Lab Exercise 13: 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.

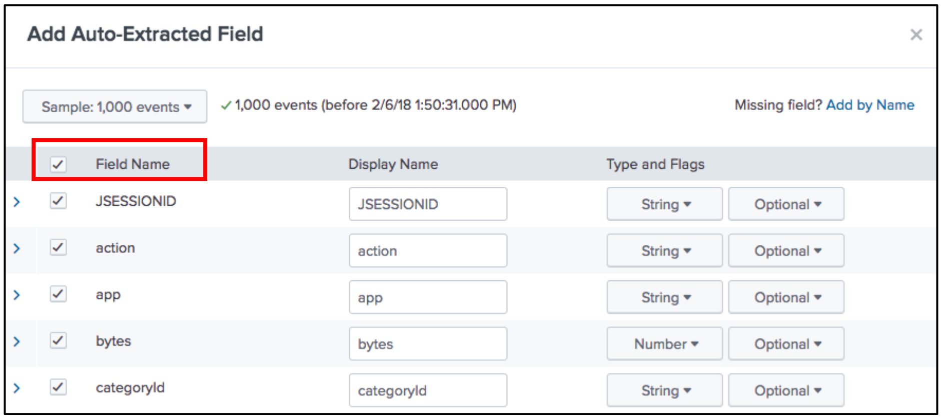
Task 1: Use Instant Pivot to create the Web Requests root event.

1. Search for index=web sourcetype=access_combined.
2. Select the **Statistics** tab, then click **Pivot.**
3. In the **Fields** dialog, select **Selected Fields**, then click **OK**. The Pivot interface will open.
4. From the **Save as** menu, select **Report**.
5. In the Title and Model Title fields, type: Buttercup Games Site Activity
6. Click **Save.** In the **Your Report Has Been Created** dialog, select **Edit Datasets.** The Data Model editor displays.
7. Use the **Rename** button and rename the Dataset: Web requests

Task 2: Add auto-extracted fields.

8. Make sure the root Web requests dataset is selected.
9. Click **Add Field** and select **Auto-Extracted**. A dialog box opens and displays all auto-extracted fields.
10. Select all fields by checking the **Field Name** checkbox. Selecting this box selects all auto-extracted fields.

Example:



Add Auto-Extracted Field ×

Sample: 1,000 events ▾ ✓1,000 events (before 2/6/18 1:50:31.000 PM) Missing field? Add by Name

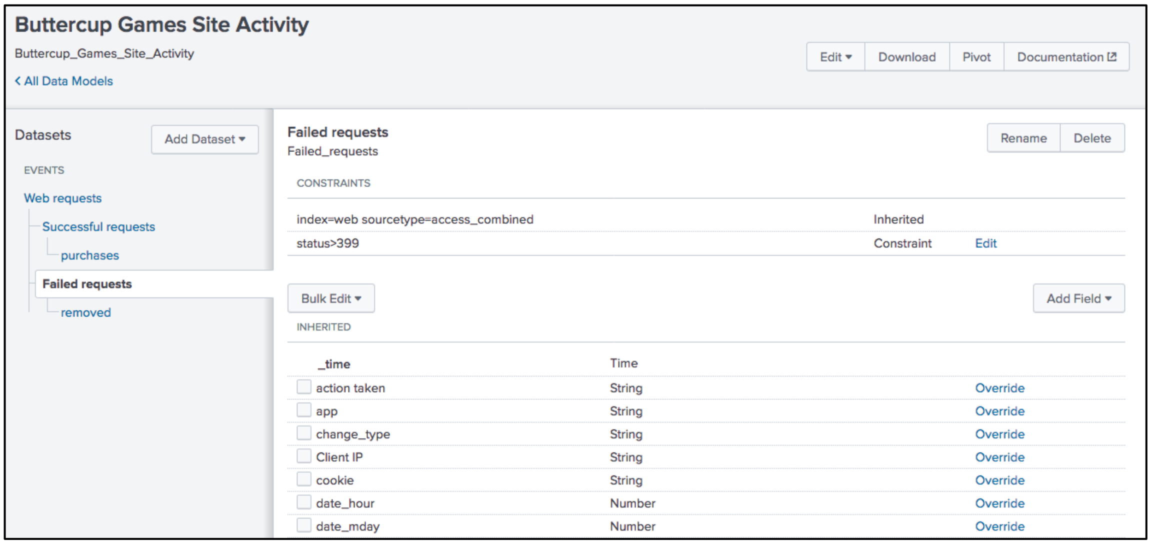
	☑	Field Name	Display Name	Type and Flags	
›	☑	JSESSIONID	JSESSIONID	String ▾	Optional ▾
›	☑	action	action	String ▾	Optional ▾
›	☑	app	app	String ▾	Optional ▾
›	☑	bytes	bytes	Number ▾	Optional ▾
›	☑	categoryId	categoryId	String ▾	Optional ▾

