splunk>

Module 14 Lab – Using the Common Information Model (CIM)

Description

In this lab exercise, you normalize your data to the Splunk Common Information Model (CIM) using the CIM add-on.

Steps

Scenario: The Buttercup Games sales team wants to correlate sales data across multiple data sources, but not all source types use the same field names. To ensure that all data is reported correctly, the IT team has installed the CIM app to use as a standard for field names.

Task 1: Examine your data.

1. Return to the Search & Reporting app.
2. Search sales online transactions over the **last 4 hours**.
   index=web sourcetype=access_combined
3. Examine the values of the following fields. These fields are required for your dashboard:
   - host
   - action
   - clientip
   - status
   - useragent
4. In a separate browser tab or window, examine the Web data model in the CIM Reference Tables from the following link:
   https://docs.splunk.com/Documentation/CIM/latest/User/Howtousethesereferencetables
5. In the browser you opened in step 4, select **Web** from the data model list on the left.
6. Examine the **Fields for Web event datasets** table. Based on the fields in `access_combined`, which fields in the data model match the fields needed for your dashboard?

Field name in source type	Field in Data Model
host	dest
action	action
clientip	src
status	status
useragent	http_user_agent

Task 2: Create an event type and tag.

7. Search for all action types related to online transactions in the **last 4 hours**.
   index=web sourcetype=access_combined action=*

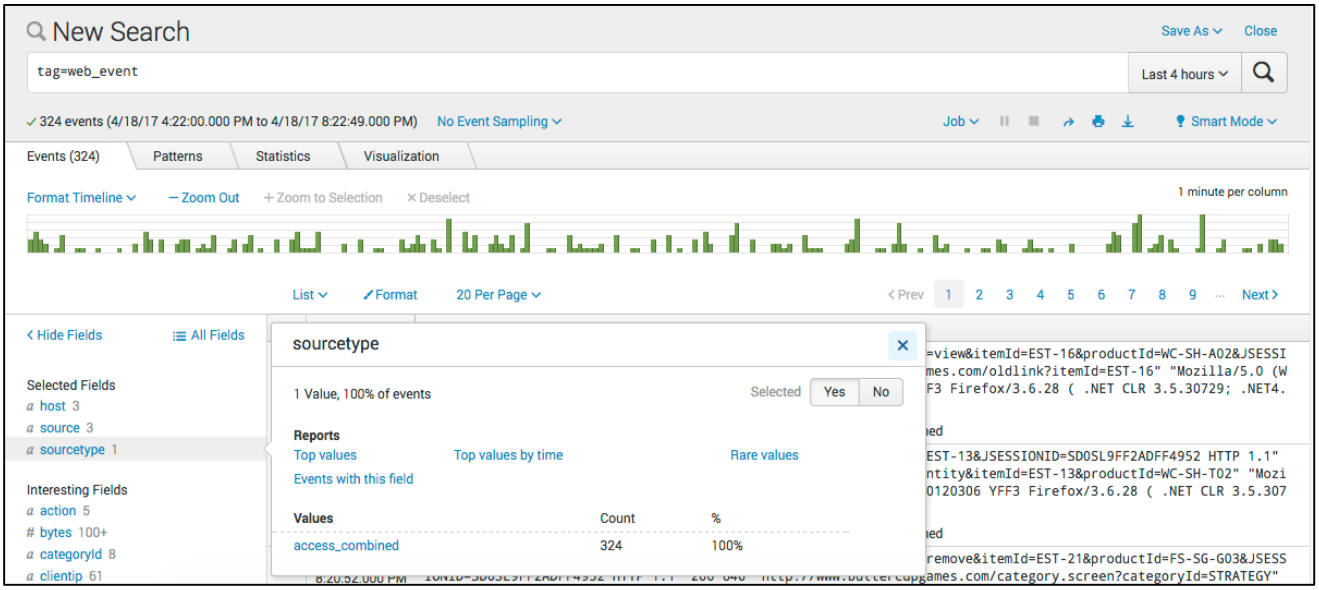
8. Save the search as an event type named: `access_combined` with a tag named `web_event`. Optionally, select a color and set a priority.
    a) Select Save As > Event Type.
        – Name: access_combined
        – Tags: `web_event`
    b) Click **Save**.
    c) Click **Done**.

NOTE: In a production environment, a Splunk administrator would later set the permissions of this event type to Global.

Task 3: Test your tag and event type.

