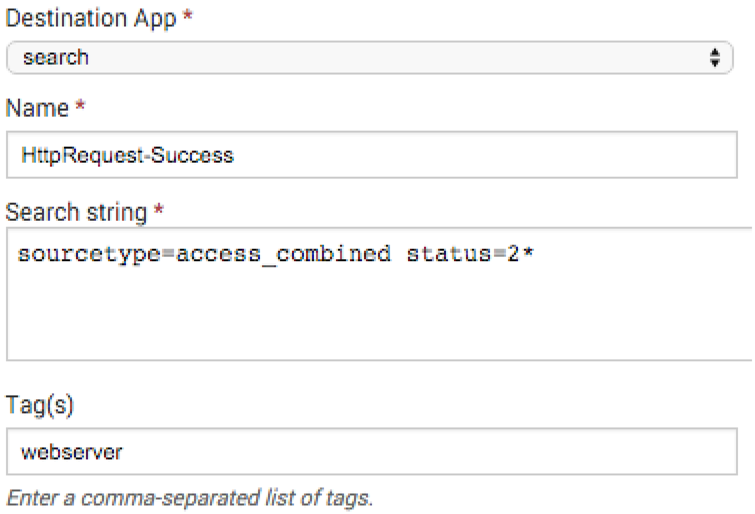


Destination App *
search

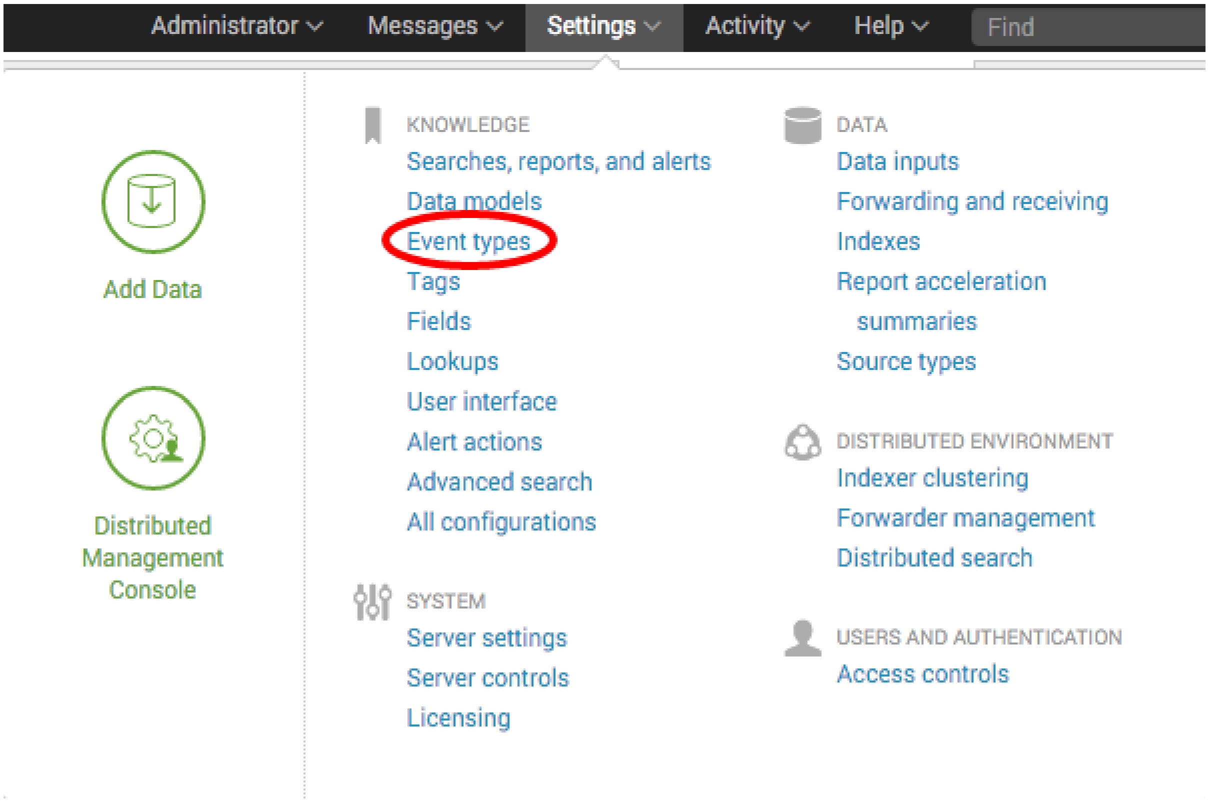
Name *
HttpRequest-Success

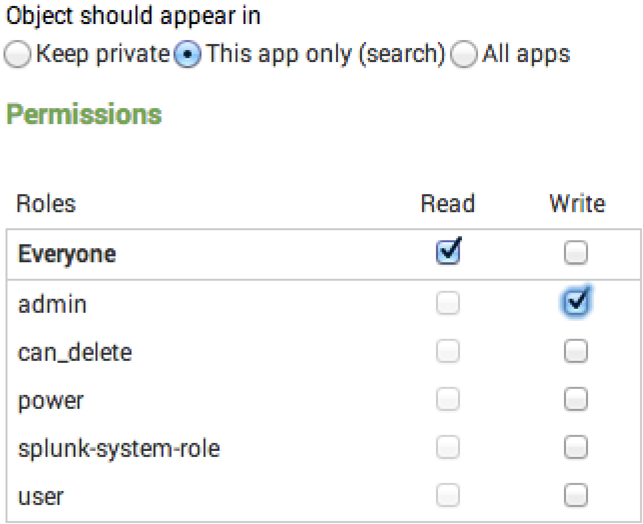
Search string *

```
sourcetype=access_combined status=2*
```

Tag(s)
webserver

Enter a comma-separated list of tags.



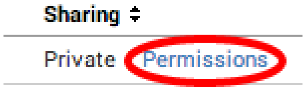


Object should appear in

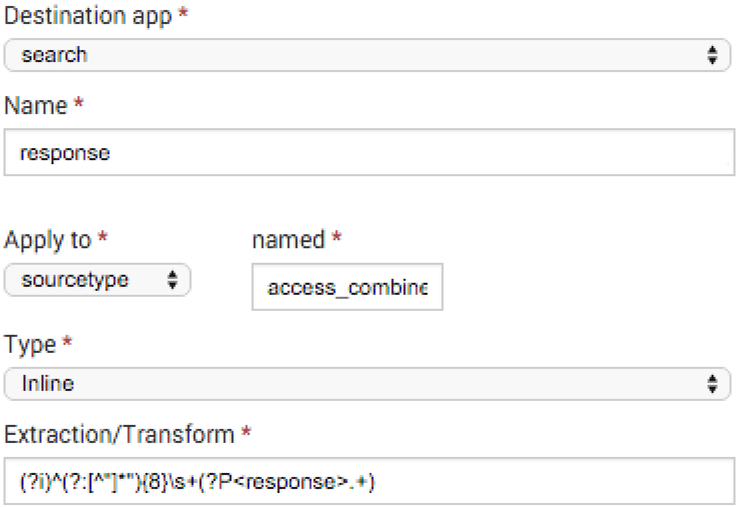
○ Keep private ● This app only (search) ○ All apps

Permissions

Roles	Read	Write
Everyone	☑	□
admin	□	☑
can_delete	□	□
power	□	□
splunk-system-role	□	□
user	□	□



Sharing ⇕
Private Permissions



Destination app *

search

Name *

response

Apply to *

sourcetype

named *

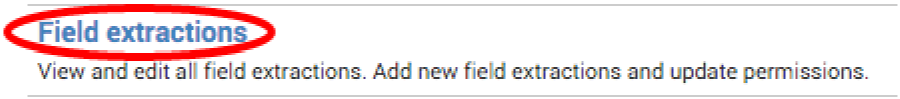
access_combine

Type *

Inline

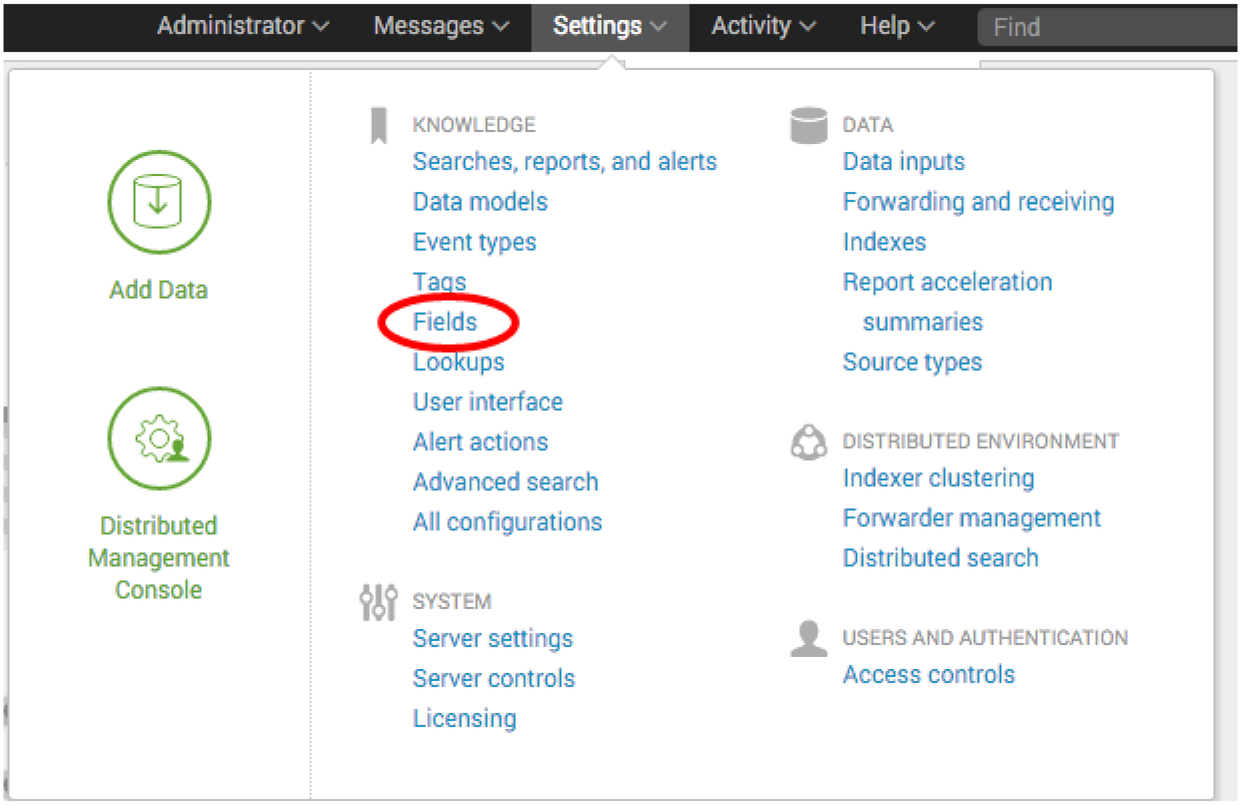
Extraction/Transform *

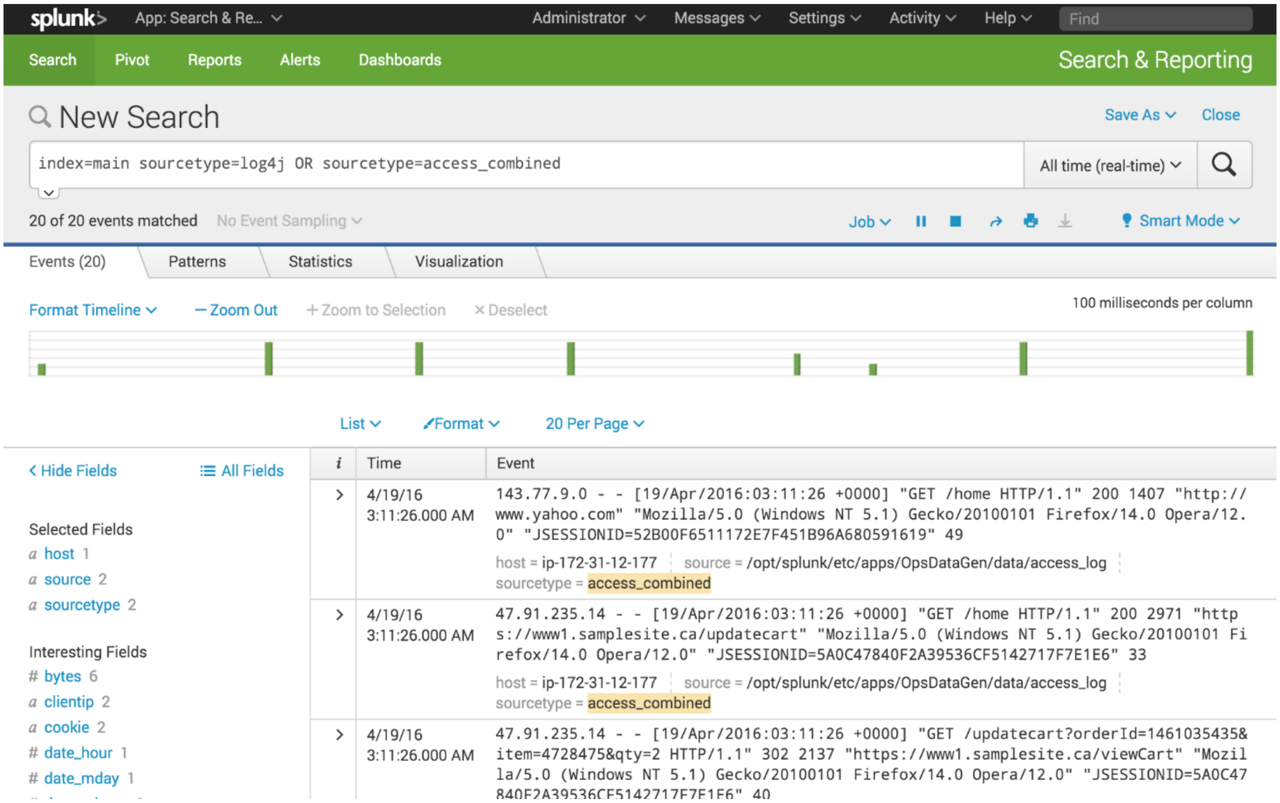
```
(?i)^(?:[^"]*"){8}\s+(?P<response>.+)
```



Field extractions

View and edit all field extractions. Add new field extractions and update permissions.





```
index=main sourcetype=log4j OR sourcetype=access_combined
```

20 of 20 events matched

Selected Fields
- a host 1
- a source 2
- a sourcetype 2

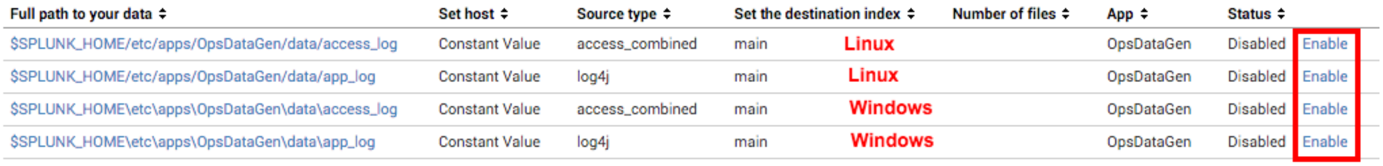
Interesting Fields
- # bytes 6
- a clientip 2
- a cookie 2
- # date_hour 1
- # date_mday 1

i	Time	Event

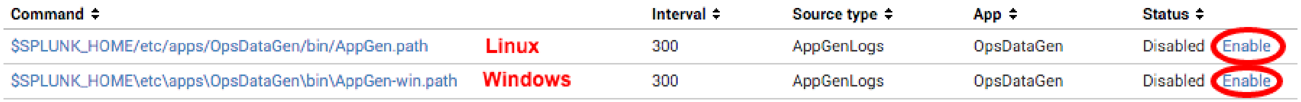
>	4/19/16
	3:11:26.000 AM
		143.77.9.0 - - [19/Apr/2016:03:11:26 +0000] "GET /home HTTP/1.1" 200 1407 "http://www.yahoo.com" "Mozilla/5.0 (Windows NT 5.1) Gecko/20100101 Firefox/14.0 Opera/12.0" "JSESSIONID=52B00F6511172E7F451B96A680591619" 49
		host = ip-172-31-12-177 source = /opt/splunk/etc/apps/OpsDataGen/data/access_log
		sourcetype = access_combined

>	4/19/16
	3:11:26.000 AM
		47.91.235.14 - - [19/Apr/2016:03:11:26 +0000] "GET /home HTTP/1.1" 200 2971 "https://www1.samplesite.ca/updatecart" "Mozilla/5.0 (Windows NT 5.1) Gecko/20100101 Firefox/14.0 Opera/12.0" "JSESSIONID=5A0C47840F2A39536CF5142717F7E1E6" 33
		host = ip-172-31-12-177 source = /opt/splunk/etc/apps/OpsDataGen/data/access_log
		sourcetype = access_combined

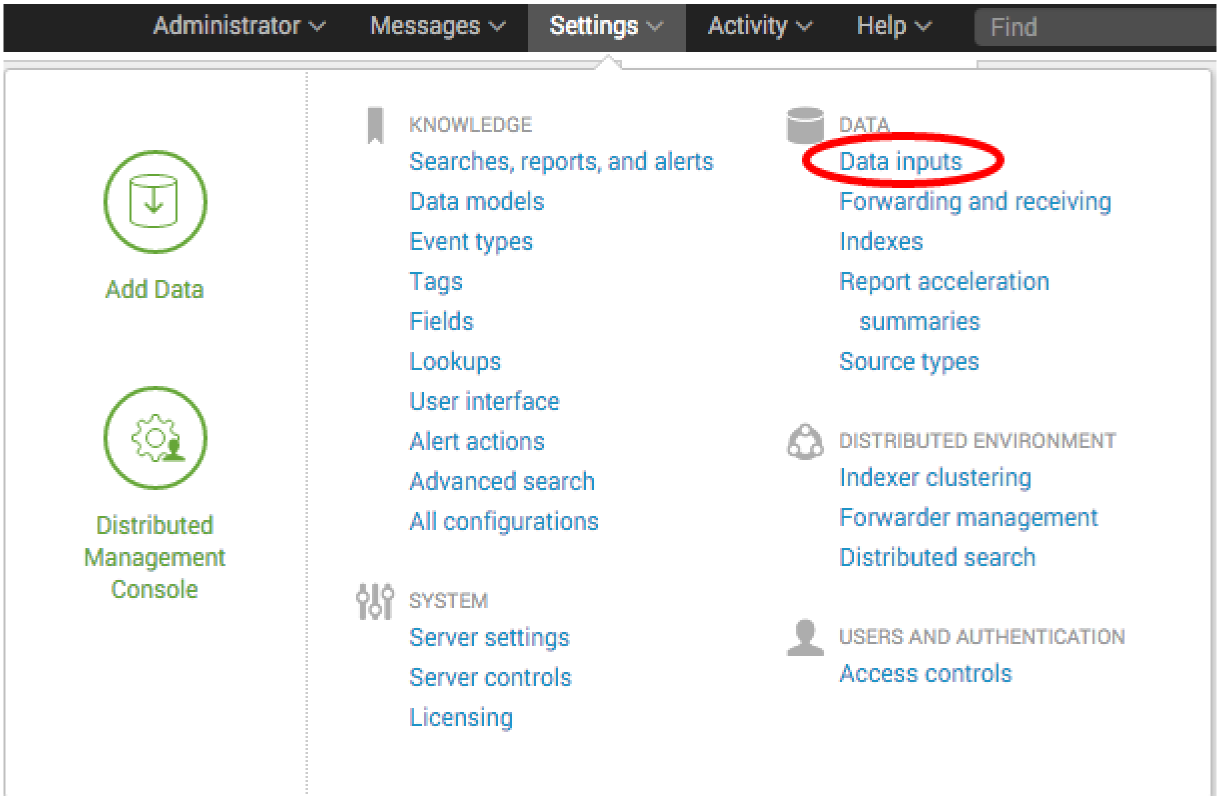
>	4/19/16 3:11:26.000 AM	47.91.235.14 - - [19/Apr/2016:03:11:26 +0000] "GET /updatecart?orderId=1461035435&item=4728475&qty=2 HTTP/1.1" 302 2137 "https://www1.samplesite.ca/viewCart" "Mozilla/5.0 (Windows NT 5.1) Gecko/20100101 Firefox/14.0 Opera/12.0" "JSESSIONID=5A0C47840F2A39536CF5142717F7E1E6" 40

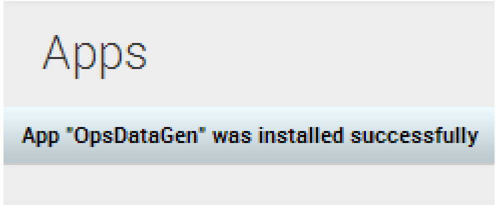


Full path to your data ⬍	Set host ⬍	Source type ⬍	Set the destination index ⬍	Number of files ⬍	App ⬍	Status ⬍	
$SPLUNK_HOME/etc/apps/OpsDataGen/data/access_log	Constant Value	access_combined	main **Linux**		OpsDataGen	Disabled	Enable
$SPLUNK_HOME/etc/apps/OpsDataGen/data/app_log	Constant Value	log4j	main **Linux**		OpsDataGen	Disabled	Enable
$SPLUNK_HOME\etc\apps\OpsDataGen\data\access_log	Constant Value	access_combined	main **Windows**		OpsDataGen	Disabled	Enable
$SPLUNK_HOME\etc\apps\OpsDataGen\data\app_log	Constant Value	log4j	main **Windows**		OpsDataGen	Disabled	Enable

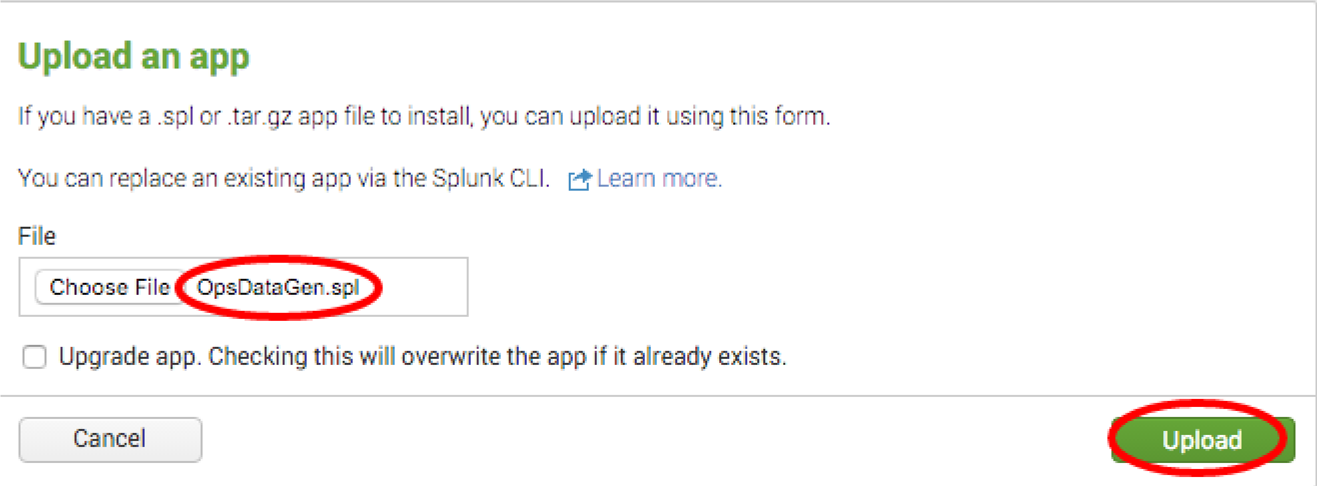


Command ⬍	Interval ⬍	Source type ⬍	App ⬍	Status ⬍	
$SPLUNK_HOME/etc/apps/OpsDataGen/bin/AppGen.path **Linux**	300	AppGenLogs	OpsDataGen	Disabled	Enable
$SPLUNK_HOME\etc\apps\OpsDataGen\bin\AppGen-win.path **Windows**	300	AppGenLogs	OpsDataGen	Disabled	Enable





App "OpsDataGen" was installed successfully



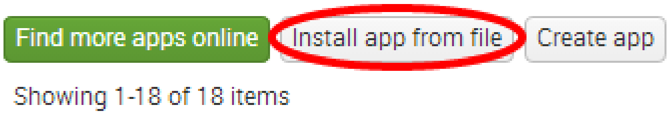
Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

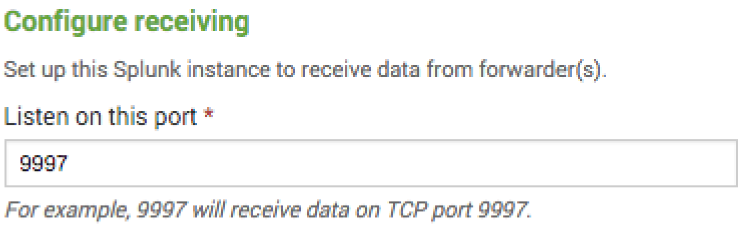
You can replace an existing app via the Splunk CLI. Learn more.

File: OpsDataGen.spl

□ Upgrade app. Checking this will overwrite the app if it already exists.



Showing 1-18 of 18 items

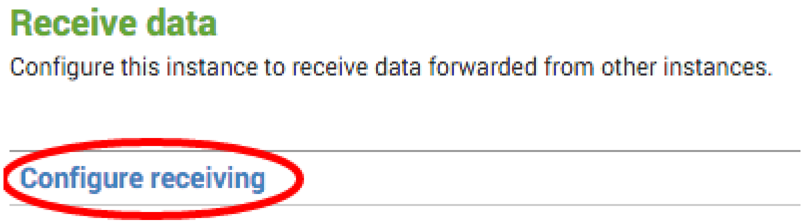


Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

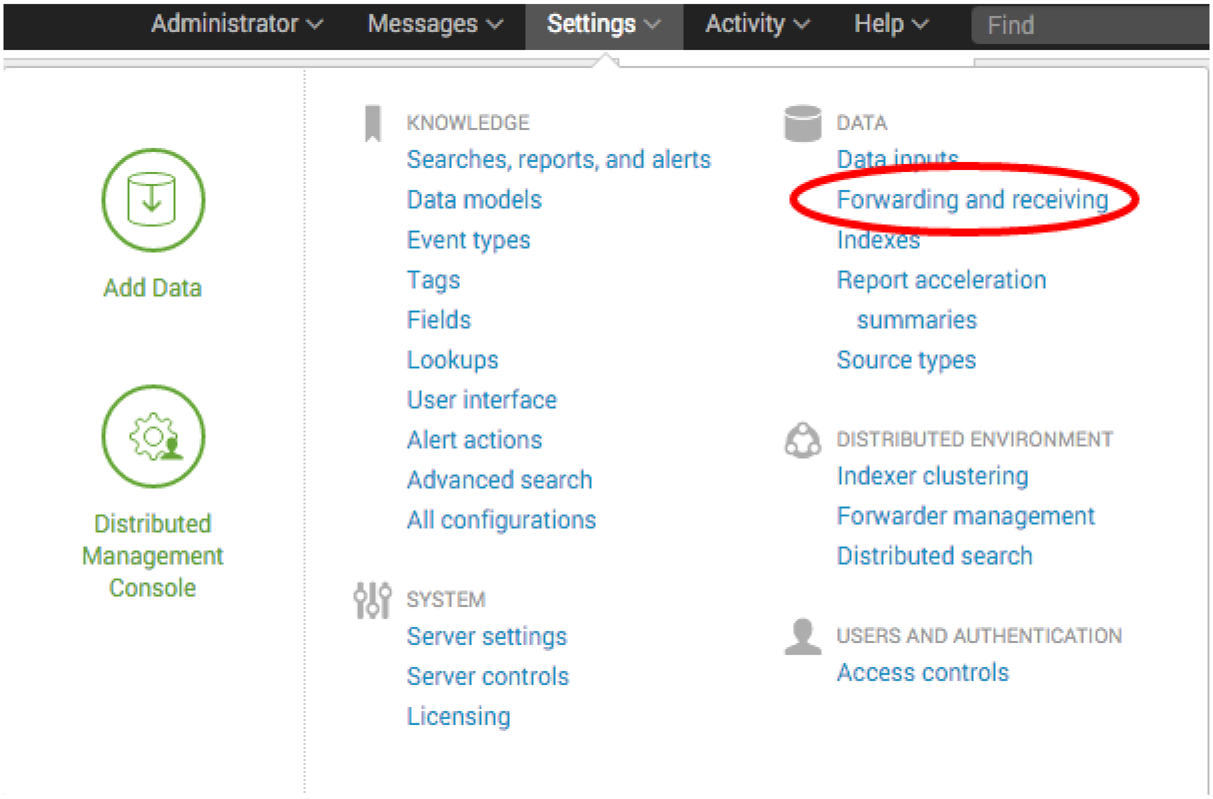
Listen on this port *: 9997

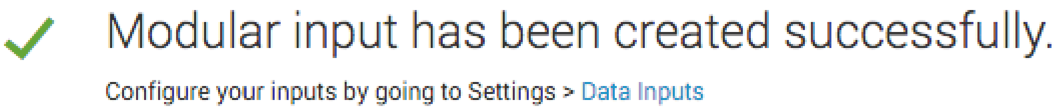
For example, 9997 will receive data on TCP port 9997.



Receive data

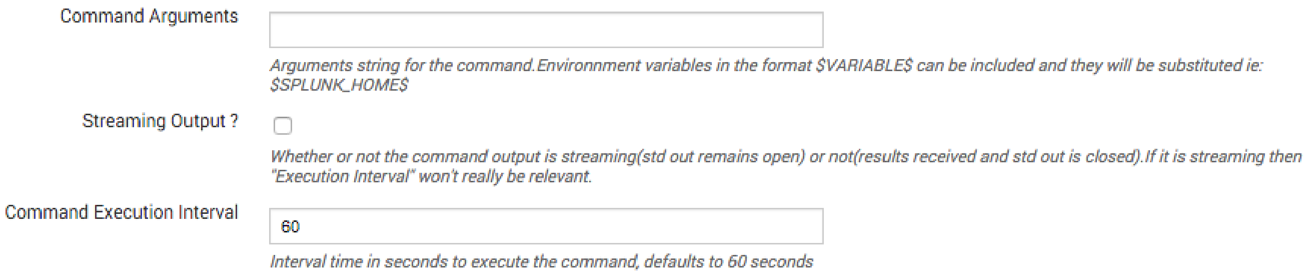
Configure this instance to receive data forwarded from other instances.





Modular input has been created successfully.

Configure your inputs by going to Settings > Data Inputs



Command Arguments

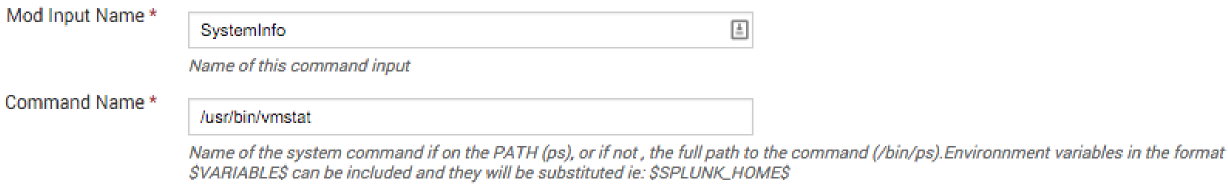
Arguments string for the command.Environnment variables in the format $VARIABLE$ can be included and they will be substituted ie: $SPLUNK_HOME$

Streaming Output ? □

Whether or not the command output is streaming(std out remains open) or not(results received and std out is closed).If it is streaming then "Execution Interval" won't really be relevant.

Command Execution Interval: 60

Interval time in seconds to execute the command, defaults to 60 seconds

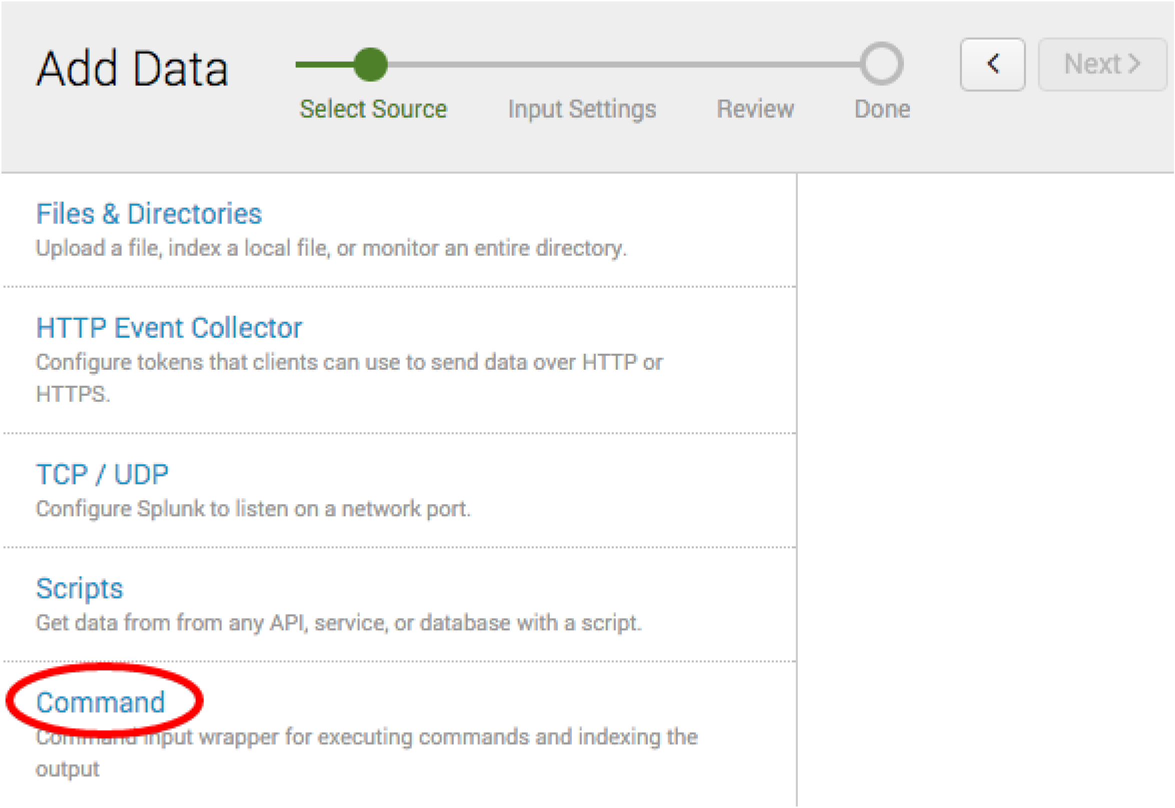


Mod Input Name * SystemInfo

Name of this command input

Command Name * /usr/bin/vmstat

Name of the system command if on the PATH (ps), or if not , the full path to the command (/bin/ps).Environnment variables in the format $VARIABLE$ can be included and they will be substituted ie: $SPLUNK_HOME$



Files & Directories

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

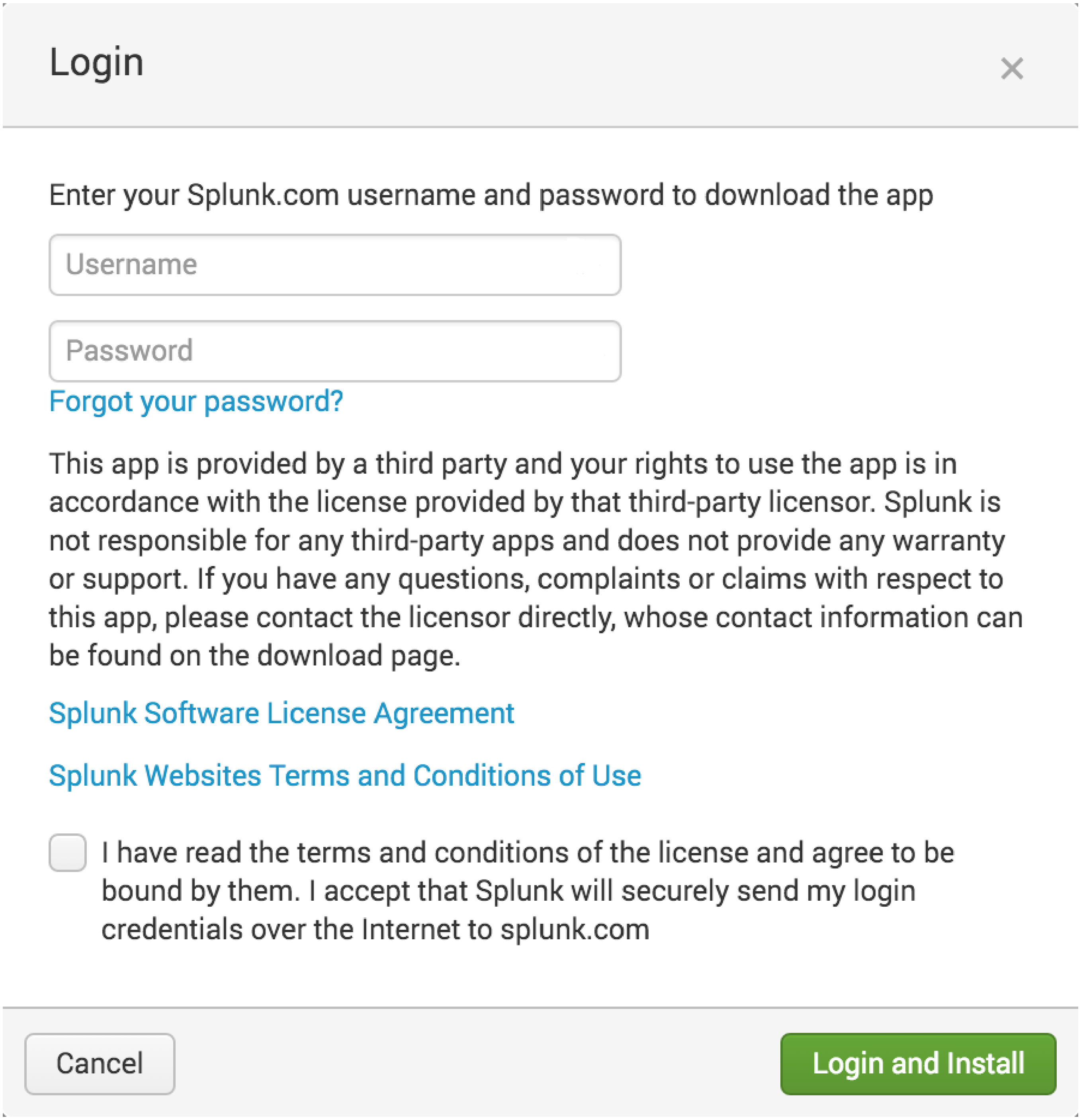
Configure Splunk to listen on a network port.

