Lab Exercise 12 : Creating Data Models

Description

This exercise walks you through the process of creating a data model. After the data model is created, create a pivot to verify your data model provides the expected results.

Steps

Scenario: **The VP of Sales wants to run reports based on daily activity from the online store but doesn't have the time to learn the search language.**

Task 1: Create a data model and add a Web Requests root event. The root event will be the base search for all child events.

1. Navigate to Settings > Data models.
2. Click New Data Model .
3. In the **Title field**, type: Buttercup Games Site Activity. (Notice that this automatically fills in the ID field. **Don't** delete this value. The ID field cannot be blank.)
4. For **App**, make sure **Search & Reporting** is selected.

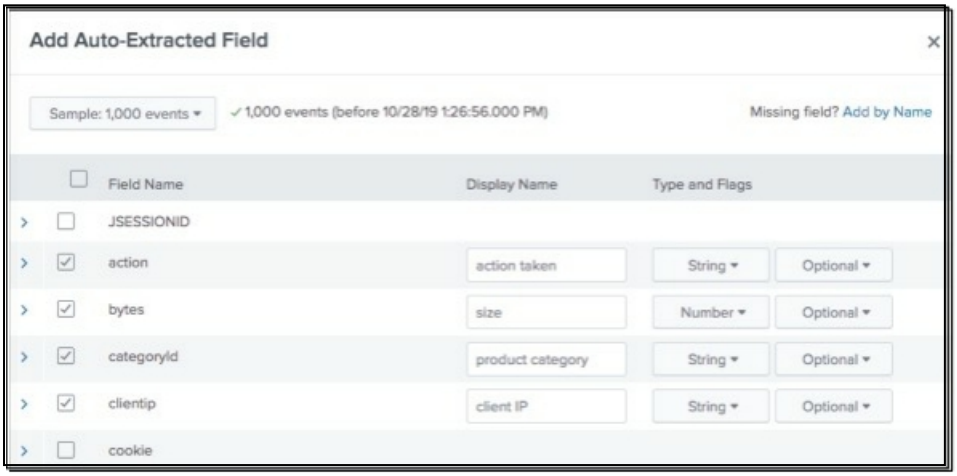
NOTE: Students are logged in with the power role and in this environment, power users have read-only permissions. Therefore, students can only create data models in the default Search & Reporting app, not in the CLASS: Intermediate app.

5. Click **Create**.
6. Click **Add Dataset** and select Root Event.
7. In the **Dataset Name** field, type: Web requests.
8. In the **Constraints** field, type: index=web sourcetype=access_combined
9. Click **Preview** to see a sampling of the events.
10. After the data has been verified, save the root event.

Task 2: Add auto-extracted fields.

11. Make sure the root Web requests dataset is selected.
12. Click **Add Field** and select **Auto-Extracted**. A dialog box opens and displays all auto-extracted fields.
13. Click the checkboxes to select the following fields, and rename them for pivot users as indicated:
    - action > action taken
    - bytes > size
    - categoryId > product category
    - clientip > client IP
    - date-mday > date-mday (use same name)
    - productId > product ID
    - product_name > product name
    - req_time > request time
    - status > status (use same name)

Example:

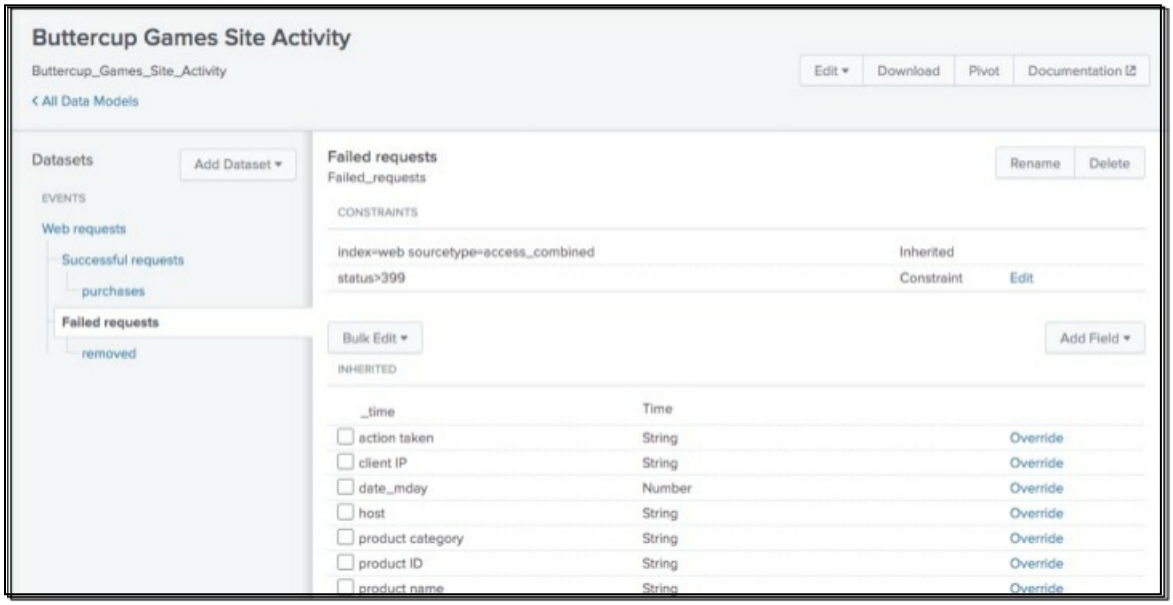


14. Click **Save**.

Task 3: Add two child events, one for actions that were successful and one for actions that failed.

15. Click **Add Dataset** and select Child.
16. In the **Dataset Name** field, type: Successful requests
17. In the **Additional Constraints** field, type: `status<400`
18. Click **Preview** to see a test sample of your results.
19. **Save** the child dataset.
20. Select the Successful requests dataset. Add a child dataset called **purchases** with an **Additional Constraints** value of `action=purchase productId=*`. Preview your results, then click **Save**.
21. Select the Web requests event and add a child dataset named: Failed requests**.**
22. In the **Additional Constraints** field, type: `status>399`
23. Click **Preview** to receive a test sample of your results.
24. **Save** the child dataset.
25. Under the Failed requests dataset, add a child dataset named **removed** with an **Additional Constraints** value of `action=remove productId=*`. Remember to click **Save**.

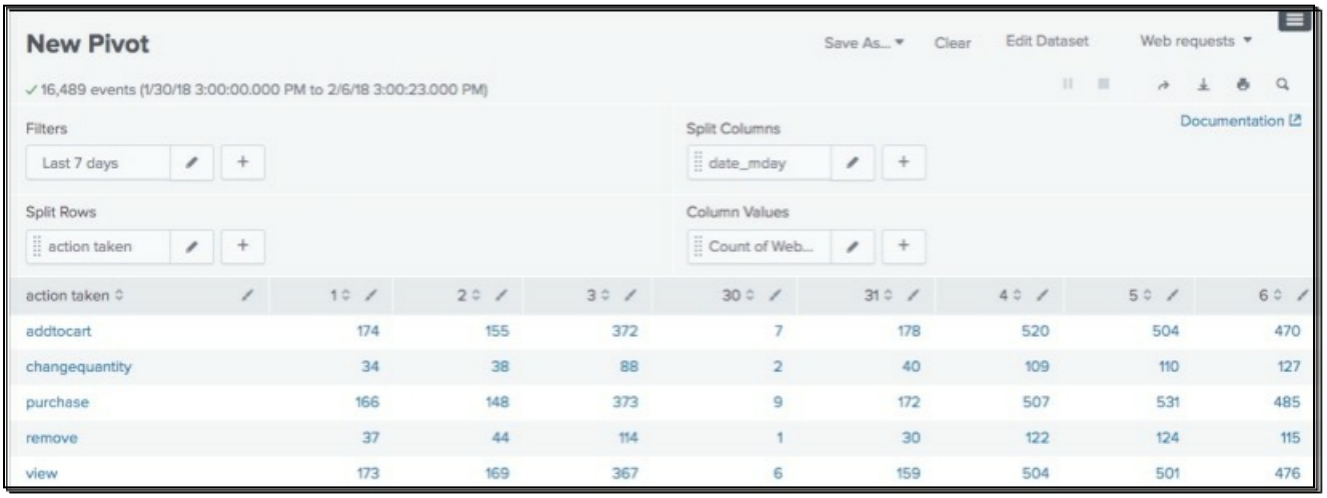
Results Example:



Task 4: Test your data model by creating a pivot.

26. Click **Pivot** in the upper right corner to test the d ata model.
27. Select the Web requests dataset**.**
28. In the **New Pivot** window, change the following:
    - Filter on the Last 7 days
    - Split Rows by action taken and click **Add To Table**
    - Split Columns by date_mday and click **Add To Table**

Results Example:



action taken	1	2	3	30	31	4	5	6
addtocart	174	155	372	7	178	520	504	470
changequantity	34	38	88	2	40	109	110	127
purchase	166	148	373	9	172	507	531	485
remove	37	44	114	1	30	122	124	115
view	173	169	367	6	159	504	501	476

Task 5: Add a field that uses an eval expression. The eval expression will display events chronologically by date and day of the week.

29. Select Edit Dataset.
30. Make sure Web requests is selected.

31. From the **Add Field** dropdown, select **Eval Expression**.
32. In the **Eval Expression** field, type: strftime(_time,"%m-%d %A")

NOTE: `strftime` is a function that converts epoch time to a readable format. You'll learn more about it in Splunk Fundamentals 3.