9. Search using the event type.
   eventtype=access_combined
   What sourcetype is returned? _____
   access_combined
10. Search using the tag.
    tag=web_event
    What source type is returned? _____
    access_combined

Results Example:



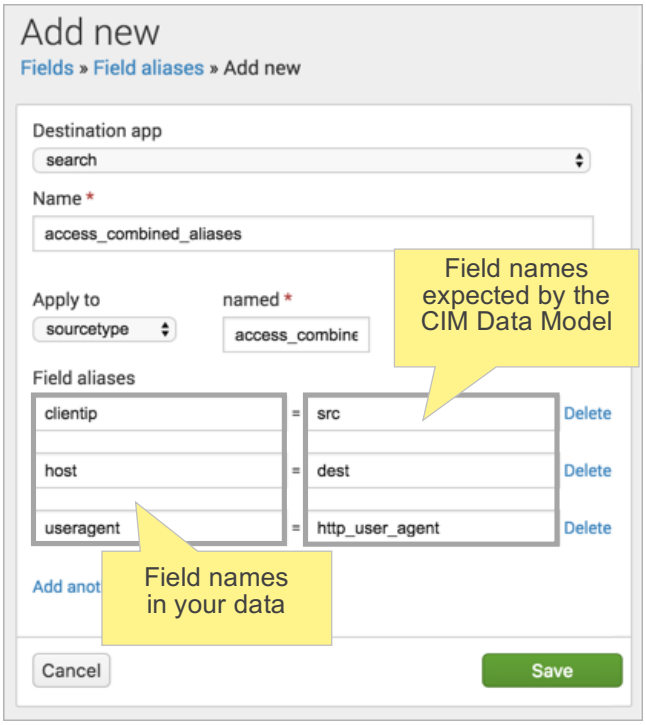
11. Using the `datamodel` command, are the fields in your data populated in the Web data model?
    | datamodel Web Web search | fields Web*

Field in Your Data	Matching Attribute	Data Model Field Populated?
host	dest	No
action	action	Yes
clientip	src	No
status	status	Yes
useragent	http_user_agent	No

Task 4: Create field aliases for the fields that aren't populated in the data model.

12. Create field aliases for the needed attributes that didn't populate.
    a) Navigate to **Settings > Fields > Field aliases**.
    b) Click **New**.
    c) Verify Destination app is: search
    d) In the Name box, type: `access_combined_aliases`
    e) From the Apply dropdown, make sure **sourcetype** is selected.
    f) In the **named** field, type: `access_combined`
    g) In the **Field aliases** left box, type: `clientip`
    h) In the **Field aliases** right box, type: `src`
    i) Click **Add another field**.
    j) Repeat the previous steps for the remaining fields and field aliases:
    k) host = dest
    l) useragent = http_user_agent
    m) Make sure your page looks identical to the example shown, and then click **Save**.

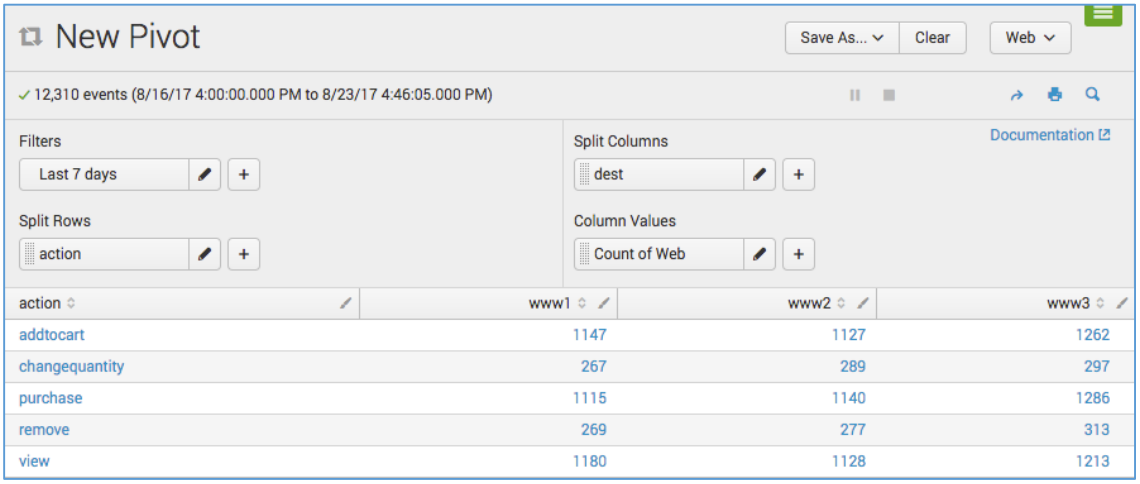
Example:



Task 5: Validate your data against the CIM Web data model.

13. Return to the Search & Reporting app.
14. Navigate to **Settings > Data models**.
15. Using the **Web** data model, select **Pivot**.
16. Select the **Web** dataset object.
17. Filter on the **Last 7 days** and **Split Rows** by *action* and **Split Columns** by *dest*.

Results Example:



action	www1	www2	www3
addtocart	1147	1127	1262
changequantity	267	289	297
purchase	1115	1140	1286
remove	269	277	313
view	1180	1128	1213

18. Change your pivot to **Split Rows** by *src*. Then change Split Columns by *status*. Are you able to split on all the expected fields in the Web data model?

NOTE: If your data model fields are not populating, delete the field alias and create it again. Be careful to avoid typos.