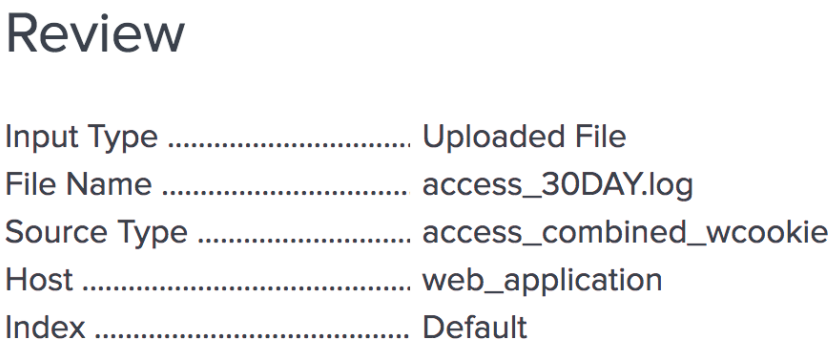



11. ファイルのアップロードが完了したら、**次へ**ボタンをクリックします。
12. **ソースタイプ設定**ステップで、Splunk が自動的にソースタイプを **access_combined_wcookie** として正しく設定しているか確認します。 **次へ**ボタンをクリックします。


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。




14. **レビュー**ステップに移ります。 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。

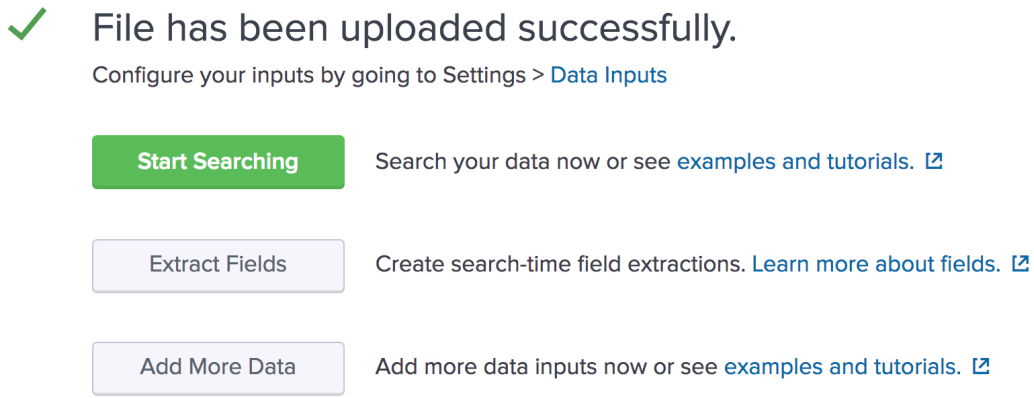



15. Splunk がファイルを処理します。

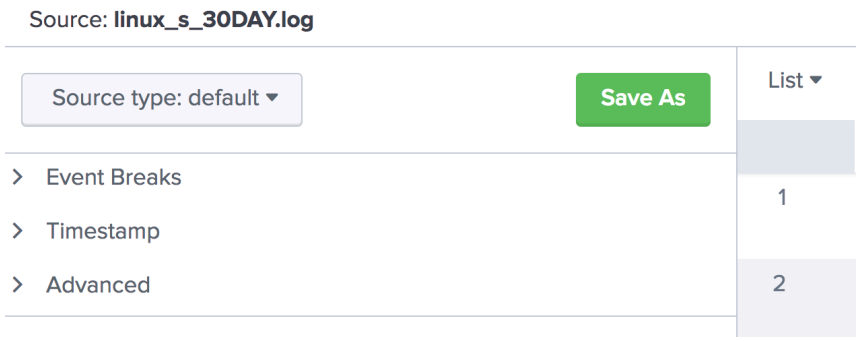

16. 完了すると、ダイアログが表示され、ファイルが正常にアップロードされたことを知らせます。