Scripts

Get data from from any API, service, or database with a script.

Command

Command input wrapper for executing commands and indexing the output



Enter your Splunk.com username and password to download the app

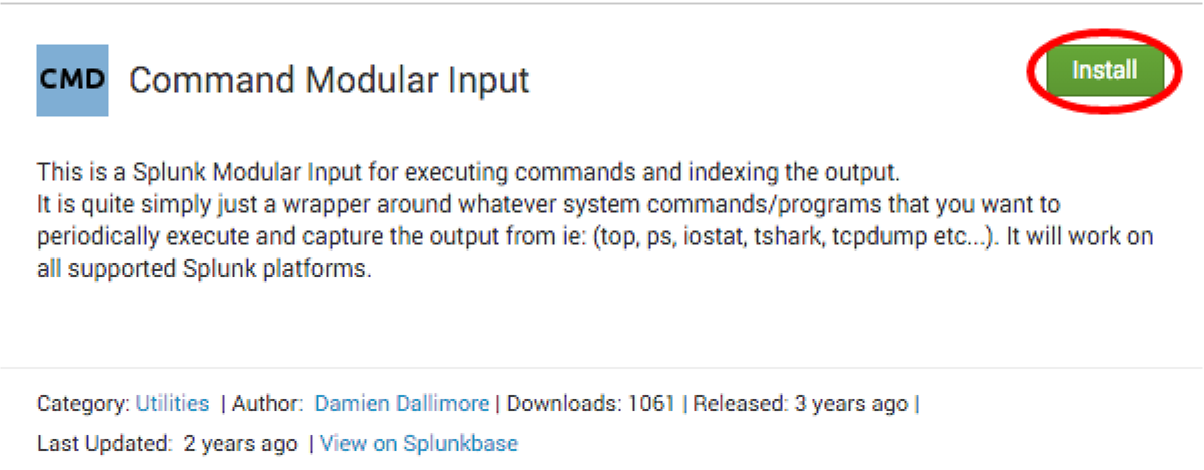
Forgot your password?

This app is provided by a third party and your rights to use the app is in accordance with the license provided by that third-party licensor. Splunk is not responsible for any third-party apps and does not provide any warranty or support. If you have any questions, complaints or claims with respect to this app, please contact the licensor directly, whose contact information can be found on the download page.

Splunk Software License Agreement

Splunk Websites Terms and Conditions of Use

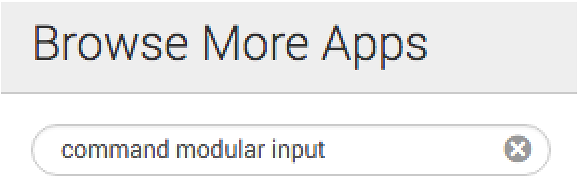
□ I have read the terms and conditions of the license and agree to be bound by them. I accept that Splunk will securely send my login credentials over the Internet to splunk.com



Command Modular Input

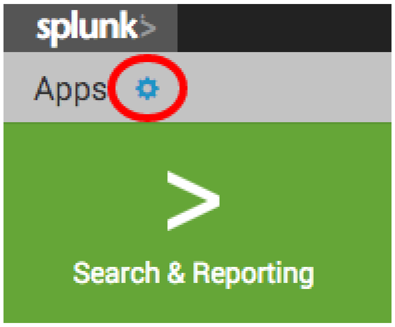
This is a Splunk Modular Input for executing commands and indexing the output.
It is quite simply just a wrapper around whatever system commands/programs that you want to periodically execute and capture the output from ie: (top, ps, iostat, tshark, tcpdump etc...). It will work on all supported Splunk platforms.

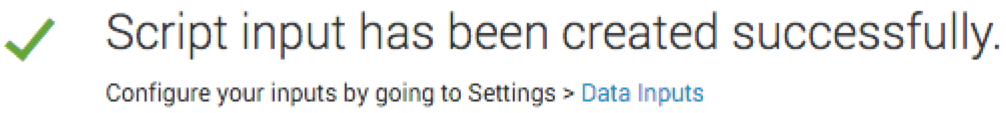
Category: Utilities | Author: Damien Dallimore | Downloads: 1061 | Released: 3 years ago |
Last Updated: 2 years ago | View on Splunkbase



Browse More Apps

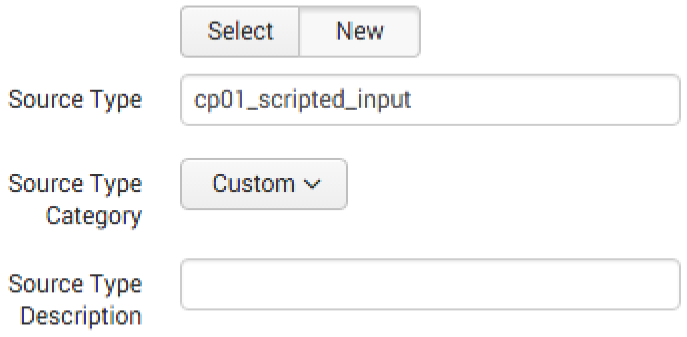
command modular input





✓ Script input has been created successfully.

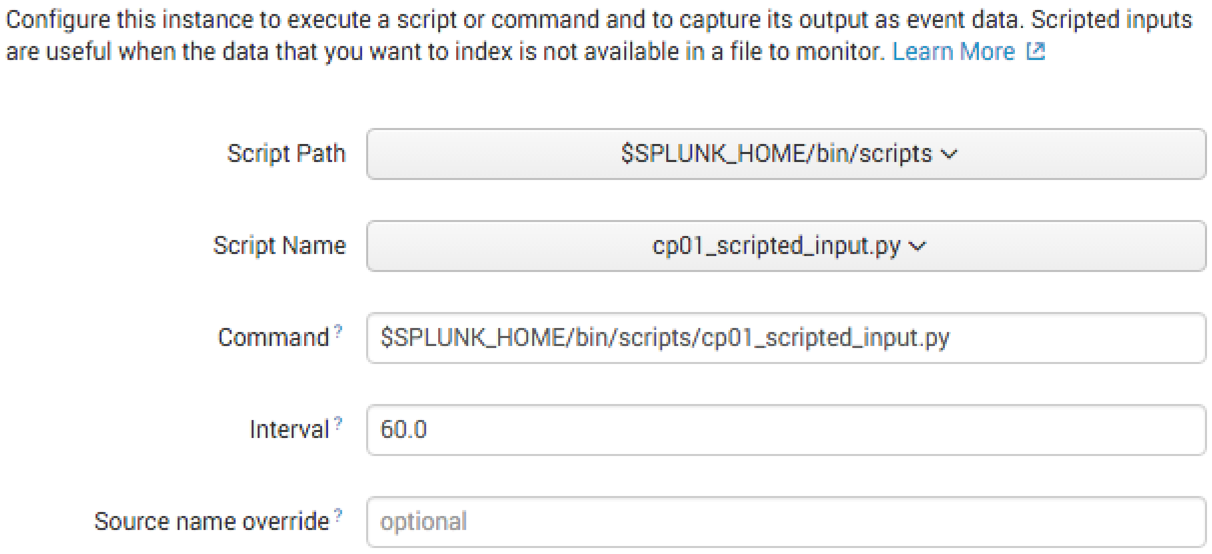
Configure your inputs by going to Settings > Data Inputs



Source Type: cp01_scripted_input

Source Type Category: Custom

Source Type Description:



Configure this instance to execute a script or command and to capture its output as event data. Scripted inputs are useful when the data that you want to index is not available in a file to monitor. Learn More

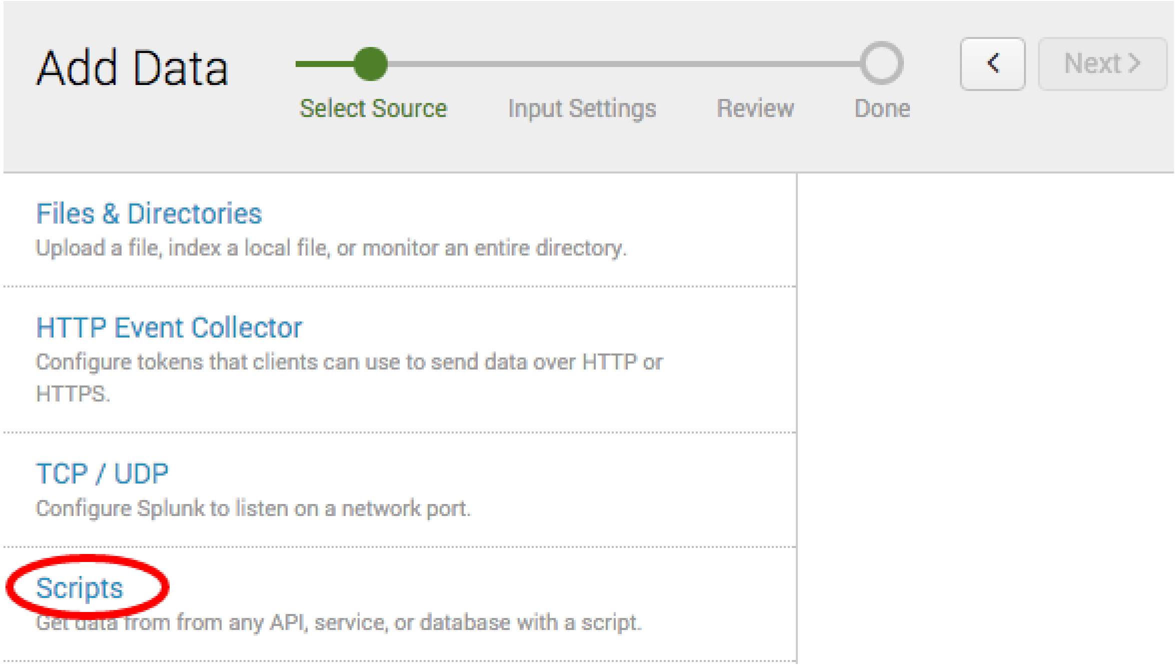
Script Path: $SPLUNK_HOME/bin/scripts

Script Name: cp01_scripted_input.py

Command: $SPLUNK_HOME/bin/scripts/cp01_scripted_input.py

Interval: 60.0

Source name override: optional

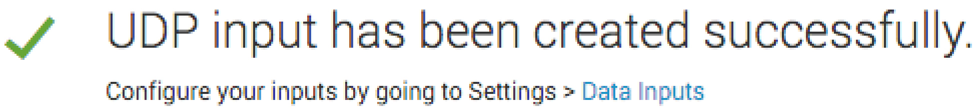


Files & Directories
Upload a file, index a local file, or monitor an entire directory.

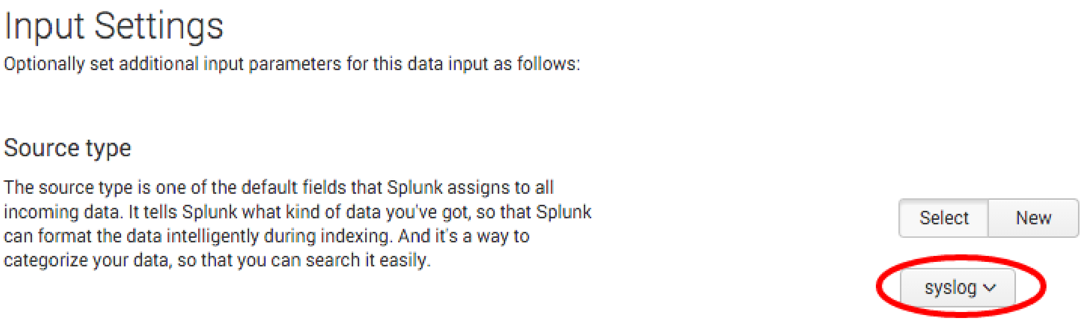
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from from any API, service, or database with a script.


UDP input has been created successfully.

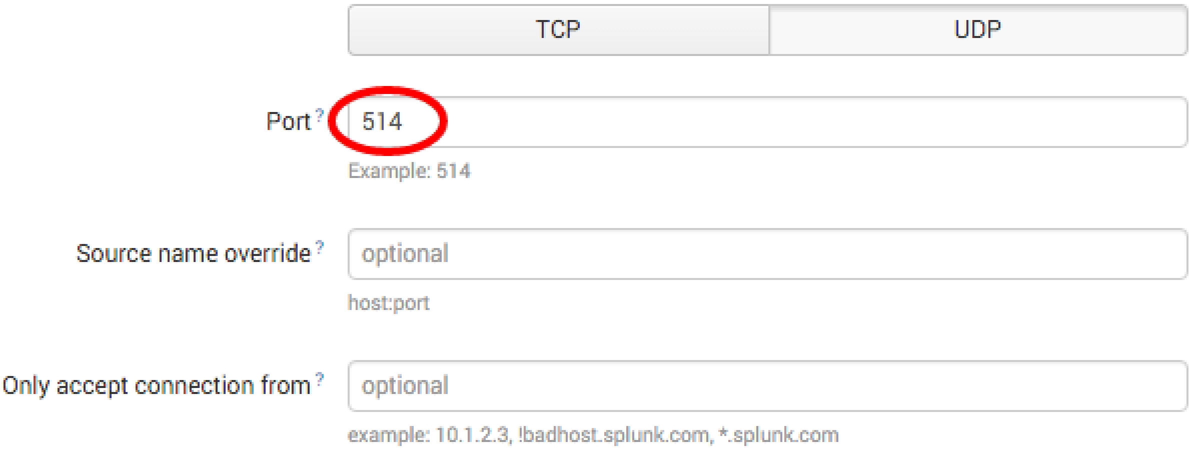
Configure your inputs by going to Settings > Data Inputs


Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.



Port ? 514

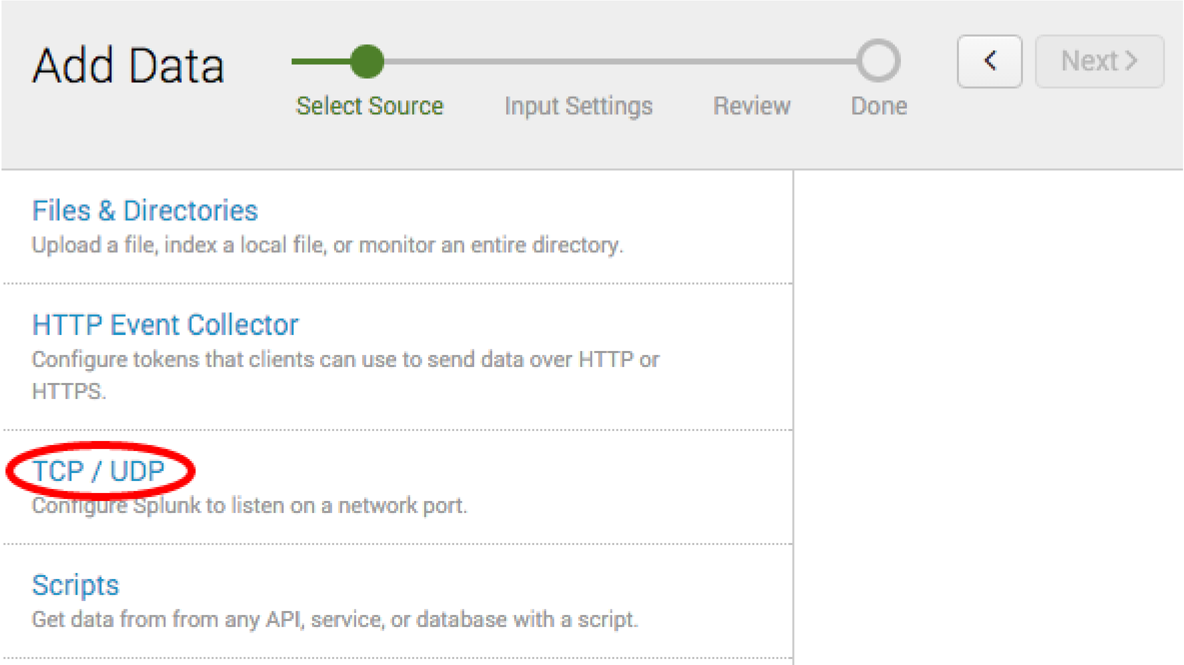
Example: 514

Source name override ? optional

host:port

Only accept connection from ? optional

example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

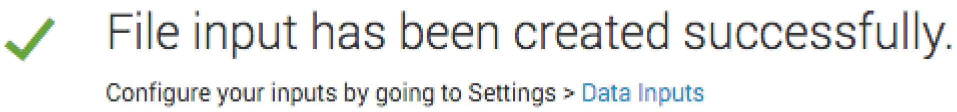


Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

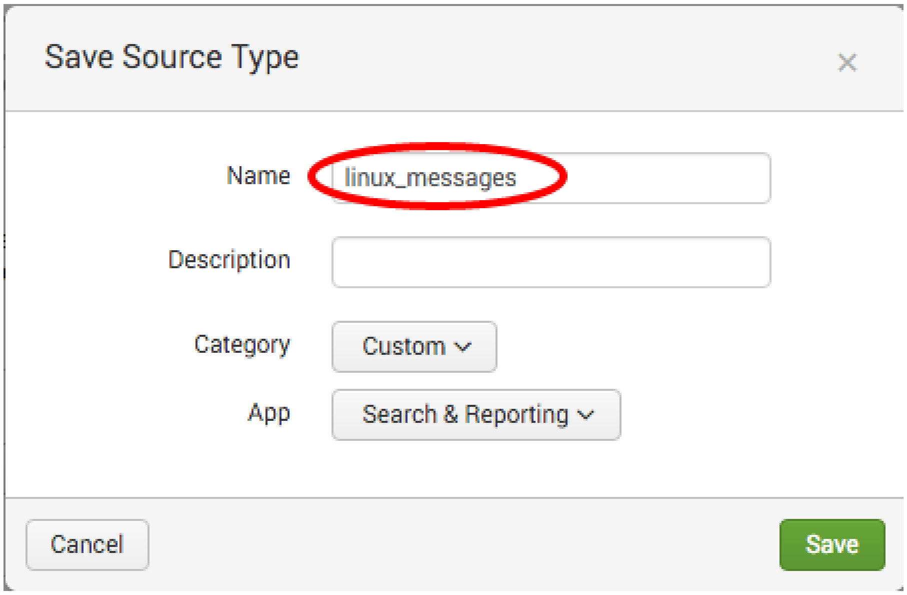
TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from from any API, service, or database with a script.



✓ File input has been created successfully.

Configure your inputs by going to Settings > Data Inputs



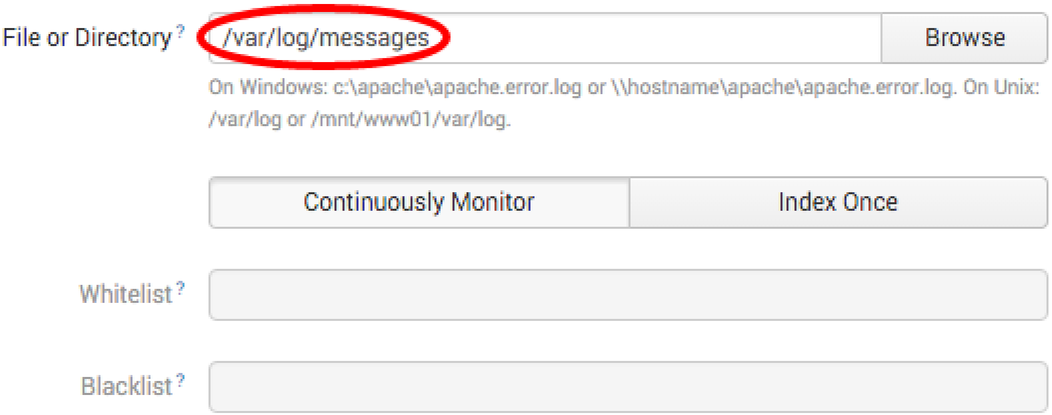
Save Source Type

Name: linux_messages

Description:

Category: Custom

App: Search & Reporting

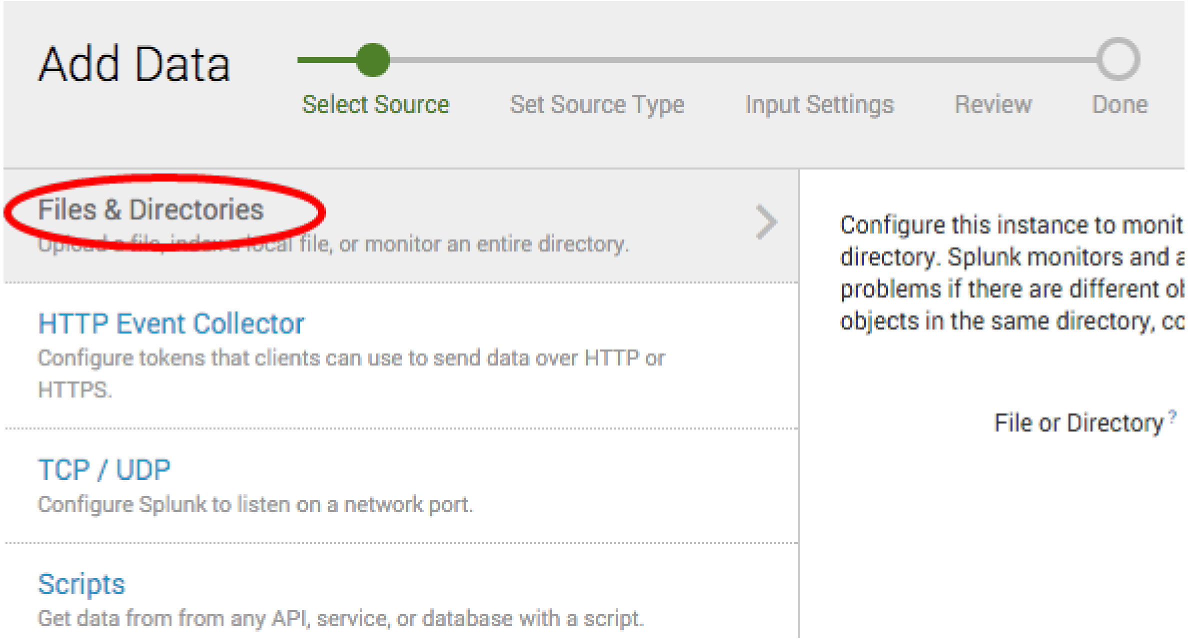


File or Directory: /var/log/messages

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Whitelist:

Blacklist:



Add Data

Select Source | Set Source Type | Input Settings | Review | Done

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

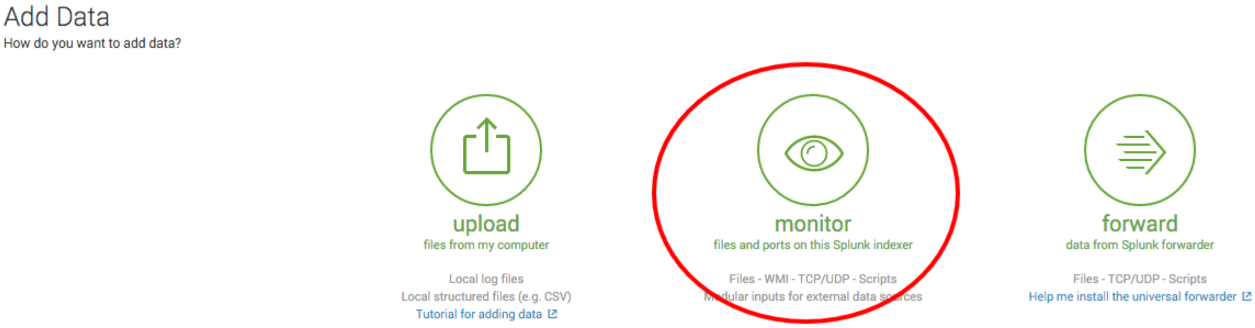
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from from any API, service, or database with a script.

Configure this instance to monit
directory. Splunk monitors and a
problems if there are different ol
objects in the same directory, cc

File or Directory ?

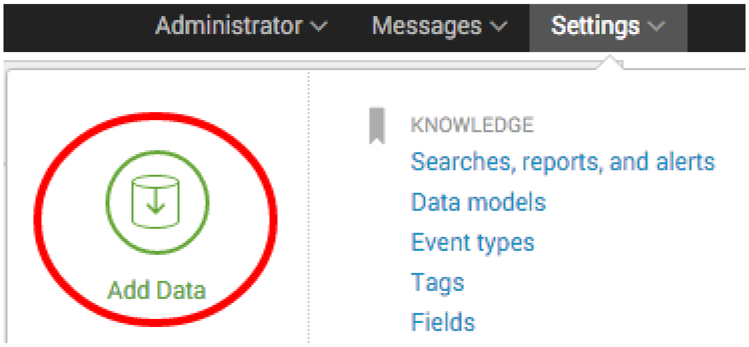


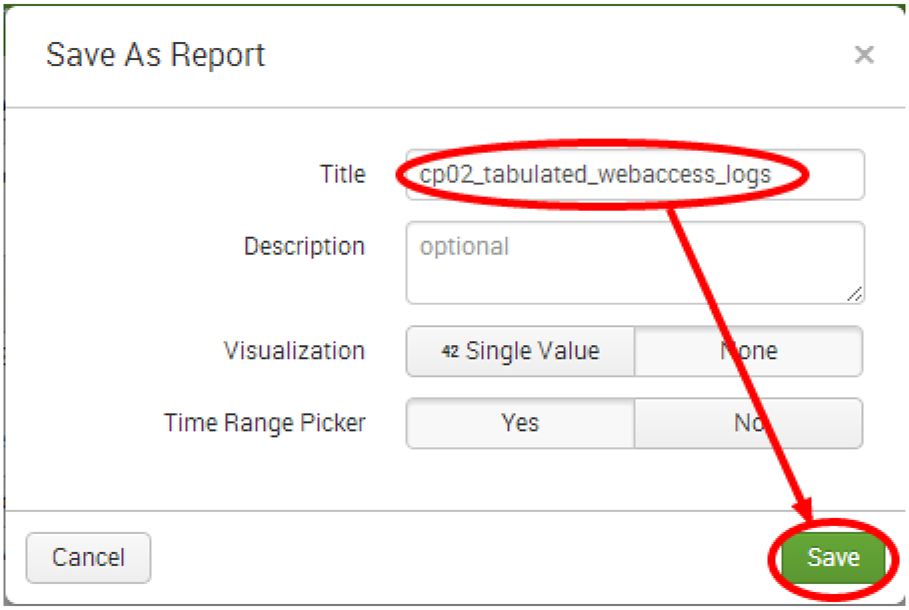
Add Data
How do you want to add data?

upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

monitor
files and ports on this Splunk indexer
Files - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

forward
data from Splunk forwarder
Files - TCP/UDP - Scripts
Help me install the universal forwarder





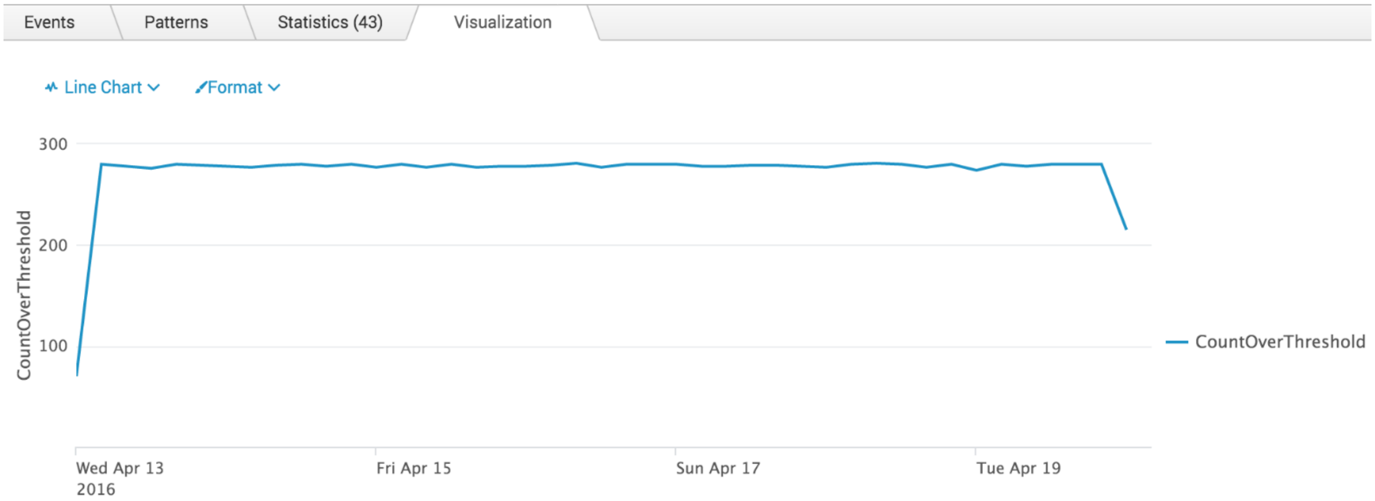
Save As Report

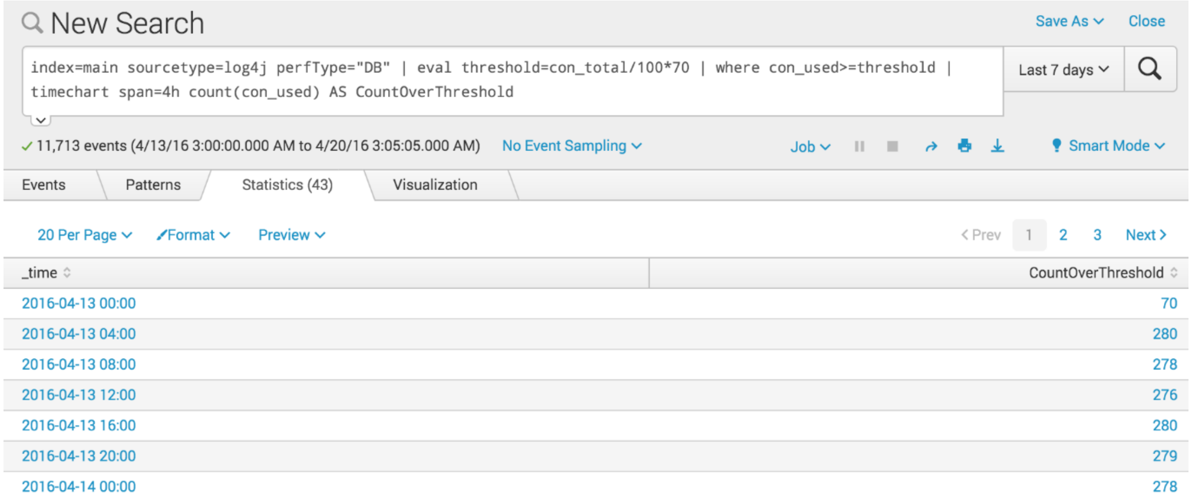
Title: cp02_tabulated_webaccess_logs

Description: optional

Visualization: 42 Single Value | None

Time Range Picker: Yes | No

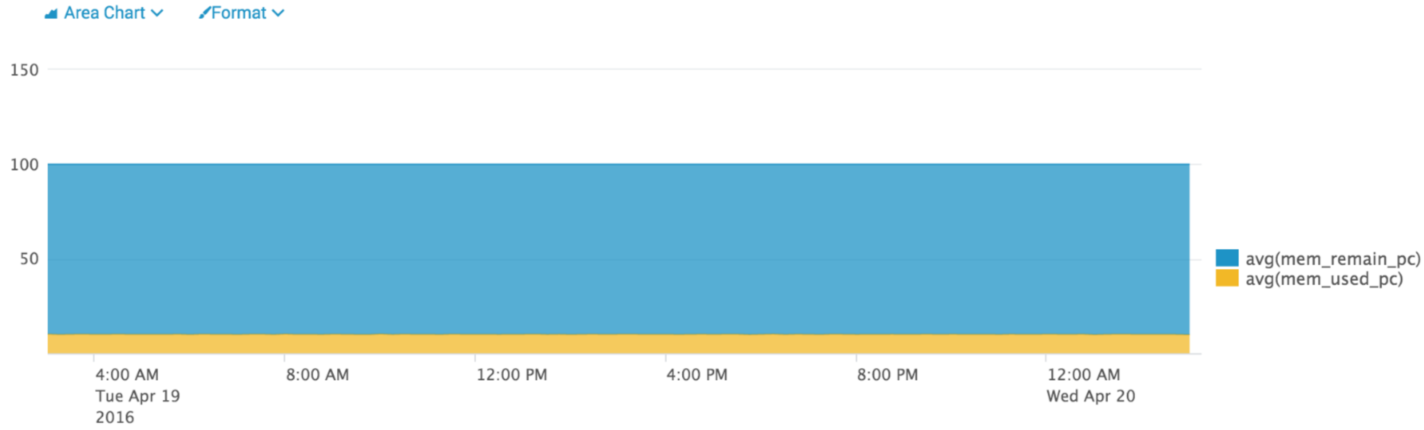


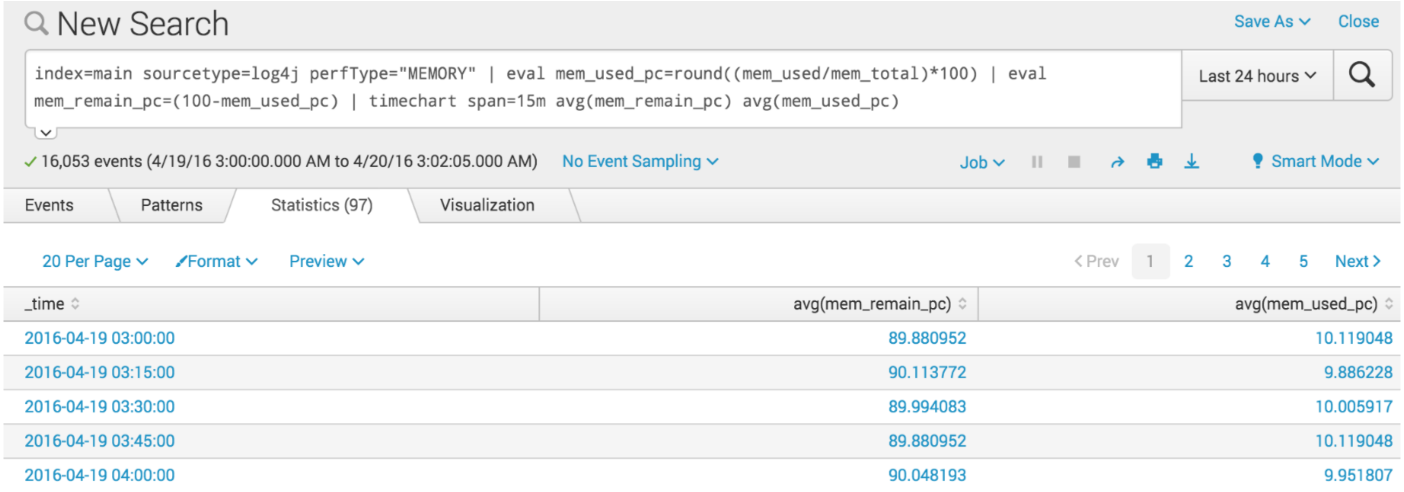


```
index=main sourcetype=log4j perfType="DB" | eval threshold=con_total/100*70 | where con_used>=threshold |
timechart span=4h count(con_used) AS CountOverThreshold
```

✓ 11,713 events (4/13/16 3:00:00.000 AM to 4/20/16 3:05:05.000 AM)

_time	CountOverThreshold
2016-04-13 00:00	70
2016-04-13 04:00	280
2016-04-13 08:00	278
2016-04-13 12:00	276
2016-04-13 16:00	280
2016-04-13 20:00	279
2016-04-14 00:00	278

