splunk>

Lab Exercise 6 – Correlating Events

Description

Use the transaction command to correlate events.

Steps

Task 1: Analyze transactions in the online store during the last 60 minutes.

Final Results Example:

JSESSIONID	clientip	action
SD7SL8FF6ADFF4957	86.9.190.90	addtocart purchase view
SD6SL9FF5ADFF4961	81.18.148.190	addtocart purchase view
SD2SL10FF2ADFF4963	194.215.205.19	addtocart purchase remove

1. Search for all events in the online store [`access_combined`] during the **last 60 minutes**.

```
index=web sourcetype=access_combined
```

2. Display a table that shows the `_time`, `clientip`, `JSESSIONID`, and the `action`. Note that the actions are listed in reverse chronological order (most to least recent.)

```
index=web sourcetype=access_combined
| table _time, clientip, JSESSIONID, action
```

Results Example:

_time	clientip	JSESSIONID	action
2018-02-05 12:40:03	211.166.11.101	SD0SL3FF5ADFF4950	
2018-02-05 12:39:45	211.166.11.101	SD0SL3FF5ADFF4950	
2018-02-05 12:37:35	211.245.24.3	SD6SL7FF4ADFF4956	
2018-02-05 12:37:18	211.245.24.3	SD6SL7FF4ADFF4956	addtocart
2018-02-05 12:28:05	91.199.80.24	SD1SL10FF7ADFF4953	
2018-02-05 12:27:55	91.199.80.24	SD1SL10FF7ADFF4953	purchase

3. Modify your search to only include events with a value in the `action` field.

```
index=web sourcetype=access_combined action=*
| table _time, clientip, JSESSIONID, action
```

Results Example:

_time	clientip	JSESSIONID	action
2018-02-05 12:44:02	195.2.240.99	SD0SL6FF5ADFF4959	view
2018-02-05 12:43:51	195.2.240.99	SD0SL6FF5ADFF4959	addtocart
2018-02-05 12:37:18	211.245.24.3	SD6SL7FF4ADFF4956	addtocart
2018-02-05 12:27:55	91.199.80.24	SD1SL10FF7ADFF4953	purchase
2018-02-05 12:27:55	91.199.80.24	SD1SL10FF7ADFF4953	purchase

4. Remove the `table` command and all the arguments being passed to it. Using the `transaction` command, create groups of transactions based on the `JSESSIONID` field.

```
index=web sourcetype=access_combined action=*
| transaction JSESSIONID
```

Results Example:

i	Time	Event
>	2/5/18 12:46:10.000 PM	194.215.205.19 - - [05/Feb/2018:20:46:10] "POST /cart.do?action=addtocart&itemId=EST-19&productId=PZ-SG-G05&JSESSIONID=SD2SL10FF2ADFF4963 HTTP 1.1" 200 3407 "http://www.buttercupgames.com/product.screen?productId=PZ-SG-G05" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 647 194.215.205.19 - - [05/Feb/2018:20:46:14] "POST /cart.do?action=purchase&itemId=EST-19&JSESSIONID=SD2SL10FF2ADFF4963 HTTP 1.1" 200 3746 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-19&categoryId=STRATEGY&productId=PZ-SG-G05" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 936 194.215.205.19 - - [05/Feb/2018:20:46:14] "POST /cart/success.do?JSESSIONID=SD2SL10FF2ADFF4963 HTTP 1.1" 200 3014 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 911 194.215.205.19 - - [05/Feb/2018:20:46:23] "POST /cart.do?action=addtocart&itemId=EST-15&productId=MB-AG-T01&JSESSIONID=SD2SL10FF2ADFF4963 HTTP 1.1" 200 3572 "http://www.buttercupgames.com/product.screen?productId=MB-AG-T01" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 420 194.215.205.19 - - [05/Feb/2018:20:46:25] "POST /cart.do?action=purchase&itemId=EST-15&JSESSIONID=SD2SL10FF2ADFF4963 HTTP 1.1" 200 2743 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-15&categoryId=TEE&productId=MB-AG-T01" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 830 Show all 9 lines host = www1 source = /opt/log/www1/access.log sourcetype = access_combined