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

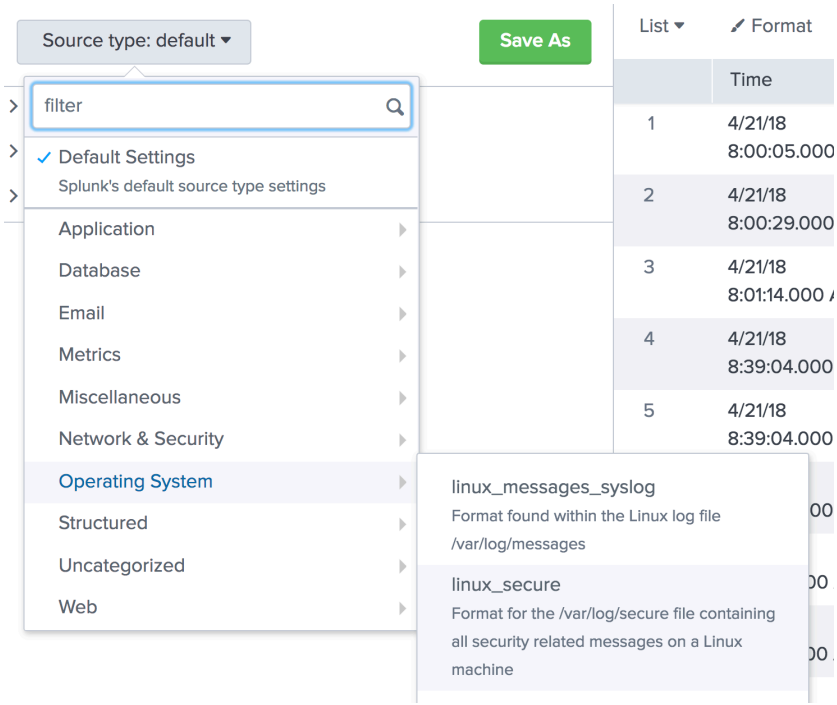
17. **他のデータを追加**ボタンをクリックします。



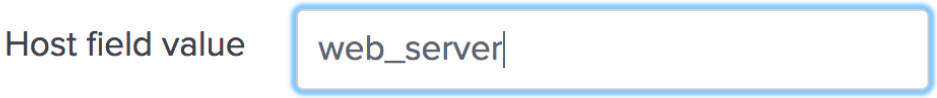

18. **アップロード**アイコンと**ファイル選択**ボタンをクリックします。
19. 前もってダウンロードし解凍した linux_s_30Day.log ファイルを選択し、**次へ**ボタンをクリックします。
20. 今回は Splunk が自動的にデータ用のソースタイプを選択できないことに注意してください。



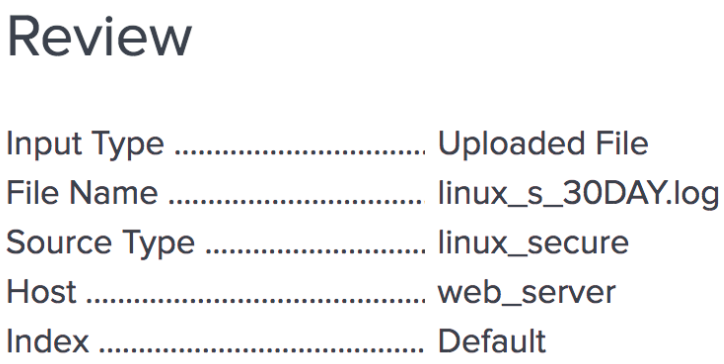

21. **ソースタイプ**ボタンを選択し、**オペレーティングシステム**メニューから **linux_secure** を選択して、ソースタイプを手動で割り当てます。




