

## 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 10 – Creating Reports and Dashboards

**NOTE:** 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 building reports and dashboards for members of the Butter Cups Games organization.

### Steps

**Scenario:** The security team would like a report of IPs that seem to be up to no good.

**Task 1:** Use the stats count function to get a report of users trying to access forbidden pages in the Buttercup Games web application.

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 with a forbidden status (403).

*Results Example:*

i	Time	Event
>	4/30/17 11:15:37.000 PM	67.133.102.54 - - [30/Apr/2017:23:15:37] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD2SL4FF6ADFF4958 HTTP 1.1" 403 282 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 773 host = web_application : source = access_30DAY.log : sourcetype = access_combined_wcookie
>	4/30/17 11:07:46.000 PM	91.205.189.15 - - [30/Apr/2017:23:07:46] "GET /cart.do?action=remove&JSESSIONID=SD0SL7FF8ADFF4960 HTTP 1.1" 403 720 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (compatible; NetcraftSurveyAgent/1.0/cc-prepass-https; +info@netcraft.com)" 378 host = web_application : source = access_30DAY.log : sourcetype = access_combined_wcookie
>	4/30/17 10:43:51.000 PM	76.169.7.252 - - [30/Apr/2017:22:43:51] "GET /oldlink?&JSESSIONID=SD4SL6FF8ADFF4960 HTTP 1.1" 403 3640 "http://www.buttercupgames.com/oldlink" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 122 host = web_application : source = access_30DAY.log : sourcetype = access_combined_wcookie

3. Use the `stats count` function to count the events by `clientip` and rename the count to `attempts`.

*Results Example:*

clientip	attempts
107.3.146.207	11
108.65.113.83	3
109.169.32.135	4
110.138.30.229	2
110.159.208.78	3

- Use the `sort` command to display the results so that the `clientip` with the highest `attempts` appears first.
- For the `clientip` with the most `attempts`, what was the total number of `attempts`? This might show up during the quiz module.
- Use the **Save As** menu (above the time range picker) to select **Report**.
- Enter a **Title** of `403_by_clientip` for the report and click **Save**.

*Example:*

Save As Report

Title

403\_by\_clientip

Description

optional

Content

Statistics Table

Time Range Picker

Yes

No

Cancel

Save

- Use the **Permissions** link to make the report display for the App, run as Owner, and be readable by Everyone. Click **Save**.

*Example:*

Display For
 

Owner App All apps

Run As
 

Owner User

[Learn More](#)

	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

- Access a list of the reports available to you using the **Reports** menu option on the green bar at the top of the screen.
- Notice that the `403_by_clientip` report is in the list. Click on the report title to run the report.

Scenario: The CFO has asked you to create a dashboard where she can see how product sales are doing in one place.

## Task 2: Use stats functions to create visualizations of products sold, and add them to a dashboard.

- Navigate to a new Search view. (Access the Search view by clicking the **Search** menu option on the green bar at the top of the screen.)
- Enter a search that returns all web application events for all time where an item was successfully purchased. Remember, when an item is successfully purchased a `success.do` file is served and a 200 status is returned.
- Use the `stats count` function with a `by` clause to count events by the `productId`.

Results Example:

productId	count
BS-AG-G09	935
CU-PG-G06	935
DB-SG-G01	1319
DC-SG-G02	1308
FI-AG-G08	988

- Select the **Visualization** tab and choose the **Column Chart** from the visualization selections.

Example:

Column Chart

Format

Trellis

Splunk Visualizations

Find more visualizations
 

**Column Chart**  
 Compare values or fields.  
 Search Fragment  
 | stats count by comparison\_category

15. Use the **Save As** menu to select **Dashboard Panel**.

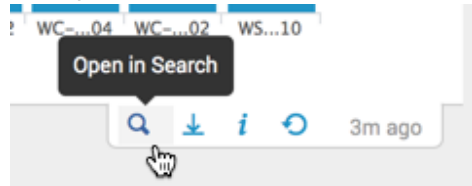
16. Save the dashboard with these values:

- Dashboard: *New*
- Dashboard Title: *Sales Dashboard*
- Panel Title: *Product Sales*

17. Once saved, click **View Dashboard**.

18. Roll over the columns in the chart to see the interaction, and notice the tools at the bottom of the panel.

*Example:*



19. Use the **Open in Search** icon at the bottom of the panel to open the search view and run the search.

20. Remove the `by` clause from the search to return the total count of products sold.

21. Select the **Visualization** tab and choose the **Single Value** visualization from the **Splunk Visualizations** menu.