5. Modify your search to display the transactions in a table. Include `JSESSIONID`, `clientip`, and `action`.

```
index=web sourcetype=access_combined action=*
| transaction JSESSIONID
| table JSESSIONID, clientip, action
```

Results Example:

JSESSIONID	clientip	action
SD6SL9FF5ADFF4961	81.18.148.190	addtocart purchase view
SD8SL6FF5ADFF4954	59.162.167.100	changequantity view
SD2SL10FF2ADFF4963	194.215.205.19	addtocart purchase remove
SD0SL6FF5ADFF4959	195.2.240.99	addtocart remove view

NOTE: By default, the values in the action column are ordered by an alphabetic sort discounting duplicates.

6. View only transactions that contain at least one purchase event. Use the `search` command to find transactions containing a purchase.

NOTE: The search command must be downstream from the transaction command.

```
index=web sourcetype=access_combined action=*
| transaction JSESSIONID
| table JSESSIONID, clientip, action
| search action=purchase
```

Results Example:

JSESSIONID	clientip	action
SD7SL8FF6ADFF4957	86.9.190.90	addtocart purchase view
SD6SL9FF5ADFF4961	81.18.148.190	addtocart purchase view
SD2SL10FF2ADFF4963	194.215.205.19	addtocart purchase remove

7. Save your search as report, **L5S1**. Click **View.**

Task 2: Display the online store purchase transactions lasting more than one minute and include the number of events in each transaction.

Final Results Example:

JSESSIONID	clientip	action	durationMinutes	eventcount
SD7SL8FF6ADFF4957	86.9.190.90	addtocart purchase view	1.3	11
SD1SL10FF7ADFF4953	91.199.80.24	addtocart purchase remove view	2.7	13
SD3SL8FF9ADFF4955	195.69.252.22	addtocart purchase remove view	1.4	9

8. Select `Open in Search` from the `Edit` menu.
9. Set the search mode to **Verbose Mode**, which will re-execute your search.
10. Click the Events tab. Notice the new fields generated by the `transaction` command: `duration` and `eventcount`.

11. Modify your search to add the `duration` and `eventcount` fields to your table after the `clientip` field. Run your search in **Smart Mode**.

```
index=web sourcetype=access_combined action=*
| transaction JSESSIONID
| table JSESSIONID, clientip, duration, eventcount, action
| search action=purchase
```

Results Example:

JSESSIONID	clientip	duration	eventcount	action
SD7SL8FF6ADFF4957	86.9.190.90	77	11	addtocart purchase view
SD6SL9FF5ADFF4961	81.18.148.190	32	5	addtocart purchase view
SD2SL10FF2ADFF4963	194.215.205.19	46	9	addtocart purchase remove

12. Use `eval` to create a new field named `durationMinutes`, which is the rounded value of `duration` divided by 60. Round to one decimal place.

```
index=web sourcetype=access_combined action=*
| transaction JSESSIONID
| table JSESSIONID, clientip, duration, eventcount, action
| search action=purchase
| eval durationMinutes=round(duration/60,1)
```

Results Example:

JSESSIONID	clientip	duration	eventcount	action	durationMinutes
SD7SL8FF6ADFF4957	86.9.190.90	77	11	addtocart purchase view	1.3
SD6SL9FF5ADFF4961	81.18.148.190	32	5	addtocart purchase view	0.5
SD2SL10FF2ADFF4963	194.215.205.19	46	9	addtocart purchase remove	0.8

13. Modify your search to find data where the `durationMinutes` is greater than one minute. Also, remove the `duration` field from the table.

```
index=web sourcetype=access_combined action=*
| transaction JSESSIONID
| search action=purchase
| eval durationMinutes=round(duration/60,1)
| table JSESSIONID, clientip, action, durationMinutes, eventcount
| where durationMinutes > 1
```

Results Example:

JSESSIONID	clientip	action	durationMinutes	eventcount
SD7SL8FF6ADFF4957	86.9.190.90	addtocart purchase view	1.3	11
SD1SL10FF7ADFF4953	91.199.80.24	addtocart purchase remove view	2.7	13
SD3SL8FF9ADFF4955	195.69.252.22	addtocart purchase remove view	1.4	9

14. Save your search as report, **L5S2**.

Task 3: Search for online store transactions that begin with an `addtocart` action and end with a `purchase` action.

