

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。

ラボマニュアルは示されるデータタイプ別にソースタイプを参照しています:

タイプ	ソースタイプ	関連のフィールド
ウェブアプリケーション	access_combined_wcookie	action、bytes、categoryId、clientip、itemId、JSESSIONID、productId、referer、referer_domain、status、useragent、file
データベース	db_audit	Command、Duration、Type
Web サーバー	linux_secure	COMMAND、PWD、pid、process

ラボモジュール 11 - ピボットの使用

備考: このラボ文書には2つのセクションがあります。
最初のセクションには解答の記載がない指示が含まれます。
次のセクションには予想されるサーチ文字列 (解答) が赤で記載された指示が含まれます。

説明

このラボでは、ピボットインターフェースを使用してレポートを構築します。

手順

シナリオ: CFO はあなたが作成したシンプルなダッシュボードをととても気に入っていますが、当社の顧客の出身地を記載したレポートを追加したいと考えています。 彼女はユーザーがショッピングカートに追加したアイテムの内容と、そのユーザーの出身地を把握したいと思っています。

タスク 1: インスタントピボットで非変換コマンドを利用します。

1. サーチビューに移動します。(ホーム App にいる場合は、画面左側にある列から**サーチ & レポート**をクリックしてください。サーチビューへは、画面一番上の緑のバーにある**サーチメニュー**をクリックしてもアクセスすることができます。)

備考: このコースでは、常時メインインデックスを使用してサーチすることになります。これは運用環境で最適な実例ではありませんが、データセット制限の性質により、これらのラボに必要となります。

- 常にすべてのウェブアプリケーションイベントを返す検索を入力してください。
- 視覚エフェクトタブをクリックすると、ピボット、クイックレポート、検索コマンドの3つのアイコンが表示されます。

例:

 Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.



Pivot

Build tables and visualizations using multiple fields and metrics without writing searches.



Quick Reports

Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'.




Search Commands

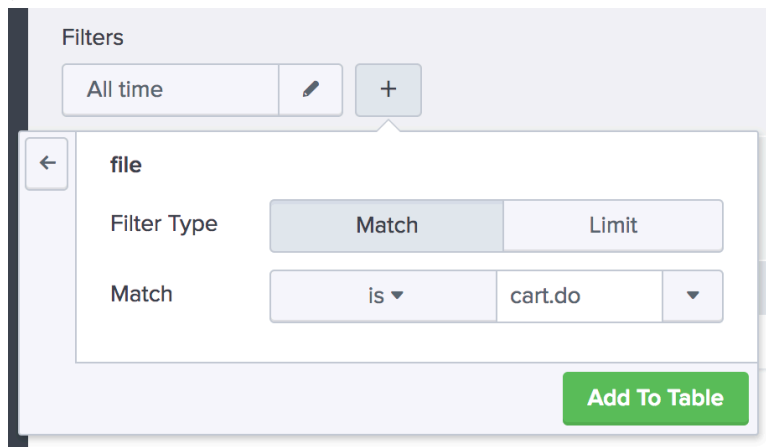
Use a transforming search command, like timechart or stats, to summarize the data.



- ピボットアイコンをクリックします。
- モーダルウィンドウで、すべてのフィールド表示を選択し、OK をクリックします。

タスク 2: ピボットインターフェースを使用してレポートを構築します。

- フィルターから  をクリックしてフィルターセレクトを開き、フィールドリストからファイルを選択します。
- マッチメニューから **cart.do** を選択し、テーブルに追加をクリックします。


例:



- 分割行から  をクリックして分割行セレクトを開き、プロダクト ID をクリックします。
- ラベルについては、「カートに追加されたプロダクト」と入力します。
- デフォルト値で他の設定を維持し、テーブルに追加をクリックします。
- 分割列から  をクリックして分割列セレクトを開き、参照者_ドメインをクリックします。
- デフォルト値で他の設定を維持し、テーブルに追加をクリックします。
- 大量のウェブトラフィックは **buttercupgames.com** ドメインに起因していることに注意してください。これらをフィルターで除去します。