11. Rename the following fields for pivot users:
    - action > action taken
    - bytes > size
    - categoryId > product category
    - clientip > client IP
    - productId > product ID
    - product_name > product name
    - req_time > request time
12. Click **Save**.

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

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



Buttercup Games Site Activity
Buttercup_Games_Site_Activity
< All Data Models

Datasets

EVENTS
- Web requests
  - Successful requests
    - purchases
  - Failed requests
    - removed

Failed requests
Failed_requests

CONSTRAINTS

index=web sourcetype=access_combined	Inherited	
status>399	Constraint	Edit

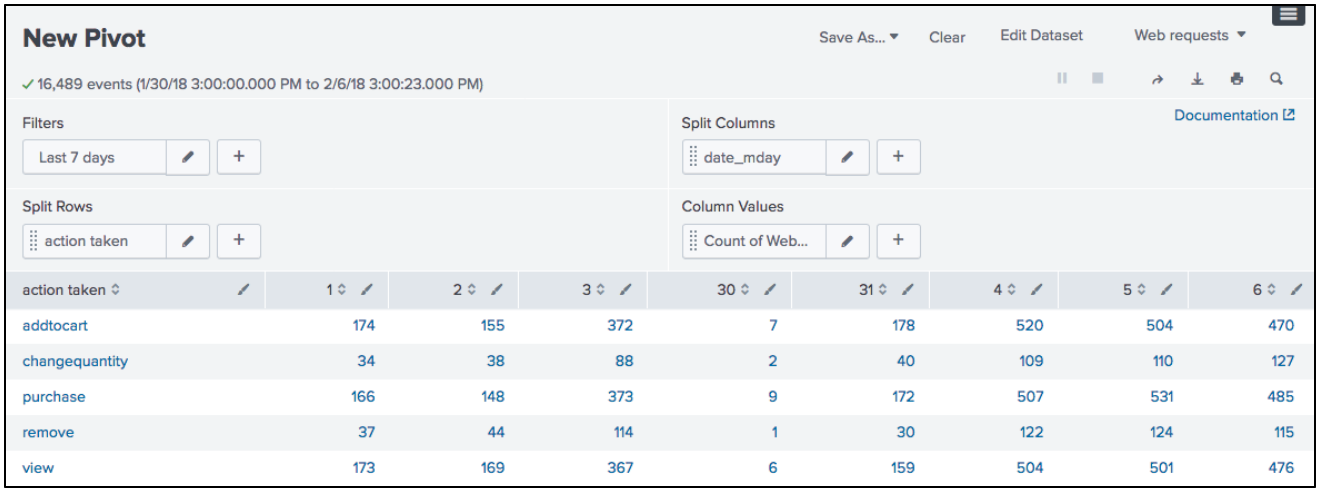
INHERITED

_time	Time	
□ action taken	String	Override
□ app	String	Override
□ change_type	String	Override
□ Client IP	String	Override
□ cookie	String	Override
□ date_hour	Number	Override
□ date_mday	Number	Override

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

24. Click **Pivot** in the upper right-hand corner to test the data model.
25. Select the Web requests dataset**.**
26. 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:



New Pivot

✓ 16,489 events (1/30/18 3:00:00.000 PM to 2/6/18 3:00:23.000 PM)

Filters: Last 7 days
Split Columns: date_mday
Split Rows: action taken
Column Values: Count of Web...

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.