22. Use the **Save As** menu to select **Dashboard Panel**.

23. Save the dashboard with these values:

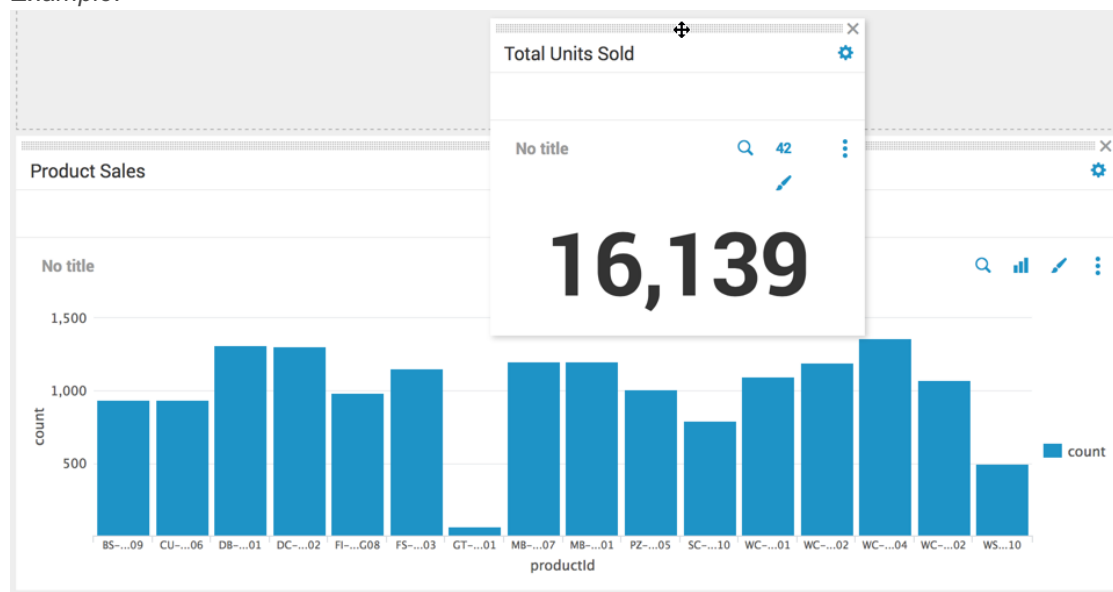
- Dashboard: *Existing*
- Dashboard Title: *Sales Dashboard*
- Panel Title: *Total Units Sold*

24. Once saved, click **View Dashboard**.

25. The `Total Units Sold` panel is probably the first item our CFO will want to see. Click the **Edit** button at the top of the dashboard.

26. Click and hold the bar at the top of the `Total Units Sold` panel and drag the panel to the top of the dashboard. Once in place, drop and click **Save**.

*Example:*



27. What other panels might be useful to the CFO? Return to some of the searches you have previously run, and add them to the dashboard.

## 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 10 – Creating Reports and Dashboards with Solutions

**NOTE:** 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 building reports and dashboards for members of the Butter Cups Games organization.

### Steps

**Scenario:** The security team would like a report of IPs that seem to be up to no good.

**Task 1:** Use the stats count function to get a report of users trying to access forbidden pages in the Buttercup Games web application.

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 with a forbidden status (403).