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。

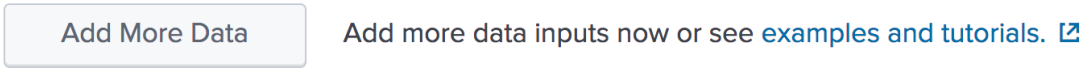



24. **レビュー**ステップで、設定が下に示されるものと一致していることを確認し、**提出**ボタンをクリックします。



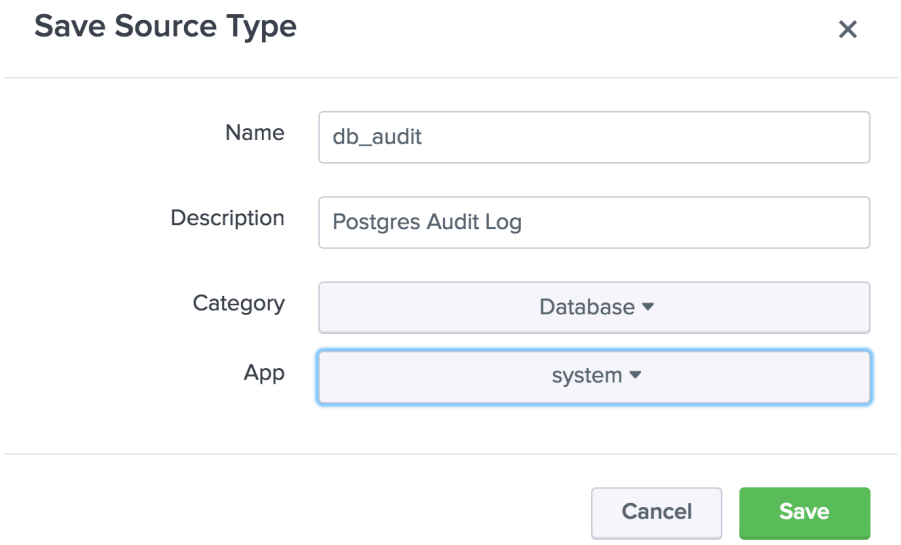

タスク **4:** データベースサーバーデータを **Splunk Enterprise** に取り込みます。

25. **他のデータを追加**ボタンをクリックします。



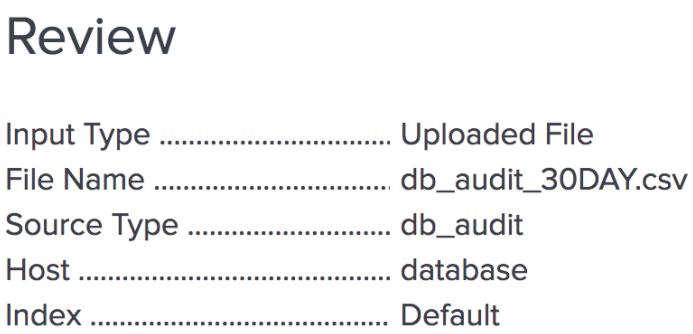

26. **アップロード**アイコンと**ファイル選択**ボタンをクリックします。
27. 前もってダウンロードし解凍した db_audit_30DAY.csv ファイルを選択し、**次へ**ボタンをクリックします。
28. Splunk が自動的にデータ用の csv ソースタイプを選択していることに注意してください。 このデータ用に新しいソースタイプを作成したいので、**名前をつけて保存**ボタンをクリックします。


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。



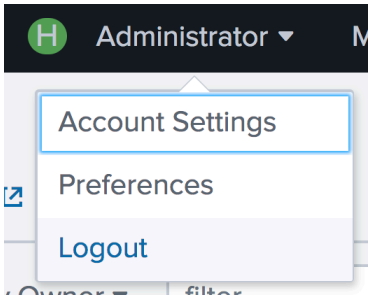

30. **次へ**ボタンをクリックし、**設定入力**ステップを続けます。
31. **ホストフィールド値**として「database」と入力し、**レビュー**ボタンをクリックします。


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。

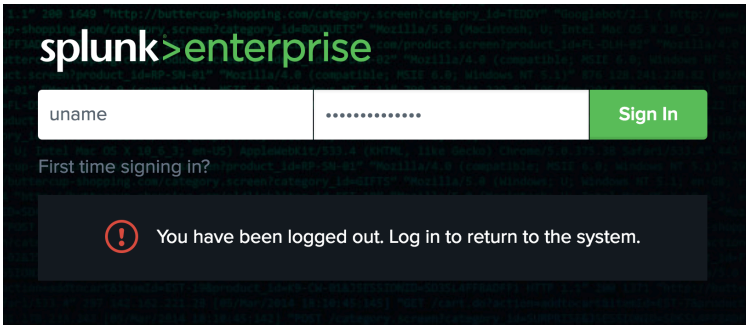



タスク **5: Splunk Enterprise** にパワーユーザーとしてログインします。

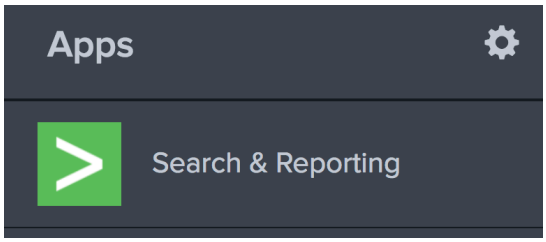
33. **ユーザー**メニューの**ログアウト**リンクを使用し、インスタンスをログアウトします。



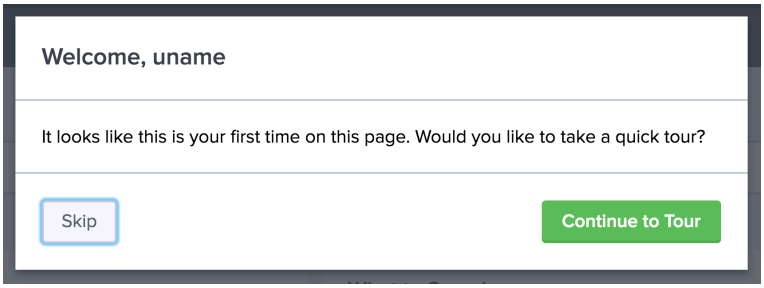

34. 前もって作成したパワーユーザーアカウントを使用してログインしなおします。 提案された認証情報に従った場合は、**ユーザー名**欄に「`uname`」を、**パスワード**欄に「`5p1unkbcup`」を使用してください。




35. サイドバーの**サーチ & 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。