

Splunk Fundamentals 1 Lab Exercises

Lab typographical conventions:

[sourcetype=db_audit] **OR** [cs_mime_type] indicates either a source type or the name of a field.

NOTE: Lab work will be done on your personal computer or virtual machine, no lab environment is provided. We suggest you **DO NOT** do the lab work on your production environment.

The lab instructions refer to these source types by the types of data they represent:

Type	Sourcetype	Fields of interest
Web Application	access_combined_wcookie	action, bytes, categoryId, clientip, itemId, JSESSIONID, productId, referer, referer_domain, status, useragent, file
Database	db_audit	Command, Duration, Type
Web server	linux_secure	COMMAND, PWD, pid, process

Lab Module 8 – Basic Commands

NOTE: Now that you understand the basics of searching in Splunk, we will make labs a little more challenging. This lab document has two sections. The first section includes the instructions without answers. The second section includes instructions with the expected search string (answer) in **red**.

Description

In this lab, you will be using some of the common Splunk commands including fields, table, rename and dedup.

Steps

Scenario: The Marketing team tracks all user sessions related to marketing campaigns. It would like a report of all user sessions that include purchase actions so that it can put a value on the different campaigns it's running.

Task 1: Search for the requested data.

1. Navigate to the Search view. (If you are in the **Home** app, click **Search & Reporting** from the column on the left side of the screen. You can also access the Search view by clicking the **Search** menu option on the green bar at the top of the screen.)

NOTE: For this course, you will be searching across all time using the main index. This is NOT a best practice in a production environment, but needed for these labs due to the nature of the limited dataset.

2. Enter a search that returns all web application events that include a purchase action with a web status of 200.

Results Example:

Hide Fields	All Fields	<i>i</i>	Time	Event
Selected Fields		>	4/30/17 11:57:14.000 PM	109.169.32.135 - - [30/Apr/2017:23:57:14] "POST /cart/success.do?JSESSIONID=SD1SL7FF6ADFF89341&productId=FI-AG-G08 HTTP 1.1" 200 3767 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
Interesting Fields		>	4/30/17 11:57:13.000 PM	109.169.32.135 - - [30/Apr/2017:23:57:13] "POST /success.do?action=purchase&categoryId=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP 1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
		>	4/30/17 11:53:43.000 PM	198.35.3.23 - - [30/Apr/2017:23:53:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 200 2915 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
		>	4/30/17 11:51:56.000 PM	198.35.3.23 - - [30/Apr/2017:23:51:56] "POST /cart/success.do?JSESSIONID=SD8SL8FF6ADFF4957&productId=DC-SG-G02 HTTP 1.1" 200 594 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
		>	4/30/17 11:51:56.000 PM	198.35.3.23 - - [30/Apr/2017:23:51:56] "POST /success.do?action=purchase&categoryId=STRATEGY&productId=DC-SG-G02&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 200 2752 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
		>	4/30/17 11:50:48.000 PM	92.46.53.223 - - [30/Apr/2017:23:50:48] "POST /cart/success.do?JSESSIONID=SD2SL10FF6ADFF4955&productId=WC-SH-A01 HTTP 1.1" 200 816 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 231

3. Select the `file` field in the **Interesting Fields** list.

Results Example:



4. Notice that there are two different files that were returned from the web server. They are: `error.do` and `success.do`. Our web development team informs us that the `success.do` is served when the order is processed and `error.do` is served when there is an error with the information being processed.
5. The team is only looking for successful purchases, so change your search to only return those.

Results Example:

Hide Fields	All Fields	<i>i</i>	Time	Event
Selected Fields		>	4/30/17 11:57:14.000 PM	109.169.32.135 - - [30/Apr/2017:23:57:14] "POST /cart/success.do?JSESSIONID=SD1SL7FF6ADFF89341&productId=FI-AG-G08 HTTP 1.1" 200 3767 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
Interesting Fields		>	4/30/17 11:57:13.000 PM	109.169.32.135 - - [30/Apr/2017:23:57:13] "POST /success.do?action=purchase&categoryId=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP 1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
		>	4/30/17 11:53:43.000 PM	198.35.3.23 - - [30/Apr/2017:23:53:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 200 2915 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
		>	4/30/17 11:51:56.000 PM	198.35.3.23 - - [30/Apr/2017:23:51:56] "POST /cart/success.do?JSESSIONID=SD8SL8FF6ADFF4957&productId=DC-SG-G02 HTTP 1.1" 200 594 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie
		>	4/30/17 11:51:56.000 PM	198.35.3.23 - - [30/Apr/2017:23:51:56] "POST /success.do?action=purchase&categoryId=STRATEGY&productId=DC-SG-G02&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 200 2752 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie

6. You will see fields that do not matter to the team. Use the `fields` command to only return the `action`, `JSESSIONID` and `status` fields. Does your search run faster using the command?