33. For **Field Name**, type: day
34. For **Display Name**, type: day
35. Click **Preview** to verify your eval expression returns results.
36. **Save** the eval expression.

Task 6: Verify the eval expression works as expected by using Pivot to create a dashboard.

37. Click **Pivot**.
38. Select the Web requests dataset.
39. Change the time filter to the **Last 7 days**.
40. **Split Rows** by action taken.
41. Click Add To Table.
42. Split Columns by day.
43. Click Add To Table.
44. Click Save As and select Dashboard Panel .
45. For **Dashboard Title**, type: Weekly Website Activity
46. For **Panel Title**, type: Shopping cart activity by day
47. Click **Save**.

48. Click **View Dashboard**. You should see the web requests categorized and counted by day.

Results Example:

Weekly Website Activity

Edit | Export | ...

Shopping cart activity by day

action taken	10-21 Monday	10-22 Tuesday	10-23 Wednesday	10-24 Thursday	10-25 Friday	10-26 Saturday	10-27 Sunday	10-28 Monday
addtocart	1054	2150	2071	2081	2171	2078	2102	1079
changequantity	87	188	170	162	161	177	167	93
purchase	1707	3498	3382	3475	3586	3507	3457	1776
remove	79	156	170	160	167	162	191	85
view	252	479	498	522	457	498	455	254

Task 7: Add fields from a lookup. The lookup table will provide descriptions of status codes.

49. Verify that you are still in the **Search & Reporting** app. If necessary, click the dropdown list next to the **splunk>** logo at the top left of the window and choose **App: Search & Reporting**.
50. Navigate to Settings > Data models.
51. Select the Buttercup Games Site Activity data model.

52. Make sure the Web requests root dataset is selected.
53. Click **Add Field** and select **Lookup**.
54. From the **Lookup Table** dropdown list, select **http_status_lookup**.
55. For the **Input** section in the **Field in Lookup** dropdown, select **code**.
56. From the **Field in Dataset** dropdown**,** select **status**. This maps the `status` field in your indexed data to the `code` column in the lookup table.
57. For the lookup **Output** section in the **Field in Lookup** field, check the **description** checkbox.
58. In the **Display Name** field, type: status description
59. Click the **Preview** button. You should see a **description** column in the results.
60. Click **Save**.

Task 8: Verify the lookup works properly by creating a Pivot report .

61. Click **Pivot**.
62. Select the **Web requests** dataset.
63. Change the Filter to **Last 7 days**.
64. From **Split Rows**, add the status description attribute and click **Add To Table**.
65. Click the + button to split by another row and add the **status** attribute. Click **Add To Table**.

NOTE: This is a double row split, not a column split.

Results Example:

status description	status	Count of Web requests
Bad Request.	400	204
Forbidden.	403	56
HTTP Version Not Supported.	505	146
Internal Server Error.	500	170
Not Acceptable.	406	201
Not Found.	404	192
OK.	200	11119
Request Timeout.	408	192
Service Unavailable.	503	261

66. Split Columns by day and click Add To Table.
67. Click Save As and select Dashboard Panel .
68. Select Existing Dashboard and select Weekly Website Activity.
69. For the **Panel Title**, type: Web requests summary
70. Click **Save**.
71. Click View Dashboard.

Results Example:

Weekly Website Activity

Edit | Export | ...

Shopping cart activity by day

action taken	10-21 Monday	10-22 Tuesday	10-23 Wednesday	10-24 Thursday	10-25 Friday	10-26 Saturday	10-27 Sunday	10-28 Monday
addtocart	1054	2150	2071	2081	2171	2078	2102	1087
changequantity	87	188	170	162	161	177	167	94
purchase	1707	3498	3382	3475	3586	3507	3457	1792
remove	79	156	170	160	167	162	191	87
view	252	479	498	522	457	498	455	255

Web requests summary

status description	status	10-21 Monday	10-22 Tuesday	10-23 Wednesday	10-24 Thursday	10-25 Friday	10-26 Saturday	10-27 Sunday	10-28 Monday
Bad Request.	400	63	90	108	95	103	104	96	49
Forbidden.	403	13	31	44	41	43	28	36	15
HTTP Version Not Supported.	505	24	50	66	65	60	71	71	31
Internal Server Error.	500	41	104	91	91	102	98	87	51
Not Acceptable.	406	39	92	102	109	104	90	98	51
Not Found.	404	52	99	107	109	91	82	85	50
OK.	200	4569	9264	9061	9244	9478	9339	9212	4853
Request Timeout.	408	55	88	107	103	90	92	96	49
Service Unavailable.	503	119	234	232	237	244	215	219	106