27. Select Edit Dataset.

28. Make sure Web requests is selected.
29. From the **Add Field** dropdown, select **Eval Expression**.
30. In the **Eval Expression** field, type: strftime(_time,"%m-%d %A")

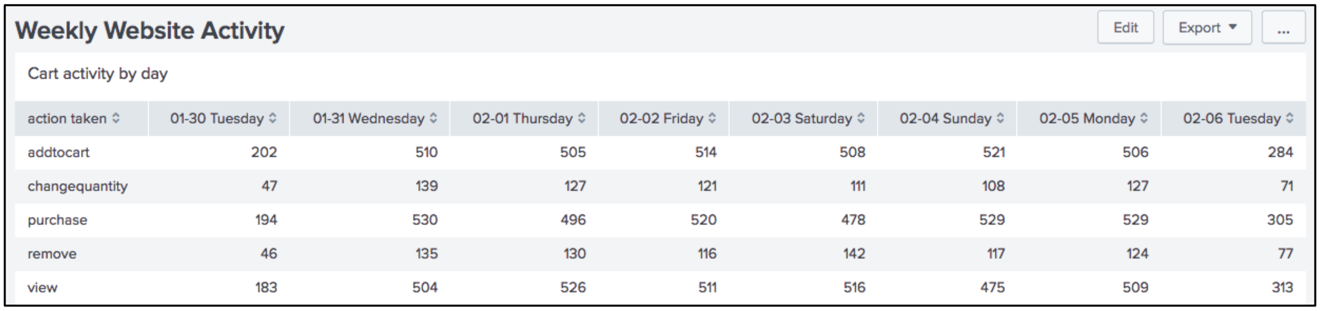
> **NOTE:** strftime is a method that converts epoch time to a readable format.

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

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

35. Click **Pivot**.
36. Select the Web requests dataset.
37. Change the time filter to the **Last 7 days**.
38. **Split Rows** by action taken.
39. Click Add To Table.
40. Split Columns by day.
41. Click Add To Table.
42. Click Save As and select Dashboard Panel.
43. For **Dashboard Title**, type: Weekly Website Activity
44. For **Panel Title**, type: Cart activity by day
45. Click **Save**.
46. Click **View Dashboard**. You should see the web requests categorized and counted by day.

Results Example:



Weekly Website Activity

Cart activity by day

action taken	01-30 Tuesday	01-31 Wednesday	02-01 Thursday	02-02 Friday	02-03 Saturday	02-04 Sunday	02-05 Monday	02-06 Tuesday
addtocart	202	510	505	514	508	521	506	284
changequantity	47	139	127	121	111	108	127	71
purchase	194	530	496	520	478	529	529	305
remove	46	135	130	116	142	117	124	77
view	183	504	526	511	516	475	509	313

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

47. 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**.
48. Navigate to Settings > Data models.
49. Select the Buttercup Games Site Activity data model.

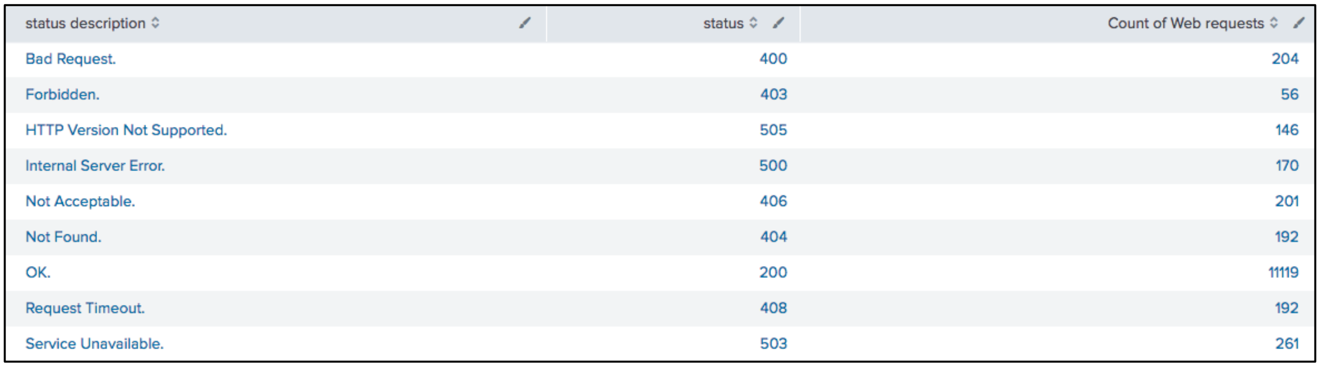
50. Make sure the Web requests root dataset is selected.
51. Click **Add Field** and select **Lookup**.
52. From the **Lookup Table** dropdown list, select **http_status_lookup**.
53. For the **Input** section in the **Field in Lookup** dropdown, select **code**.
54. From the **Field in Dataset** dropdown**,**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

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

59. Click **Pivot**.
60. Select the **Web requests** dataset.
61. Change the Filter to **Last 7 days**.
62. From **Split Rows**, add the status description attribute and click **Add To Table**.
63. 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.

