Lab Exercise 13 : Using the Common Information Model (CIM) Add - On

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 CLASS: Intermediate app.

2. Search for all action types related to online transactions over the **last 4 hours**.

3. Examine the values of the following fields. These field values are required for your dashboard, but their current names aren't CIM-compliant.
    - 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?

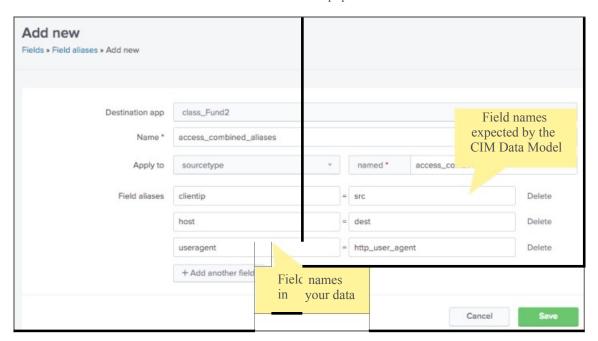| Field name in source type	Field in Data Model
host	dest
action	action
clientip	src
status	status
useragent	http_user_agent

7. Using the datamodel command, are the fields in your data populated in the Web data model?

   Hint: Refer to the example on the **datamodel Command – Example** slide and then check which fields are included in your result.

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 2: Create field aliases for the fields that aren't populated in the data model.
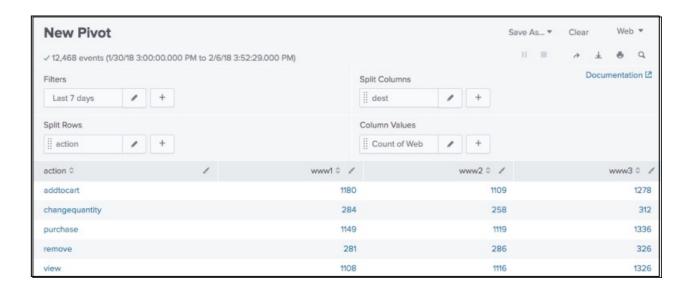
8. Create field aliases for the needed attributes that didn't populate.

Task 3: Validate your data against the CIM Web data model.

9. Return to the CLASS: Intermediate app.

10. Navigate to Settings > Data models.

11. Using the **Web** data model, select **Pivot**.

12. Select the **Web** dataset object.

13. Filter on the Last 7 days and Split Rows by action and Split Columns by dest.

Results Example:

New Pivot

✓ 12,468 events (1/30/18 3:00:00.000 PM to 2/6/18 3:52:29.000 PM)

Save As... ▾   Clear   Web ▾

Documentation ⬈

Filters

| Last 7 days | ✎ | + |

Split Rows

| ⠿ action | ✎ | + |

Split Columns

| ⠿ dest | ✎ | + |

Column Values

| ⠿ Count of Web | ✎ | + |

action ⇕	✎	www1 ⇕ ✎	www2 ⇕ ✎	www3 ⇕ ✎
addtocart		1180	1109	1278
changequantity		284	258	312
purchase		1149	1119	1336
remove		281	286	326
view		1108	1116	1326

14. 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.