Results Example:

Interesting Fields

`a action 1`
`a JSESSIONID 100+`
`# status 1`

7. The fields list looks cleaner, but seeing the events like this might still be confusing for the team.

Task 2: Put the data into an easy to read table.

8. Replace the `fields` command with the `table` command to display the data as a table. Results Example:

20 Per Page ▾			✓Format	Preview ▾	< Prev 1 2 3 4 5 6 7 8 9 ... Next >								
action	⌚	JSESSIONID	⌚									status	⌚
purchase		SD6SL5FF6ADFF89354										200	
purchase		SD6SL5FF6ADFF89354										200	
purchase		SD6SL5FF6ADFF89354										200	
purchase		SD6SL5FF6ADFF89354										200	

9. Change the order of the fields so that `JSESSIONID` is the first column.

Results Example:

20 Per Page ▾			✓Format	Preview ▾	< Prev 1 2 3 4 5 6 7 8 9 ... Next >								
JSESSIONID	⌚	action	⌚									status	⌚
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	

10. Session IDs are called "UserSessions" in the marketing data. Rename `JSESSIONID` so that your report matches the marketing data.

Results Example:

20 Per Page ▾			✓Format	Preview ▾	< Prev 1 2 3 4 5 6 7 8 9 ... Next >								
UserSessions	⌚	action	⌚									status	⌚
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	
SD6SL5FF6ADFF89354		purchase										200	

11. Sort `UserSessions` using the `sort` command.

12. Notice that some `UserSessions` values show up multiple times. Also notice the number of events returned on the **Statistics** tab.

13. Remove the `sort` command and use `dedup` to remove any identical session values.

Results Example:

20 Per Page ▾		Format	Preview ▾	◀ Prev	1	2	3	4	5	6	7	8	9	...	Next ▶
UserSessions		action	status												
SD6SL5FF6ADFF89354	purchase	200													
SD1SL7FF6ADFF89341	purchase	200													
SD3SL5FF3ADFF89564	purchase	200													
SD8SL5FF4ADFF89311	purchase	200													
SD6SL1FF6ADFF89561	purchase	200													
SD5SL9FF9ADFF89548	purchase	200													

14. How many events are now listed on the **Statistics** tab?

NOTE: As a best practice and for best performance, place dedup as early in the search as possible.

15. While having `action` and `status` fields displayed was nice for a sanity check of the data, the marketing team will not need to have these displayed. Remove them from your table display.

Results Example:

20 Per Page ▾		Format	Preview ▾	◀ Prev	1	2	3	4	5	6	7	8	9	...	Next ▶
UserSessions															
SD6SL5FF6ADFF89354															
SD1SL7FF6ADFF89341															
SD3SL5FF3ADFF89564															
SD8SL5FF4ADFF89311															
SD6SL1FF6ADFF89561															
SD5SL9FF9ADFF89548															
SD0SL4FF2ADFF89269															

Splunk Fundamentals 1 Lab Exercises

Lab typographical conventions:

[sourcetype=db_audit] **OR** [cs_mime_type] indicates either a source type or the name of a field.

NOTE: Lab work will be done on your personal computer or virtual machine, no lab environment is provided. We suggest you **DO NOT** do the lab work on your production environment.

The lab instructions refer to these source types by the types of data they represent:

Type	Sourcetype	Fields of interest
Web Application	access_combined_wcookie	action, bytes, categoryId, clientip, itemId, JSESSIONID, productId, referer, referer_domain, status, useragent, file
Database	db_audit	Command, Duration, Type
Web server	linux_secure	COMMAND, PWD, pid, process

Lab Module 8 – Basic Commands with Solutions

NOTE: Now that you understand the basics of searching in Splunk, we will make labs a little more challenging. This lab document has two sections. The first section includes the instructions without answers. The second section includes instructions with the expected search string (answer) in red.

Description

In this lab, you will be using some of the common Splunk commands including fields, table, rename and dedup.

Steps

Scenario: The Marketing team tracks all user sessions related to marketing campaigns. It would like a report of all user sessions that include purchase actions so that it can put a value on the different campaigns it's running.

Task 1: Search for the requested data.

1. Navigate to the Search view. (If you are in the **Home** app, click **Search & Reporting** from the column on the left side of the screen. You can also access the Search view by clicking the **Search** menu option on the green bar at the top of the screen.)

NOTE: For this course, you will be searching across all time using the main index. This is NOT a best practice in a production environment, but needed for these labs due to the nature of the limited dataset.