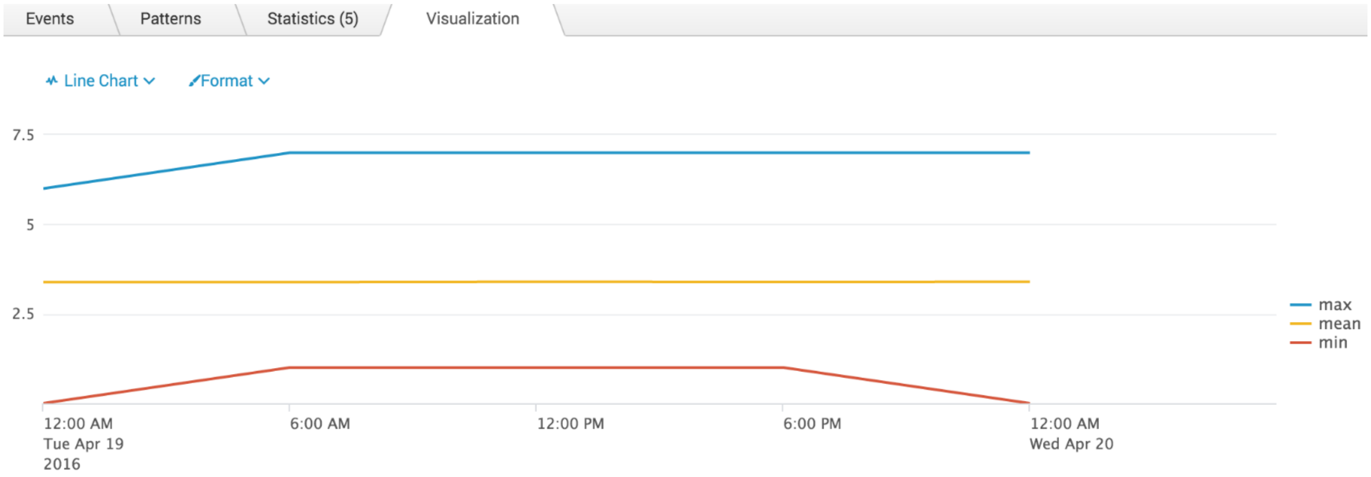


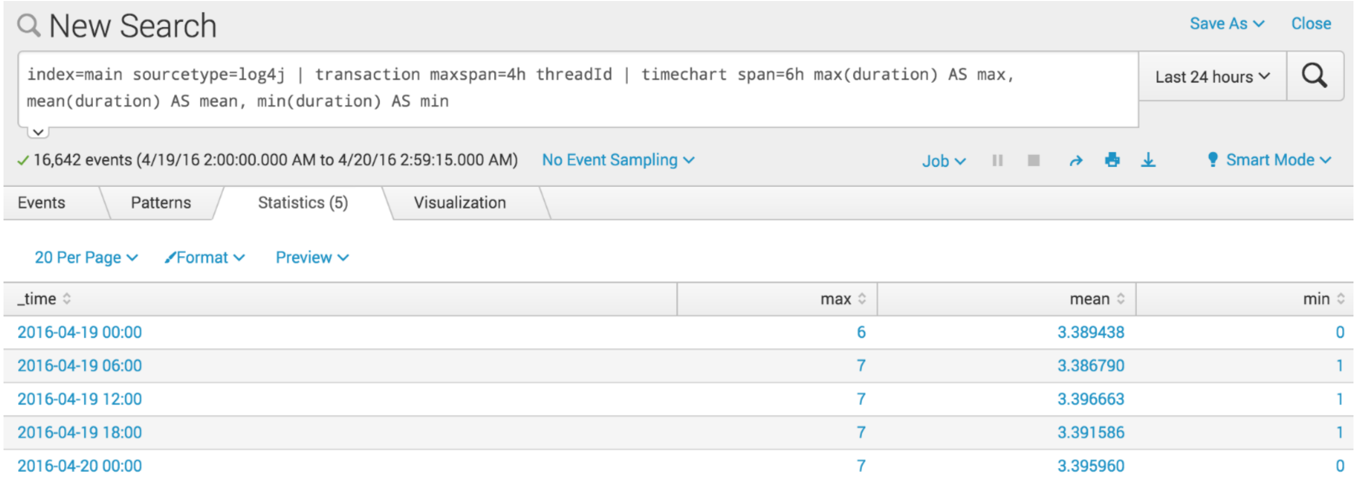


```
index=main sourcetype=log4j perfType="MEMORY" | eval mem_used_pc=round((mem_used/mem_total)*100) | eval
mem_remain_pc=(100-mem_used_pc) | timechart span=15m avg(mem_remain_pc) avg(mem_used_pc)
```

✓ 16,053 events (4/19/16 3:00:00.000 AM to 4/20/16 3:02:05.000 AM)

_time	avg(mem_remain_pc)	avg(mem_used_pc)
2016-04-19 03:00:00	89.880952	10.119048
2016-04-19 03:15:00	90.113772	9.886228
2016-04-19 03:30:00	89.994083	10.005917
2016-04-19 03:45:00	89.880952	10.119048
2016-04-19 04:00:00	90.048193	9.951807

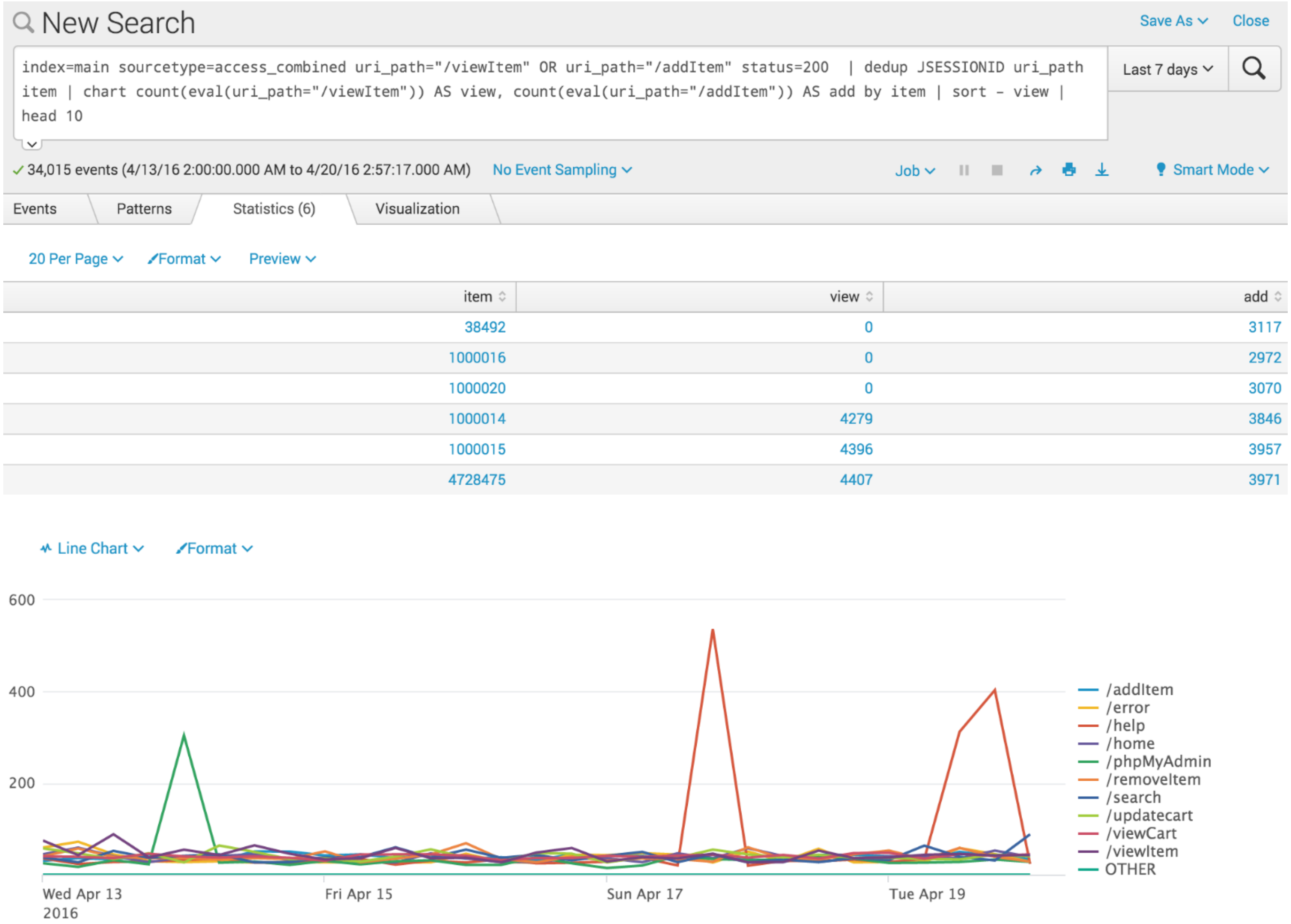




```
index=main sourcetype=log4j | transaction maxspan=4h threadId | timechart span=6h max(duration) AS max,
mean(duration) AS mean, min(duration) AS min
```

✓ 16,642 events (4/19/16 2:00:00.000 AM to 4/20/16 2:59:15.000 AM)

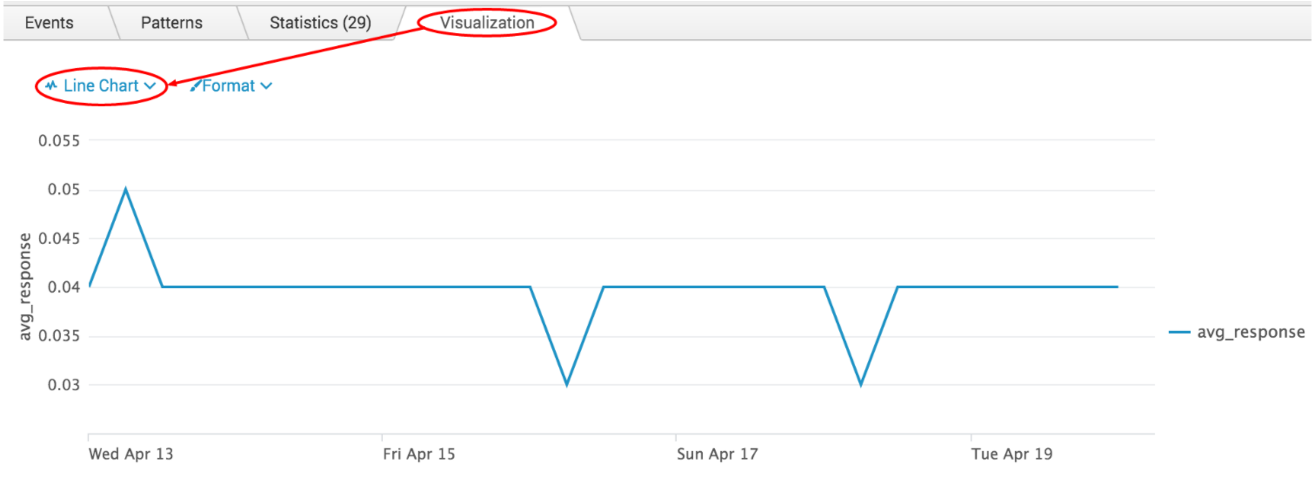
_time	max	mean	min
2016-04-19 00:00	6	3.389438	0
2016-04-19 06:00	7	3.386790	1
2016-04-19 12:00	7	3.396663	1
2016-04-19 18:00	7	3.391586	1
2016-04-20 00:00	7	3.395960	0

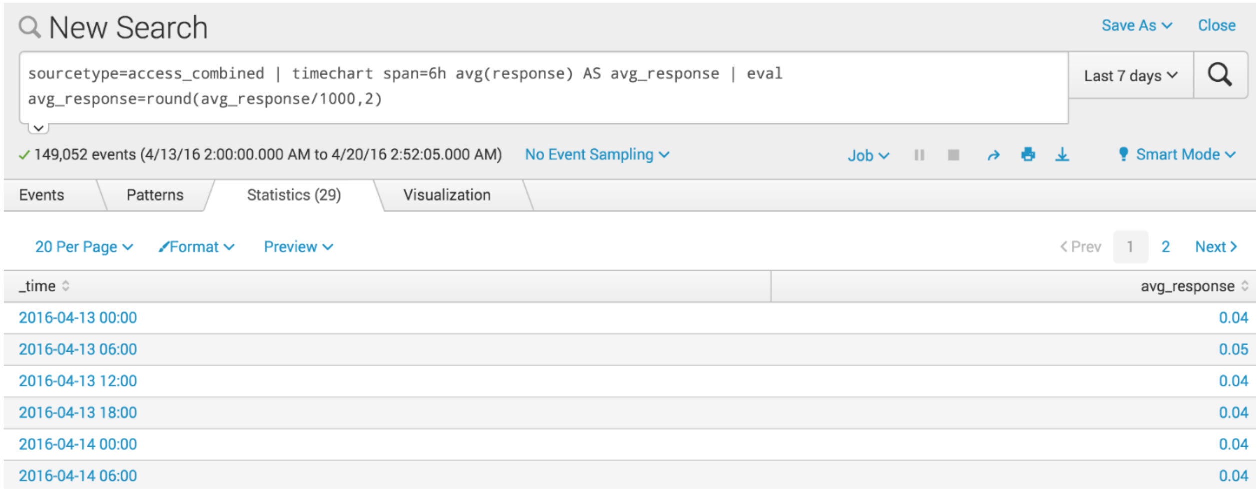


```
index=main sourcetype=access_combined uri_path="/viewItem" OR uri_path="/addItem" status=200  | dedup JSESSIONID uri_path
item | chart count(eval(uri_path="/viewItem")) AS view, count(eval(uri_path="/addItem")) AS add by item | sort - view |
head 10
```

✓ 34,015 events (4/13/16 2:00:00.000 AM to 4/20/16 2:57:17.000 AM)

item	view	add
38492	0	3117
1000016	0	2972
1000020	0	3070
1000014	4279	3846
1000015	4396	3957
4728475	4407	3971

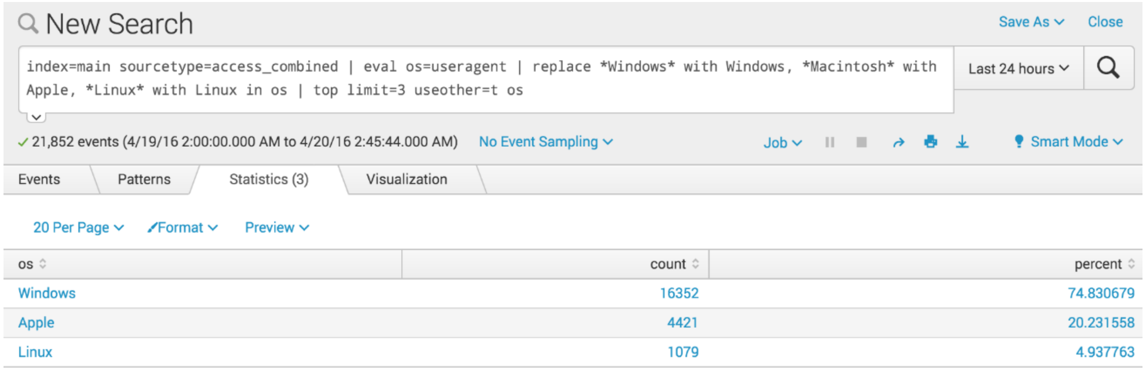




```
sourcetype=access_combined | timechart span=6h avg(response) AS avg_response | eval
avg_response=round(avg_response/1000,2)
```

✓ 149,052 events (4/13/16 2:00:00.000 AM to 4/20/16 2:52:05.000 AM) No Event Sampling

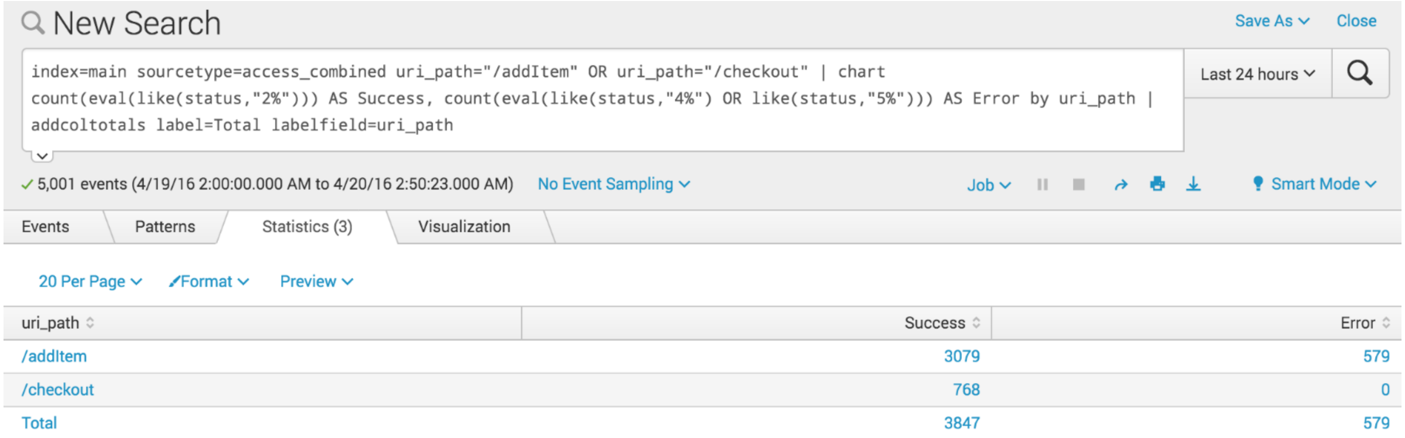
_time	avg_response
2016-04-13 00:00	0.04
2016-04-13 06:00	0.05
2016-04-13 12:00	0.04
2016-04-13 18:00	0.04
2016-04-14 00:00	0.04
2016-04-14 06:00	0.04



```
index=main sourcetype=access_combined | eval os=useragent | replace *Windows* with Windows, *Macintosh* with
Apple, *Linux* with Linux in os | top limit=3 useother=t os
```

✓ 21,852 events (4/19/16 2:00:00.000 AM to 4/20/16 2:45:44.000 AM) No Event Sampling

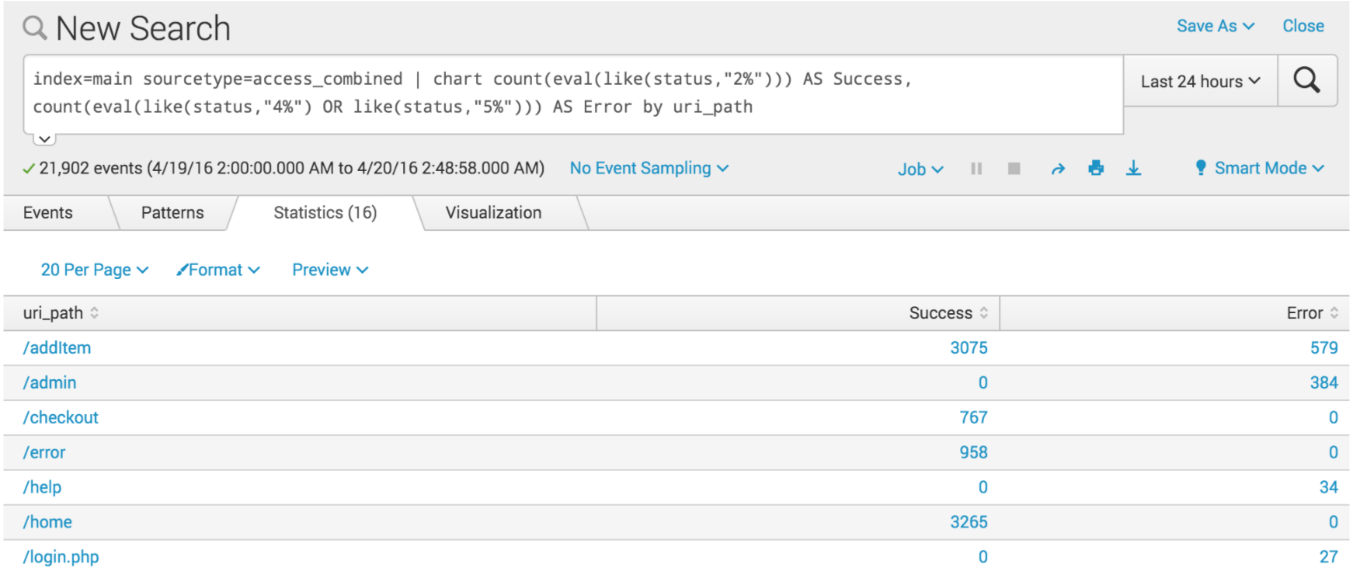
os	count	percent
Windows	16352	74.830679
Apple	4421	20.231558
Linux	1079	4.937763



```
index=main sourcetype=access_combined uri_path="/addItem" OR uri_path="/checkout" | chart
count(eval(like(status,"2%"))) AS Success, count(eval(like(status,"4%") OR like(status,"5%"))) AS Error by uri_path |
addcoltotals label=Total labelfield=uri_path
```

✓ 5,001 events (4/19/16 2:00:00.000 AM to 4/20/16 2:50:23.000 AM)

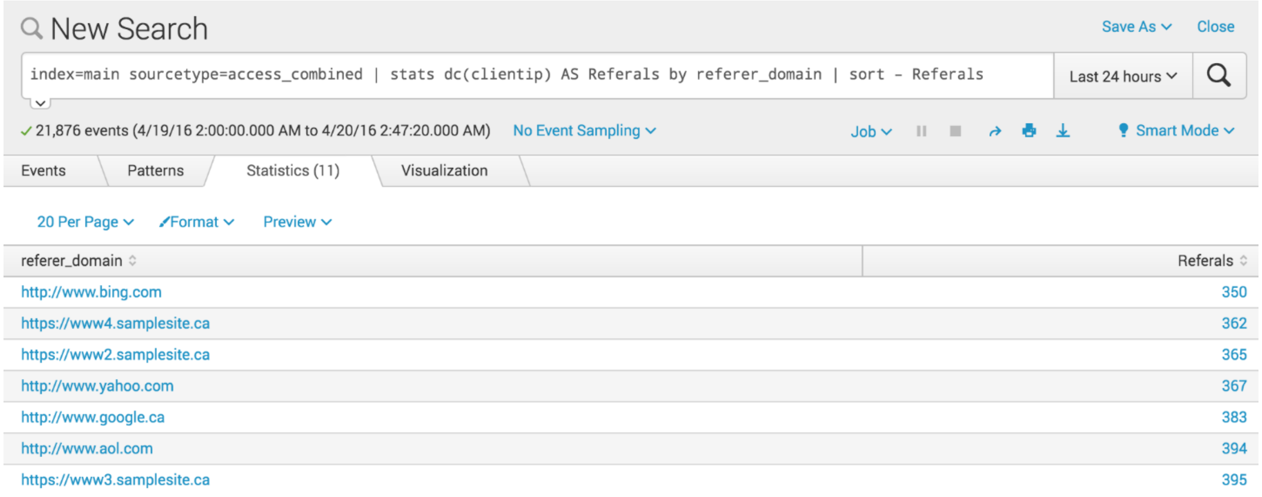
uri_path	Success	Error
/addItem	3079	579
/checkout	768	0
Total	3847	579



```
index=main sourcetype=access_combined | chart count(eval(like(status,"2%"))) AS Success,
count(eval(like(status,"4%") OR like(status,"5%"))) AS Error by uri_path
```

✓ 21,902 events (4/19/16 2:00:00.000 AM to 4/20/16 2:48:58.000 AM)

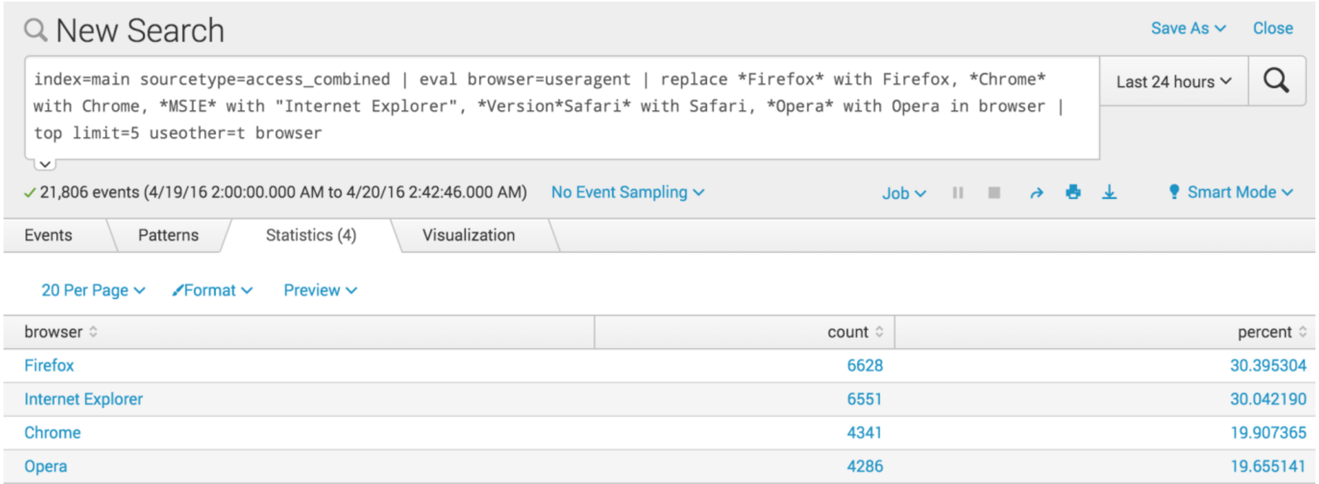
uri_path	Success	Error
/addItem	3075	579
/admin	0	384
/checkout	767	0
/error	958	0
/help	0	34
/home	3265	0
/login.php	0	27



```
index=main sourcetype=access_combined | stats dc(clientip) AS Referals by referer_domain | sort - Referals
```

✓ 21,876 events (4/19/16 2:00:00.000 AM to 4/20/16 2:47:20.000 AM)

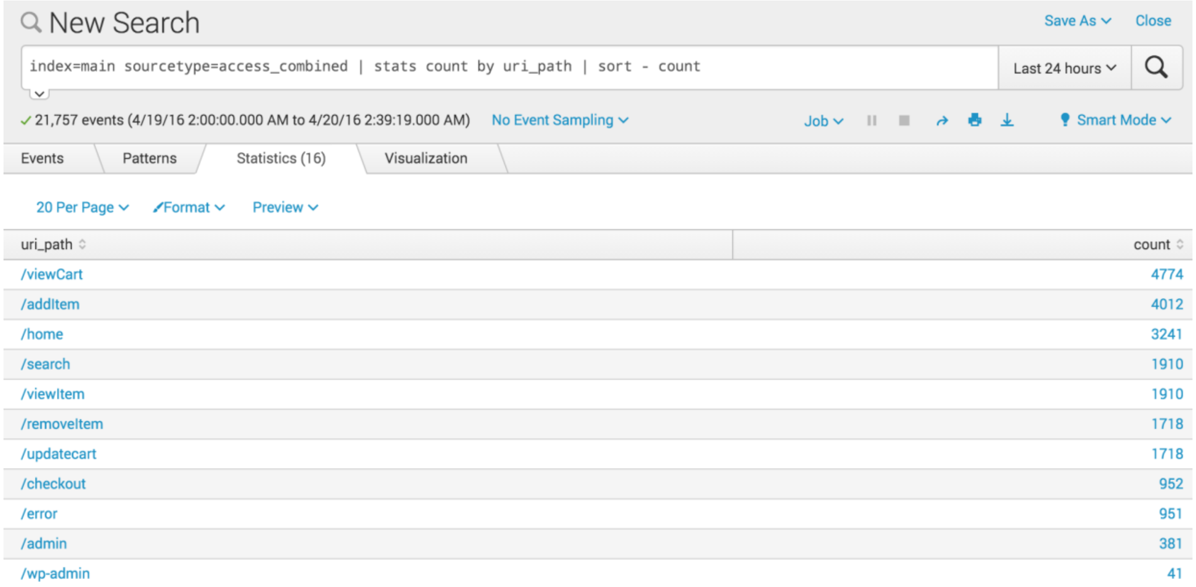
referer_domain	Referals
http://www.bing.com	350
https://www4.samplesite.ca	362
https://www2.samplesite.ca	365
http://www.yahoo.com	367
http://www.google.ca	383
http://www.aol.com	394
https://www3.samplesite.ca	395



```
index=main sourcetype=access_combined | eval browser=useragent | replace *Firefox* with Firefox, *Chrome*
with Chrome, *MSIE* with "Internet Explorer", *Version*Safari* with Safari, *Opera* with Opera in browser |
top limit=5 useother=t browser
```

✓ 21,806 events (4/19/16 2:00:00.000 AM to 4/20/16 2:42:46.000 AM)

browser	count	percent
Firefox	6628	30.395304
Internet Explorer	6551	30.042190
Chrome	4341	19.907365
Opera	4286	19.655141

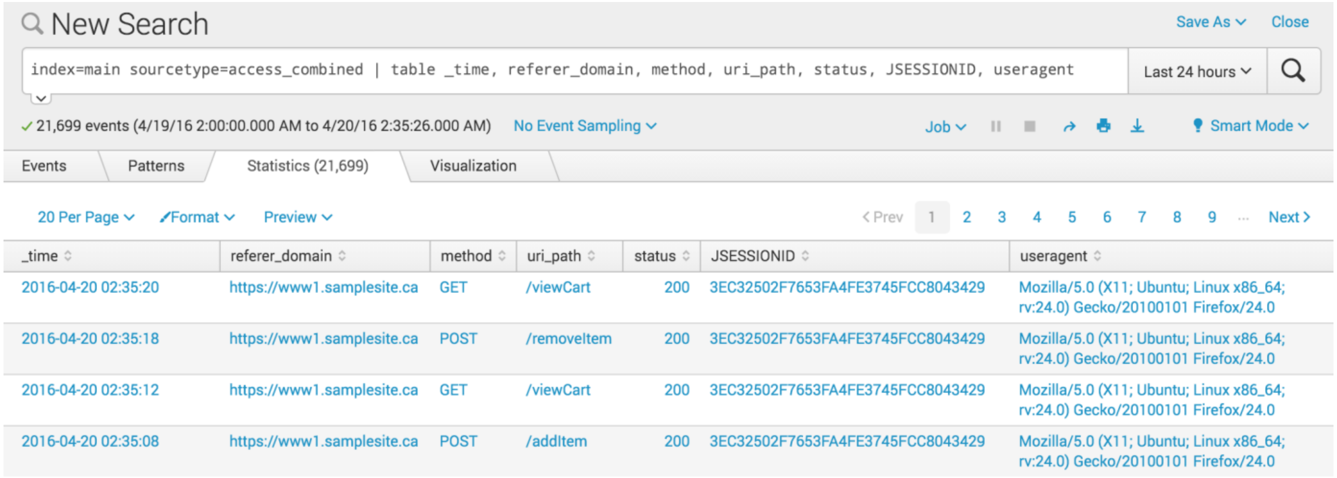


```
index=main sourcetype=access_combined | stats count by uri_path | sort - count
```

✓ 21,757 events (4/19/16 2:00:00.000 AM to 4/20/16 2:39:19.000 AM)

Statistics (16)

uri_path	count
/viewCart	4774
/addItem	4012
/home	3241
/search	1910
/viewItem	1910
/removeItem	1718
/updatecart	1718
/checkout	952
/error	951
/admin	381
/wp-admin	41

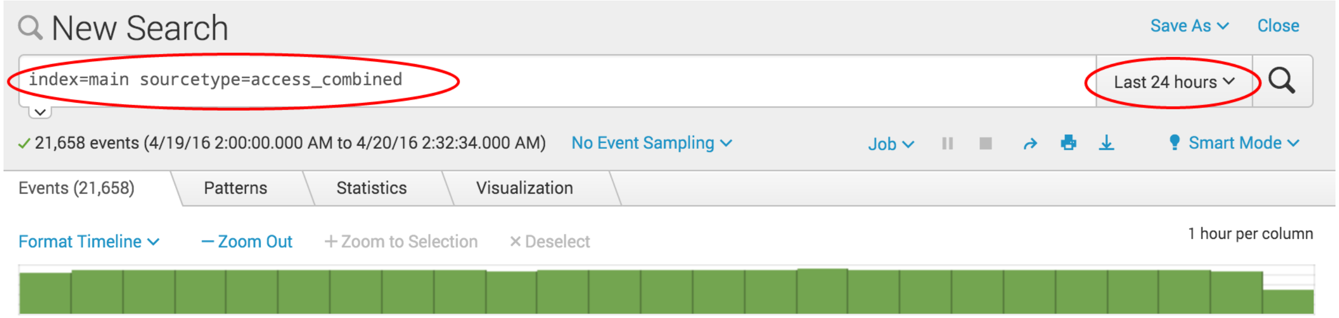


```
index=main sourcetype=access_combined | table _time, referer_domain, method, uri_path, status, JSESSIONID, useragent
```

✓ 21,699 events (4/19/16 2:00:00.000 AM to 4/20/16 2:35:26.000 AM)

Statistics (21,699)

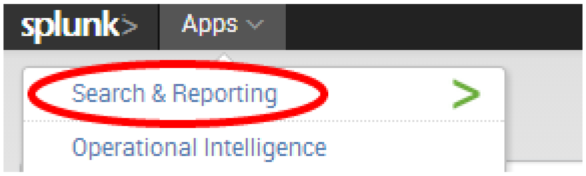
_time	referer_domain	method	uri_path	status	JSESSIONID	useragent
2016-04-20 02:35:20	https://www1.samplesite.ca	GET	/viewCart	200	3EC32502F7653FA4FE3745FCC8043429	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0
2016-04-20 02:35:18	https://www1.samplesite.ca	POST	/removeItem	200	3EC32502F7653FA4FE3745FCC8043429	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0
2016-04-20 02:35:12	https://www1.samplesite.ca	GET	/viewCart	200	3EC32502F7653FA4FE3745FCC8043429	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0
2016-04-20 02:35:08	https://www1.samplesite.ca	POST	/addItem	200	3EC32502F7653FA4FE3745FCC8043429	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0

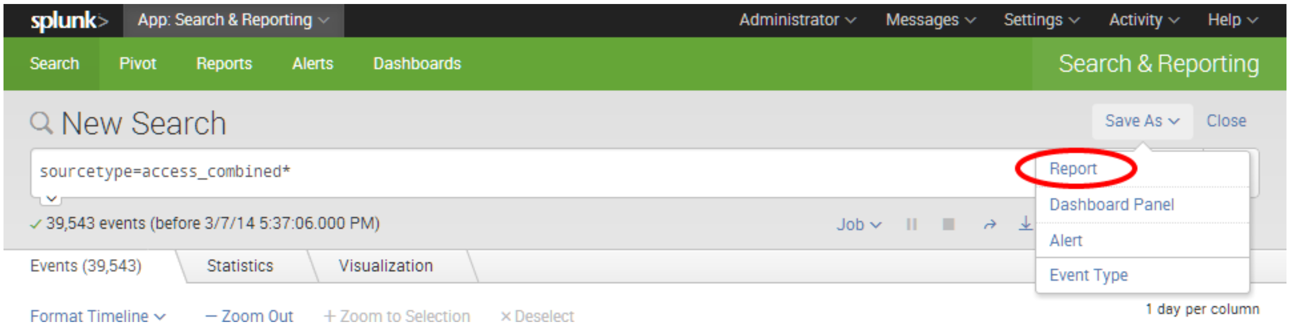


```
index=main sourcetype=access_combined
```

✓ 21,658 events (4/19/16 2:00:00.000 AM to 4/20/16 2:32:34.000 AM)

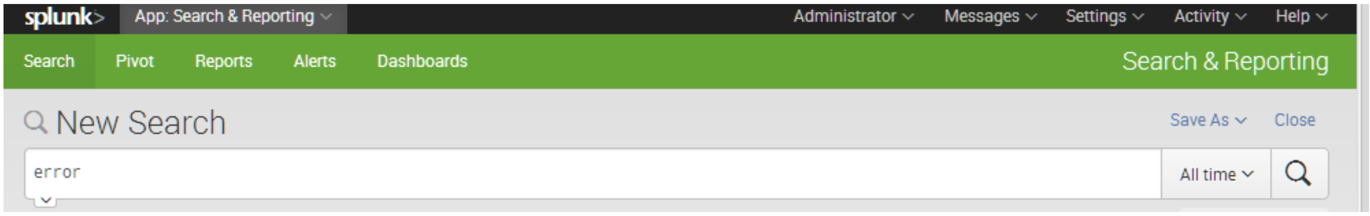
Events (21,658)



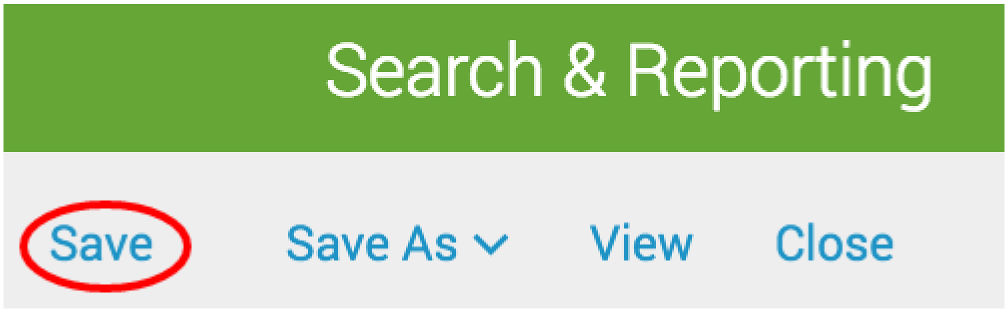


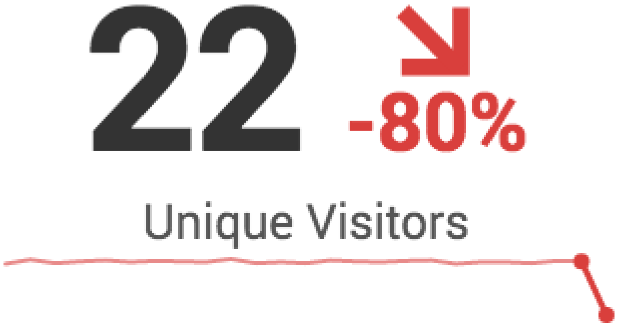
sourcetype=access_combined*

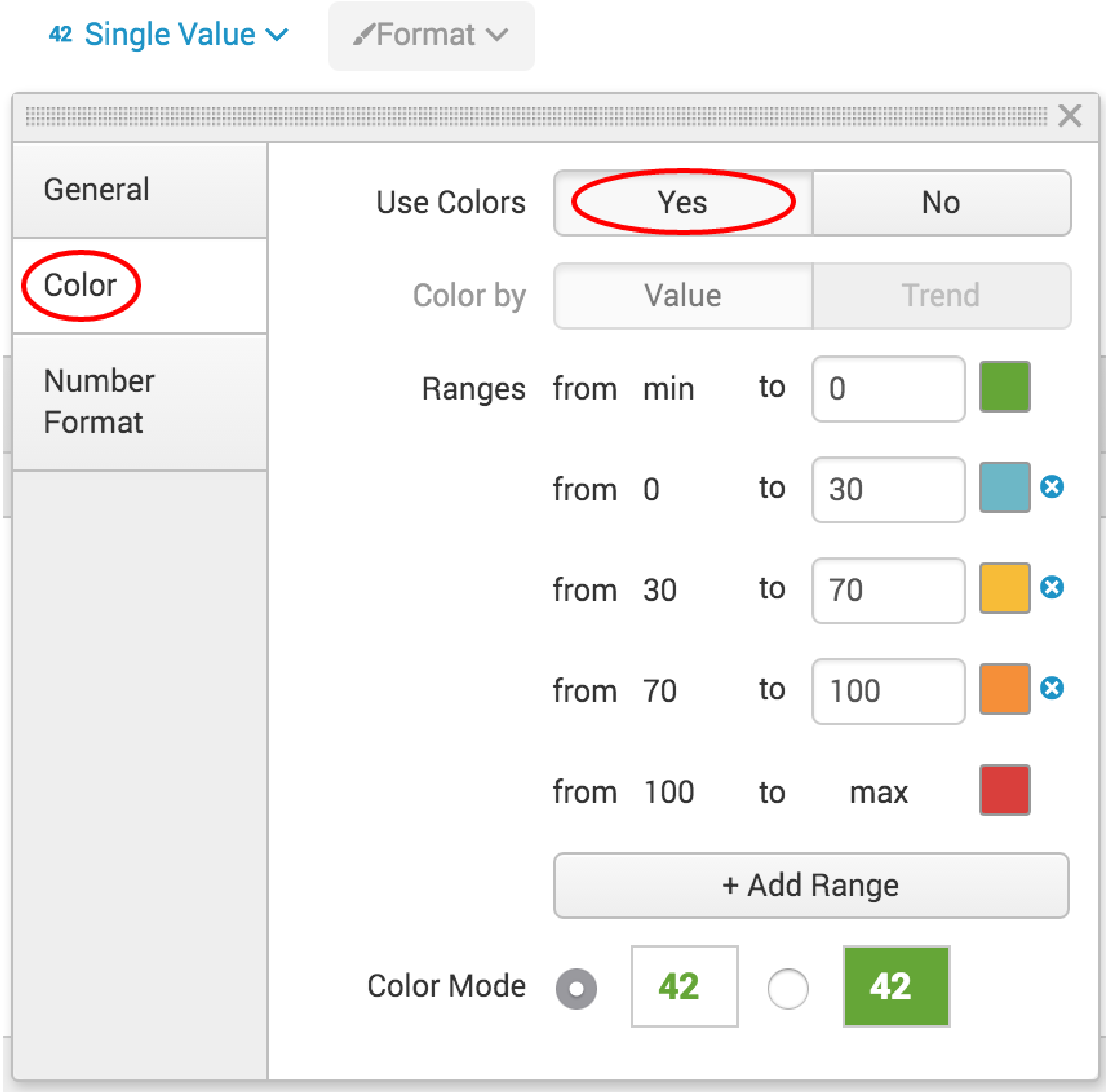
✓ 39,543 events (before 3/7/14 5:37:06.000 PM)



error


Search & Reporting
Save
Save As
View
Close


22
-80%
Unique Visitors



[✓ Color]