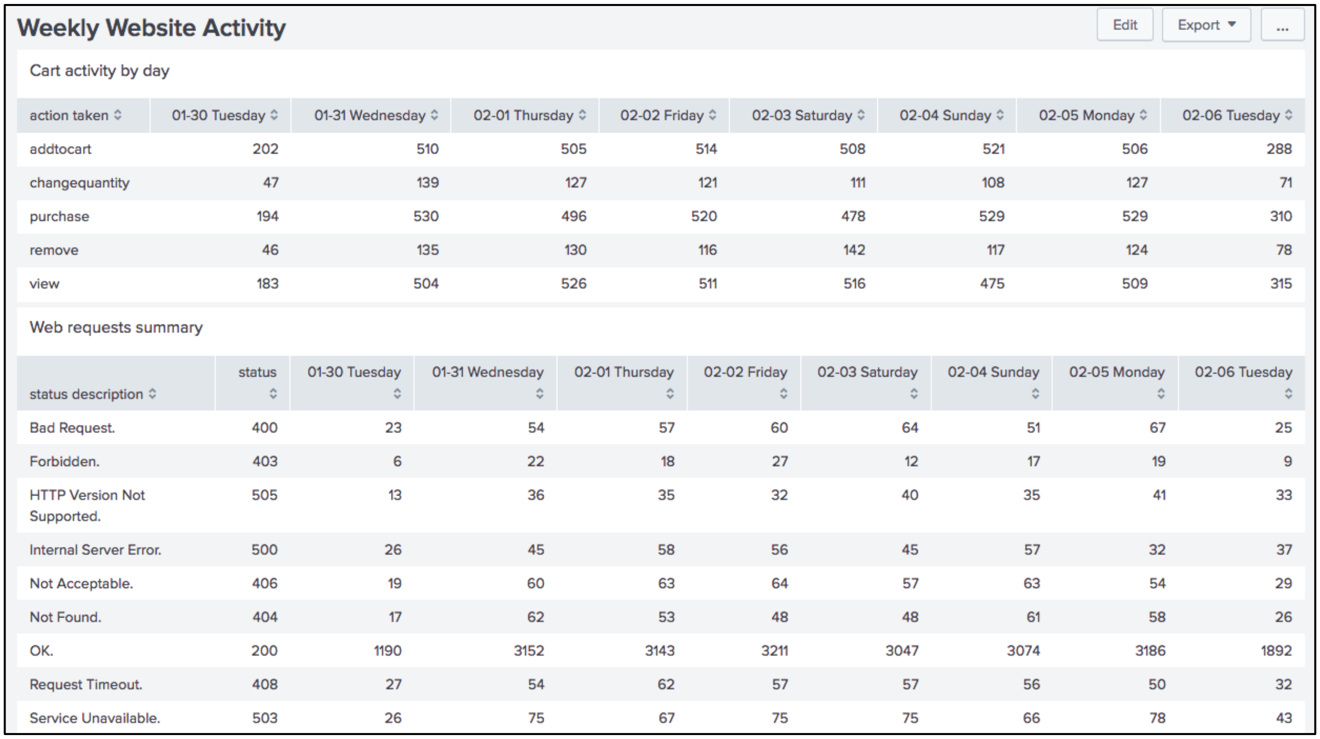
Results Example:



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

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

Results Example:



Weekly Website Activity

Cart activity by day

action taken ⇕	01-30 Tuesday ⇕	01-31 Wednesday ⇕	02-01 Thursday ⇕	02-02 Friday ⇕	02-03 Saturday ⇕	02-04 Sunday ⇕	02-05 Monday ⇕	02-06 Tuesday ⇕
addtocart	202	510	505	514	508	521	506	288
changequantity	47	139	127	121	111	108	127	71
purchase	194	530	496	520	478	529	529	310
remove	46	135	130	116	142	117	124	78
view	183	504	526	511	516	475	509	315