2. Enter a search that returns all web application events that include a purchase action with a web status of 200. (`index=main sourcetype=access_combined_wcookie action=purchase status=200`)

Results Example:

 	<i>i</i>	Time	Event
Selected Fields			
<i>a host</i> 1			
<i>a source</i> 1			
<i>a sourcetype</i> 1			
Interesting Fields			
<i>a action</i> 1			
<i># bytes</i> 100+			
<i>a categoryid</i> 7			
<i>a clientip</i> 100+			
<i># date_hour</i> 24			
<i># date_mday</i> 31			
<i># date_minute</i> 60			
<i>a date_month</i> 2			
<i># date_second</i> 60			
<i>a date_wday</i> 7			
<i># date_year</i> 1			
<i>a date_zone</i> 1			
<i>a file</i> 2			
<i>a ident</i> 1			
<i>a index</i> 1			

3. Select the `file` field in the **Interesting Fields** list.

Results Example:



4. Notice that there are two different files that were returned from the web server. They are: `error.do` and `success.do`. Our web development team informs us that the `success.do` is served when the order is processed and `error.do` is served when there is an error with the information being processed.
5. The team is only looking for successful purchases, so change your search to only return those. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do`)

Results Example:

 	<i>i</i>	Time	Event
Selected Fields			
<i>a host</i> 1			
<i>a source</i> 1			
<i>a sourcetype</i> 1			
Interesting Fields			
<i>a action</i> 1			
<i># bytes</i> 100+			
<i>a categoryid</i> 7			
<i>a clientip</i> 100+			
<i># date_hour</i> 24			
<i># date_mday</i> 31			
<i># date_minute</i> 60			
<i>a date_month</i> 2			
<i># date_second</i> 60			
<i>a date_wday</i> 7			
<i># date_year</i> 1			
<i>a date_zone</i> 1			
<i>a file</i> 1			

6. You will see fields that do not matter to the team. Use the `fields` command to only return the `action`, `JSESSIONID` and `status` fields. Does your search run faster using the command?

(index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields action, JSESSIONID, status)

Results Example:

Interesting Fields

```
a action 1
a JSESSIONID 100+
# status 1
```

7. The fields list looks cleaner, but seeing the events like this might still be confusing for the team.

Task 2: Put the data into an easy to read table.

8. Replace the `fields` command with the `table` command to display the data as a table. (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table action, JSESSIONID, status).

Results Example:

20 Per Page ▾			Format	Preview ▾	< Prev 1 2 3 4 5 6 7 8 9 ... Next >								
action	JSESSIONID				status								
purchase	SD6SL5FF6ADFF89354												200
purchase	SD6SL5FF6ADFF89354												200
purchase	SD6SL5FF6ADFF89354												200
purchase	SD6SL5FF6ADFF89354												200

9. Change the order of the fields so that `JSESSIONID` is the first column. (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status).

Results Example:

20 Per Page ▾			Format	Preview ▾	< Prev 1 2 3 4 5 6 7 8 9 ... Next >								
JSESSIONID	action				status								
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200

10. Session IDs are called "UserSessions" in the marketing data. Rename `JSESSIONID` so that your report matches the marketing data. (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions).

Results Example:

20 Per Page ▾			Format	Preview ▾	< Prev 1 2 3 4 5 6 7 8 9 ... Next >								
UserSessions	action				status								
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200
SD6SL5FF6ADFF89354	purchase												200

11. Sort `UserSessions` using the `sort` command. (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions | sort UserSessions)

12. Notice that some `UserSessions` values show up multiple times. Also notice the number of events returned on the **Statistics** tab.

13. Remove the `sort` command and use `dedup` to remove any identical session values. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID, action, status | rename JSESSIONID as UserSessions`)

Results Example:

20 Per Page ▾ Format Preview ▾

◀ Prev 1 2 3 4 5 6 7 8 9 ... Next ▶

UserSessions	action	status
SD6SL5FF6ADFF89354	purchase	200
SD1SL7FF6ADFF89341	purchase	200
SD3SL5FF3ADFF89564	purchase	200
SD8SL5FF4ADFF89311	purchase	200
SD6SL1FF6ADFF89561	purchase	200
SD5SL9FF9ADFF89548	purchase	200

14. How many events are now listed on the **Statistics** tab?

NOTE: As a best practice and for best performance, place `dedup` as early in the search as possible.

15. While having `action` and `status` fields displayed was nice for a sanity check of the data, the marketing team will not need to have these displayed. Remove them from your table display. (`index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID | rename JSESSIONID as UserSessions`).

Results Example:

20 Per Page ▾ Format Preview ▾

◀ Prev 1 2 3 4 5 6 7 8 9 ... Next ▶

UserSessions
SD6SL5FF6ADFF89354
SD1SL7FF6ADFF89341
SD3SL5FF3ADFF89564
SD8SL5FF4ADFF89311
SD6SL1FF6ADFF89561
SD5SL9FF9ADFF89548
SD0SL4FF2ADFF89269