

Splunk Fundamentals 2 – Lab Exercises

There are a number of source types used in these lab exercises.

Index	Туре	Sourcetype	Interesting Fields
web	Online sales	access_combined	<pre>action, bytes, categoryId, clientip, itemId, JSESSIONID, price, productId, product_name, referer, referer_domain, sale_price, status, user, useragent</pre>
security	Active Directory	winauthentication_security	action, app, Authentication_Package, name, Reason, signature, src_ip, subject
	Badge reader	history_access	Address_Description, Department, Device, Email, Event_Description, First_Name, last_Name, Rfid, Username
	Web server	linux_secure	<pre>action, app, COMMAND, dest, process, src_city, src_country, src_ip, src_port, user, vendor_action</pre>
sales	Business Intelligence server	sales_entries	AcctCode, CustomerID, TransactionID
	Retail sales	vendor_sales	AcctID, categoryId, product_name, productId, sale_price, Vendor, VendorCity, VendorCountry, VendorID, VendorStateProvince
network	Email security data	cisco_esa	dcid, icid, mailfrom, mailto, mid
	Web security appliance data	cisco_wsa_squid	action, cs_method, cs_mime_type, cs_url, cs_username, sc_bytes, sc_http_status, sc_result_code, severity, src_ip, status, url, usage, x_mcafee_virus_name, x_wbrs_score, x_webcat_code_abbr
	Firewall data	cisco_firewall	<pre>bcg_ip, dept, Duration, name, IP, lname, location, rfid, splunk_role, splunk_server, Username</pre>
games	Game logs	SimCubeBeta	<pre>date_hour, date_mday, date_minute, date_month, date_second, data_wday, data_year, data_zone, eventtype, index, linecount, punct, splunk_server, timeendpos, timestartpos</pre>



Lab Exercise 2 – Beyond Search Fundamentals

Description

This exercise reviews the concepts presented in Module 2, including using the Job Inspector.

NOTE: If at any point you do not see results, check your search syntax and/or expand your time range.

Questions

Examine these searches. Which searches would not return results?

- 1. index=security sourcetype=linux_secure
- 2. index=web Sourcetype=access_combined [No results]
- 3. index=web sourcetype=AcceSS_Combined
- 4. index=security sourcetype=linux_se% [No results]

What is the most efficient filter?

time

Identify the 3 Selected Fields that Splunk returns by default for every event.

host

source

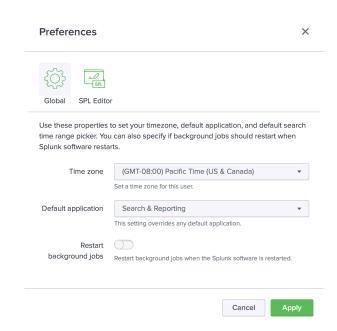
sourcetype

Steps

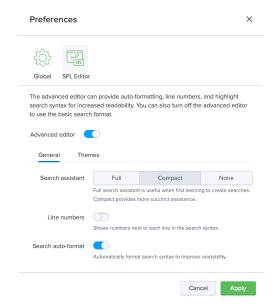
Task 1: Change your account time zone setting to reflect your local time.

- 1. If you have not done so, launch the lab server by clicking the "Connect to Lab Server" button in the module for this lab.
- 2. Click your user name on the navigation bar and select **Preferences**.
- 3. From the **Time zone** dropdown, select your local time zone.
- 4. From the Default app dropdown, select Search & Reporting.





- Select the SPL Editor button.
- 6. Turn on the **Search auto-format** selector. This option will auto-format line breaks in your search bar for easier reading. If you decide you do not like this functionality, please turn it off.
- 7. Click Apply.



Task 3: Use the Search Job Inspector to troubleshoot problems.

8. Navigate to the Search & Reporting app. Perform and save all your searches in this app.



9.	Search for index=web sourcetype=access_combined productid=* over the last 15 minutes. B sure to retain case. Are any results returned? no
10.	. Click Job > Inspect Job to open the Search Job Inspector and inspect the results.
11.	Now, search for index=web sourcetype=access_combined productId=* over the last 15 minutes. Be sure to retain case. Are any results returned? yes
12.	. Open the Search Job Inspector again and inspect the results.
Sc	enario: IT wants to check for issues with customer purchases in the online store.
13.	. Search for online sales transactions during the last 30 days. Using the table command, display only the customer IP [clientip], the customer action [action], and the http status [status] of each event.
	Be sure to include an index in your search.
Ta	Be sure to include an index in your search. index=web sourcetype=access_combined action=purchase
	Be sure to include an index in your search. index=web sourcetype=access_combined action=purchase table clientip, action, status
14.	Be sure to include an index in your search. index=web sourcetype=access_combined action=purchase table clientip, action, status sk 4: Use Search Job Inspector to view performance. Search for index=web sourcetype=access_combined over the last 30 days using the Verbose search mode, then open the Job Inspector (Job > Inspect Job). How much time did it take for the search