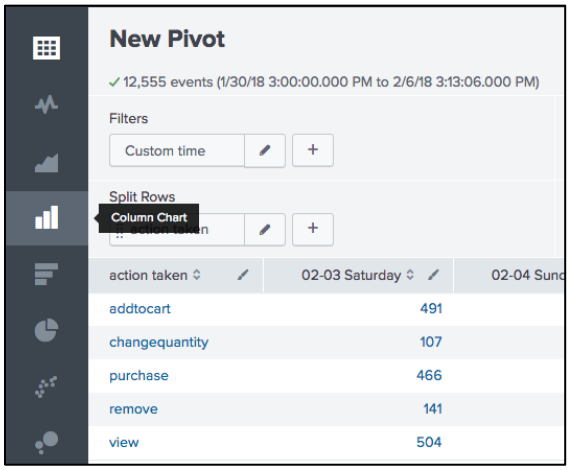
Web requests summary

status description ⇕	status ⇕	01-30 Tuesday ⇕	01-31 Wednesday ⇕	02-01 Thursday ⇕	02-02 Friday ⇕	02-03 Saturday ⇕	02-04 Sunday ⇕	02-05 Monday ⇕	02-06 Tuesday ⇕
Bad Request.	400	23	54	57	60	64	51	67	25
Forbidden.	403	6	22	18	27	12	17	19	9
HTTP Version Not Supported.	505	13	36	35	32	40	35	41	33
Internal Server Error.	500	26	45	58	56	45	57	32	37
Not Acceptable.	406	19	60	63	64	57	63	54	29
Not Found.	404	17	62	53	48	48	61	58	26
OK.	200	1190	3152	3143	3211	3047	3074	3186	1892
Request Timeout.	408	27	54	62	57	57	56	50	32
Service Unavailable.	503	26	75	67	75	75	66	78	43

Task 9: From the pivot editor, add a filter to narrow your results.

1. Hover your mouse in the lower right corner of the **Cart Activity by day** dashboard panel. Click the **Open in Pivot** icon ⟲.
2. Refine your search results by selecting the **Column chart** icon from the table formats on the left.

Results Examples:



New Pivot

✓ 12,555 events (1/30/18 3:00:00.000 PM to 2/6/18 3:13:06.000 PM)

Filters

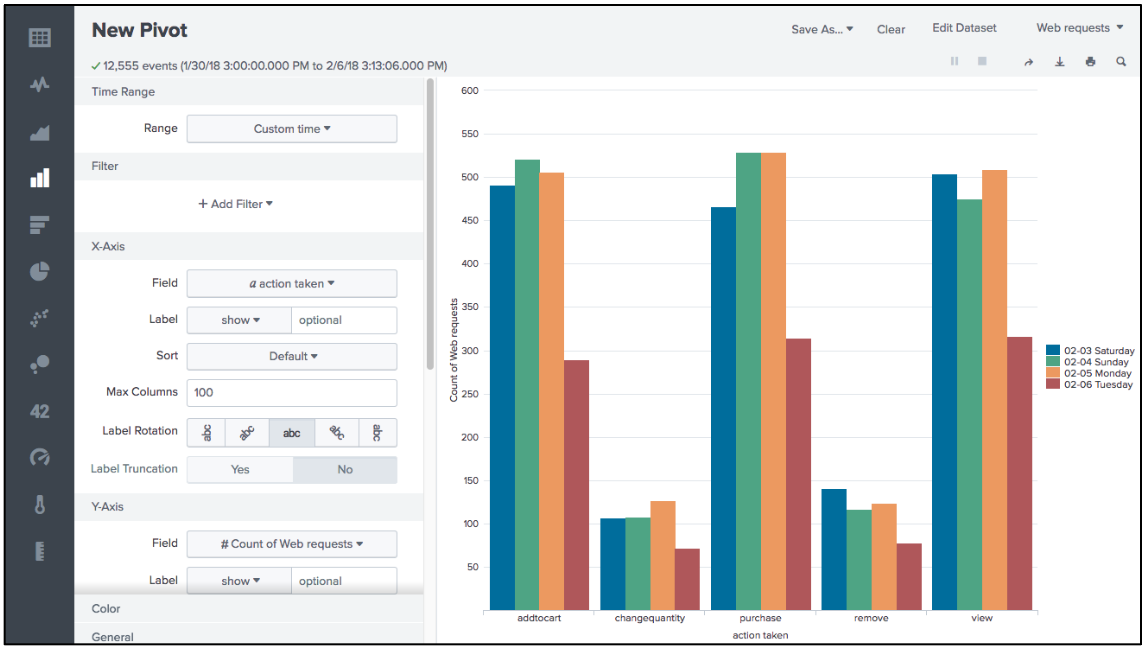
Custom time

Split Rows

Column Chart

action taken

action taken	02-03 Saturday	02-04 Sund
addtocart	491	
changequantity	107	
purchase	466	
remove	141	
view	504	