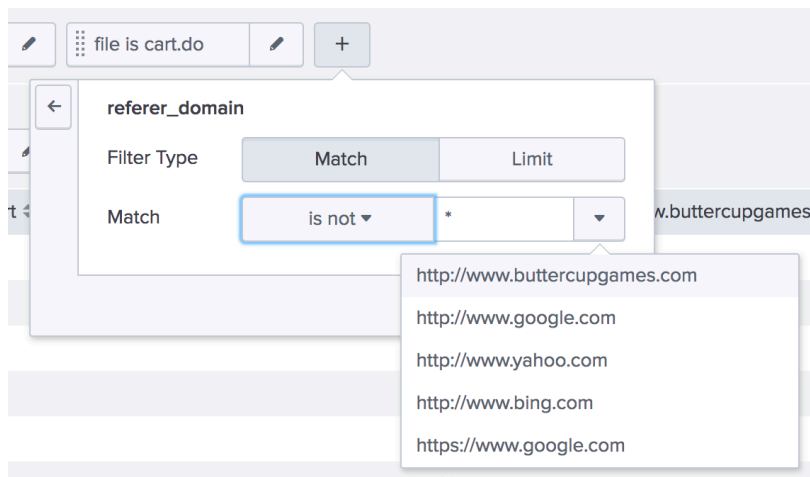
結果例:

Product Added To Cart	http://www.bing.com	http://www.buttercupgames.com	http://www.google.com	http://www.yahoo.com
BS-AG-G09	23	1421	56	36
CU-PG-G06	17	1452	58	35
DB-SG-G01	26	2367	100	46
DC-SG-G02	15	2269	92	34
FI-AG-G08	12	1603	50	25
FS-SG-G03	21	1967	85	25

14. フィルターから  をクリックしてフィルターセクターを開き、フィールドリストから **referrer_domain** を選択します。

15. **is not (以外)** とマッチメニューの **http://www.buttercupgames.com** を選択します。

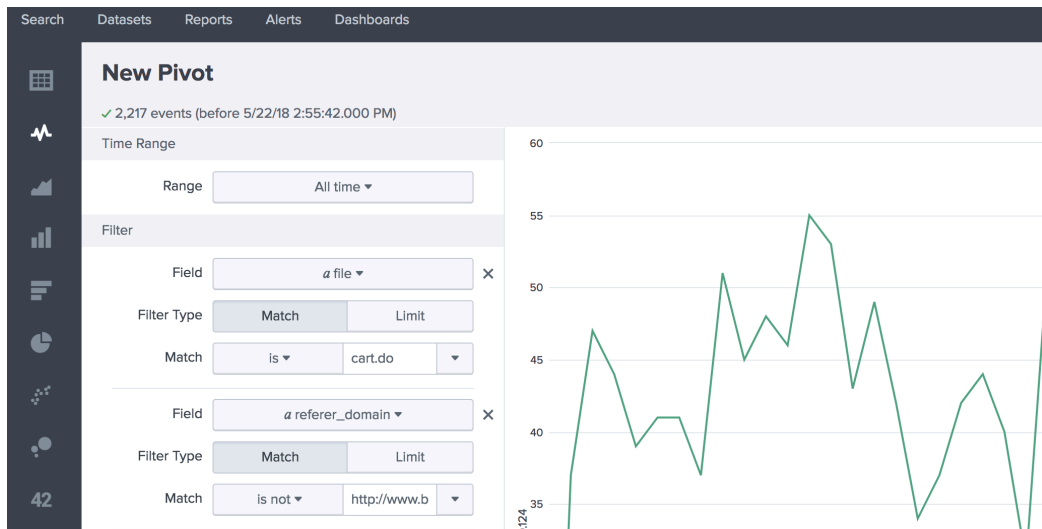
例:



16. テーブルに追加をクリックします。

17. 黒いサイドバーを使用して折れ線グラフ視覚エフェクトを選択します。

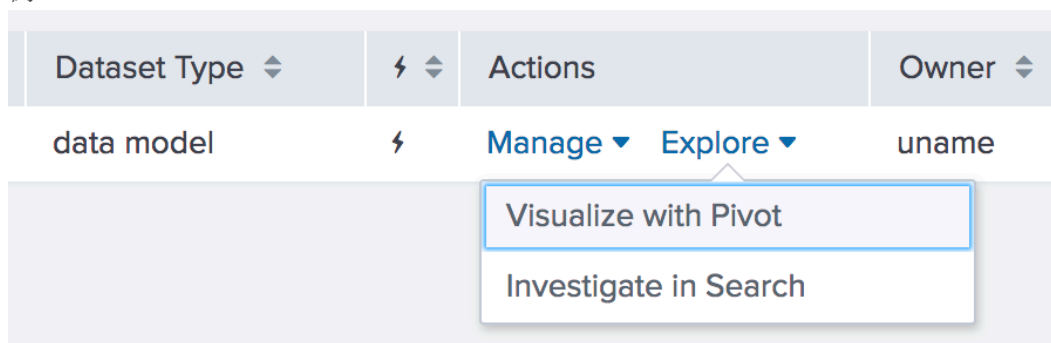
例:



タスク 3: ピボットからダッシュボードにパネルを追加し、データモデルを作成します。

18. 名前をつけて保存メニューを使用してダッシュボードパネルを選択します。
19. モデルタイトルおよびモデル ID の書式フィールドがあることに注意してください。 ピボットレポートにはデータモデルが必要です。 インスタントピボットを視覚エフェクトタブから使用しているため、現在のレポートにはデータモデルがありません。 レポートを保存して元の検索から新しいデータモデルを作成します。
20. これらの値でダッシュボードを保存します:
 - ダッシュボード: 既存
 - ダッシュボードのタイトル: セールスダッシュボード
 - パネルタイトル: 参照ドメイン別セールス
 - モデルタイトル: ウェブアプリケーションデータセット
 - モデル ID: web_app_ds
21. ダッシュボードを表示をクリックしてダッシュボードを表示します。
22. 画面一番上のバーにあるデータセットメニューオプションをクリックします。
23. フィルターツールバーにある自分用をクリックして自分のデータセットのみを表示します。
24. アクションメニューの検証を選択してピボットで視覚化をクリックします。

例:



25. フィルターおよび分割ツールを使用して、ピボットインターフェースのデータを検証します。

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。

ラボマニュアルは示されるデータタイプ別にソースタイプを参照しています:

タイプ	ソースタイプ	関連のフィールド
ウェブアプリケーション	access_combined_wcookie	action、bytes、categoryId、clientip、itemId、JSESSIONID、productId、referer、referer_domain、status、useragent、file
データベース	db_audit	Command、Duration、Type
Web サーバー	linux_secure	COMMAND、PWD、pid、process

ラボモジュール 11 - ピボットの使用 (ソリューション付)

備考: このラボ文書には2つのセクションがあります。
最初のセクションには解答の記載がない指示が含まれます。
次のセクションには予想されるサーチ文字列 (解答) が赤で記載された指示が含まれます。

説明

このラボでは、ピボットインターフェースを使用してレポートを構築します。

手順

シナリオ: CFO はあなたが作成したシンプルなダッシュボードをととても気に入っていますが、当社の顧客の出身地を記載したレポートを追加したいと考えています。彼女はユーザーがショッピングカートに追加したアイテムの内容と、そのユーザーの出身地を把握したいと思っています。


タスク 1: インスタントピボットで非変換コマンドを利用します。

1. サーチビューに移動します。(ホーム App にいる場合は、画面左側にある列から**サーチ & レポート**をクリックしてください。サーチビューへは、画面一番上の緑のバーにある**サーチメニュー**をクリックしてもアクセスすることができます。)

備考: このコースでは、常時メインインデックスを使用してサーチすることになります。
これは運用環境で最適な実例ではありませんが、データセット制限の性質により、これらのラボに必要となります。

- 常にすべてのウェブアプリケーションイベントを返す検索を入力してください。
(`index=main sourcetype=access_combined_wcookie`)
- 視覚エフェクトタブをクリックすると、ピボット、クイックレポート、検索コマンドの3つのアイコンが表示されます。

例:

 Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.



Pivot

Build tables and visualizations using multiple fields and metrics without writing searches.



Quick Reports

Click on any field in the events tab for a list of quick reports like 'Top Referrers' and 'Top Referrers by time'.