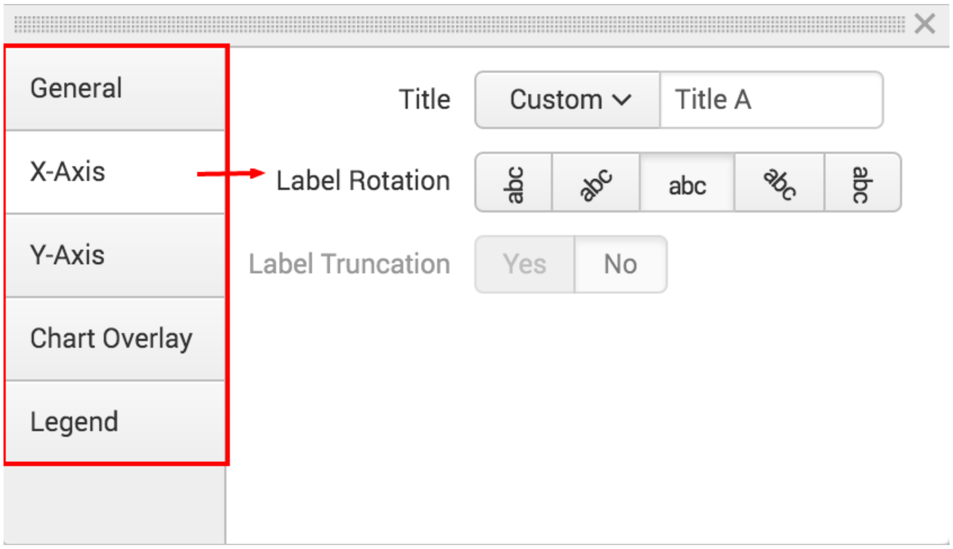
Use Colors [✓ Yes] No

Color by Value Trend

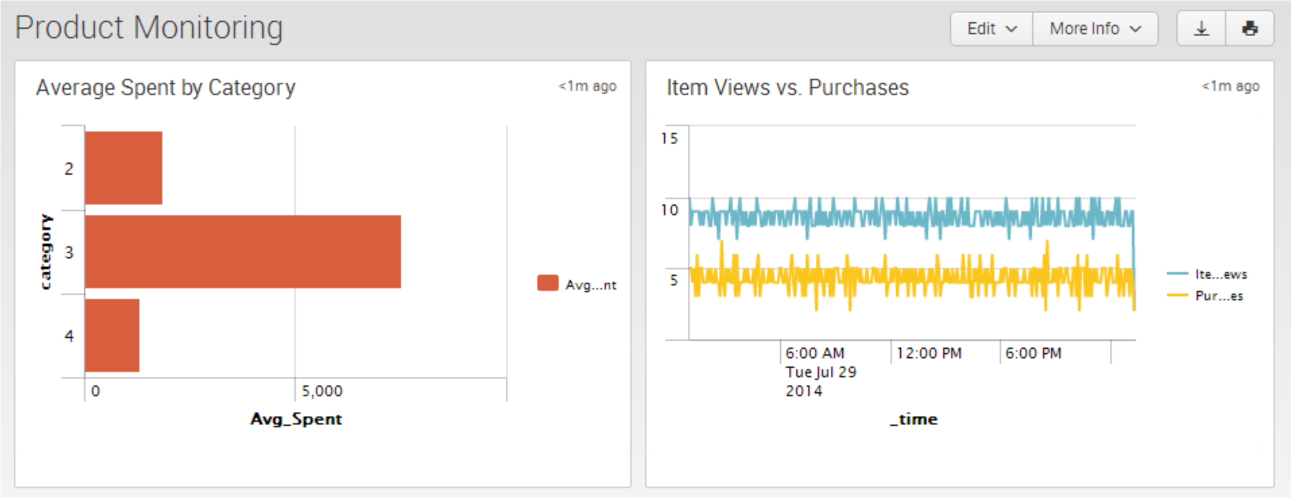
Ranges	from	min	to	0	🟩	
	from	0	to	30	🟦	⊗
	from	30	to	70	🟨	⊗
	from	70	to	100	🟧	⊗
	from	100	to	max	🟥	

+ Add Range

Color Mode ● 42 ○ 42



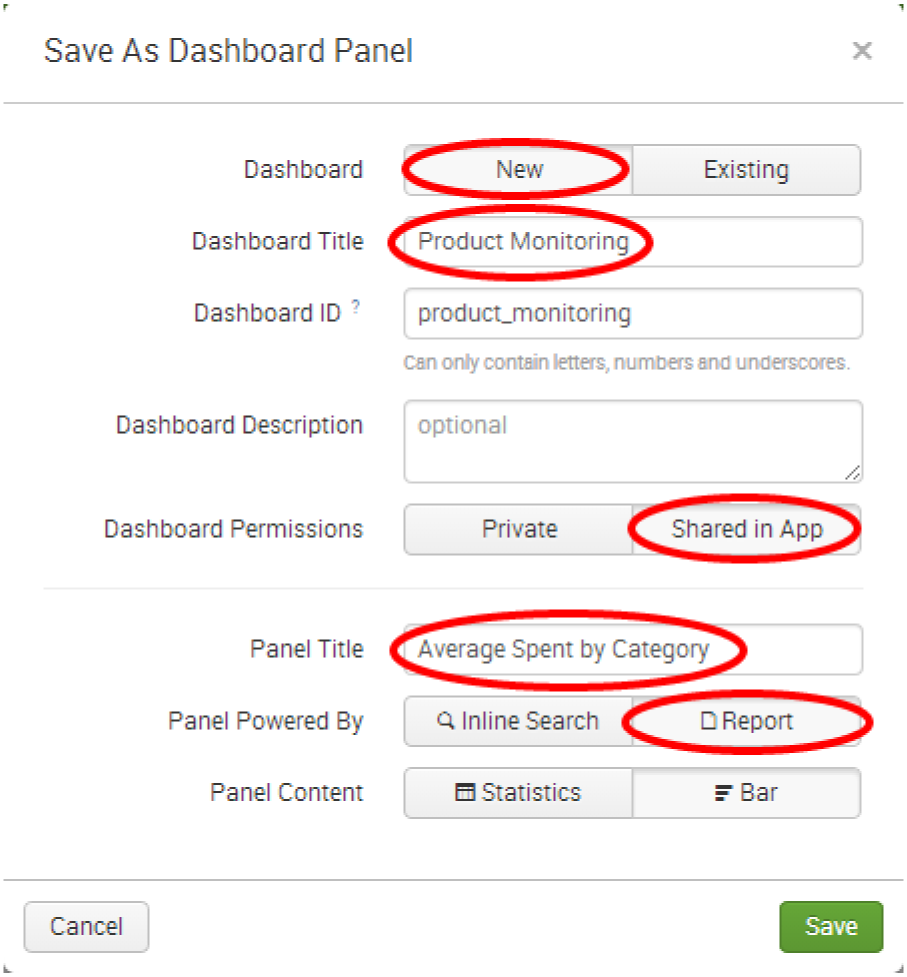
Title: Custom — Title A



Product Monitoring

Average Spent by Category

Item Views vs. Purchases



Save As Dashboard Panel

Dashboard: [✓ New] Existing

Dashboard Title: [✓ Product Monitoring]

Dashboard ID ?: product_monitoring

Can only contain letters, numbers and underscores.

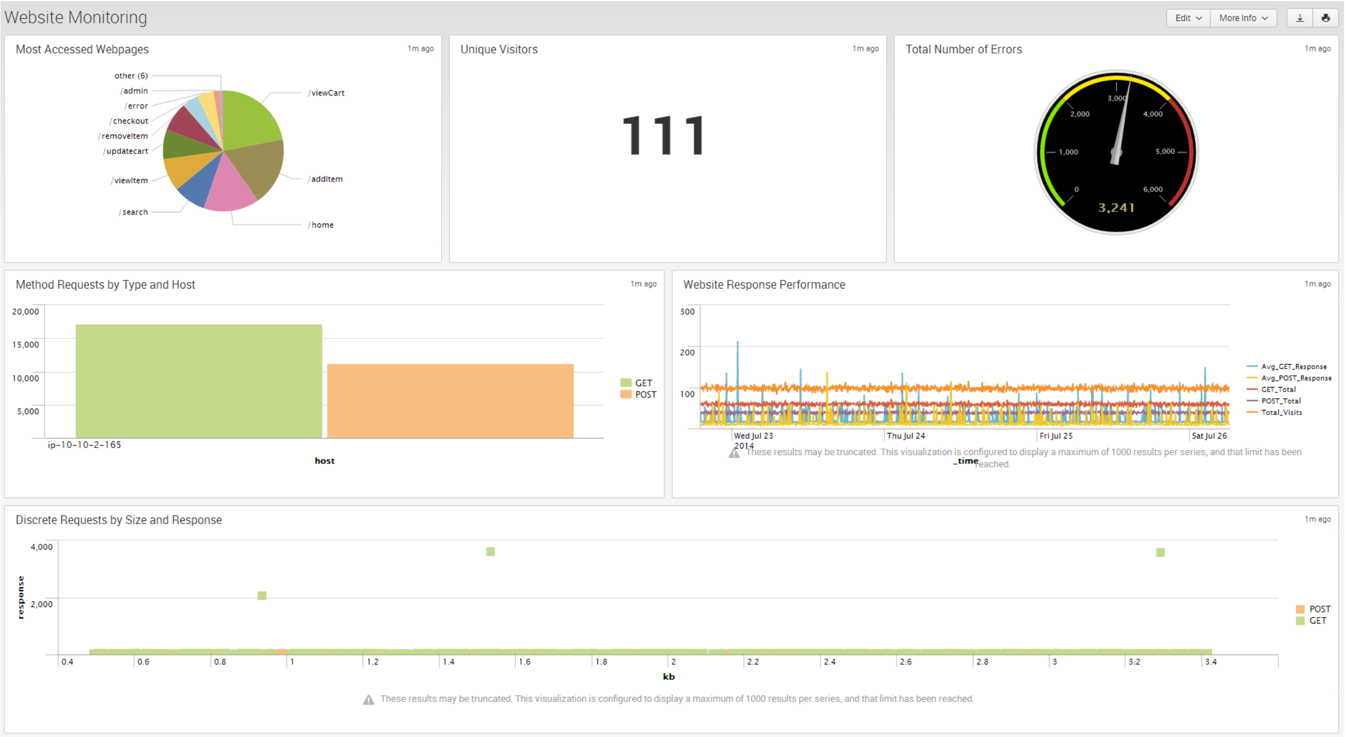
Dashboard Description: optional

Dashboard Permissions: Private [✓ Shared in App]

Panel Title: [✓ Average Spent by Category]

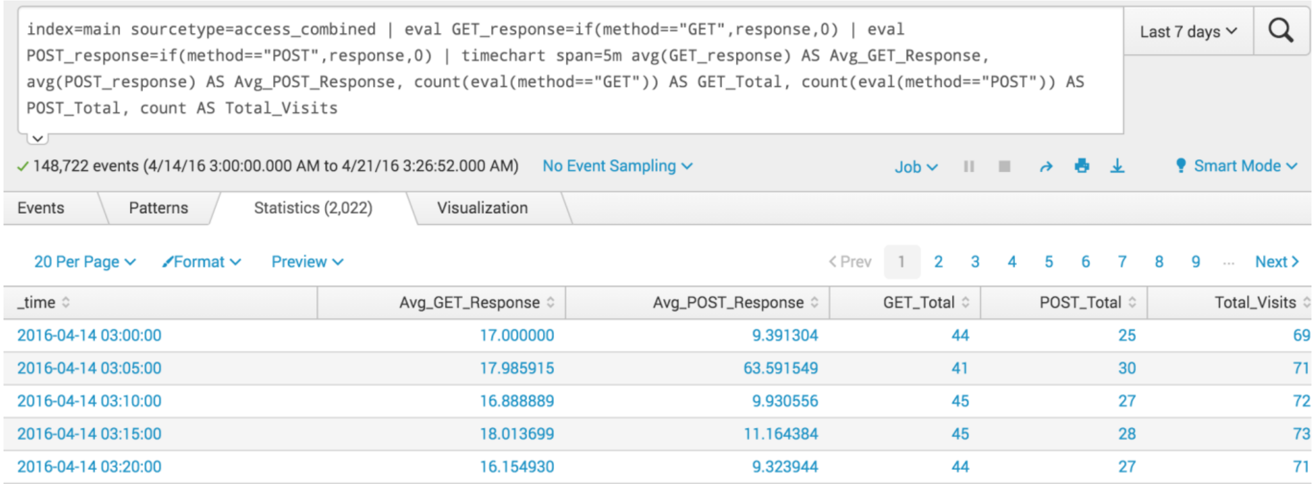
Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics Bar



These results may be truncated. This visualization is configured to display a maximum of 1000 results per series, and that limit has been reached.

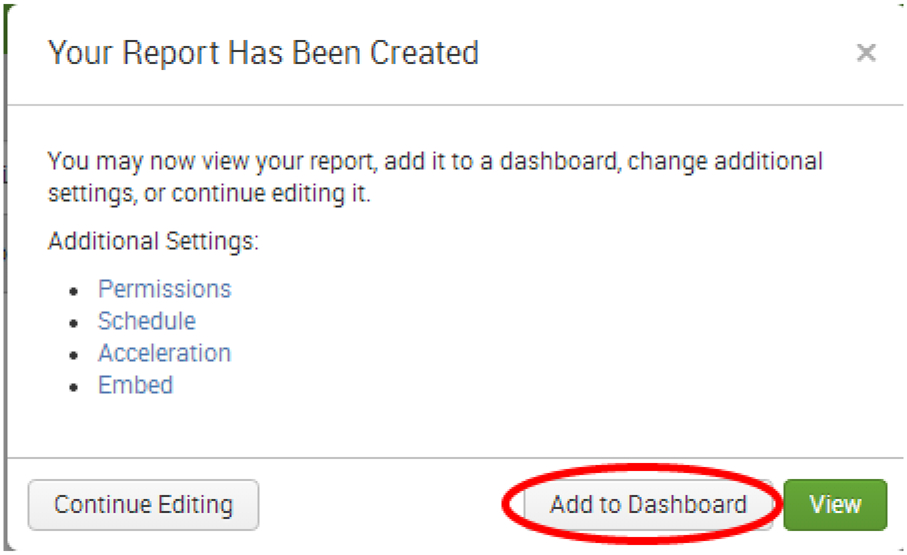
These results may be truncated. This visualization is configured to display a maximum of 1000 results per series, and that limit has been reached.



```
index=main sourcetype=access_combined | eval GET_response=if(method=="GET",response,0) | eval
POST_response=if(method=="POST",response,0) | timechart span=5m avg(GET_response) AS Avg_GET_Response,
avg(POST_response) AS Avg_POST_Response, count(eval(method=="GET")) AS GET_Total, count(eval(method=="POST")) AS
POST_Total, count AS Total_Visits
```

✓ 148,722 events (4/14/16 3:00:00.000 AM to 4/21/16 3:26:52.000 AM)

_time	Avg_GET_Response	Avg_POST_Response	GET_Total	POST_Total	Total_Visits
2016-04-14 03:00:00	17.000000	9.391304	44	25	69
2016-04-14 03:05:00	17.985915	63.591549	41	30	71
2016-04-14 03:10:00	16.888889	9.930556	45	27	72
2016-04-14 03:15:00	18.013699	11.164384	45	28	73
2016-04-14 03:20:00	16.154930	9.323944	44	27	71

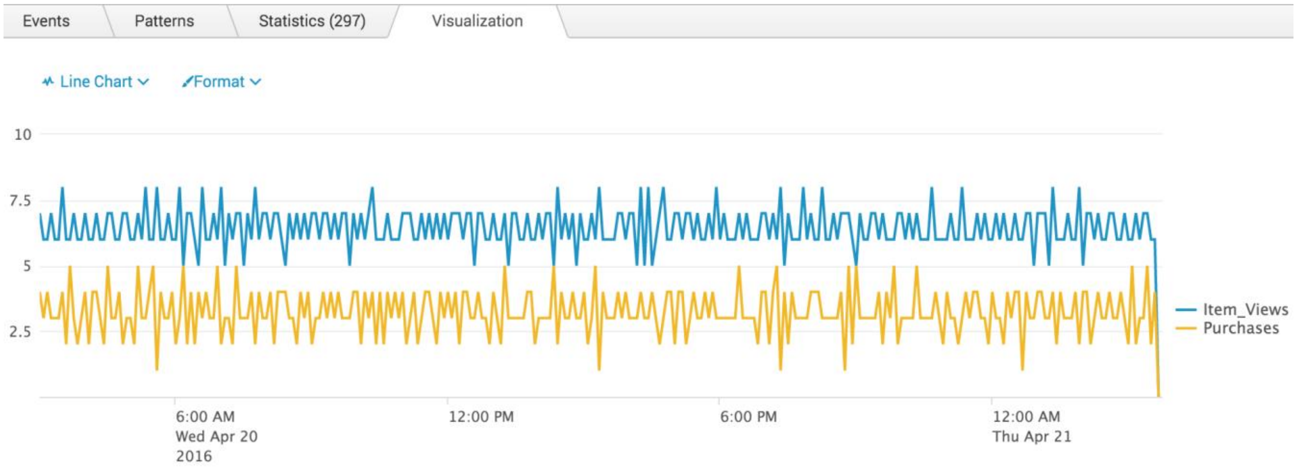


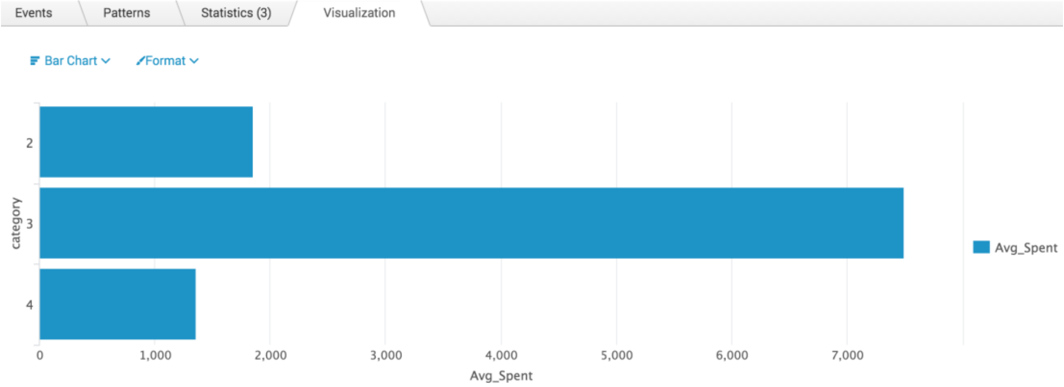
Your Report Has Been Created

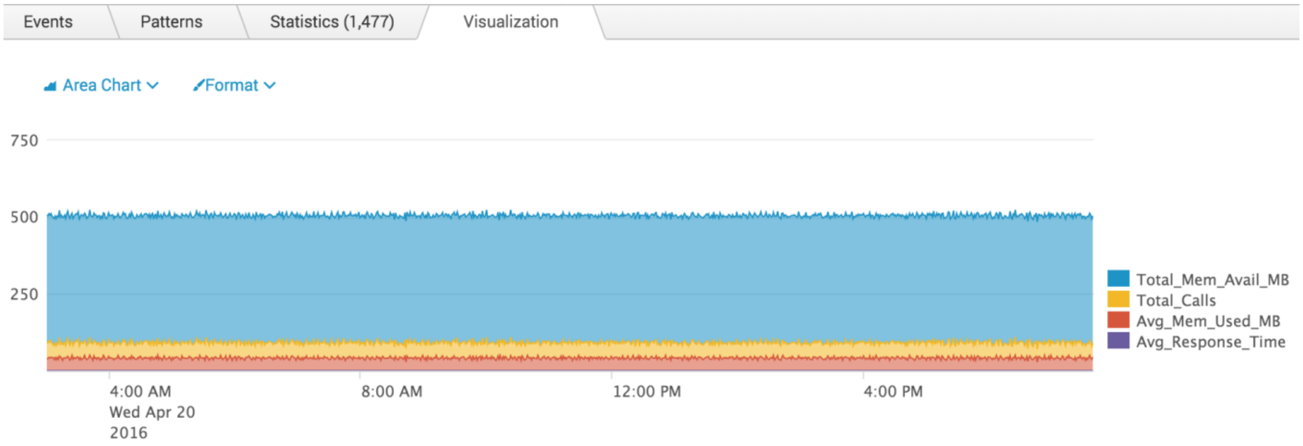
You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

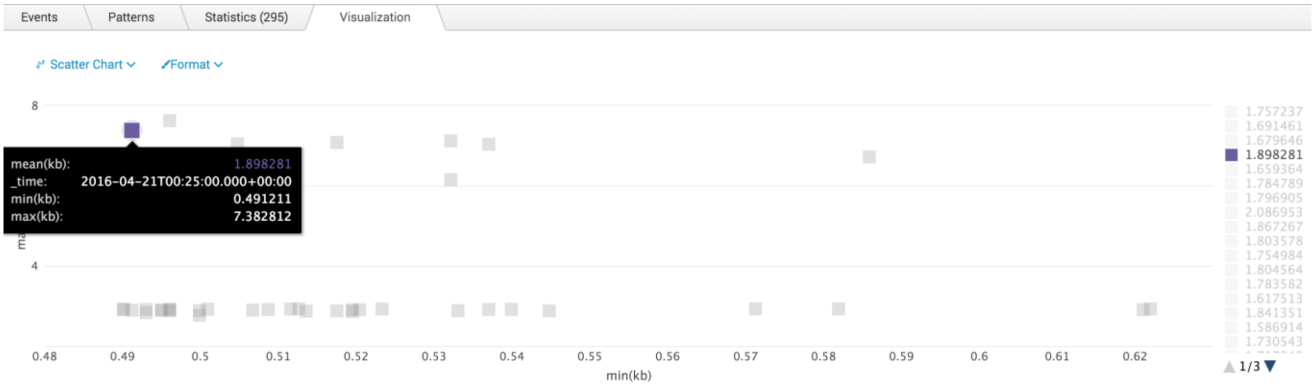
Additional Settings:

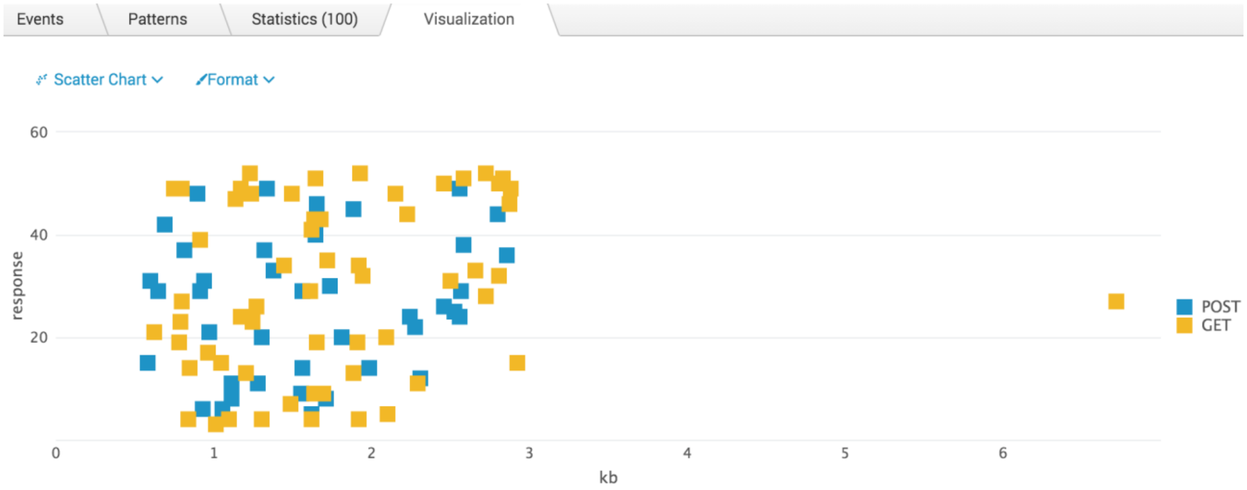
- Permissions
- Schedule
- Acceleration
- Embed

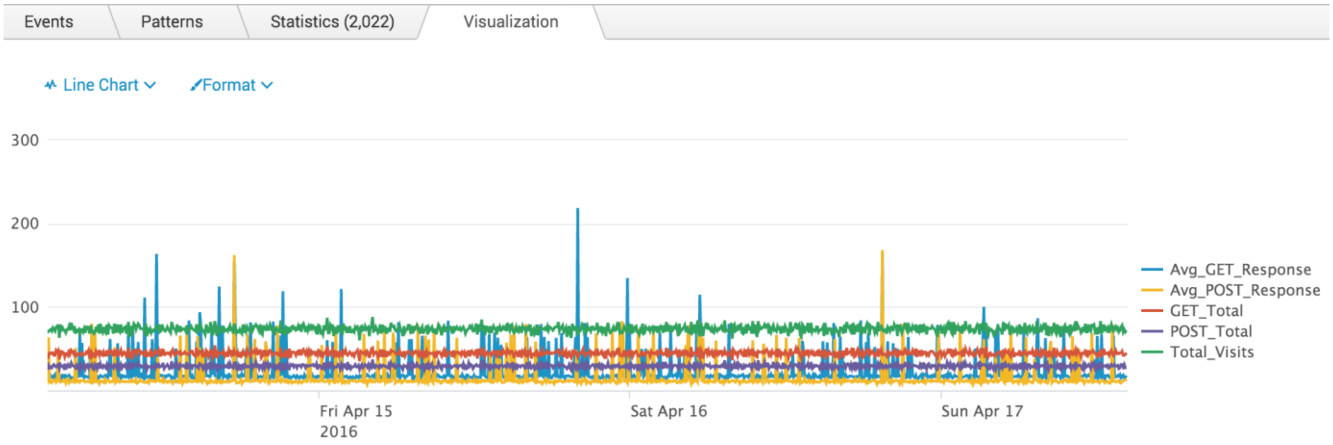


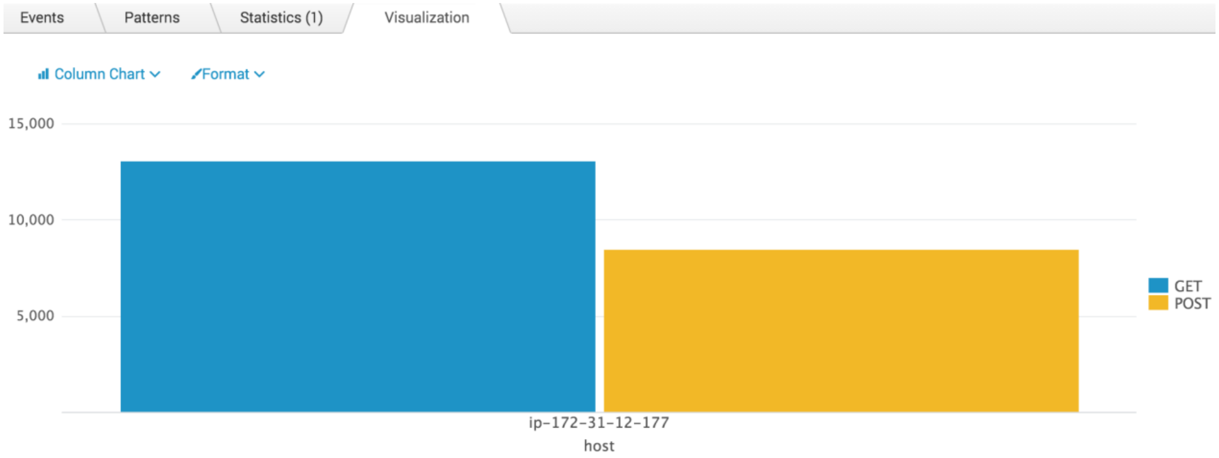


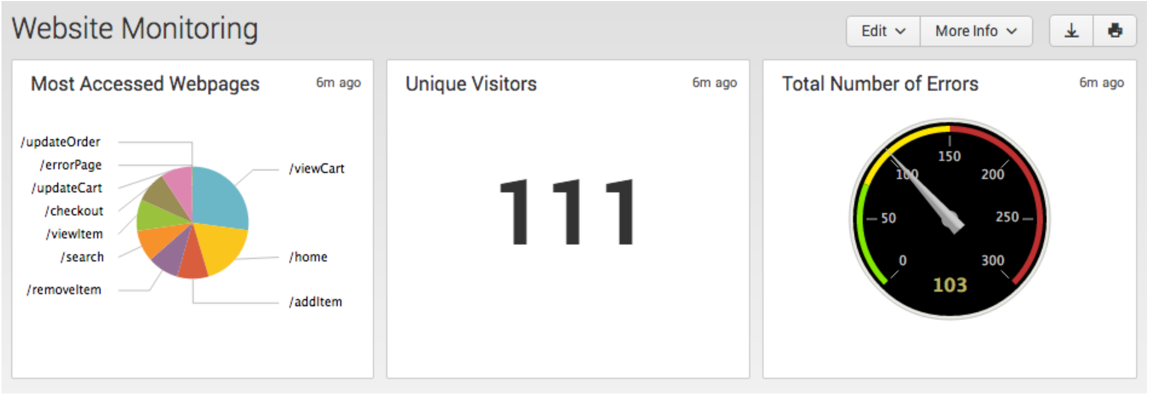


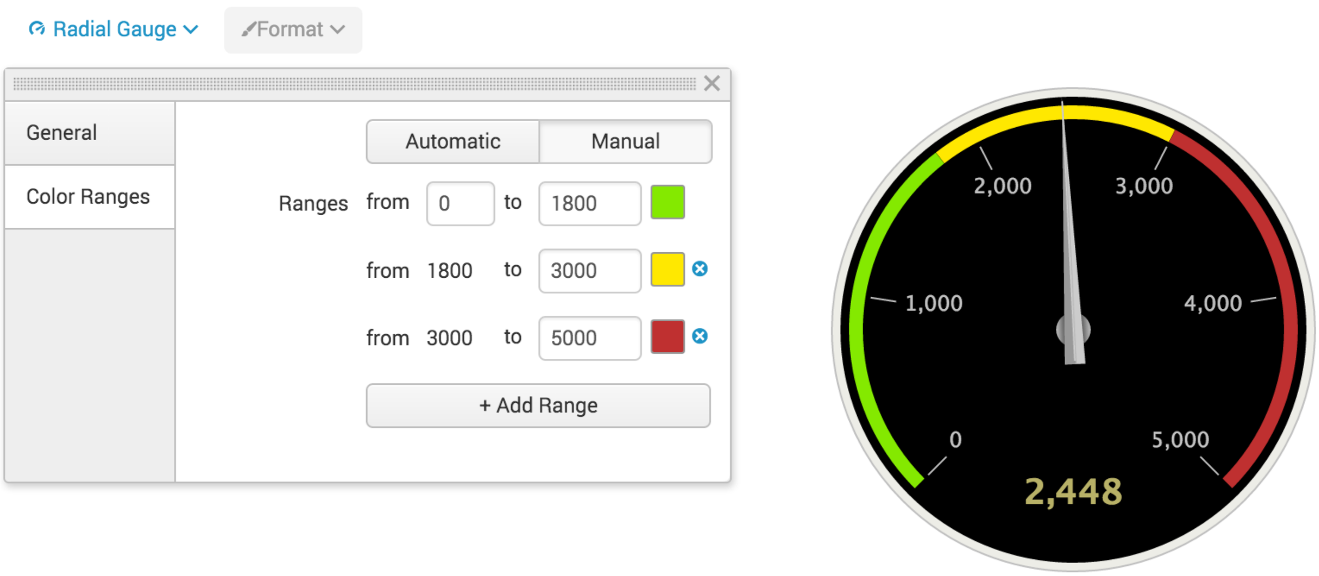

mean(kb): 1.898281
_time: 2016-04-21T00:25:00.000+00:00
min(kb): 0.491211
max(kb): 7.382812




Events
Patterns
Statistics (2,022)
Visualization
Line Chart
Format
300
200
100
Fri Apr 15
2016
Sat Apr 16
Sun Apr 17
Avg_GET_Response
Avg_POST_Response
GET_Total
POST_Total
Total_Visits


Events
Patterns
Statistics (1)
Visualization
Column Chart
Format
15,000
10,000
5,000
ip-172-31-12-177
host
GET
POST

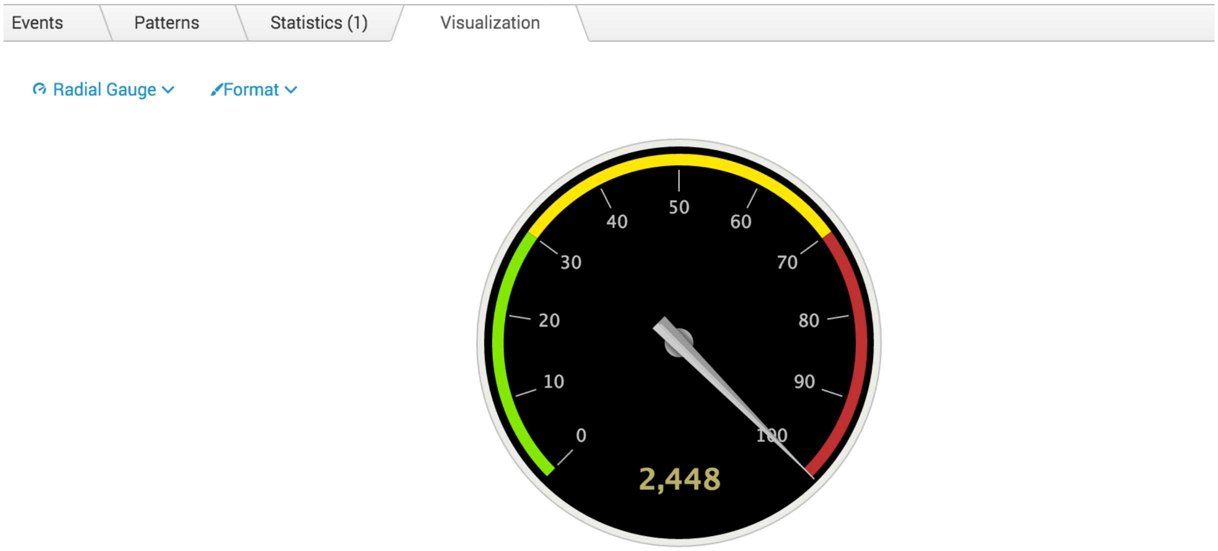

Website Monitoring
Edit
More Info
Most Accessed Webpages
6m ago
/updateOrder
/errorPage
/updateCart
/checkout
/viewItem
/search
/removeItem
/viewCart
/home
/addItem
Unique Visitors
6m ago
111
Total Number of Errors
6m ago
0
50
100
150
200
250
300
103