Final Results Example:

clientip	JSESSIONID	product_name	action	duration	eventcount	price
199.15.234.66	SD10SL10FF2ADFF4963	Dream Crusher	addtocart purchase	4	2	39.99
86.9.190.90	SD7SL8FF6ADFF4957	World of Cheese Tee	addtocart purchase	1	2	9.99
86.9.190.90	SD7SL8FF6ADFF4957	Holy Blade of Gouda	addtocart purchase	3	2	5.99

15. Search for all events from the online store [`access_combined`] in the **last 60 minutes** and correlate the events based on `clientip`.

```
index=web sourcetype=access_combined
| transaction clientip
```

16. Use the `startswith` and `endswith` options of the `transaction` command to display transactions that begin with an `addtocart` action and end with a `purchase` action.

```
index=web sourcetype=access_combined
| transaction clientip startswith=action="addtocart" endswith=action="purchase"
```

17. In a table, display clientip, JSESSIONID, product_name, action, duration, eventcount, and price.

```
index=web sourcetype=access_combined
| transaction clientip startswith=action="addtocart" endswith=action="purchase"
| table clientip, JSESSIONID, product_name, action, duration, eventcount, price
```

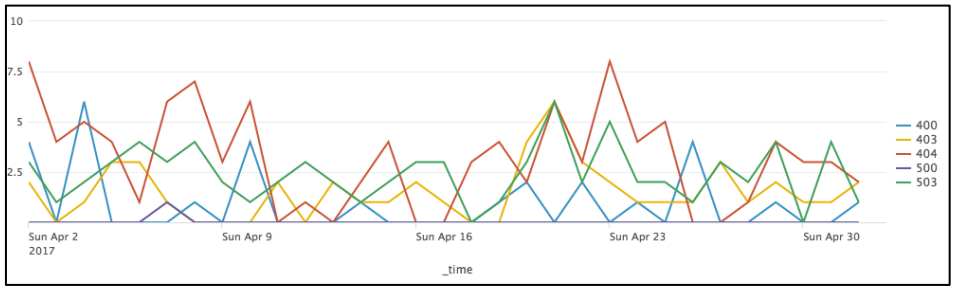
Results Example:

clientip	JSESSIONID	product_name	action	duration	eventcount	price
199.15.234.66	SD10SL10FF2ADFF4963	Dream Crusher	addtocart purchase	4	2	39.99
86.9.190.90	SD7SL8FF6ADFF4957	World of Cheese Tee	addtocart purchase	1	2	9.99
86.9.190.90	SD7SL8FF6ADFF4957	Holy Blade of Gouda	addtocart purchase	3	2	5.99

18. Save your search as report, **L5S3**.

Task 4: Report common HTTP status errors that occurred during the last 30 days on the online sales web servers and the internal web appliance within a proximity of 5 minutes or less. Only include days with more than 5 common errors.

Final Results Example:



19. Search HTTP status error events from the online sales web servers [`access_combined`] and the web appliance [`cisco_wsa_squid`] during the **last 30 days**. For best performance, limit extracted fields to only `sourcetype` and `status`.

```
(index=network sourcetype=cisco_wsa_squid) OR
(index=web sourcetype=access_combined) status>399
| fields sourcetype, status
```

20. Create transactions based on `status` field values and limit the span to 5 minutes.

NOTE: If you do not see results, increase the `maxspan` value.

```
(index=network sourcetype=cisco_wsa_squid) OR
(index=web sourcetype=access_combined) status>399
| fields sourcetype, status
| transaction status maxspan=5m
```