Search Commands 

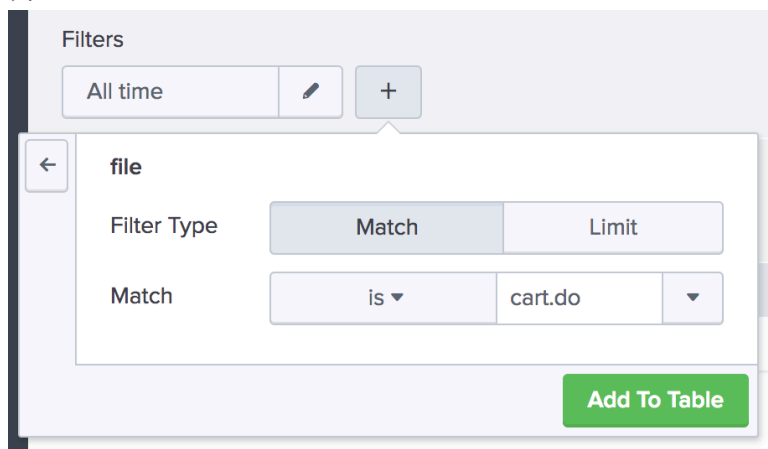
Use a transforming search command, like timechart or stats, to summarize the data.



- ピボットアイコンをクリックします。
- モーダルウィンドウで、すべてのフィールド表示を選択し、**OK** をクリックします。

タスク 2: ピボットインターフェースを使用してレポートを構築します。

- フィルターから  をクリックしてフィルターセクターを開き、フィールドリストからファイルを選択します。
- マッチメニューから **cart.do** を選択し、**テーブルに追加** をクリックします。

例:



- 分割行から  をクリックして分割行セクターを開き、**プロダクト ID** をクリックします。
- ラベルについては、「カートに追加されたプロダクト」と入力します。
- デフォルト値で他の設定を維持し、**テーブルに追加** をクリックします。
- 分割列から  をクリックして分割列セクターを開き、**参照者_ドメイン** をクリックします。
- デフォルト値で他の設定を維持し、**テーブルに追加** をクリックします。

13. 大量のウェブトラフィックは **buttercupgames.com** ドメインに起因していることに注意してください。これらをフィルターで除去します。

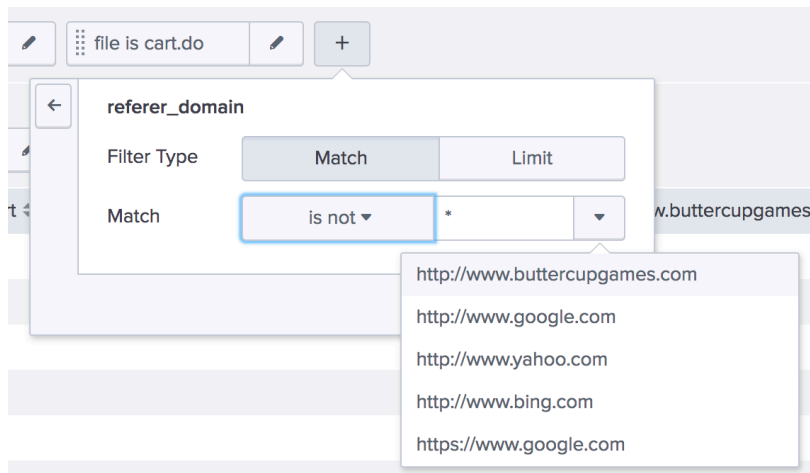
結果例:

Product Added To Cart	http://www.bing.com	http://www.buttercupgames.com	http://www.google.com	http://www.yahoo.com
BS-AG-G09	23	1421	56	36
CU-PG-G06	17	1452	58	35
DB-SG-G01	26	2367	100	46
DC-SG-G02	15	2269	92	34
FI-AG-G08	12	1603	50	25
FS-SG-G03	21	1967	85	25