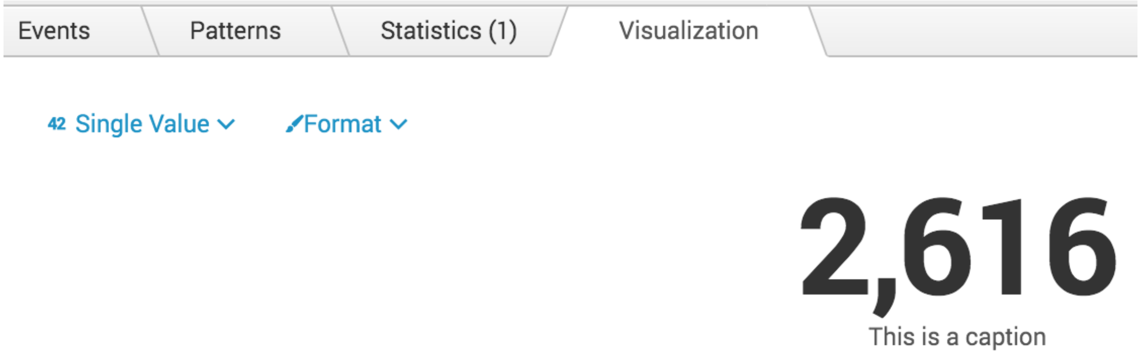


Ranges from 0 to 1800 🟩

from 1800 to 3000 🟨

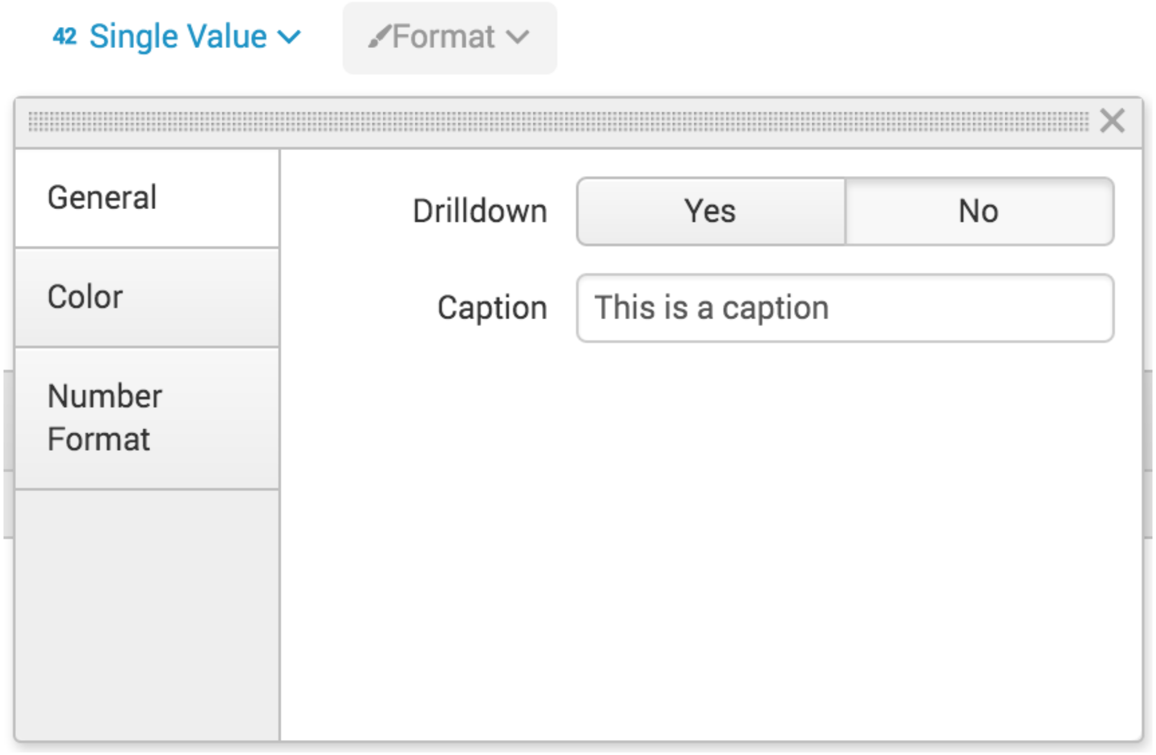
from 3000 to 5000 🟥





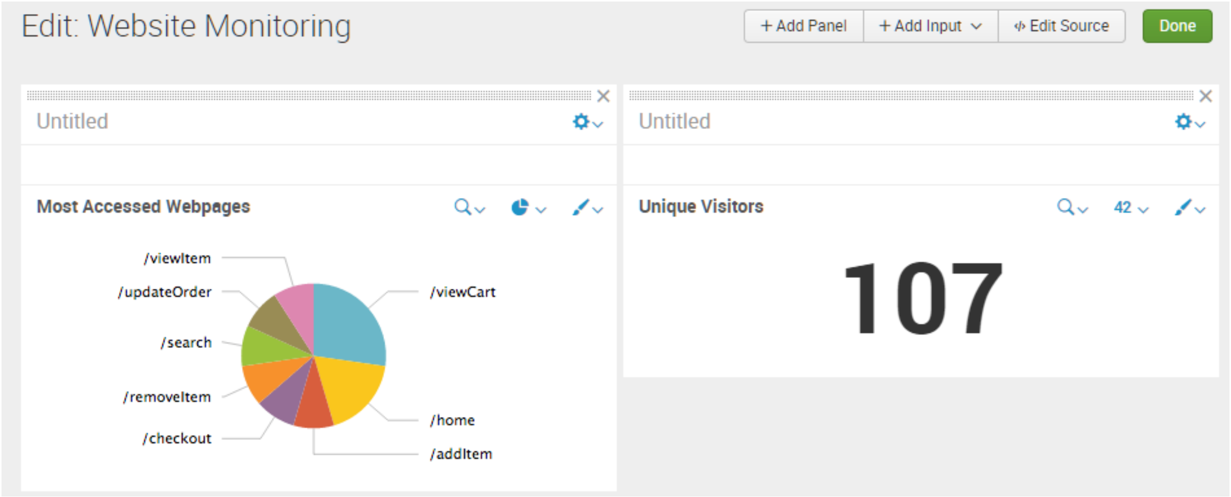
2,616

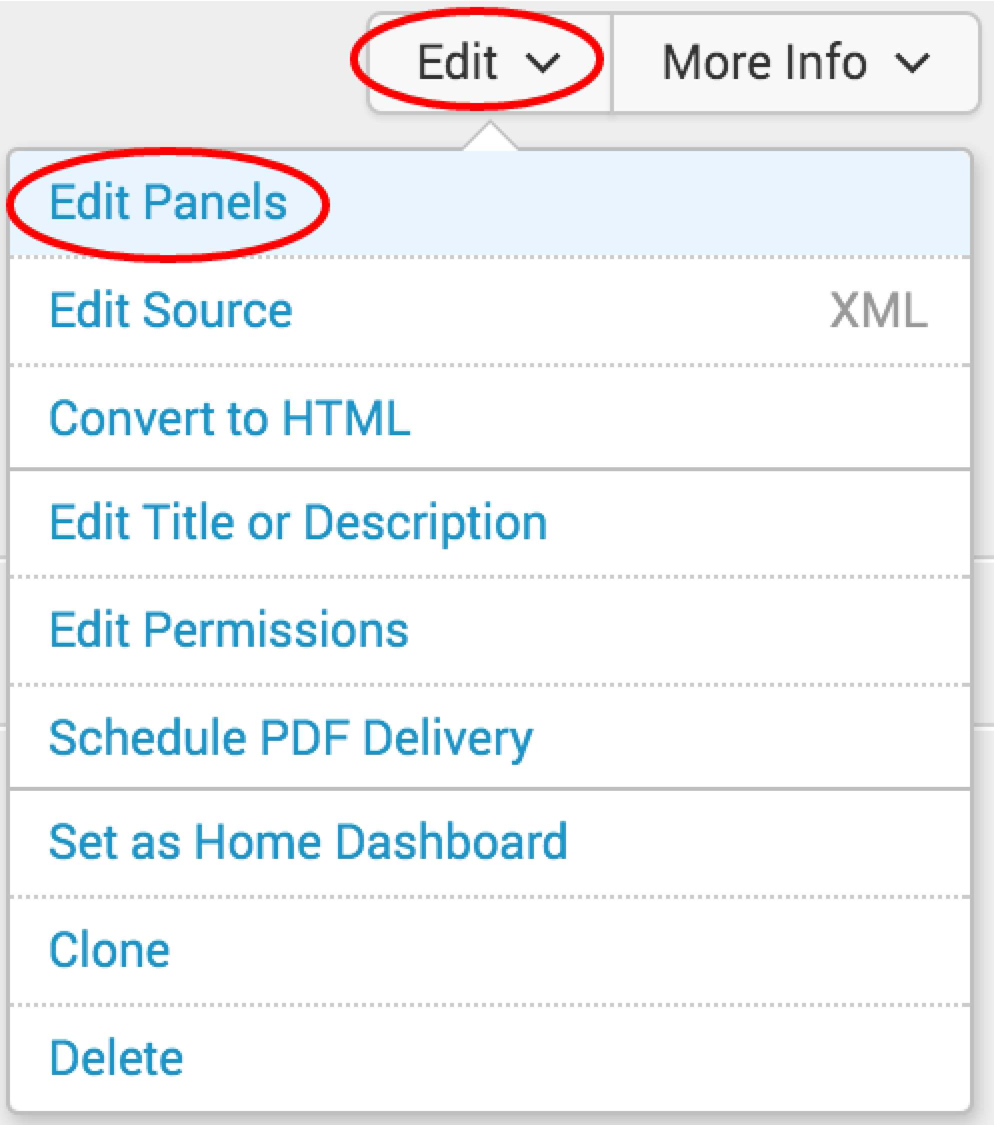
This is a caption

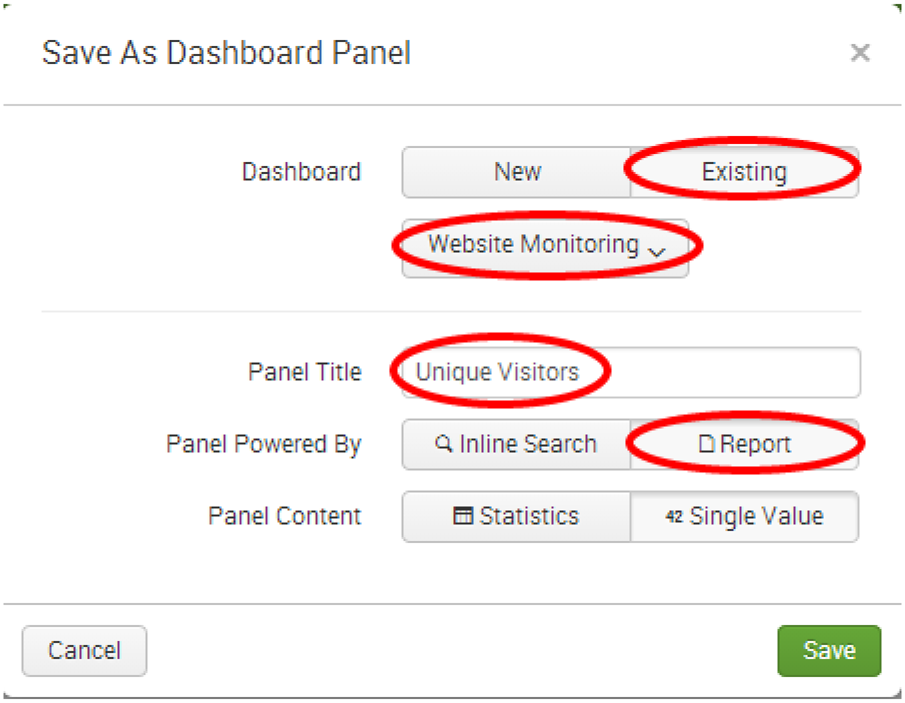


Drilldown: Yes | No

Caption: This is a caption




Edit
More Info
Edit Panels
Edit Source
XML
Convert to HTML
Edit Title or Description
Edit Permissions
Schedule PDF Delivery
Set as Home Dashboard
Clone
Delete



Save As Dashboard Panel

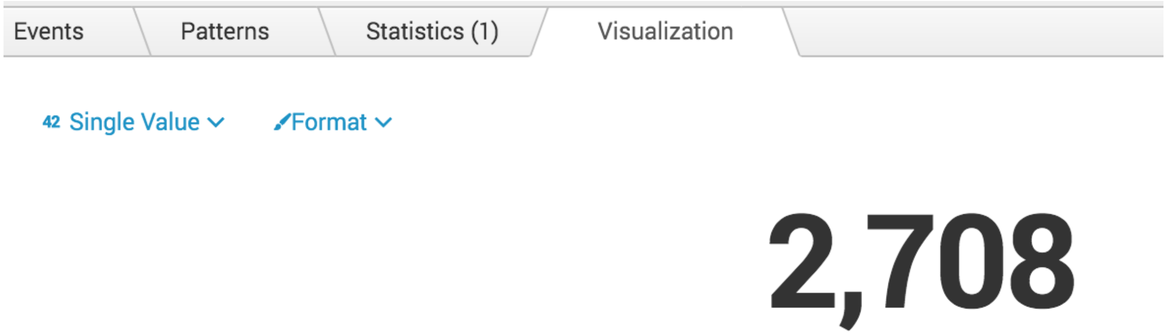
Dashboard: New [✓ Existing]

[✓ Website Monitoring]

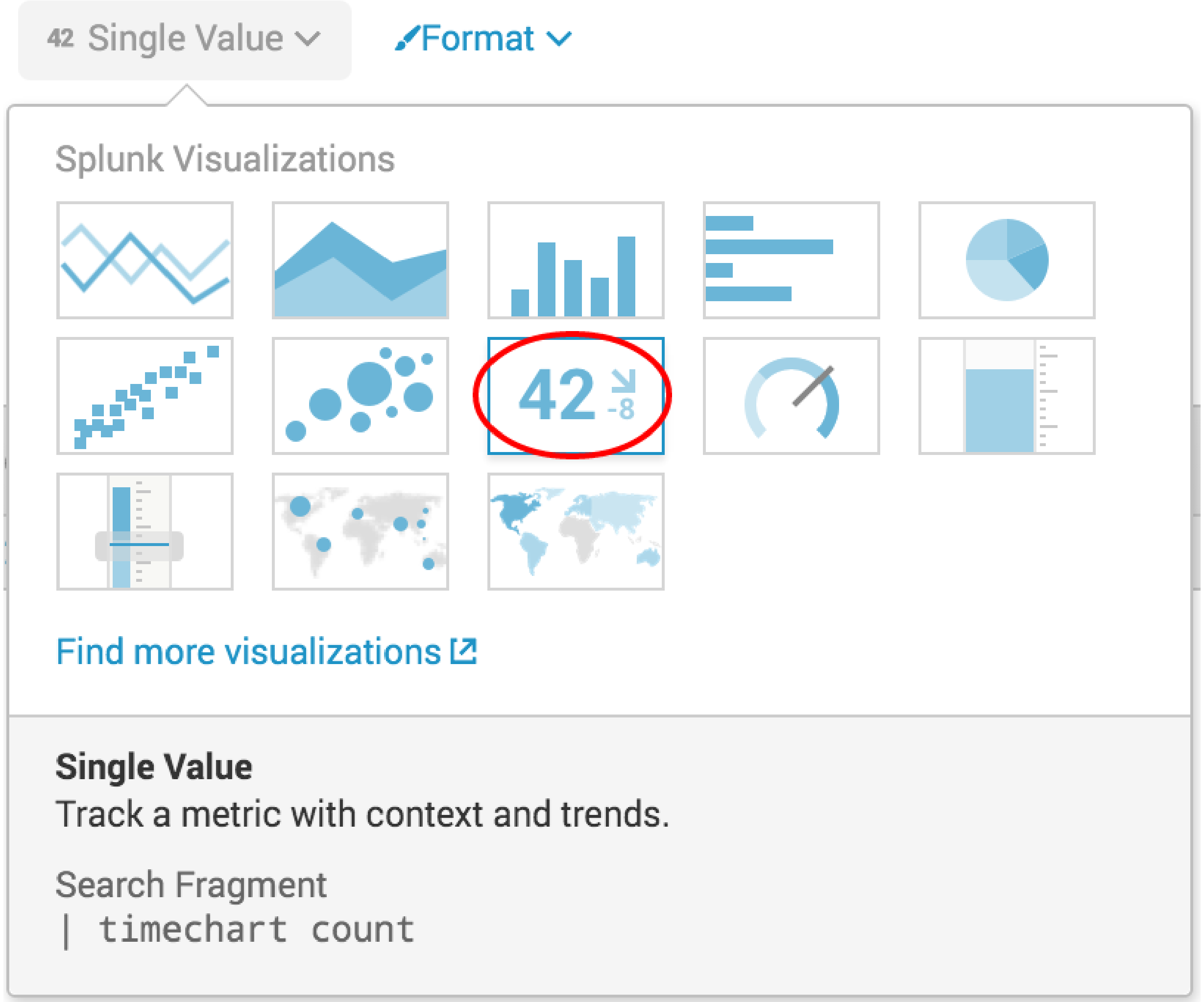
Panel Title: [✓ Unique Visitors]

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics | 42 Single Value



2,708

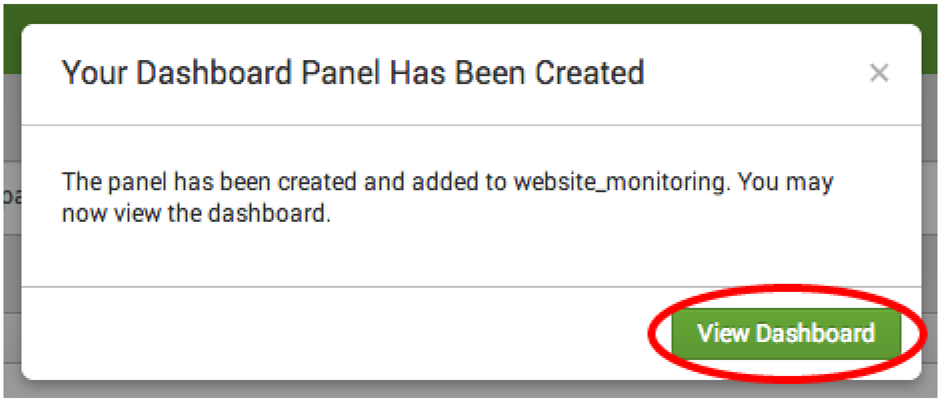


Single Value

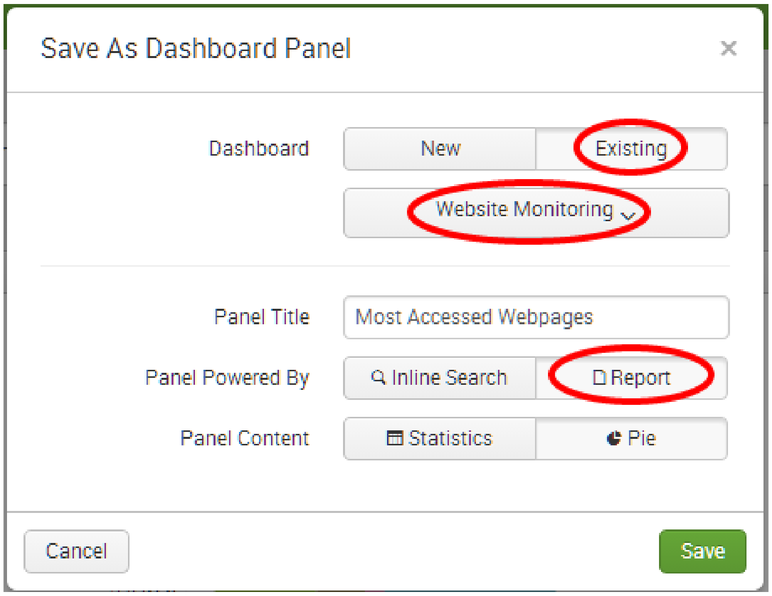
Track a metric with context and trends.

Search Fragment

```
| timechart count
```


Your Dashboard Panel Has Been Created

The panel has been created and added to website_monitoring. You may now view the dashboard.



Save As Dashboard Panel

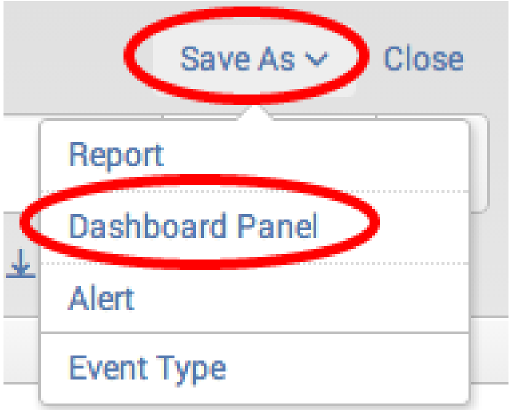
Dashboard: New [✓ Existing]

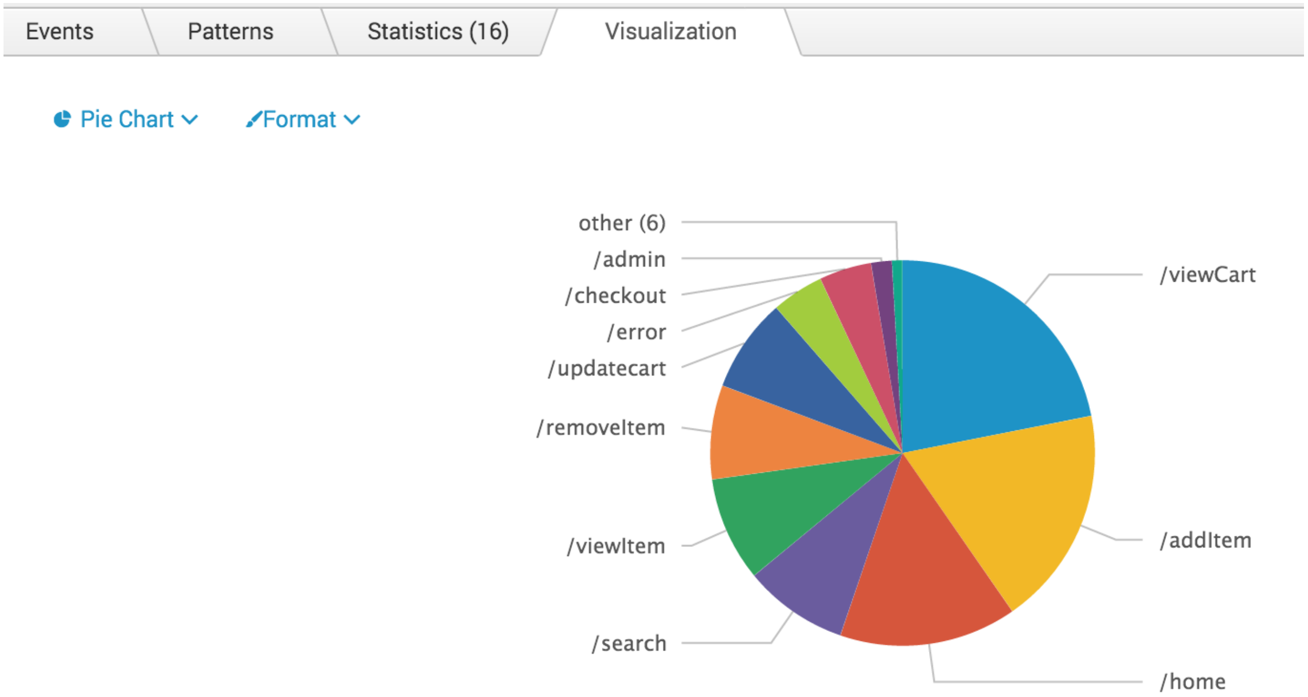
[✓ Website Monitoring]

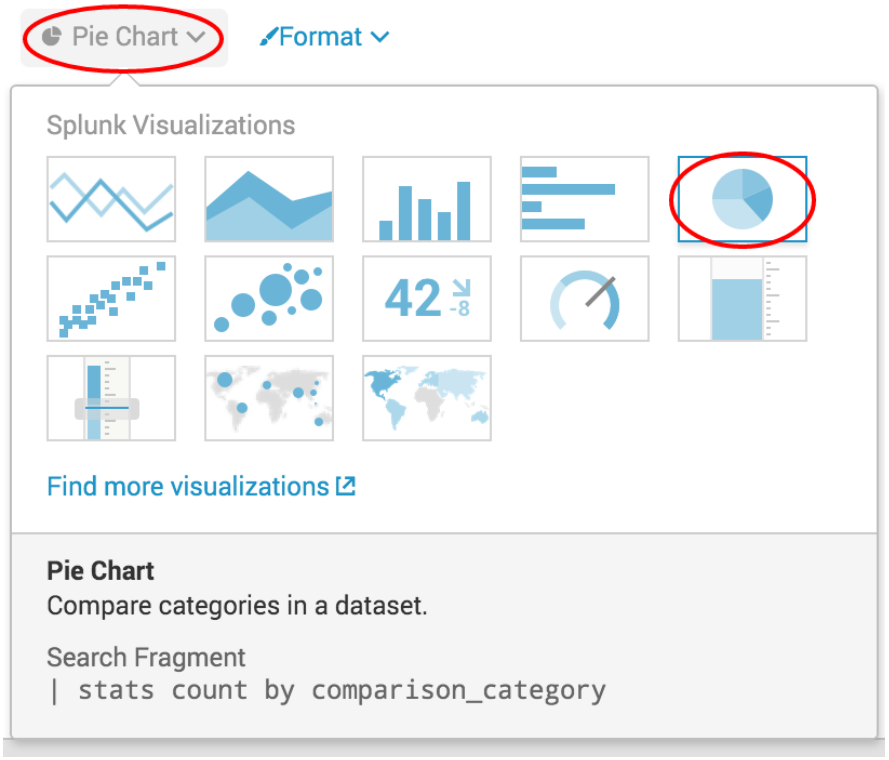
Panel Title: Most Accessed Webpages

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics Pie



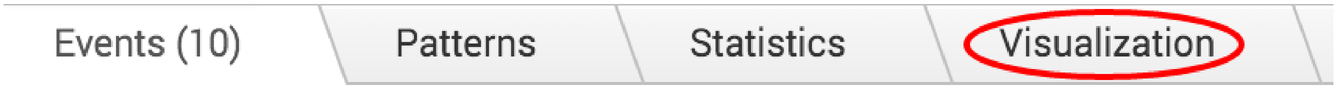


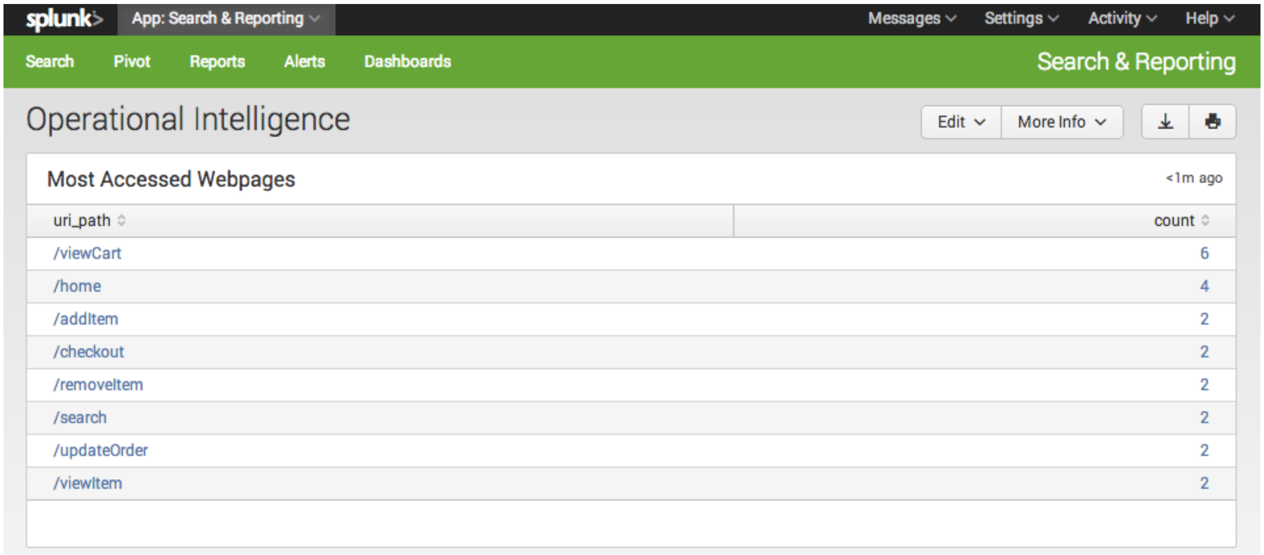


Pie Chart
Compare categories in a dataset.

Search Fragment

```
| stats count by comparison_category
```

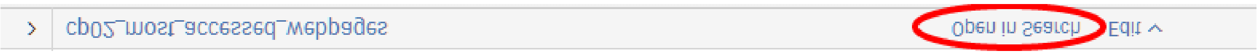


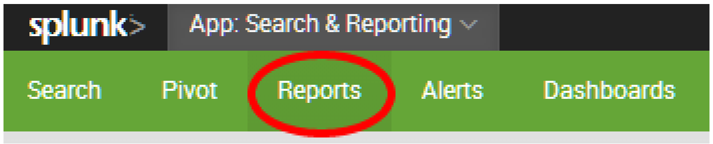


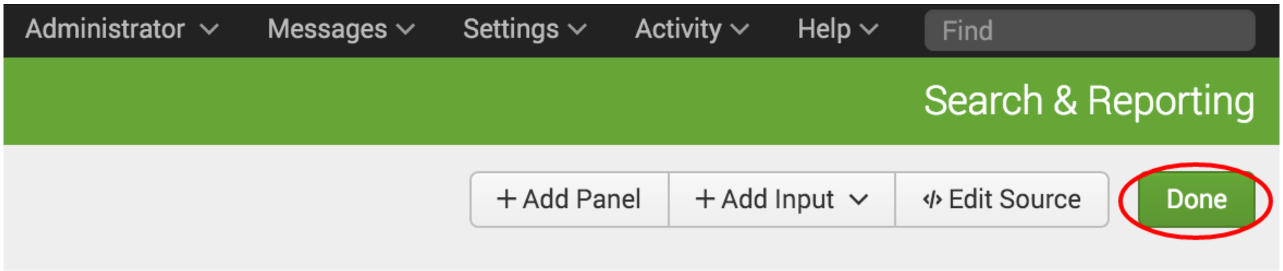
Most Accessed Webpages

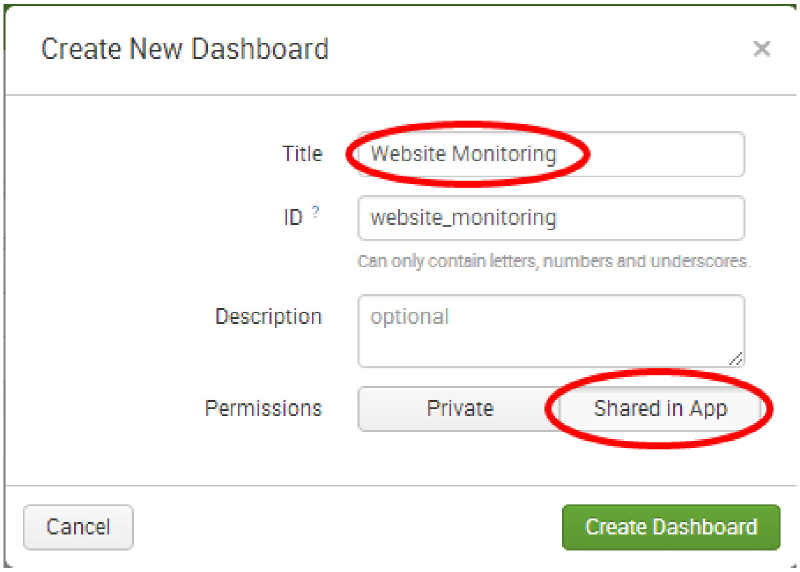
<1m ago

uri_path	count
/viewCart	6
/home	4
/addItem	2
/checkout	2
/removeItem	2
/search	2
/updateOrder	2
/viewItem	2









Create New Dashboard

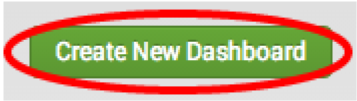
Title: Website Monitoring

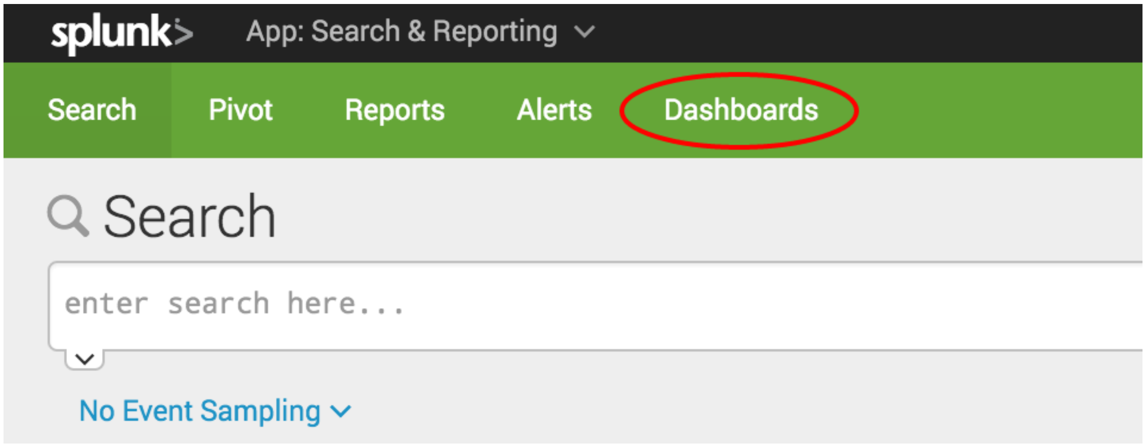
ID: website_monitoring

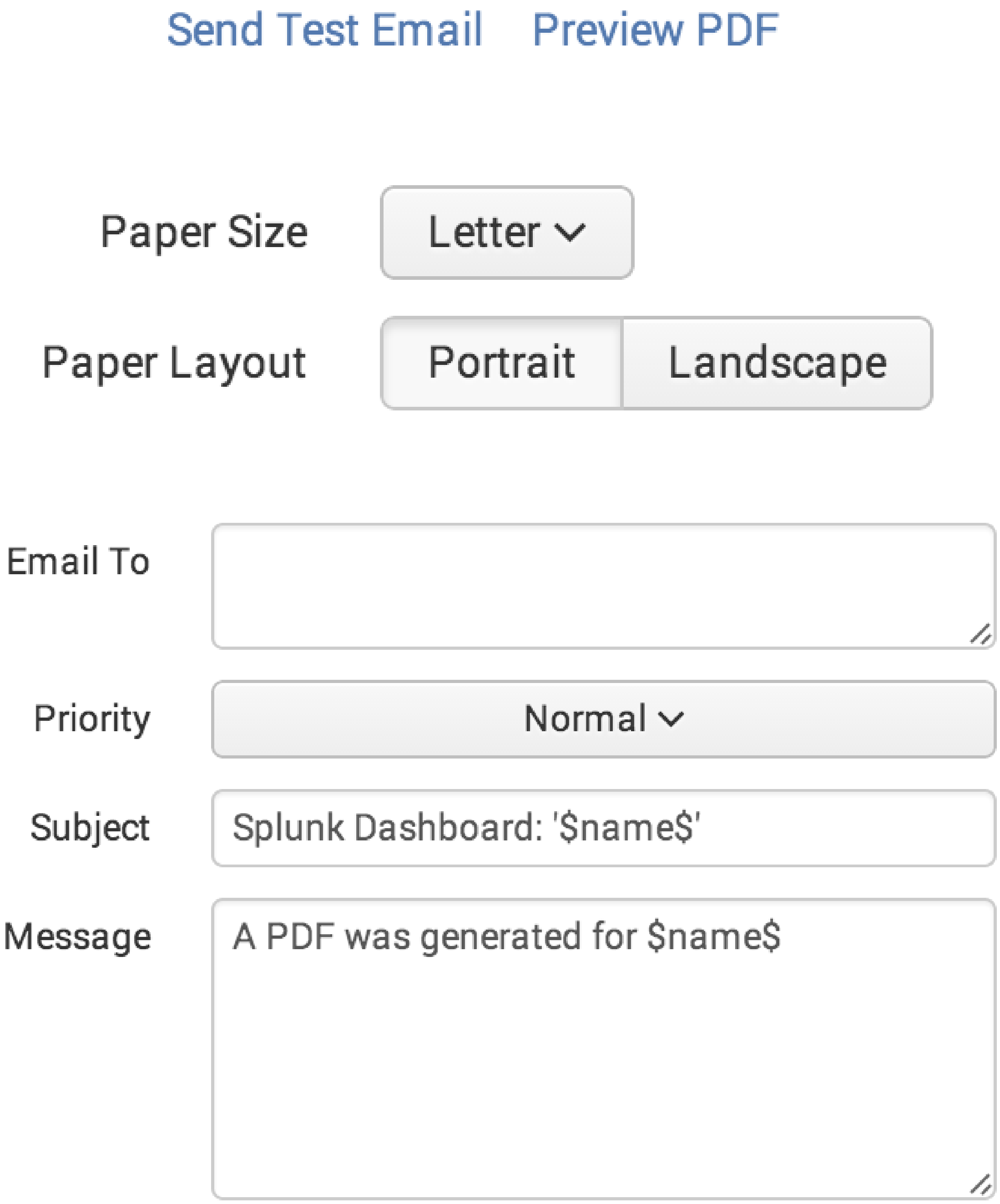
Can only contain letters, numbers and underscores.