21. Limit the results to only transactions that contain at least one event from each sourcetype.

```
(index=network sourcetype=cisco_wsa_squid) OR (index=web sourcetype=access_combined)
status>399
| fields sourcetype, status
| transaction status maxspan=5m
| search sourcetype=access_combined AND sourcetype=cisco_wsa_squid
```

22. Use `timechart` to count events by `status`.

```
(index=network sourcetype=cisco_wsa_squid) OR
(index=web sourcetype=access_combined) status>399
| fields sourcetype, status
| transaction status maxspan=5m
| search sourcetype=access_combined AND sourcetype=cisco_wsa_squid
| timechart count by status
```

Results Example:

_time	400	403	404	503
2018-01-06	3	2	3	0
2018-01-07	0	0	1	1
2018-01-08	0	6	3	3
2018-01-09	0	1	4	5

23. Discard rows that have fewer than 5 errors for all `status` values.
    Hint: Use `addtotals`.

```
(index=network sourcetype=cisco_wsa_squid) OR
(index=web sourcetype=access_combined) status>399
| fields sourcetype, status
| transaction status maxspan=5m
| search sourcetype=access_combined AND sourcetype=cisco_wsa_squid
| timechart count by status
| addtotals
| search Total>4
```

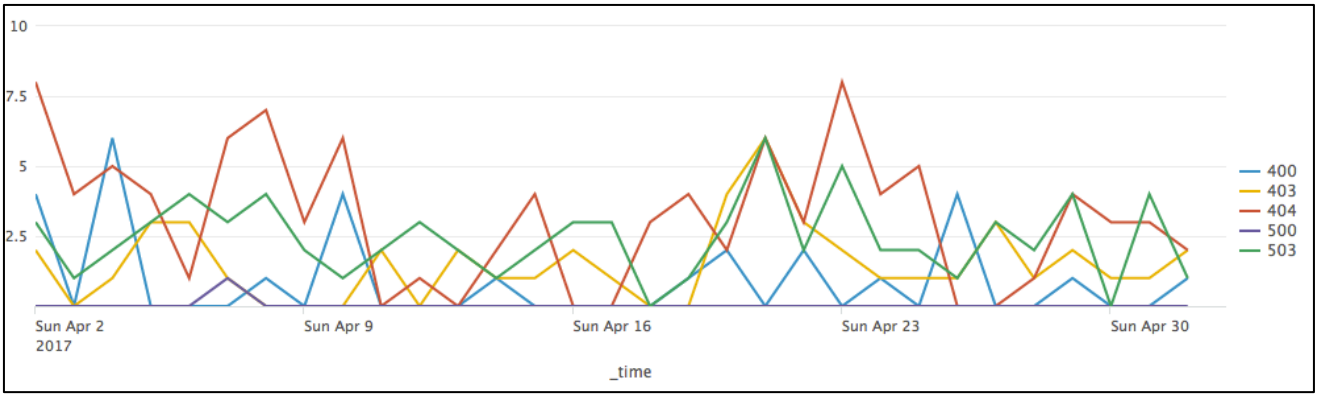
Results Example:

_time	400	403	404	503	Total
2018-01-06	3	2	3	0	8
2018-01-08	0	6	3	3	12
2018-01-09	0	1	4	5	10
2018-01-10	0	3	1	2	6

24. Remove the `Total` column and display the data as a **Line chart**.

```
(index=network sourcetype=cisco_wsa_squid) OR
(index=web sourcetype=access_combined) status>399
| fields sourcetype, status
| transaction status maxspan=5m
| search sourcetype=access_combined AND sourcetype=cisco_wsa_squid
| timechart count by status
| addtotals
| search Total>4
| fields - Total
```

Results Example:



25. Save your search as report, **L5C1**.
26. Optionally, for this line chart, set **Multi-series Mode** to **Yes**. Observe the change in how the lines are represented.

Hint: It's one of the **Format** options on the **General** tab.