(index=main sourcetype=access\_combined\_wcookie status=403)

*Results Example:*

i	Time	Event
>	4/30/17 11:15:37.000 PM	67.133.102.54 - - [30/Apr/2017:23:15:37] "GET /product.screen?productId=SF-BVS-01&JSESSIONID=SD2SL4FF6ADFF4958 HTTP 1.1" 403 282 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 773 host = web_application : source = access_30DAY.log : sourcetype = access_combined_wcookie
>	4/30/17 11:07:46.000 PM	91.205.189.15 - - [30/Apr/2017:23:07:46] "GET /cart.do?action=remove&JSESSIONID=SD0SL7FF8ADFF4960 HTTP 1.1" 403 720 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-01" "Mozilla/5.0 (compatible; NetcraftSurveyAgent/1.0/cc-prepass-https; +info@netcraft.com)" 378 host = web_application : source = access_30DAY.log : sourcetype = access_combined_wcookie
>	4/30/17 10:43:51.000 PM	76.169.7.252 - - [30/Apr/2017:22:43:51] "GET /oldlink?&JSESSIONID=SD4SL6FF8ADFF4960 HTTP 1.1" 403 3640 "http://www.buttercupgames.com/oldlink" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 122 host = web_application : source = access_30DAY.log : sourcetype = access_combined_wcookie

- Use the `stats count` function to count the events by `clientip` and rename the count to `attempts`.  
(`index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip`)

Results Example:

clientip	attempts
107.3.146.207	11
108.65.113.83	3
109.169.32.135	4
110.138.30.229	2
110.159.208.78	3

- Use the `sort` command to display the results so that the `clientip` with the highest `attempts` appears first.  
(`index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip | sort -attempts`)
- For the `clientip` with the most `attempts`, what was the total number of `attempts`? This might show up during the quiz module. (100)
- Use the **Save As** menu (above the time range picker) to select **Report**.
- Enter a **Title** of `403_by_clientip` for the report and click **Save**.

Example:

Save As Report

Title

403\_by\_clientip

Description

optional

Content

Statistics Table

Time Range Picker

Yes

No

Cancel

Save

- Use the **Permissions** link to make the report display for the App, run as Owner, and be readable by Everyone. Click **Save**.

Example:

Display For	Owner	App	All apps
Run As	Owner	User	
	<a href="#">Learn More</a>		
		Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
power	<input type="checkbox"/>	<input type="checkbox"/>	
user	<input type="checkbox"/>	<input type="checkbox"/>	

- Access a list of the reports available to you using the **Reports** menu option on the green bar at the top of the screen.
- Notice that the `403_by_clientip` report is in the list. Click on the report title to run the report.

Scenario: The CFO has asked you to create a dashboard where she can see how product sales are doing in one place.

## Task 2: Use stats functions to create visualizations of products sold, and add them to a dashboard.

- Navigate to a new Search view. (Access the Search view by clicking the **Search** menu option on the green bar at the top of the screen.)
- Enter a search that returns all web application events for all time where an item was successfully purchased. Remember, when an item is successfully purchased a `success.do` file is served and a 200 status is returned.  
(`index=main sourcetype=access_combined_wcookie file=success.do status=200`)
- Use the `stats count` function with a `by` clause to count events by the `productId`.  
(`index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count by productId`)

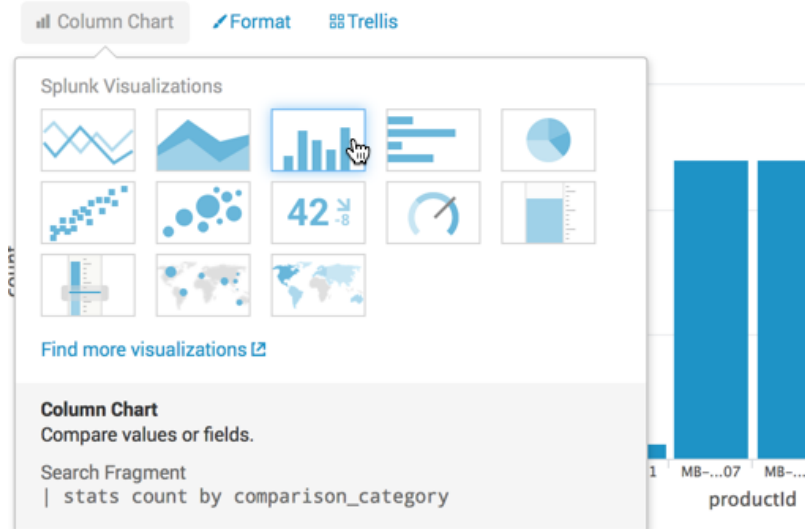
Results Example:

productId	count
BS-AG-G09	935
CU-PG-G06	935
DB-SG-G01	1319
DC-SG-G02	1308
FI-AG-G08	988

- Select the **Visualization** tab and choose the **Column Chart** from the visualization selections.