Description: optional

Permissions: Private | Shared in App







Paper Size: Letter

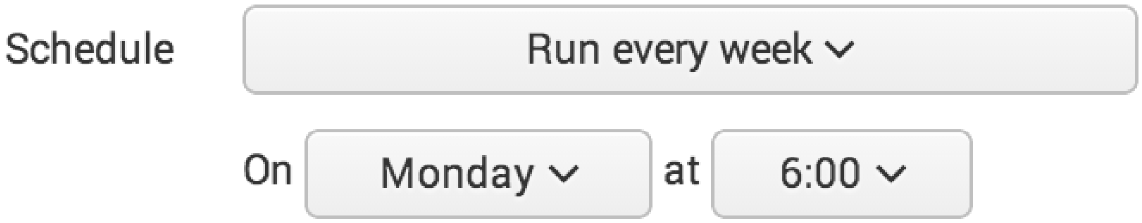
Paper Layout: Portrait | Landscape

Email To:

Priority: Normal

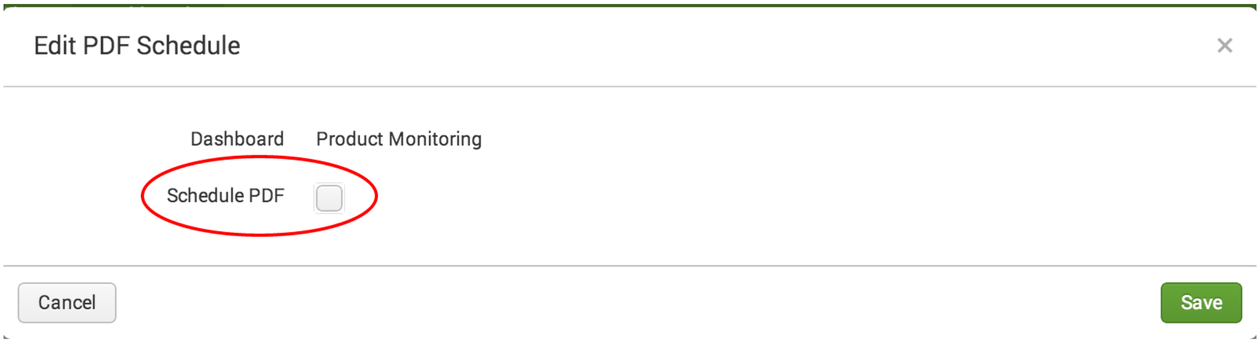
Subject: Splunk Dashboard: '$name$'

Message: A PDF was generated for $name$



Schedule Run every week

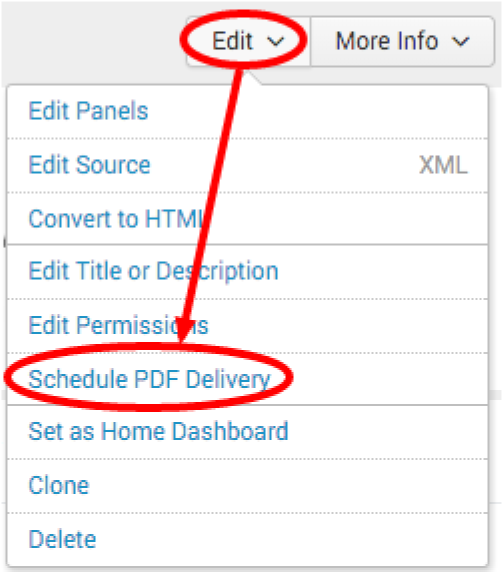
On Monday at 6:00

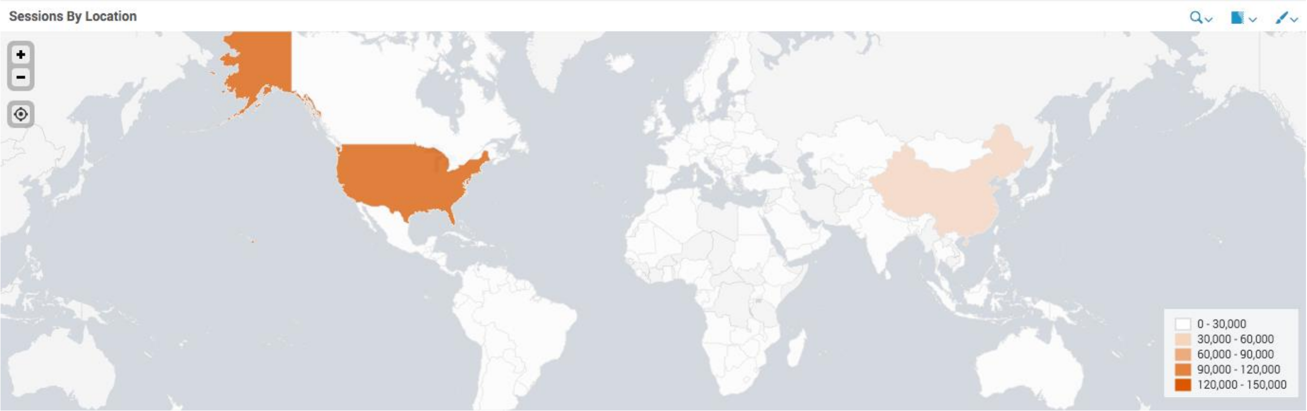


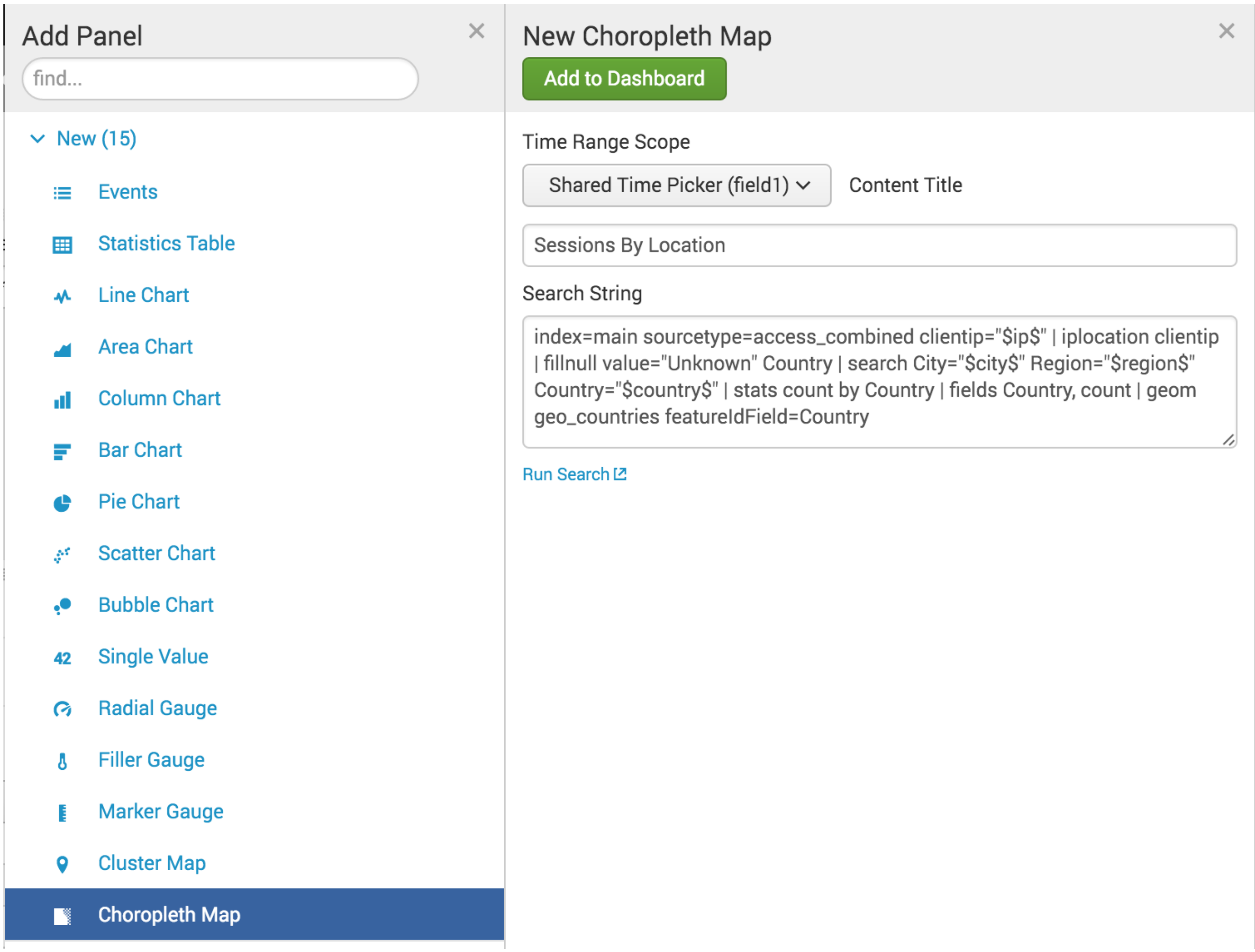
Edit PDF Schedule

Dashboard Product Monitoring

Schedule PDF □







Add Panel ✕

find...

New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart
- Single Value
- Radial Gauge
- Filler Gauge
- Marker Gauge
- Cluster Map
- Choropleth Map

New Choropleth Map ✕

Add to Dashboard

Time Range Scope

Shared Time Picker (field1)

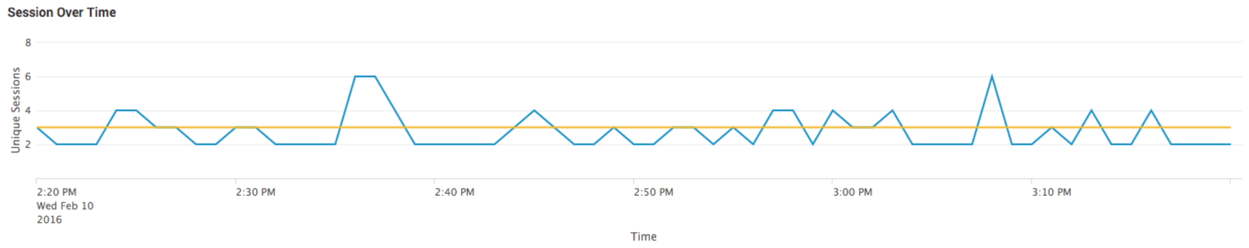
Content Title

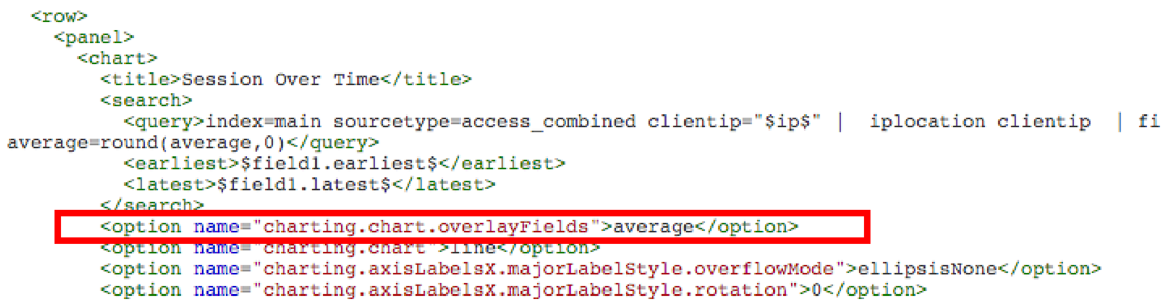
Sessions By Location

Search String

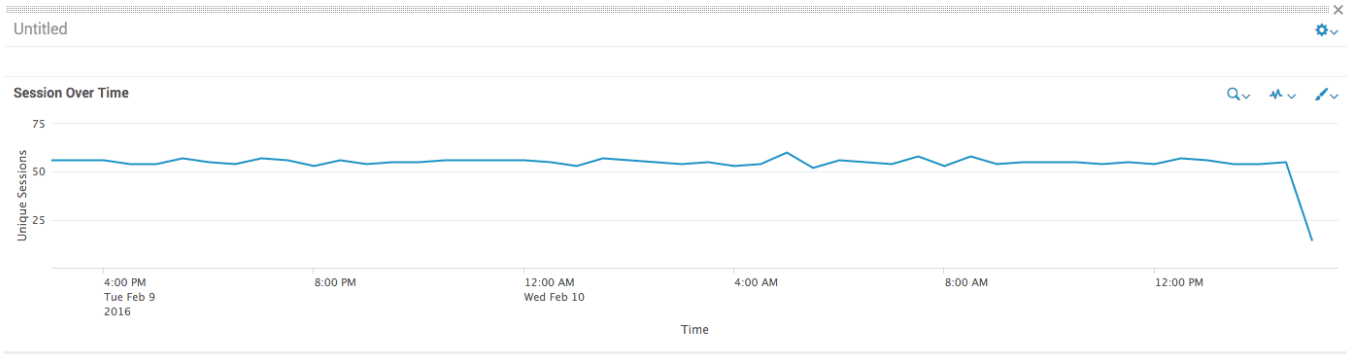
```
index=main sourcetype=access_combined clientip="$ip$" | iplocation clientip
| fillnull value="Unknown" Country | search City="$city$" Region="$region$"
Country="$country$" | stats count by Country | fields Country, count | geom
geo_countries featureIdField=Country
```

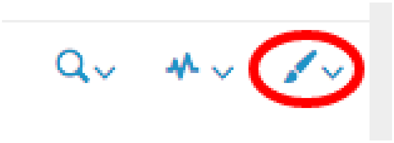
Run Search

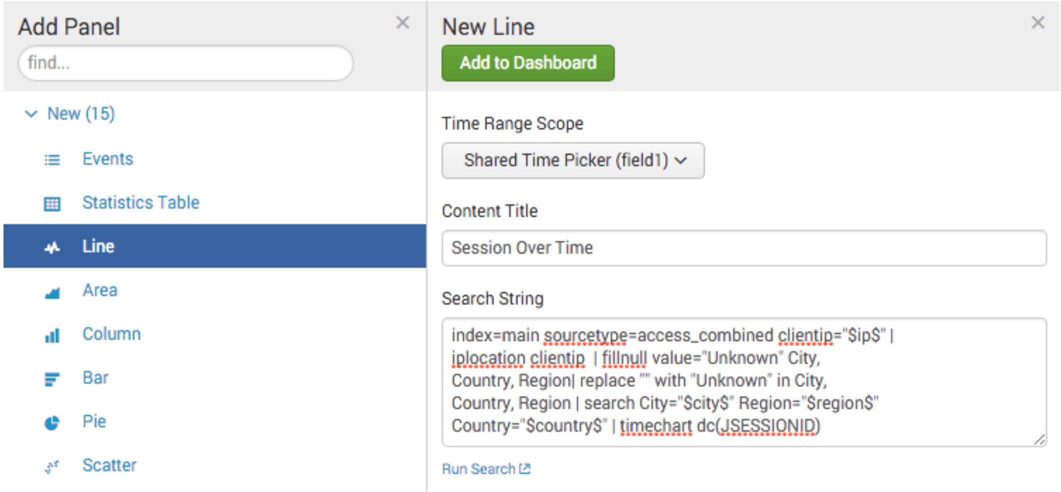




```
    <row>
      <panel>
        <chart>
          <title>Session Over Time</title>
          <search>
            <query>index=main sourcetype=access_combined clientip="$ip$" |  iplocation clientip  | fi
  average=round(average,0)</query>
            <earliest>$field1.earliest$</earliest>
            <latest>$field1.latest$</latest>
          </search>
          <option name="charting.chart.overlayFields">average</option>
          <option name="charting.chart">line</option>
          <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
          <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
```







Time Range Scope

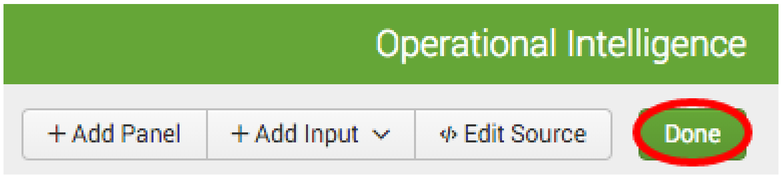
Shared Time Picker (field1)

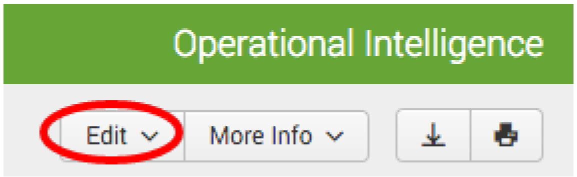
Content Title

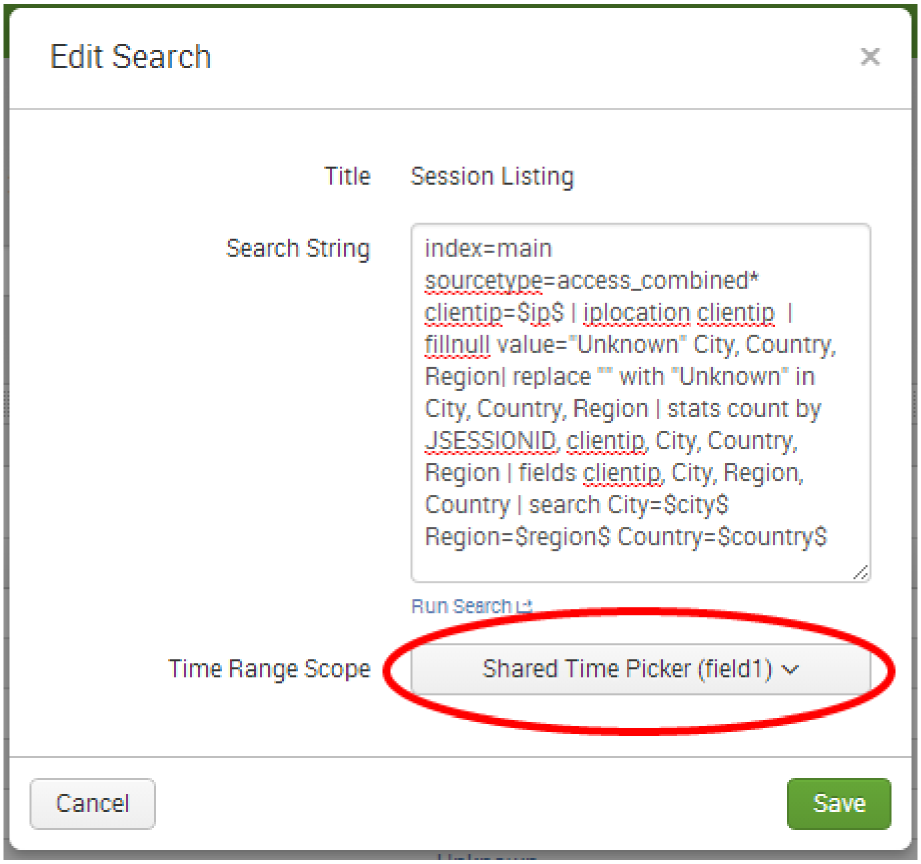
Session Over Time

Search String

```
index=main sourcetype=access_combined clientip="$ip$" |
iplocation clientip  | fillnull value="Unknown" City,
Country, Region| replace "" with "Unknown" in City,
Country, Region | search City="$city$" Region="$region$"
Country="$country$" | timechart dc(JSESSIONID)
```







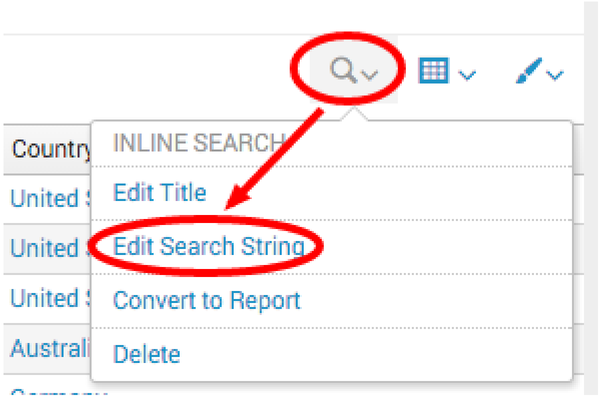
Edit Search

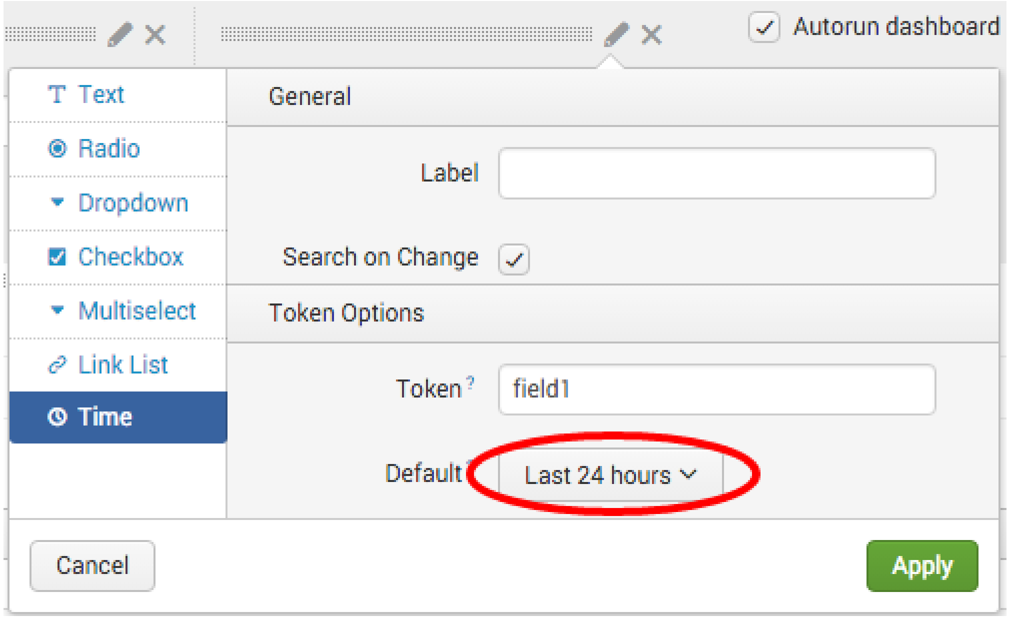
Title: Session Listing

Search String:

```
index=main
sourcetype=access_combined*
clientip=$ip$ | iplocation clientip  |
fillnull value="Unknown" City, Country,
Region| replace "" with "Unknown" in
City, Country, Region | stats count by
JSESSIONID, clientip, City, Country,
Region | fields clientip, City, Region,
Country | search City=$city$
Region=$region$ Country=$country$
```

Time Range Scope: Shared Time Picker (field1)





☑ Autorun dashboard

General

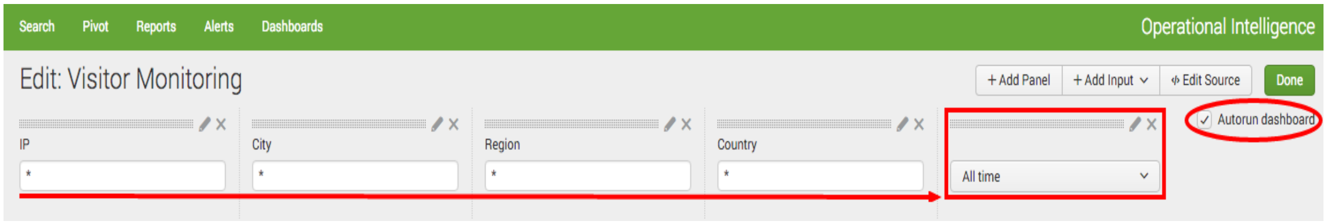
Label:

Search on Change ☑

Token Options

Token: field1

Default: Last 24 hours



Edit: Visitor Monitoring

☑ Autorun dashboard

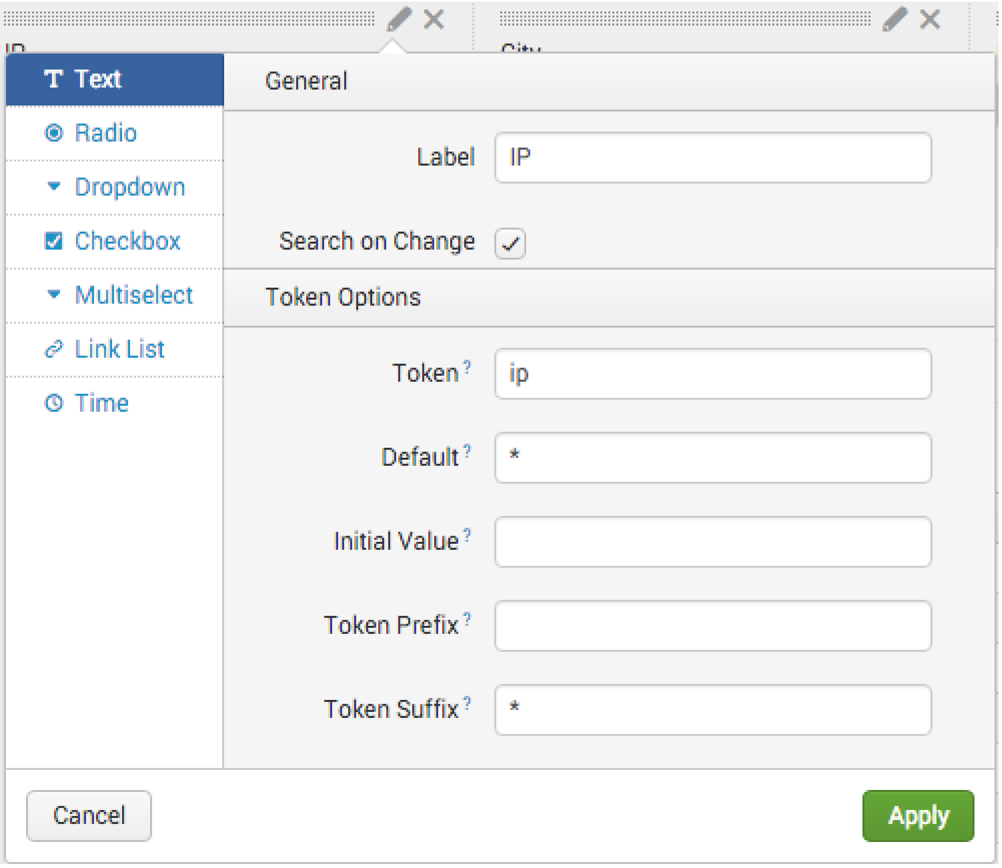
IP: *

City: *

Region: *

Country: *

All time



Label: IP

Search on Change ☑

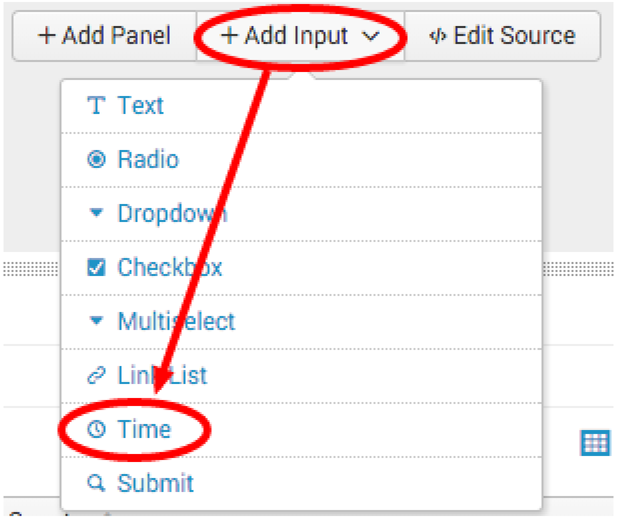
Token: ip

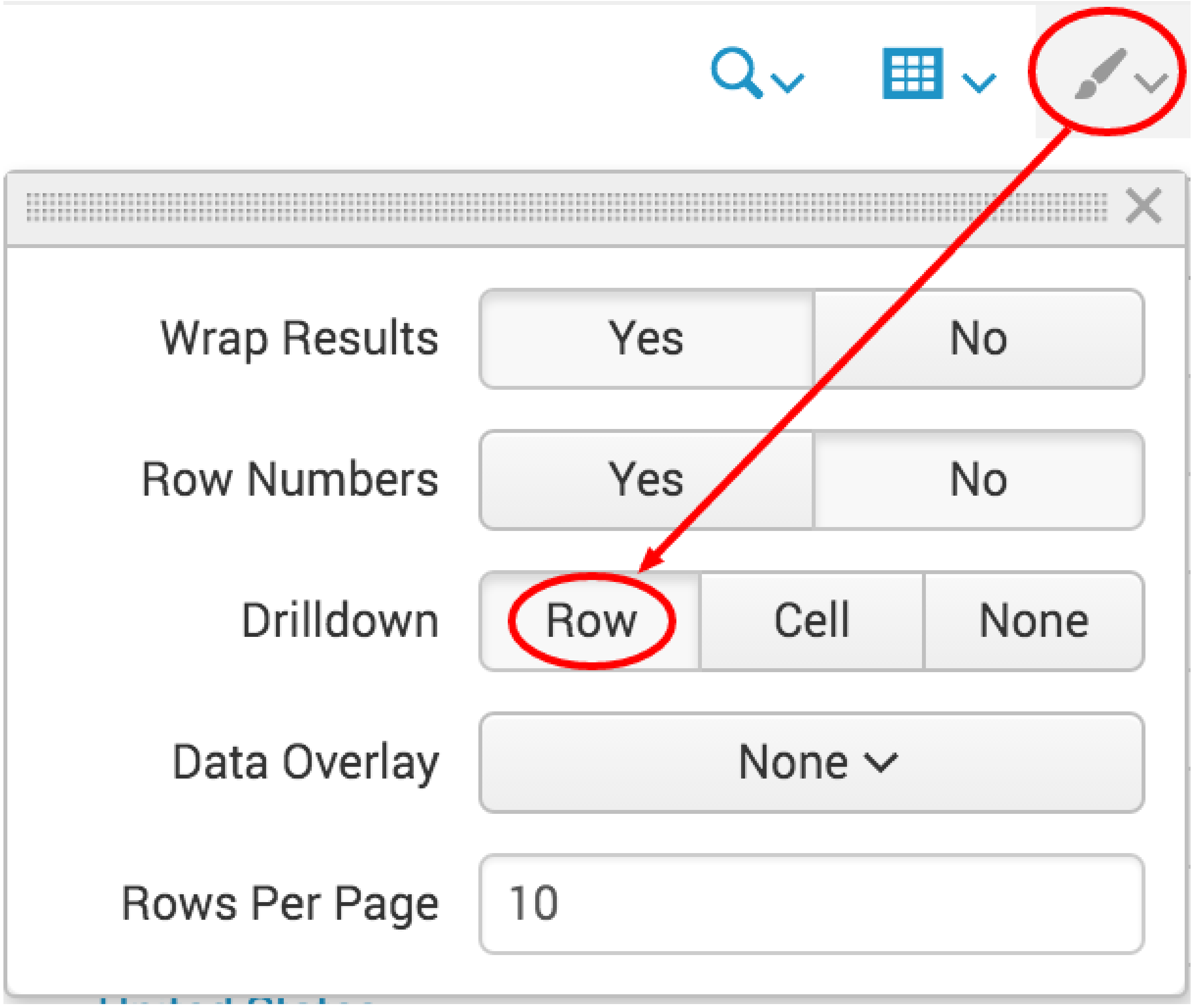
Default: *

Initial Value:

Token Prefix:

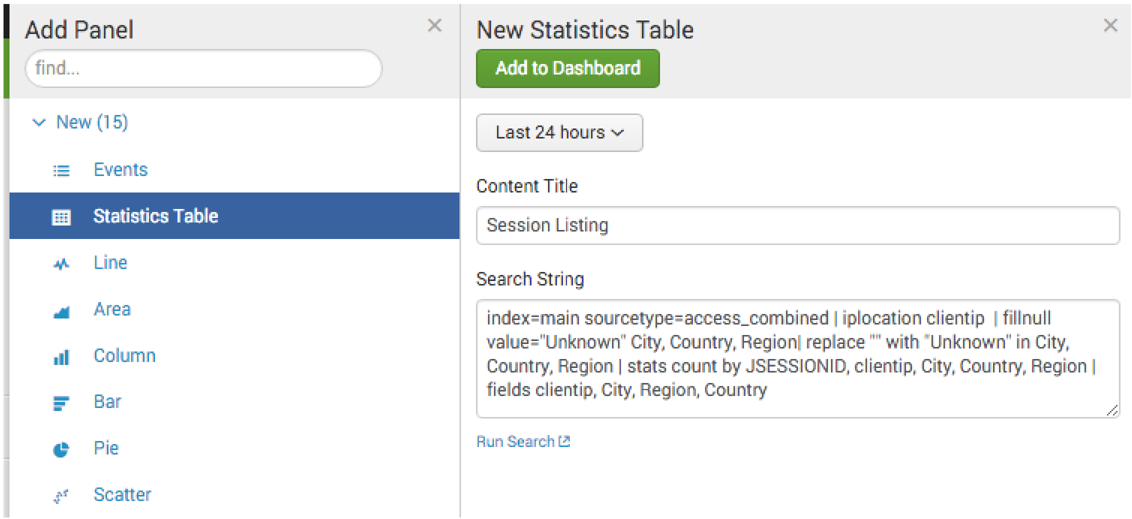
Token Suffix: *





Drilldown: [✓ Row] Cell None

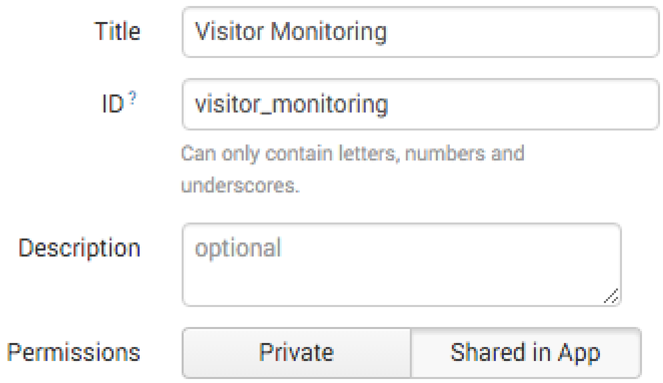
Rows Per Page: 10



Content Title: Session Listing

Search String:

```
index=main sourcetype=access_combined | iplocation clientip  | fillnull value="Unknown" City, Country, Region| replace "" with "Unknown" in City, Country, Region | stats count by JSESSIONID, clientip, City, Country, Region | fields clientip, City, Region, Country
```



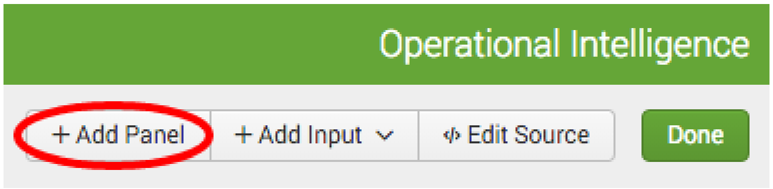
Title: Visitor Monitoring

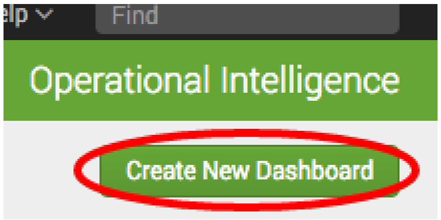
ID: visitor_monitoring

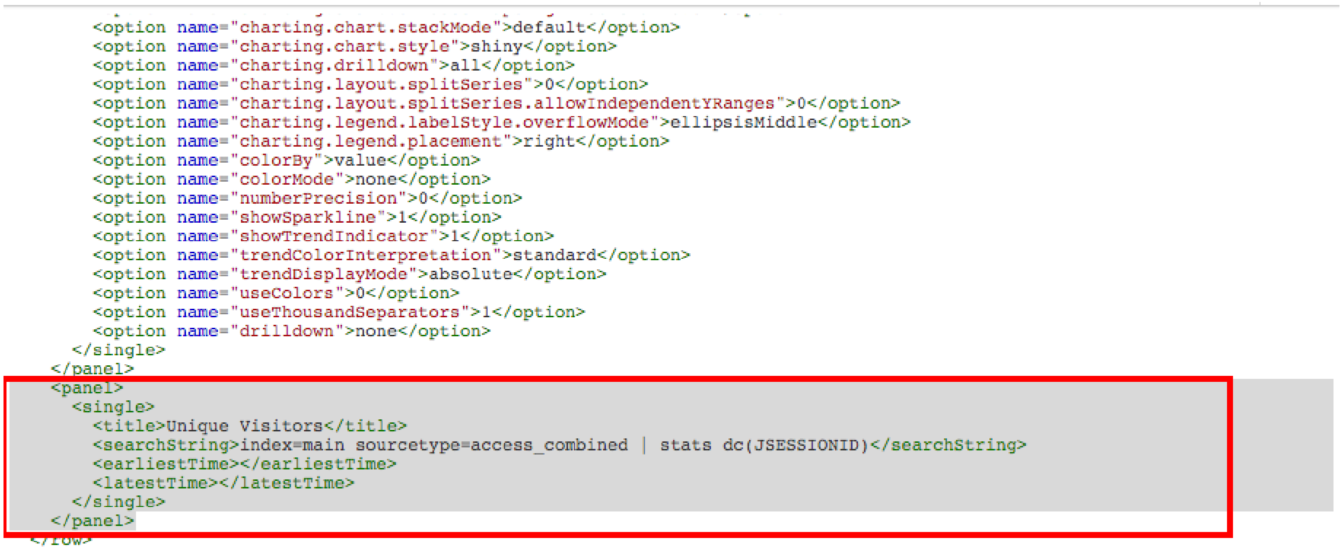
Can only contain letters, numbers and underscores.