14. フィルターから **+** をクリックしてフィルターセクターを開き、フィールドリストから **referrer_domain** を選択します。

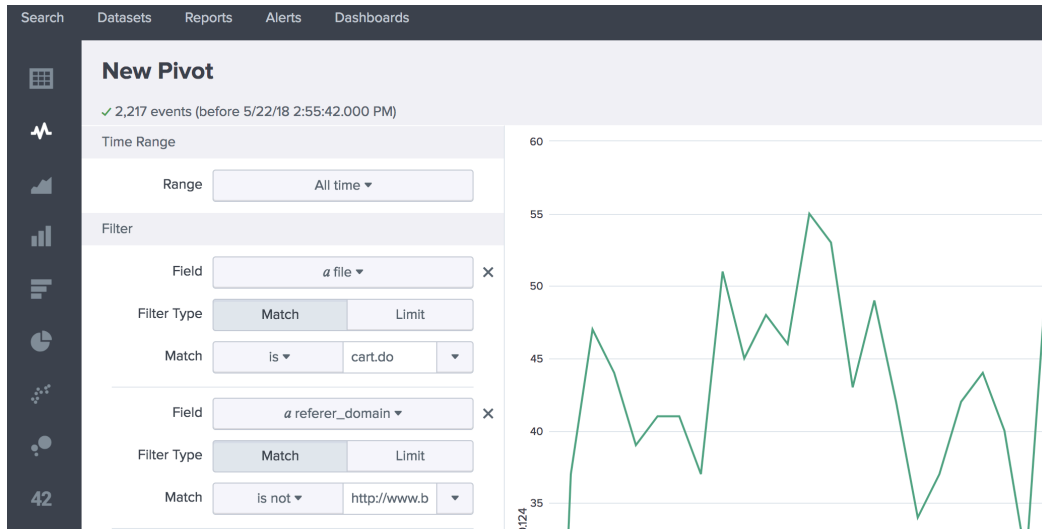
15. **is not (以外)** とマッチメニューの **http://www.buttercupgames.com** を選択します。

例:



16. テーブルに**追加**をクリックします。
17. 黒いサイドバーを使用して**折れ線グラフ**視覚エフェクトを選択します。

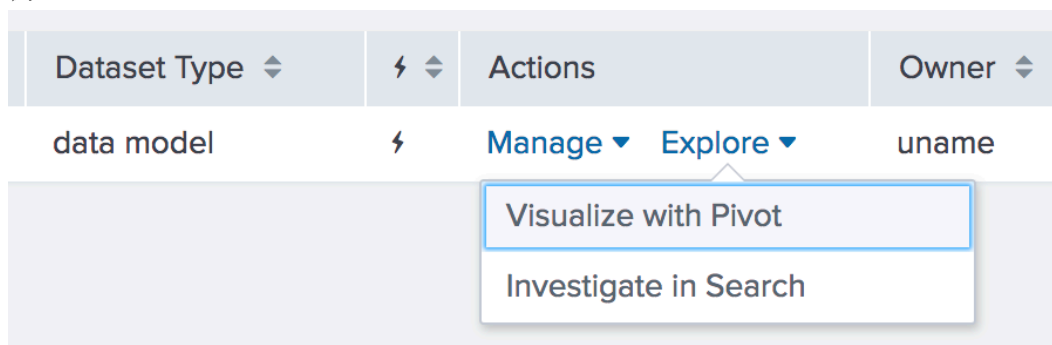
例:



タスク 3: ピボットからダッシュボードにパネルを追加し、データモデルを作成します。

18. 名前をつけて保存メニューを使用してダッシュボードパネルを選択します。
19. モデルタイトルおよびモデル ID の書式フィールドがあることに注意してください。 ピボットレポートにはデータモデルが必要です。 インスタントピボットを視覚エフェクトタブから使用しているため、現在のレポートにはデータモデルがありません。 レポートを保存して元の検索から新しいデータモデルを作成します。
20. これらの値でダッシュボードを保存します:
 - ダッシュボード: 既存
 - ダッシュボードのタイトル: セールスダッシュボード
 - パネルタイトル: 参照ドメイン別セールス
 - モデルタイトル: ウェブアプリケーションデータセット
 - モデル ID: web_app_ds
21. ダッシュボードを表示をクリックしてダッシュボードを表示します。
22. 画面一番上のバーにあるデータセットメニューオプションをクリックします。
23. フィルターツールバーにある自分用をクリックして自分のデータセットのみを表示します。
24. アクションメニューの検証を選択してピボットで視覚化をクリックします。

例:



25. フィルターおよび分割ツールを使用して、ピボットインターフェースのデータを検証します。