splunk>

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 6 - サーチにおけるフィールドの使用

説明

このラボでは、フィールドを使用してサーチを絞り込みます。

手順

シナリオ: 当社の Web サーバーがダウンタイムに見舞われています。 セールスディレクターはあなたのチームにこれが Web サイトでの販売にどのような影響を与えたのかを検証するように依頼します。

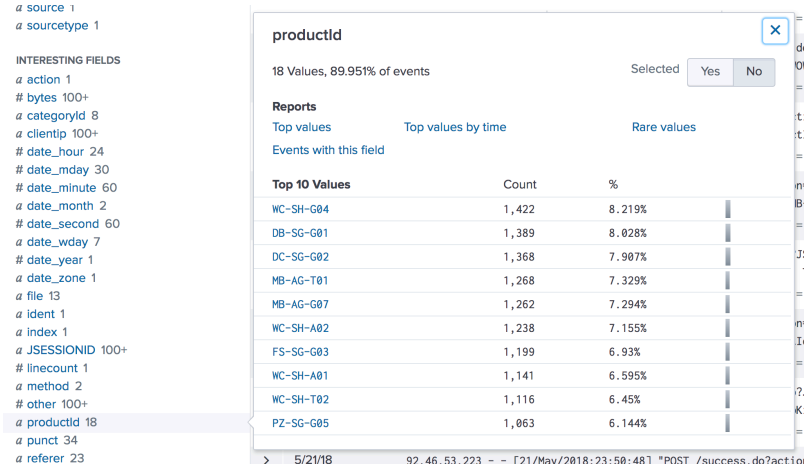
タスク 1:フィールドサイドバーを使用してサーチ結果を調査します。

1. App のナビゲーションバー (ブラウザウィンドウの上方にあるバー) で**サーチ**をクリックします。 アプリケーションバーに**サーチ**が表示されない場合、または前回のサーチをクリアする場合は、ブラウザウィンドウの一番上にある Splunk バーの **App: Search & Reporting** をクリックします。
2. 「`index=main sourcetype=access_combined_wcookie action=purchase`」を**全時間**でサーチします。これは購入アクションがとられたすべてのイベントを返します。

備考: **サーチが完了したら、サーチがスマートモードで実行されたことを検証します。サーチモードはタイムレンジピッカーで表示されます。**
サーチがスマートモードで実行されていなかった場合、スマートモードに変更してからサーチを再実行します。

3. フィールドサイドバーの**関連のフィールド**リストを検証します。「`productId`」は Splunk によって抽出されたフィールドの 1 つです。
4. フィールドサイドバーの**関連のフィールド**で **productId** をクリックします。ポップアップウィンドウにプロダクト ID 別の購入プロダクトトップ 10 が表示されます。右端上の **x** をクリックしてウィンドウを閉じます。

結果例



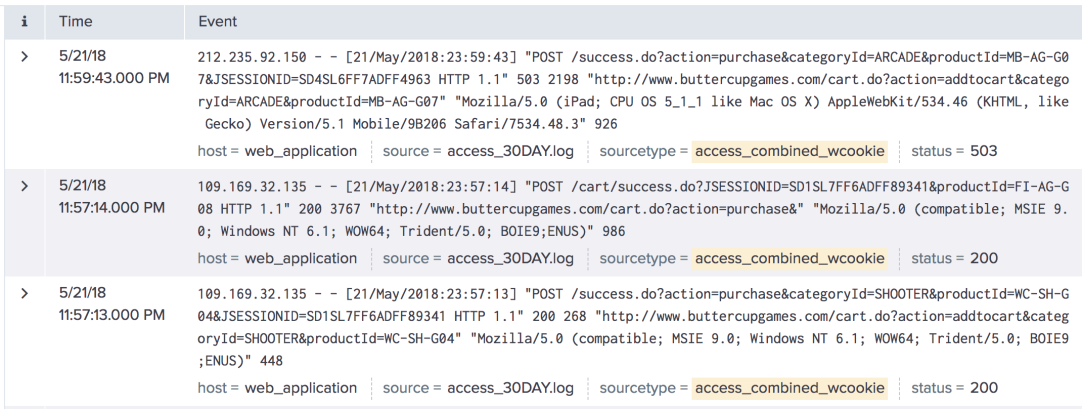
5. フィールドサイドバーの**関連のフィールド**で **status** をクリックします。このフィールドにはウェブリクエストのステータスが含まれます。 「`200`」より大きいものはすべて顧客インタラクションがエラーに終わり、購入がなされなかったことを意味します。