New Pivot

✓ 12,555 events (1/30/18 3:00:00.000 PM to 2/6/18 3:13:06.000 PM)

Time Range

Range: Custom time

Filter

+ Add Filter

X-Axis

Field: a action taken

Label: show, optional

Sort: Default

Max Columns: 100

Label Rotation: abc

Label Truncation: Yes / No

Y-Axis

Field: # Count of Web requests

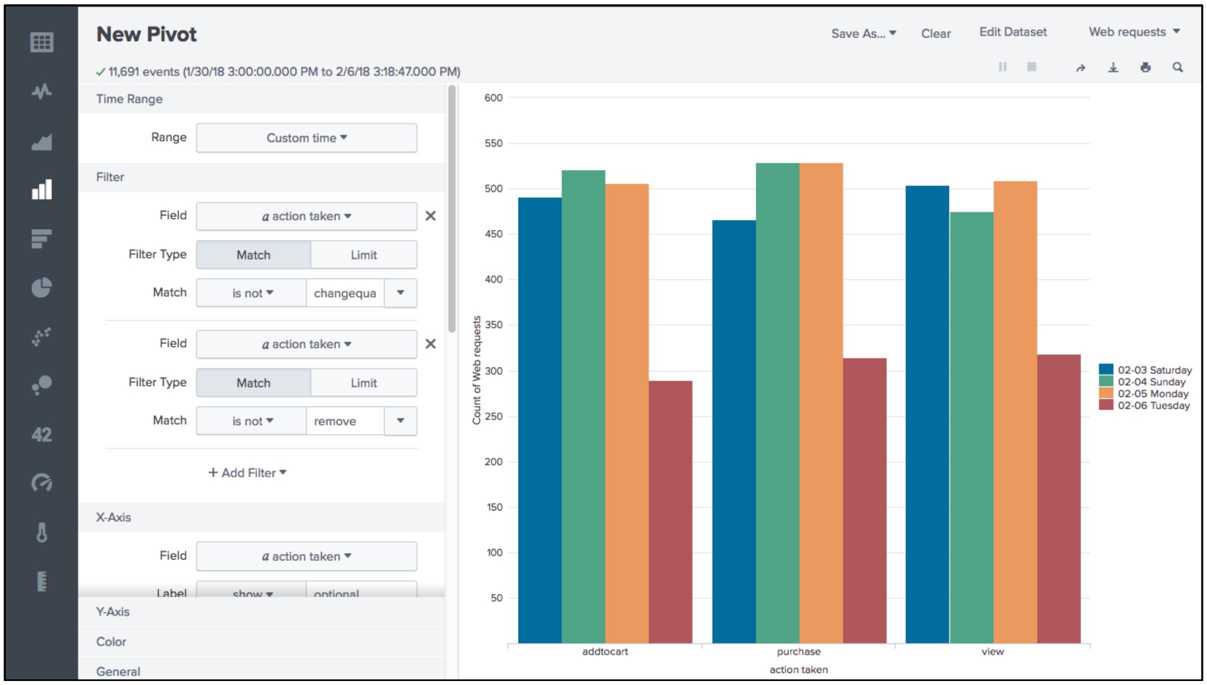
Label: show, optional

Color

General

3. Click Add Filter and choose action taken.
4. For Filter Type, select **Match**.
5. For **Match**, change the operator to **is not**, then select **changequantity**.
6. Add another filter and again choose **action taken**.
7. For the **Filter Type**, select **Match**.
8. For **Match**, change the operator to **is not** and then select **remove**.

Results Example:



New Pivot

✓ 11,691 events (1/30/18 3:00:00.000 PM to 2/6/18 3:18:47.000 PM)

Time Range

Range: Custom time

Filter

Field: a action taken

Filter Type: Match | Limit

Match: is not | changequa

Field: a action taken

Filter Type: Match | Limit

Match: is not | remove

+ Add Filter

X-Axis

Field: a action taken

Label: show | optional

Y-Axis

Color

General

9. Click Save As and select Dashboard Panel.
10. Save to the **Weekly Website Activity** dashboard.
11. For **Panel Title**, type: Add purchase view
12. **Save** and **view** your dashboard.
13. Rearrange the panels to your liking and admire your work!