Description: optional

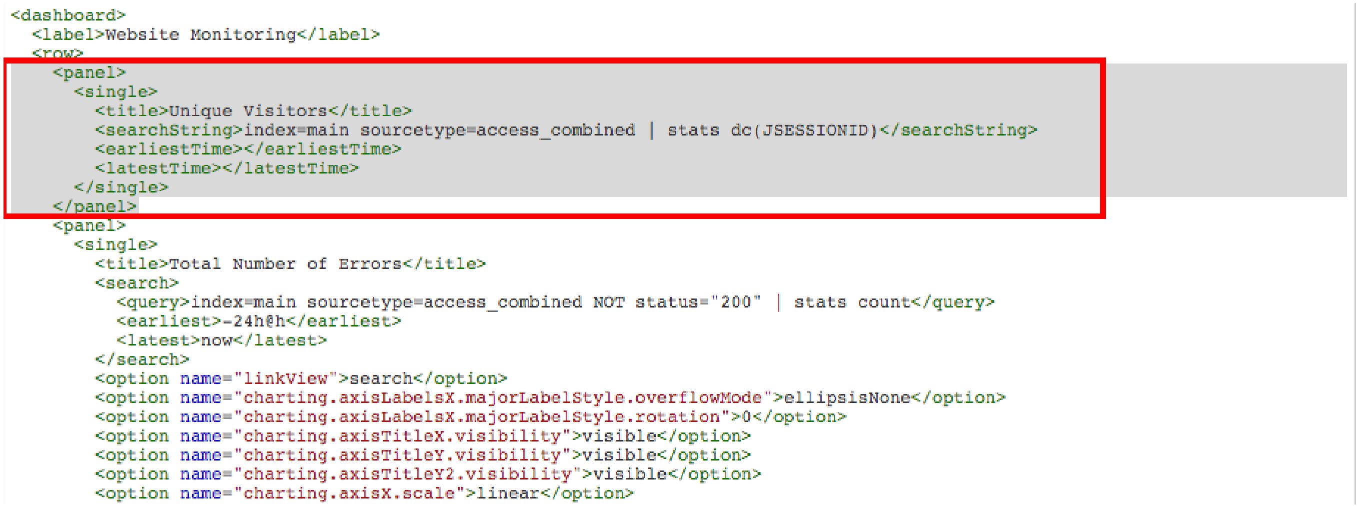
Permissions: Private | Shared in App



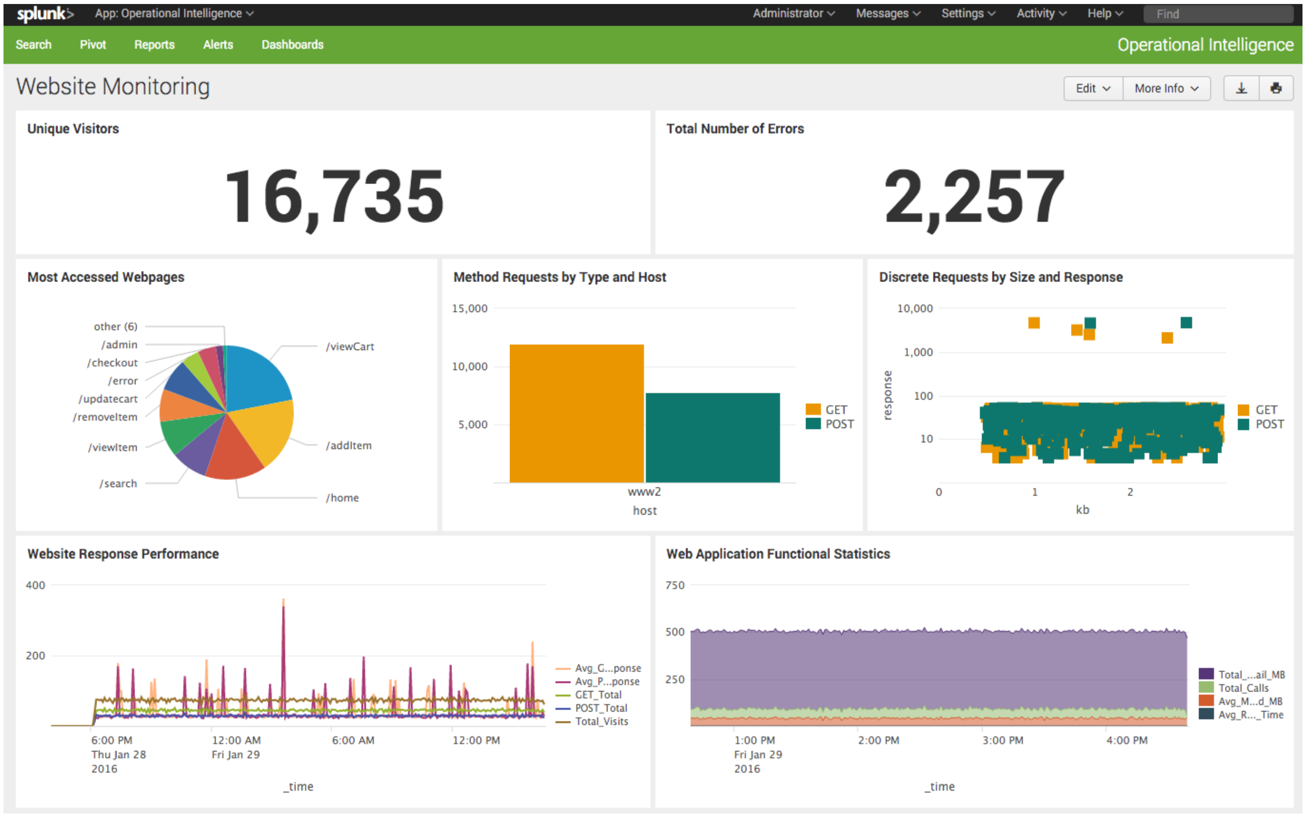


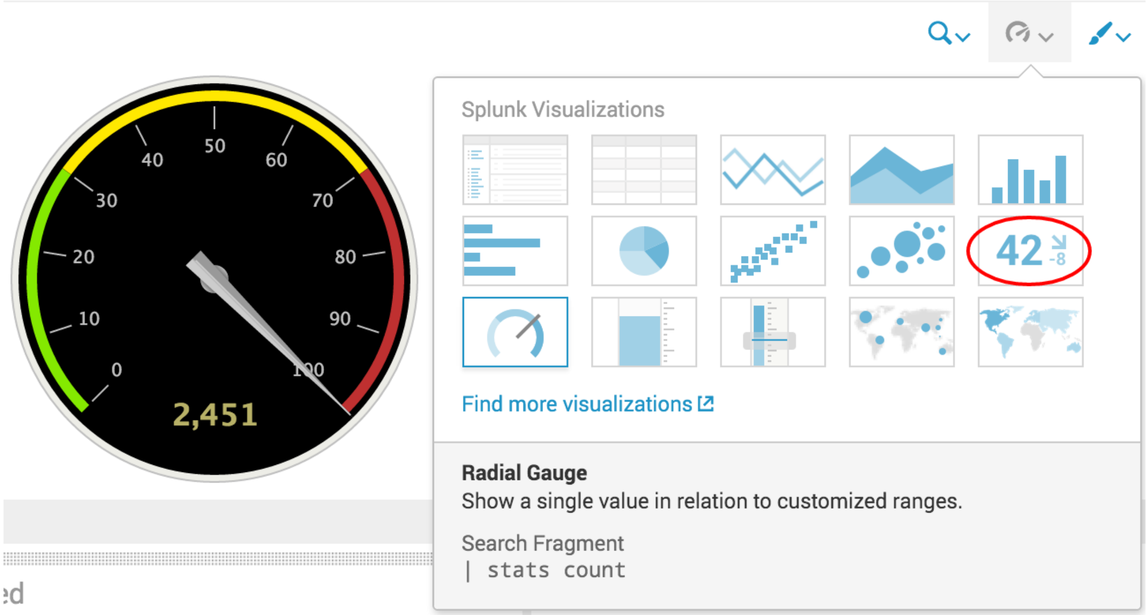


```
        <option name="charting.chart.stackMode">default</option>
        <option name="charting.chart.style">shiny</option>
        <option name="charting.drilldown">all</option>
        <option name="charting.layout.splitSeries">0</option>
        <option name="charting.layout.splitSeries.allowIndependentYRanges">0</option>
        <option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>
        <option name="charting.legend.placement">right</option>
        <option name="colorBy">value</option>
        <option name="colorMode">none</option>
        <option name="numberPrecision">0</option>
        <option name="showSparkline">1</option>
        <option name="showTrendIndicator">1</option>
        <option name="trendColorInterpretation">standard</option>
        <option name="trendDisplayMode">absolute</option>
        <option name="useColors">0</option>
        <option name="useThousandSeparators">1</option>
        <option name="drilldown">none</option>
      </single>
    </panel>
    <panel>
      <single>
        <title>Unique Visitors</title>
        <searchString>index=main sourcetype=access_combined | stats dc(JSESSIONID)</searchString>
        <earliestTime></earliestTime>
        <latestTime></latestTime>
      </single>
    </panel>
  </row>
```



```
<dashboard>
  <label>Website Monitoring</label>
  <row>
    <panel>
      <single>
        <title>Unique Visitors</title>
        <searchString>index=main sourcetype=access_combined | stats dc(JSESSIONID)</searchString>
        <earliestTime></earliestTime>
        <latestTime></latestTime>
      </single>
    </panel>
    <panel>
      <single>
        <title>Total Number of Errors</title>
        <search>
          <query>index=main sourcetype=access_combined NOT status="200" | stats count</query>
          <earliest>-24h@h</earliest>
          <latest>now</latest>
        </search>
        <option name="linkView">search</option>
        <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
        <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option name="charting.axisTitleX.visibility">visible</option>
        <option name="charting.axisTitleY.visibility">visible</option>
        <option name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
```

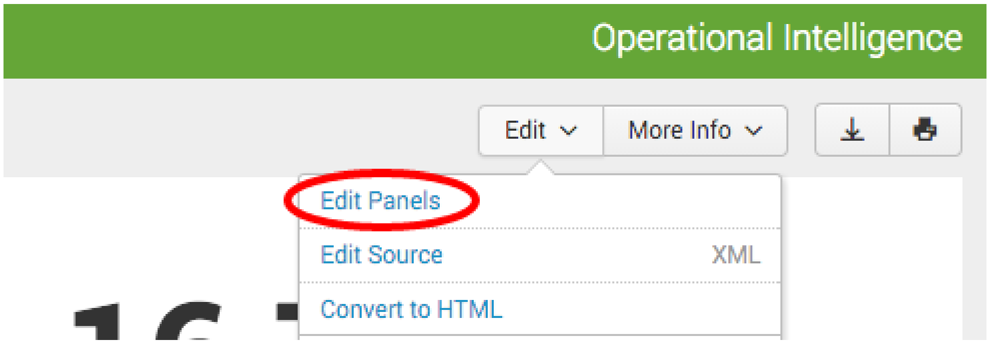


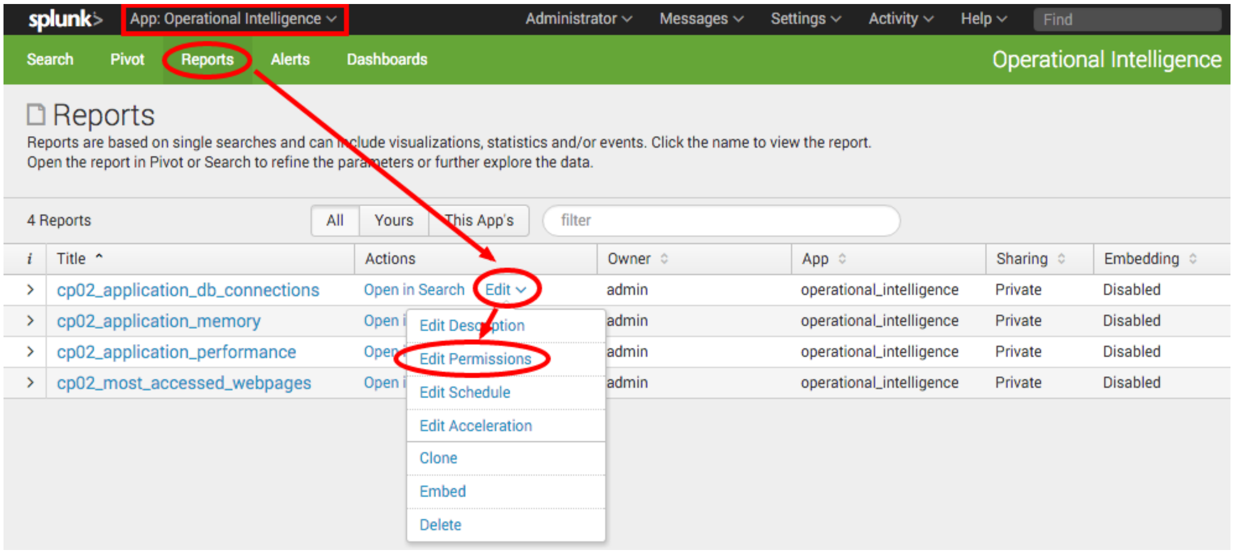


Radial Gauge
Show a single value in relation to customized ranges.

Search Fragment

```
| stats count
```



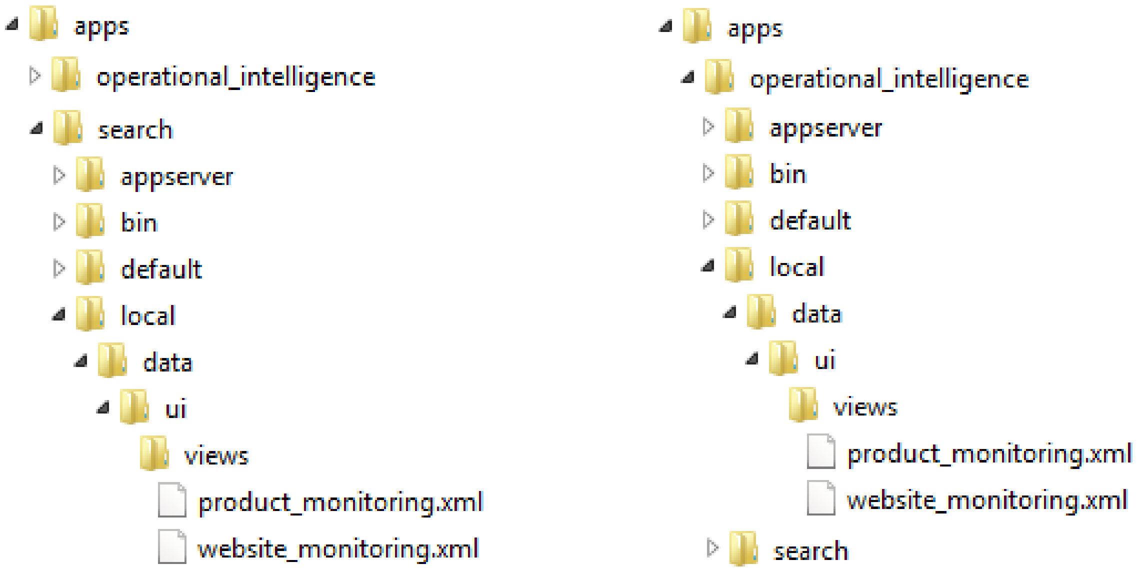


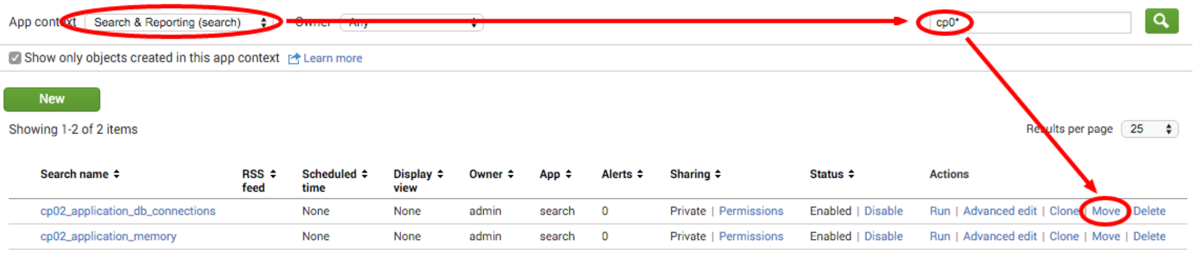
Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report.
Open the report in Pivot or Search to refine the parameters or further explore the data.

4 Reports

i	Title	Actions	Owner	App	Sharing	Embedding
>	cp02_application_db_connections	Open in Search Edit	admin	operational_intelligence	Private	Disabled
>	cp02_application_memory	Open i	admin	operational_intelligence	Private	Disabled
>	cp02_application_performance	Open	admin	operational_intelligence	Private	Disabled
>	cp02_most_accessed_webpages	Open i	admin	operational_intelligence	Private	Disabled





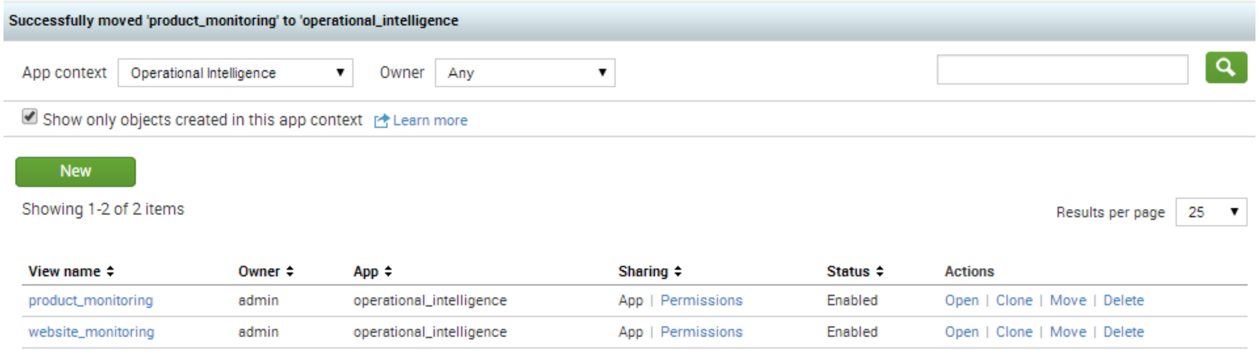
App context: Search & Reporting (search) Owner: Any   cp0*

☑ Show only objects created in this app context Learn more

New

Showing 1-2 of 2 items   Results per page 25

Search name	RSS feed	Scheduled time	Display view	Owner	App	Alerts	Sharing	Status	Actions
cp02_application_db_connections		None	None	admin	search	0	Private | Permissions	Enabled | Disable	Run | Advanced edit | Clone | Move | Delete
cp02_application_memory		None	None	admin	search	0	Private | Permissions	Enabled | Disable	Run | Advanced edit | Clone | Move | Delete



Successfully moved 'product_monitoring' to 'operational_intelligence

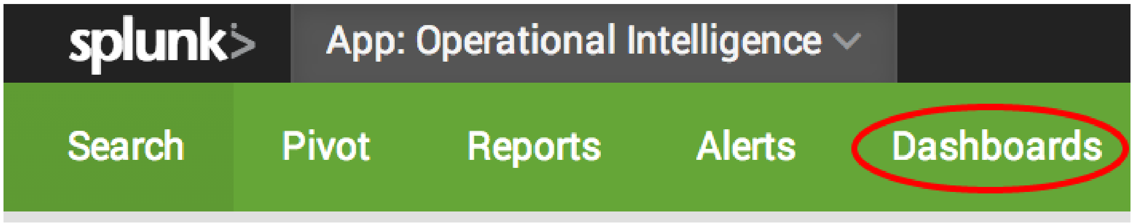
App context: Operational Intelligence Owner: Any

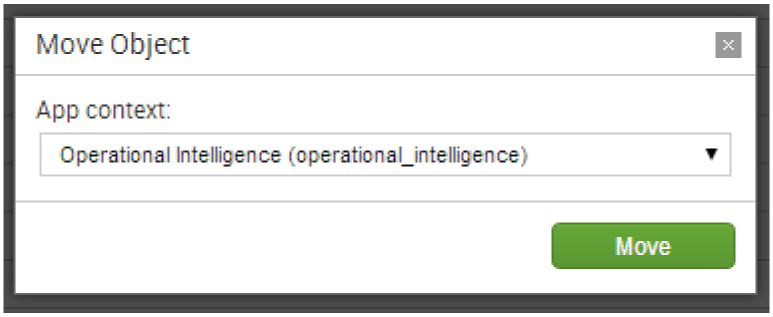
☑ Show only objects created in this app context Learn more

New

Showing 1-2 of 2 items   Results per page 25

View name	Owner	App	Sharing	Status	Actions
product_monitoring	admin	operational_intelligence	App | Permissions	Enabled	Open | Clone | Move | Delete
website_monitoring	admin	operational_intelligence	App | Permissions	Enabled	Open | Clone | Move | Delete

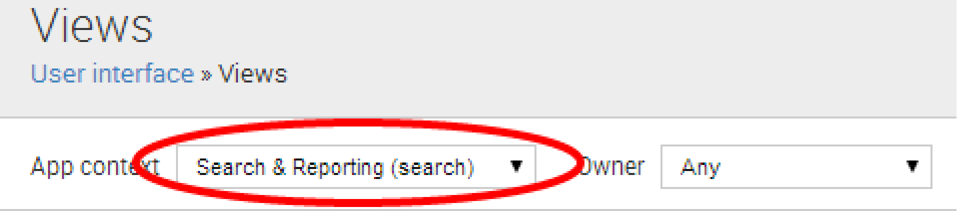




Move Object

App context:

Operational Intelligence (operational_intelligence)

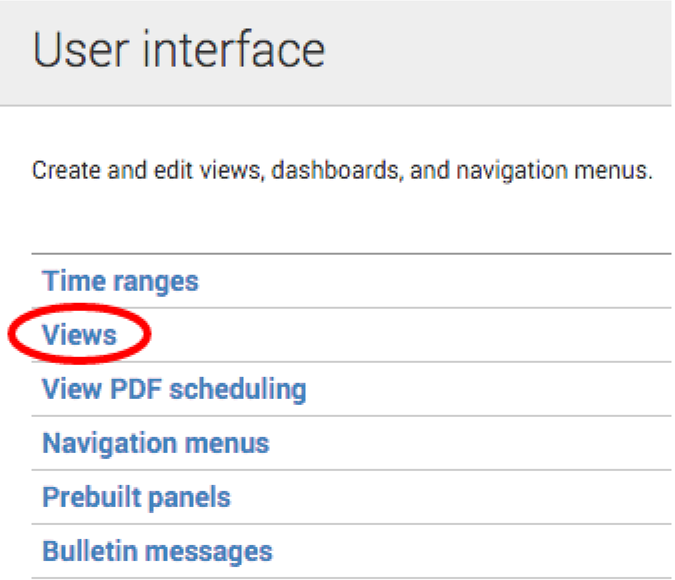


Views

User interface » Views

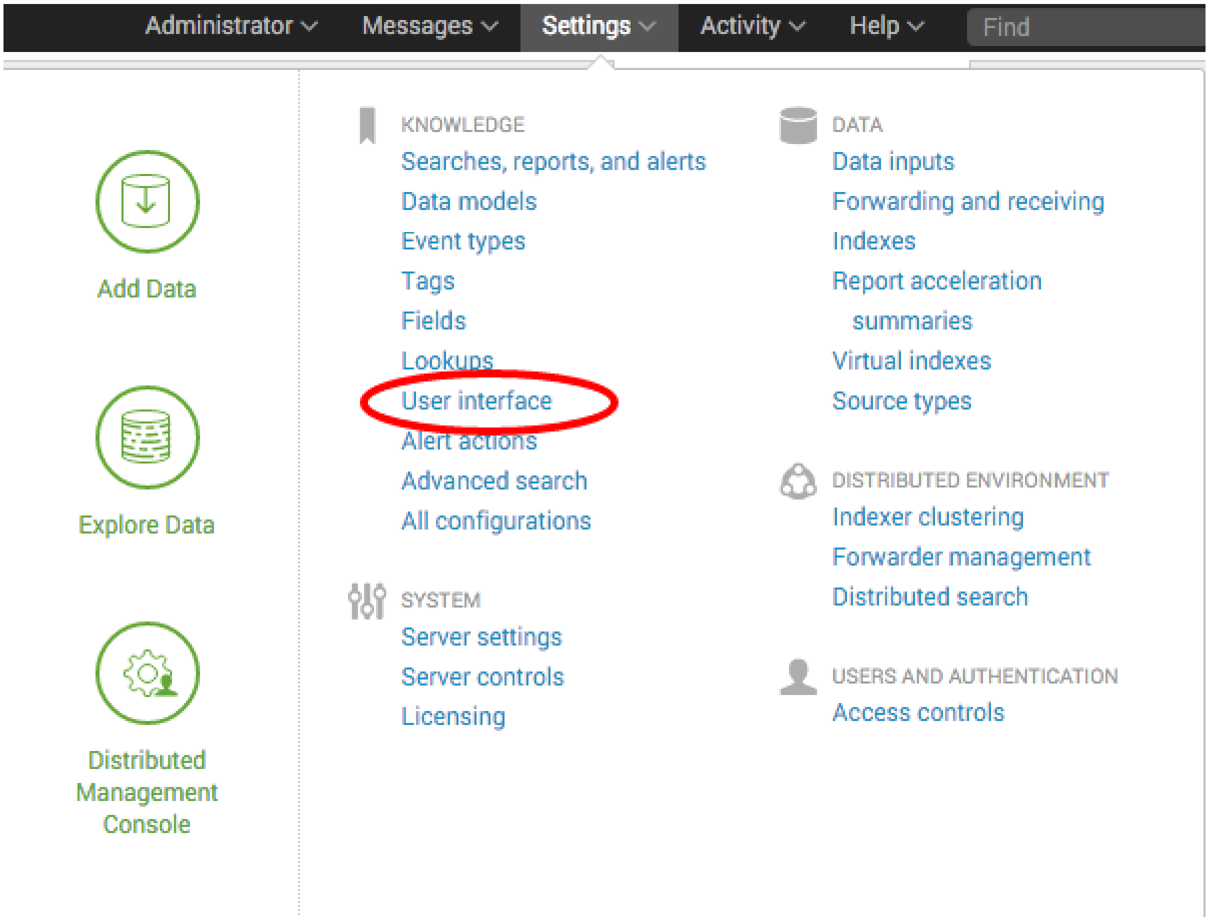
App context Search & Reporting (search)

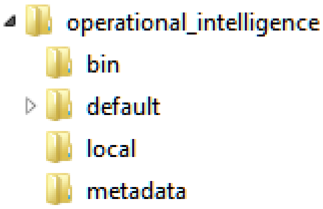
Owner Any

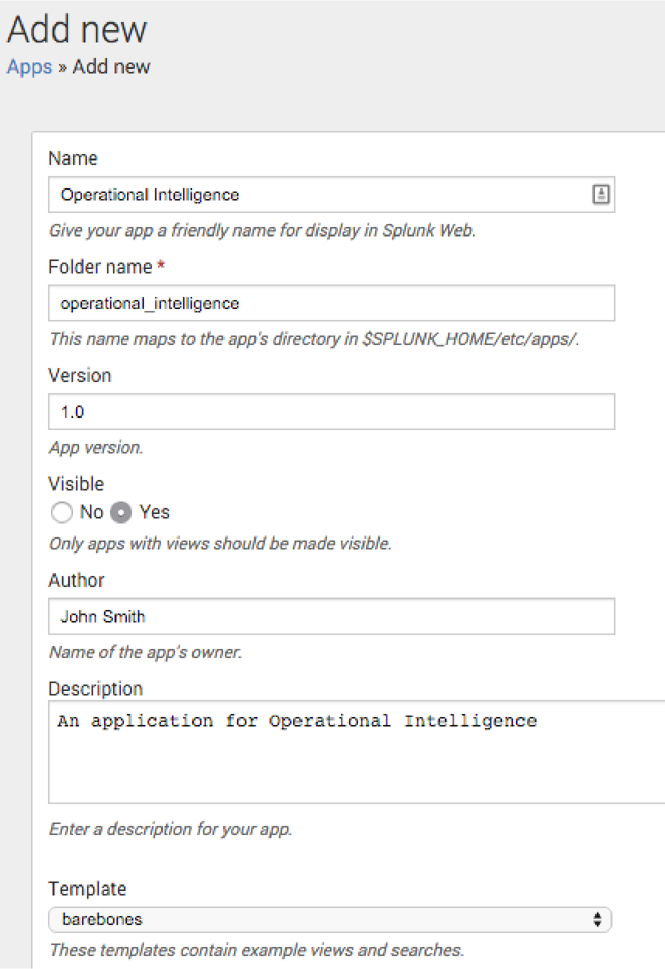


User interface

Create and edit views, dashboards, and navigation menus.


Administrator
Messages
Settings
Activity
Help
Find
Add Data
Explore Data
Distributed Management Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Licensing
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
USERS AND AUTHENTICATION
Access controls


operational_intelligence
bin
default
local
metadata



Add new

Apps » Add new

Name

Operational Intelligence

Give your app a friendly name for display in Splunk Web.

Folder name *

operational_intelligence

This name maps to the app's directory in $SPLUNK_HOME/etc/apps/.

Version

1.0

App version.

Visible

○ No ● Yes

Only apps with views should be made visible.

Author

John Smith

Name of the app's owner.

Description

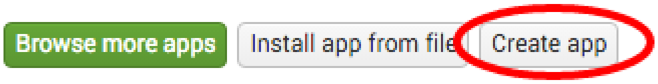
```
An application for Operational Intelligence
```

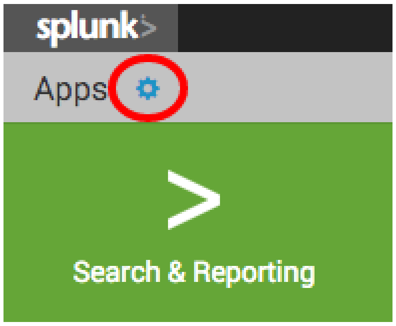
Enter a description for your app.

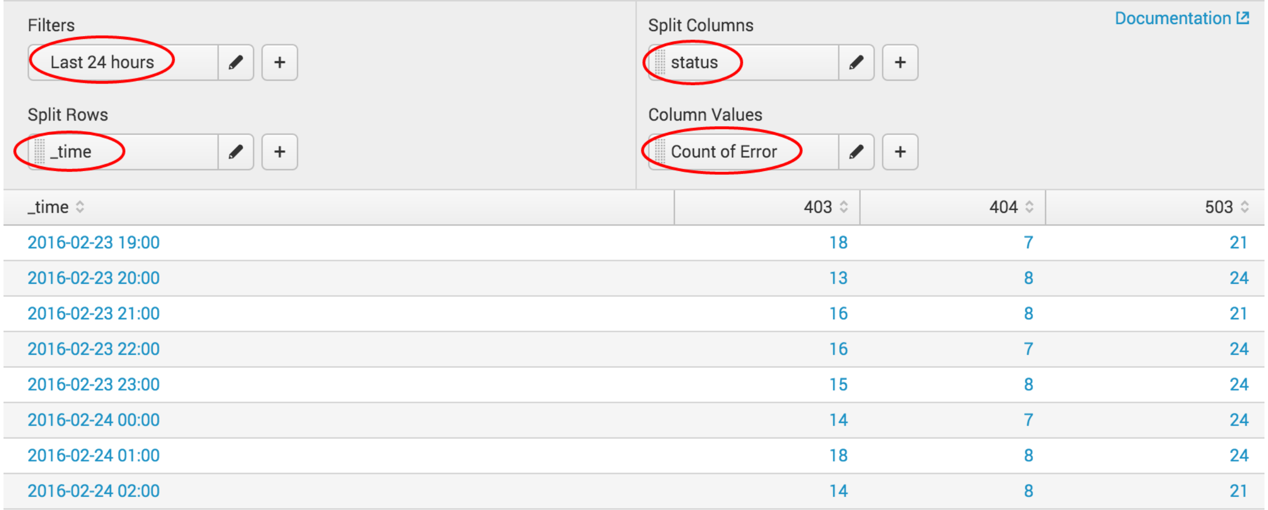
Template

barebones

These templates contain example views and searches.







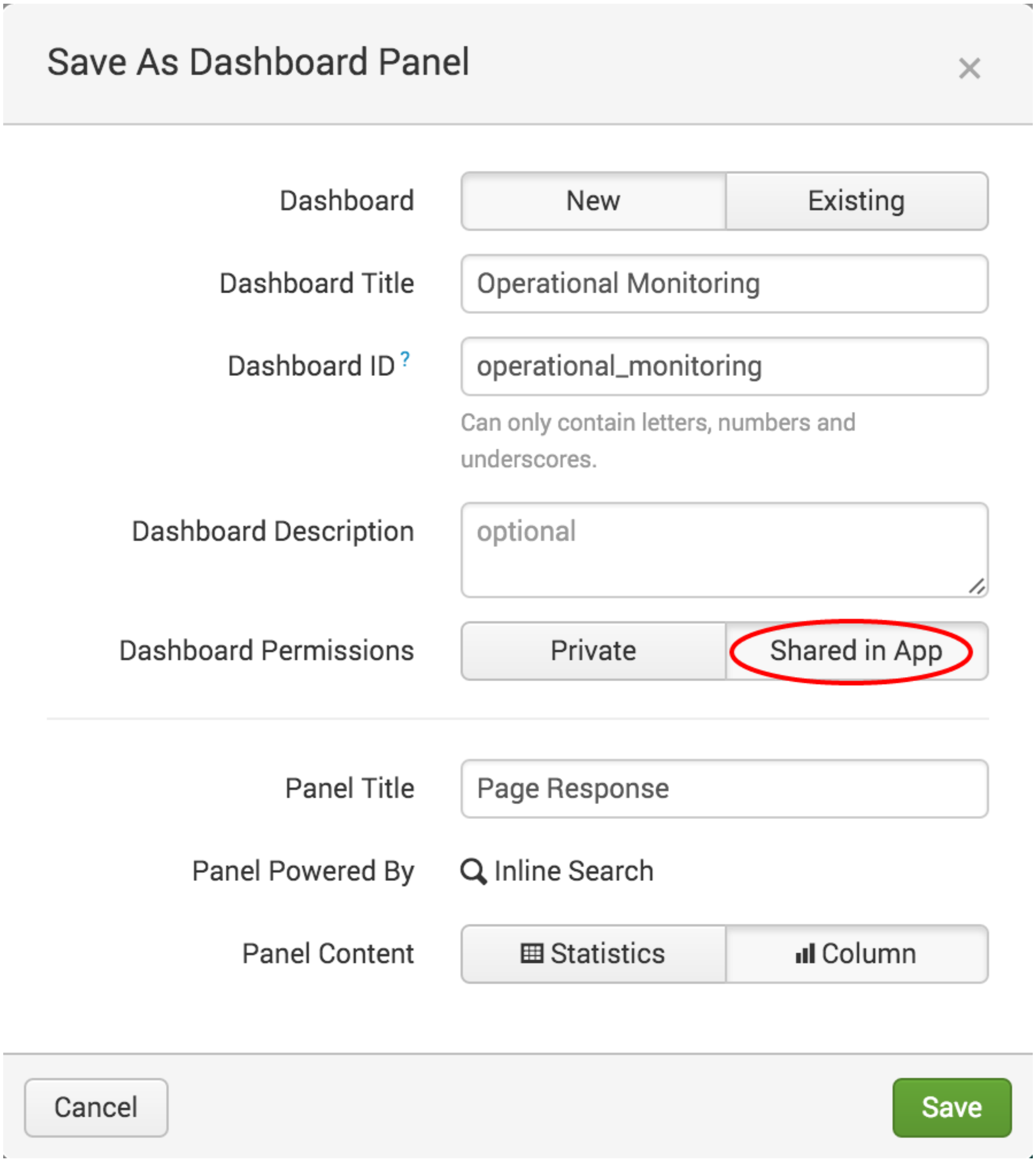
Filters: Last 24 hours

Split Rows: _time

Split Columns: status

Column Values: Count of Error

_time	403	404	503
2016-02-23 19:00	18	7	21
2016-02-23 20:00	13	8	24
2016-02-23 21:00	16	8	21
2016-02-23 22:00	16	7	24
2016-02-23 23:00	15	8	24
2016-02-24 00:00	14	7	24
2016-02-24 01:00	18	8	24
2016-02-24 02:00	14	8	21



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: Operational Monitoring

Dashboard ID ?: operational_monitoring

Can only contain letters, numbers and underscores.

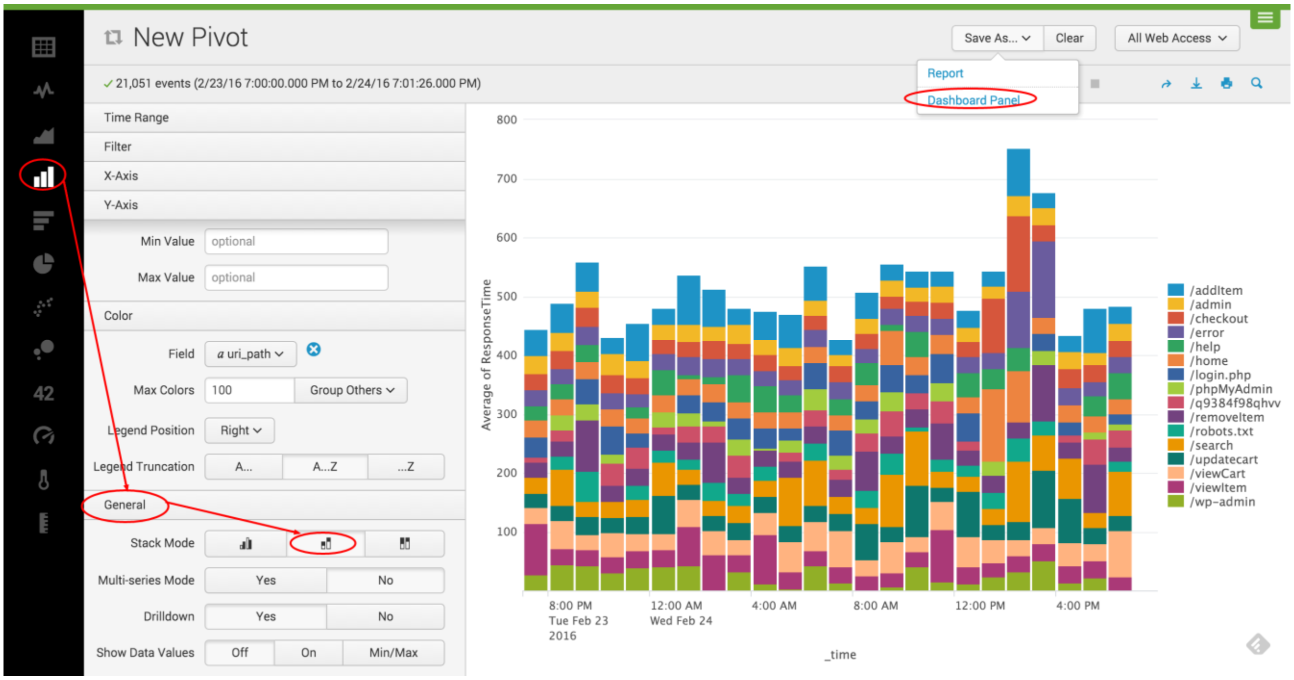
Dashboard Description: optional

Dashboard Permissions: Private [✓ Shared in App]

Panel Title: Page Response

Panel Powered By: Inline Search

Panel Content: Statistics | Column



New Pivot

✓ 21,051 events (2/23/16 7:00:00.000 PM to 2/24/16 7:01:26.000 PM)

Min Value: optional

Max Value: optional

Field: a uri_path

Max Colors: 100 — Group Others

Legend Position: Right

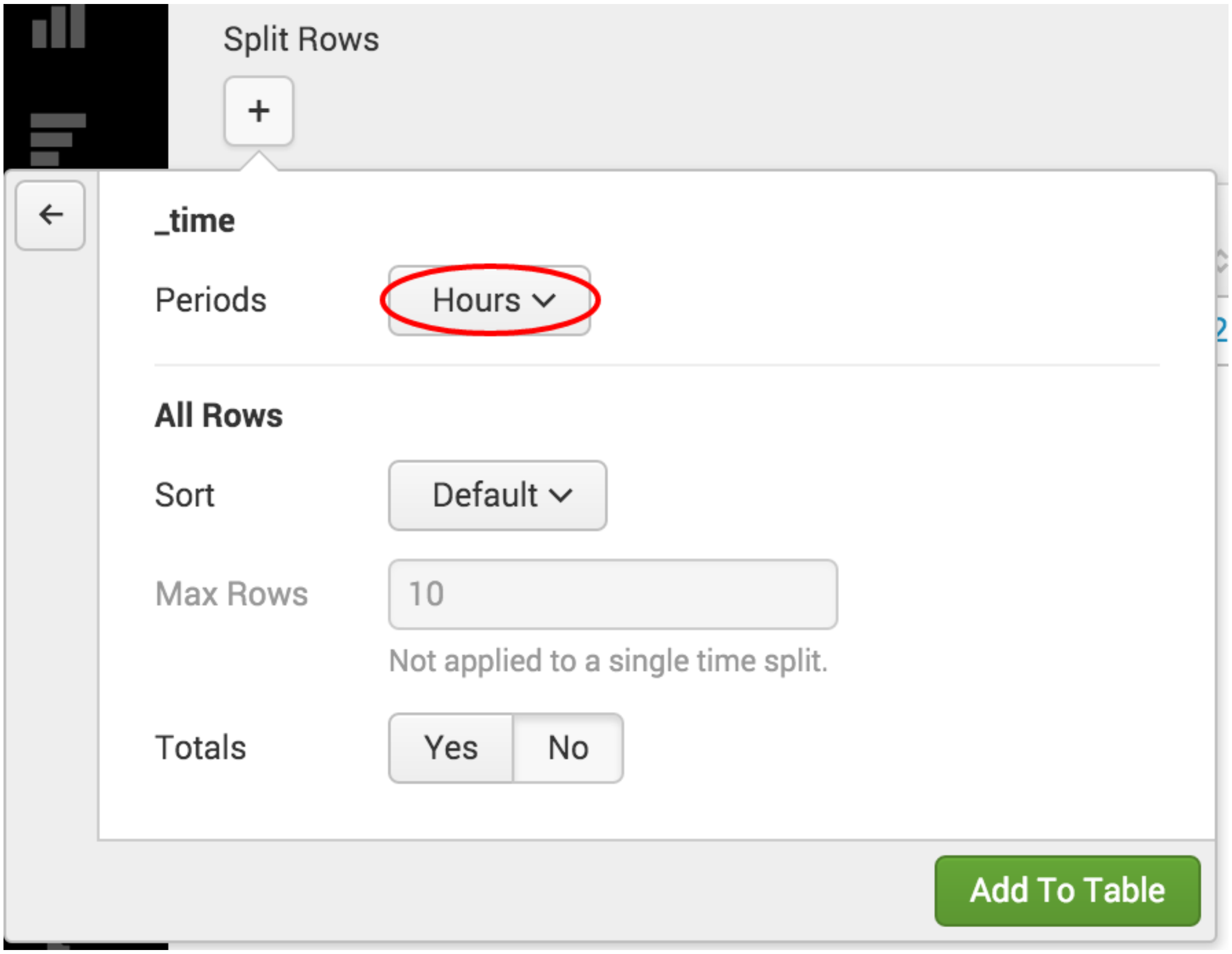
Legend Truncation: A... | A...Z | ...Z

Stack Mode

Multi-series Mode: Yes | No

Drilldown: Yes | No

Show Data Values: Off | On | Min/Max



Split Rows

_time

Periods: Hours

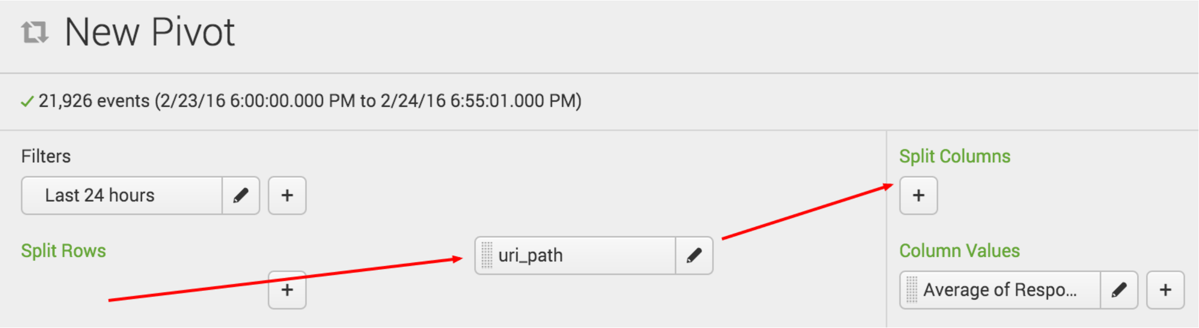
All Rows

Sort: Default

Max Rows: 10

Not applied to a single time split.