Example:





15. Use the **Save As** menu to select **Dashboard Panel**.

16. Save the dashboard with these values:

- Dashboard: *New*
- Dashboard Title: *Sales Dashboard*
- Panel Title: *Product Sales*

17. Once saved, click **View Dashboard**.

18. Roll over the columns in the chart to see the interaction, and notice the tools at the bottom of the panel.

*Example:*



19. Use the **Open in Search** icon at the bottom of the panel to open the search view and run the search.

20. Remove the `by` clause from the search to return the total count of products sold.

*(index=main sourcetype=access\_combined\_wcookie file=success.do status=200)*

21. Select the **Visualization** tab and choose the **Single Value** visualization from the **Splunk Visualizations** menu.

22. Use the **Save As** menu to select **Dashboard Panel**.

23. Save the dashboard with these values:

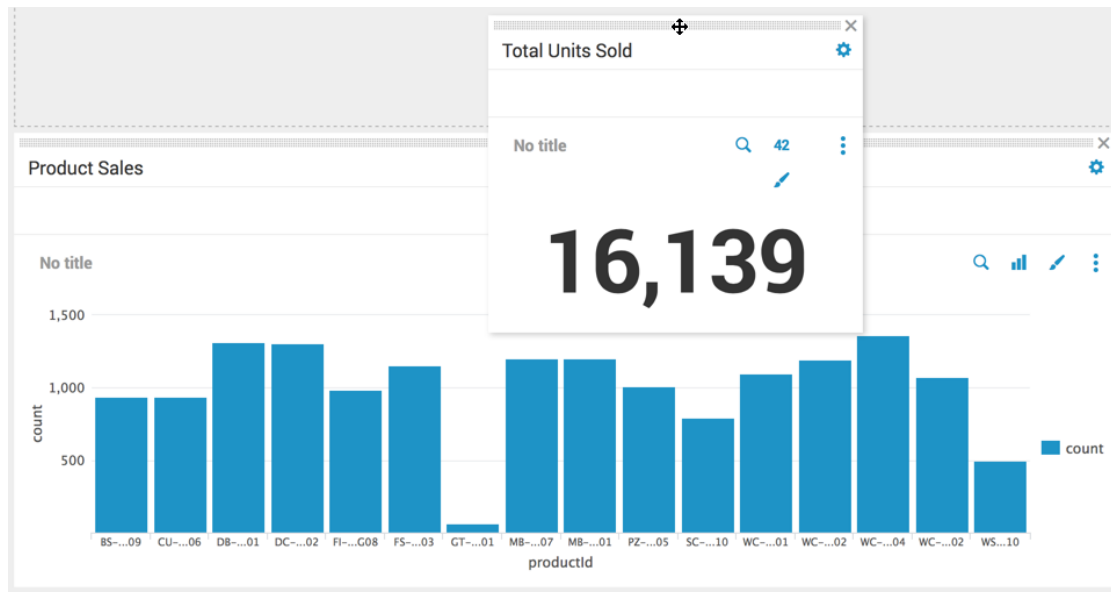
- Dashboard: *Existing*
- Dashboard Title: *Sales Dashboard*
- Panel Title: *Total Units Sold*

24. Once saved, click **View Dashboard**.

25. The `Total Units Sold` panel is probably the first item our CFO will want to see. Click the **Edit** button at the top of the dashboard.

26. Click and hold the bar at the top of the `Total Units Sold` panel and drag the panel to the top of the dashboard. Once in place, drop and click **Save**.

*Example:*



27. What other panels might be useful to the CFO? Return to some of the searches you have previously run, and add them to the dashboard.