結果例

Values	Count	%
200	17,934	93.236%
503	797	4.143%
408	104	0.541%
400	94	0.489%
406	87	0.452%
500	84	0.437%
505	69	0.359%
404	39	0.203%
403	27	0.14%

6. 各イベントのステータスのクイック表示は選択ができます。ステータスフィールドウィンドウから**選択済**の隣の右上端にある**はい**をクリックします。 右端上の **x** をクリックしてウィンドウを閉じます。
7. 「`status`」はフィールドサイドバーで選択されたフィールドで、「`status=value`」は各イベントの下に表示されています。

結果例



i	Time	Event
>	5/21/18 11:59:43.000 PM	212.235.92.150 - - [21/May/2018:23:59:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 503 2198 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 926 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503
>	5/21/18 11:57:14.000 PM	109.169.32.135 - - [21/May/2018:23:57:14] "POST /cart/success.do?JSESSIONID=SD1SL7FF6ADFF89341&productId=FI-AG-G08 HTTP 1.1" 200 3767 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200
>	5/21/18 11:57:13.000 PM	109.169.32.135 - - [21/May/2018:23:57:13] "POST /success.do?action=purchase&categoryId=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP 1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200

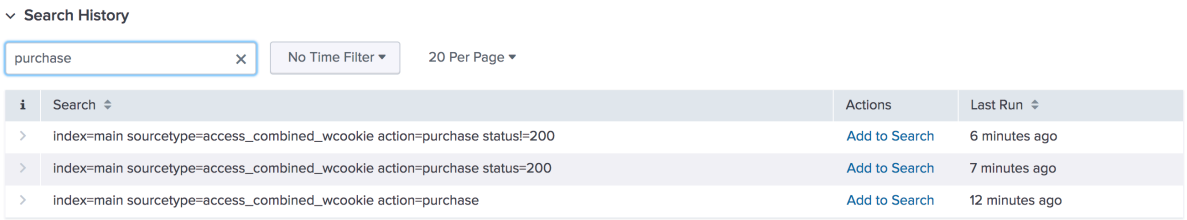
8. フィールドサイドバーの**選択済フィールド**で「status」フィールドをクリックします。フィールドウィンドウから、最高数の値をクリックします (トップに記載)。フィールドと値はサーチバーのサーチ基準に追加されているのが確認できます。また、この選択は新規サーチを引き起こし、新しいサーチ基準を使用して実行されます。
9. ほとんどの結果に示される値は 200 であるため、サーバーエラーは見られません。 比較演算子の変更でこれを修正します。
10. ステータスサーチを status!=200 に変更し、サーチを再試行します。
11. これによってエラーで終了したウェブ購入のみを返すサーチが確認できるようになります。
12. どれだけのイベントがエラーで終了していますか? サーチバーからイベント数を確認できます。 クイズで思い出すよう促される場合があるためこの数字に留意してください。

    (1301)
13. フィールドサイドバーで、もう一度 **status** をクリックし、**Selected** の隣の右端上にある **No** を選択します。 これにより**選択済フィールド**リストから削除されます。右端上の **x** をクリックしてフィールドウィンドウを閉じます。**Splunk バー**の**サーチ**リンクをクリックして、サーチ結果をクリアします。

タスク 2: サーチ履歴を使用して以前に実行したサーチを閲覧します。

14. **検索履歴**をクリックして、過去のサーチ履歴を表示します。 サーチ結果を短時間保存するジョブとは異なり、ここでは長時間保存されるサーチ基準のみを確認します。多くのサーチを頻繁に行います。サーチを検索するため時間または内容別にフィルタにかけることができます。
15. サーチ履歴フィルタボックスの中をクリックして、「purchase」とタイプします。サーチリストは短縮されています。「purchase」という言葉を含むサーチのみが残ります。

結果例



16. サーチのうちの 1 つについて、**サーチに追加**をクリックします。サーチ基準がサーチバーに表示されますが、時間範囲はまだデフォルト設定を表示しています。
17. 時間範囲を変更し、任意でサーチ基準に追加または変更してからサーチを実行します。

splunk>

タスク 3: ジョブページを使用して最新のサーチを表示します。

18. Splunk バー (ブラウザウィンドウの上方にある黒のバー) で**アクティビティ > ジョブ**をクリックします。
19. サーチ文字列を見て、キーストロークの誤りがないかを確認します。以下のようなリストが確認されることがあります: "`| metadata ...`" または "`| history ...`"。これは**あなたのサーチ履歴を拡大**にアクセスすると表示されます。