Totals: Yes | No



New Pivot

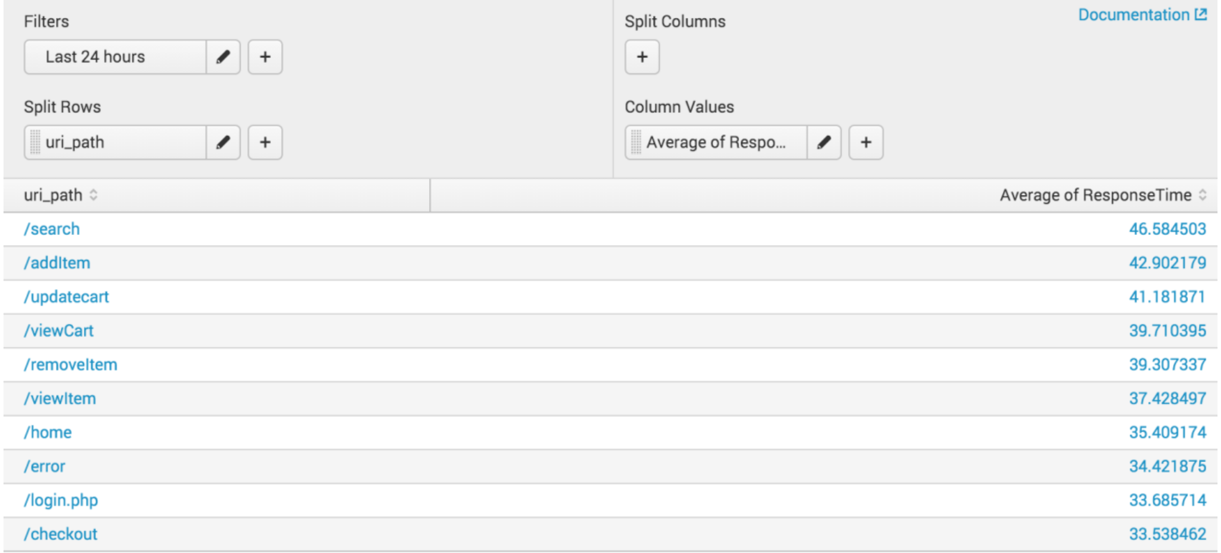
✓ 21,926 events (2/23/16 6:00:00.000 PM to 2/24/16 6:55:01.000 PM)

Filters: Last 24 hours

Split Rows: uri_path

Split Columns

Column Values: Average of Respo...



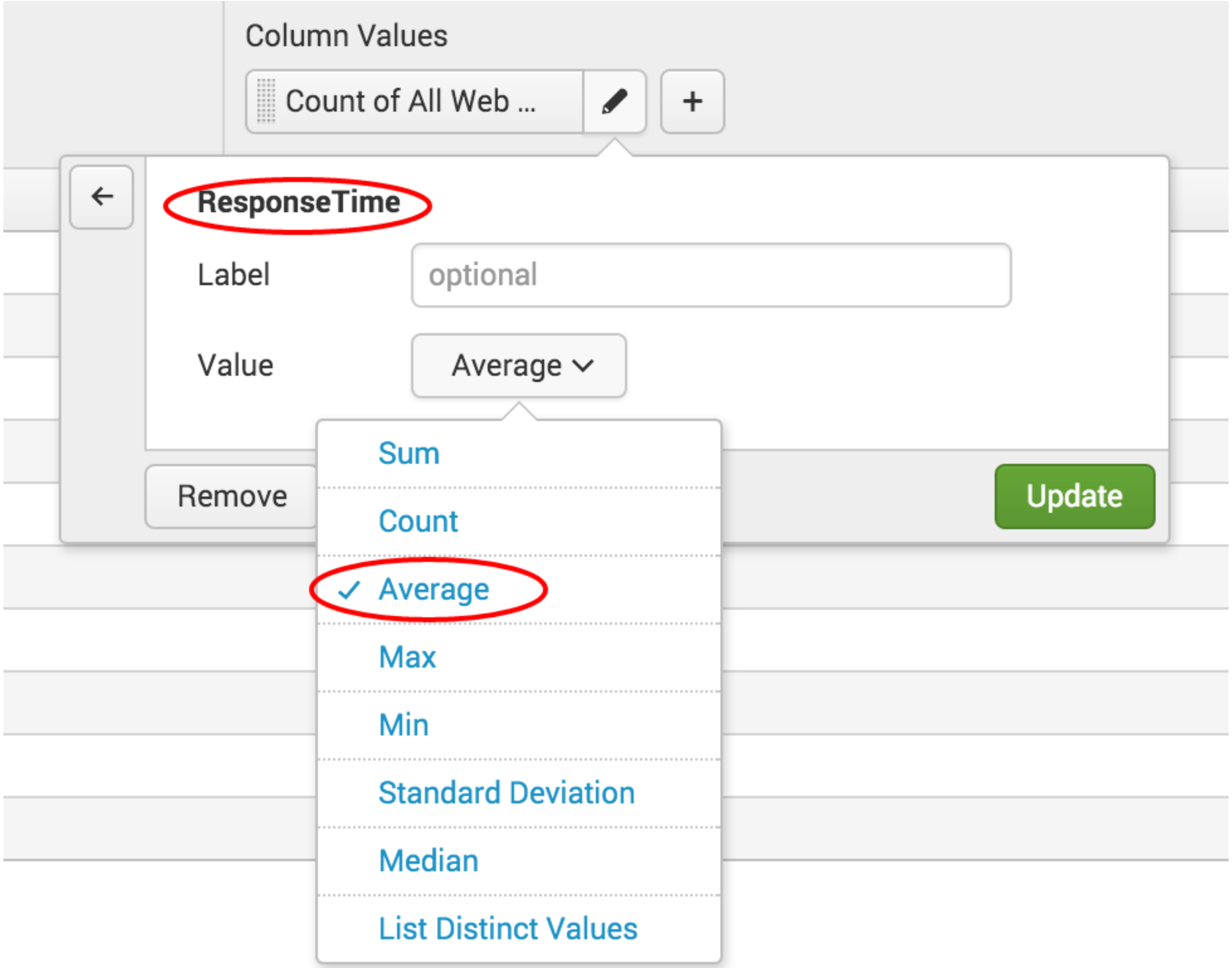
Filters: Last 24 hours

Split Rows: uri_path

Split Columns

Column Values: Average of Respo...

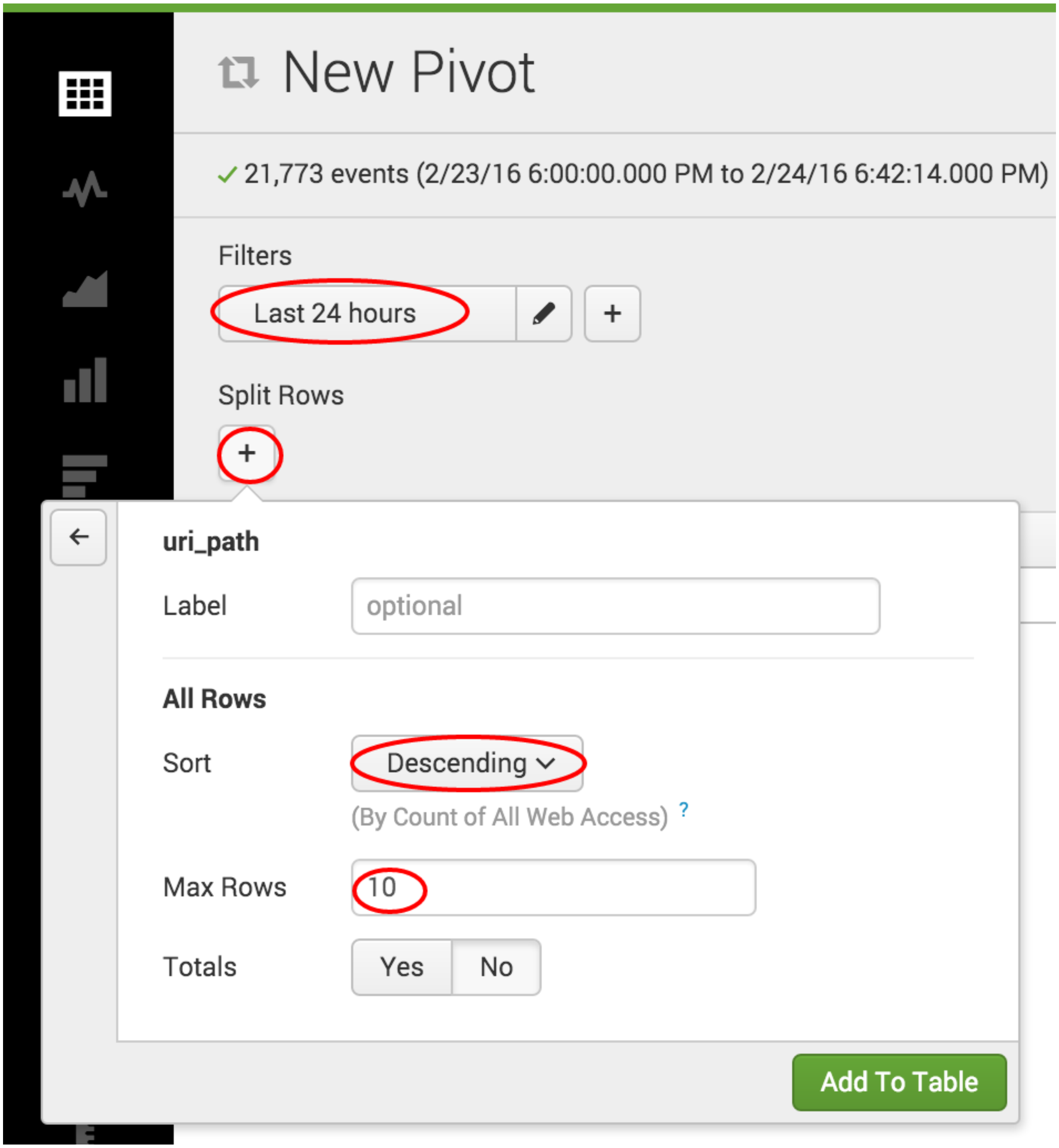
uri_path	Average of ResponseTime
/search	46.584503
/addItem	42.902179
/updatecart	41.181871
/viewCart	39.710395
/removeItem	39.307337
/viewItem	37.428497
/home	35.409174
/error	34.421875
/login.php	33.685714
/checkout	33.538462



ResponseTime

Label optional

Value Average



New Pivot

✓ 21,773 events (2/23/16 6:00:00.000 PM to 2/24/16 6:42:14.000 PM)

Filters

Last 24 hours

Split Rows

uri_path

Label: optional

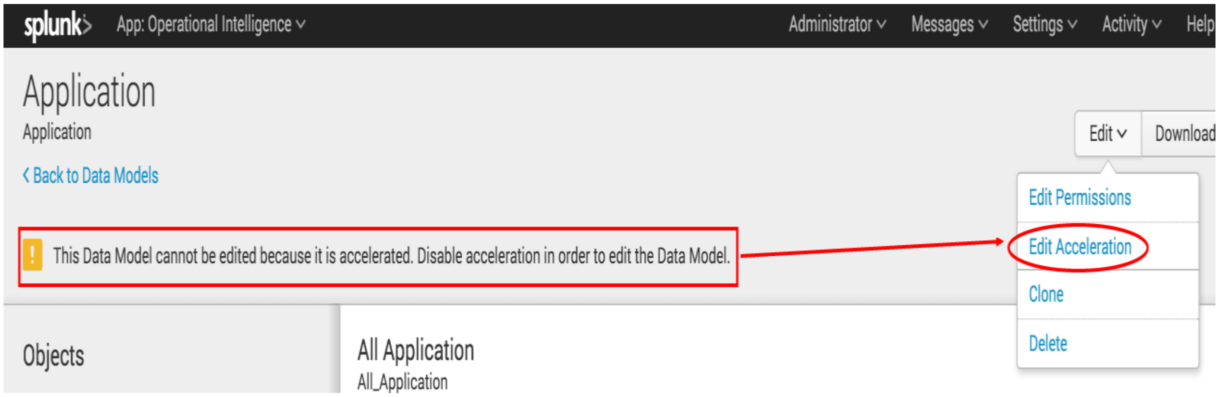
All Rows

Sort: Descending

(By Count of All Web Access) ?

Max Rows: 10

Totals: Yes No



Application

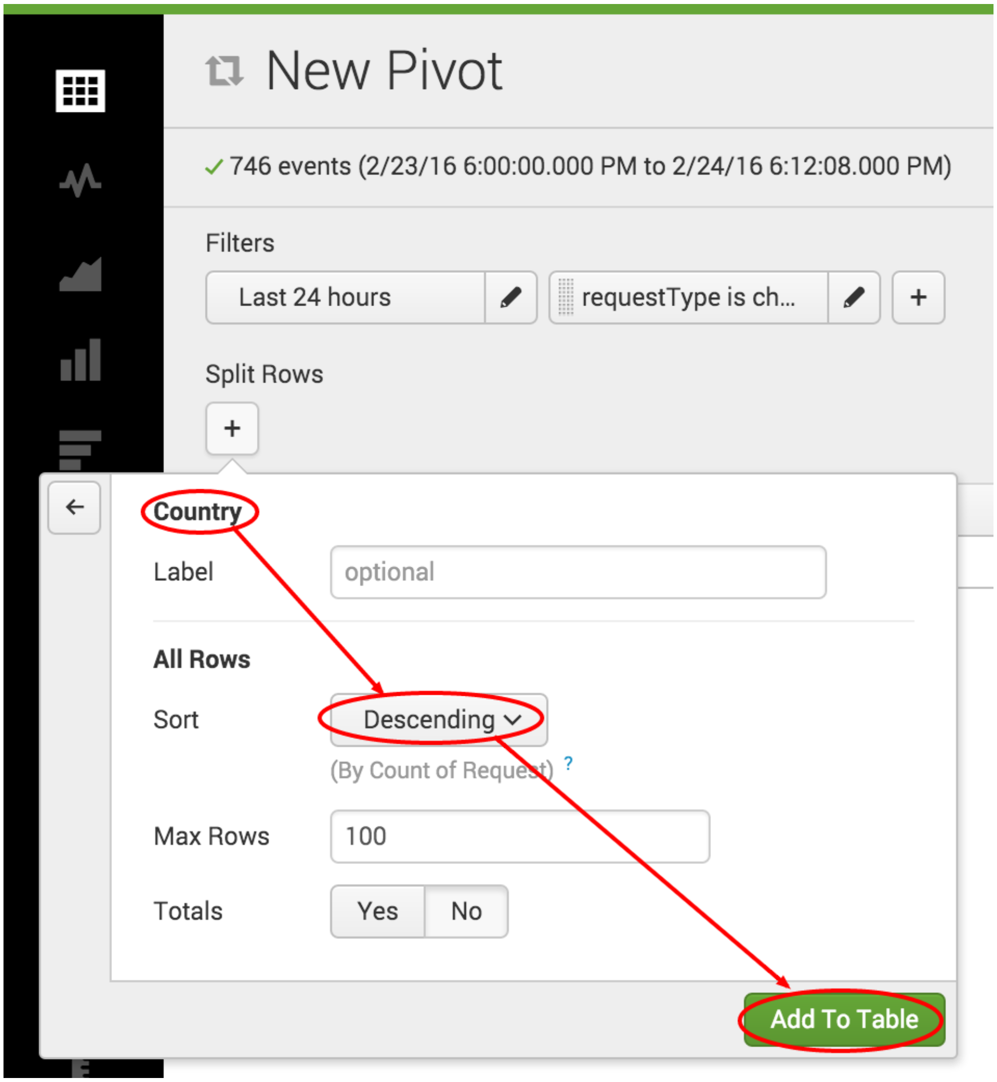
Application

‹ Back to Data Models

! This Data Model cannot be edited because it is accelerated. Disable acceleration in order to edit the Data Model.

All Application

All_Application



✓ 746 events (2/23/16 6:00:00.000 PM to 2/24/16 6:12:08.000 PM)

Filters: Last 24 hours | requestType is ch...

Country

Label: optional

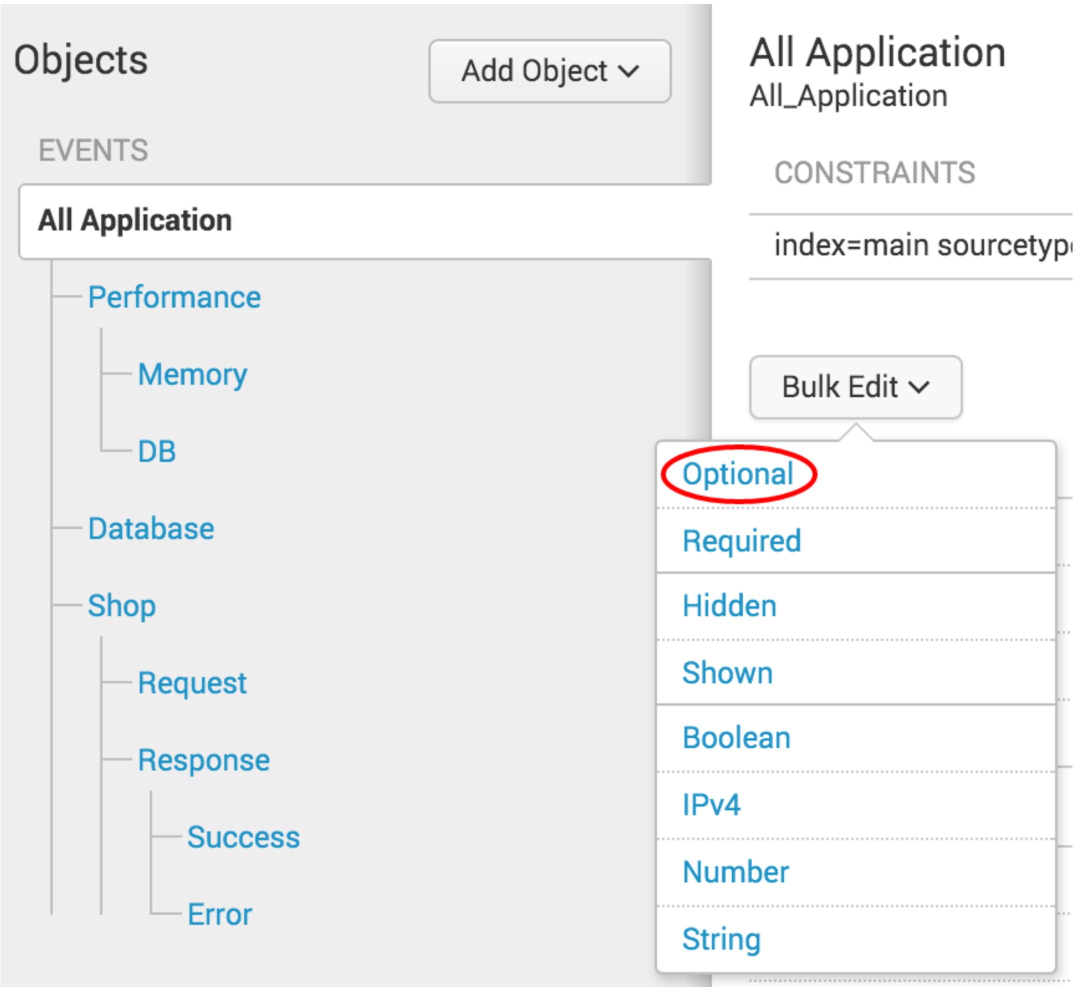
All Rows

Sort: Descending

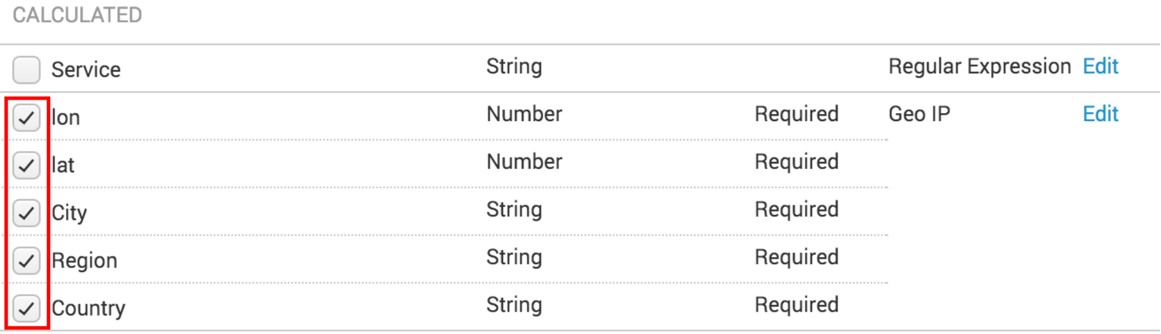
(By Count of Request) ?

Max Rows: 100

Totals: Yes No

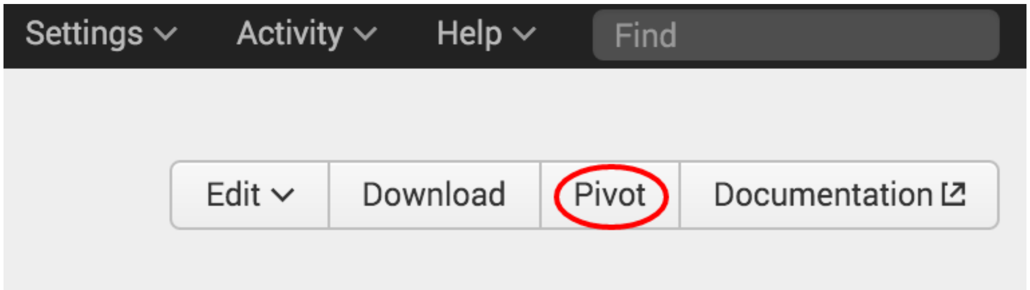


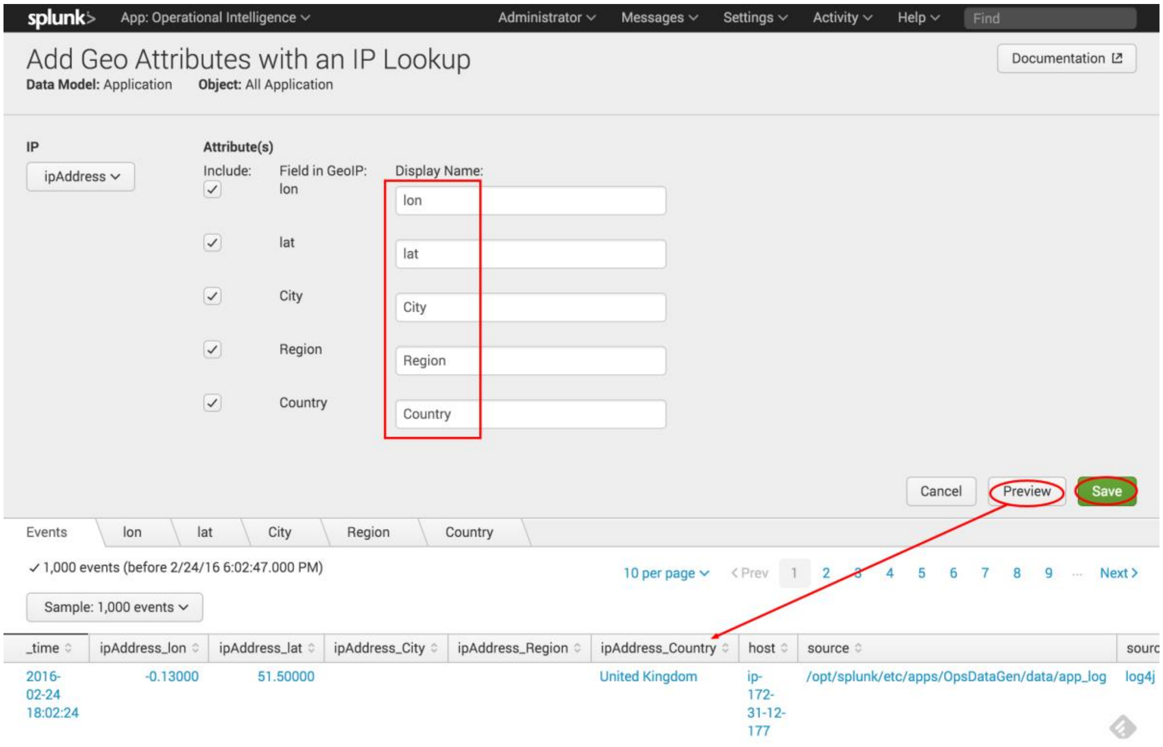
index=main sourcetyp



CALCULATED

□ Service	String		Regular Expression	Edit
☑ lon	Number	Required	Geo IP	Edit
☑ lat	Number	Required		
☑ City	String	Required		
☑ Region	String	Required		
☑ Country	String	Required		





Add Geo Attributes with an IP Lookup

Data Model: Application **Object:** All Application

IP

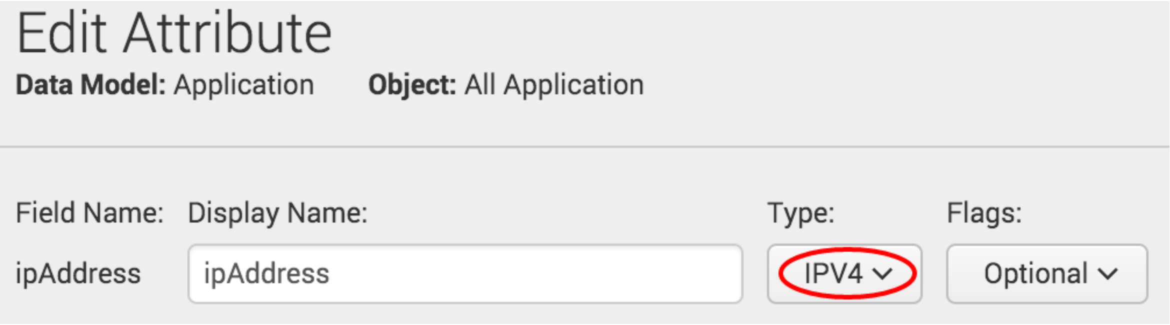
ipAddress

Attribute(s)

Include:	Field in GeoIP:	Display Name:
☑	lon	lon
☑	lat	lat
☑	City	City
☑	Region	Region
☑	Country	Country

✓ 1,000 events (before 2/24/16 6:02:47.000 PM)

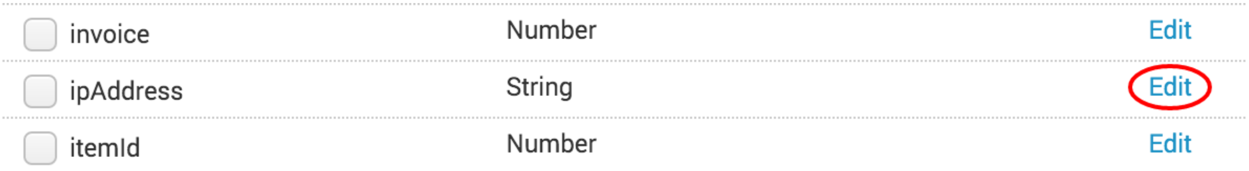
_time	ipAddress_lon	ipAddress_lat	ipAddress_City	ipAddress_Region	ipAddress_Country	host	source	sourc
2016-02-24 18:02:24	-0.13000	51.50000			United Kingdom	ip-172-31-12-177	/opt/splunk/etc/apps/OpsDataGen/data/app_log	log4j



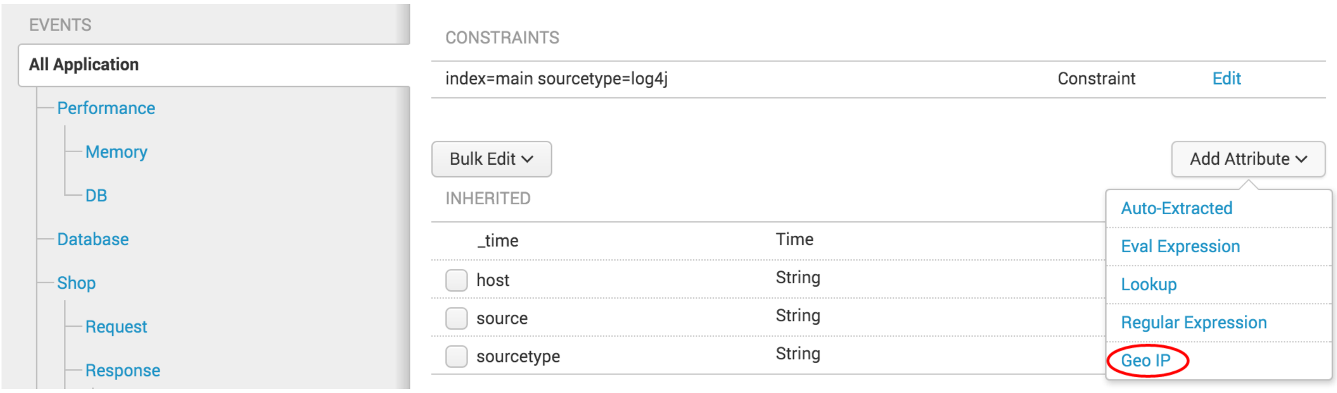
Edit Attribute

Data Model: Application **Object:** All Application

Field Name:	Display Name:	Type:	Flags:
ipAddress	ipAddress	IPV4	Optional



□ invoice	Number	Edit
□ ipAddress	String	Edit
□ itemId	Number	Edit



EVENTS

All Application

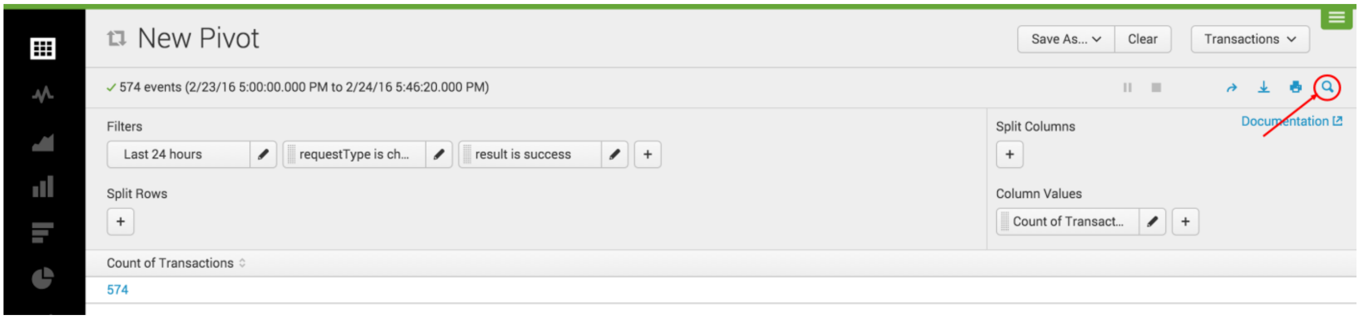
- Performance
  - Memory
  - DB
- Database
- Shop
  - Request
  - Response

CONSTRAINTS

index=main sourcetype=log4j	Constraint	Edit

INHERITED

_time	Time
□ host	String
□ source	String
□ sourcetype	String



New Pivot

✓ 574 events (2/23/16 5:00:00.000 PM to 2/24/16 5:46:20.000 PM)

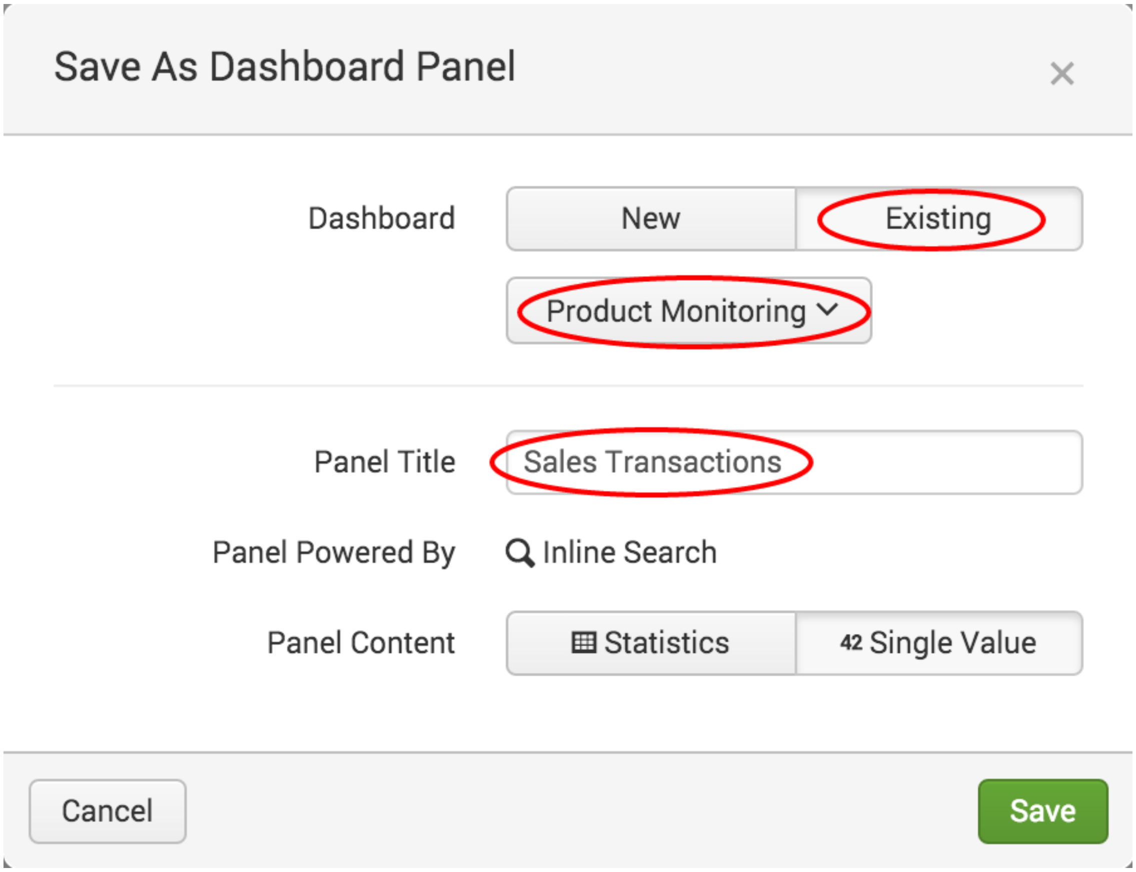
Filters: Last 24 hours | requestType is ch... | result is success

Split Rows

Split Columns

Column Values: Count of Transact...

Count of Transactions
574



Save As Dashboard Panel

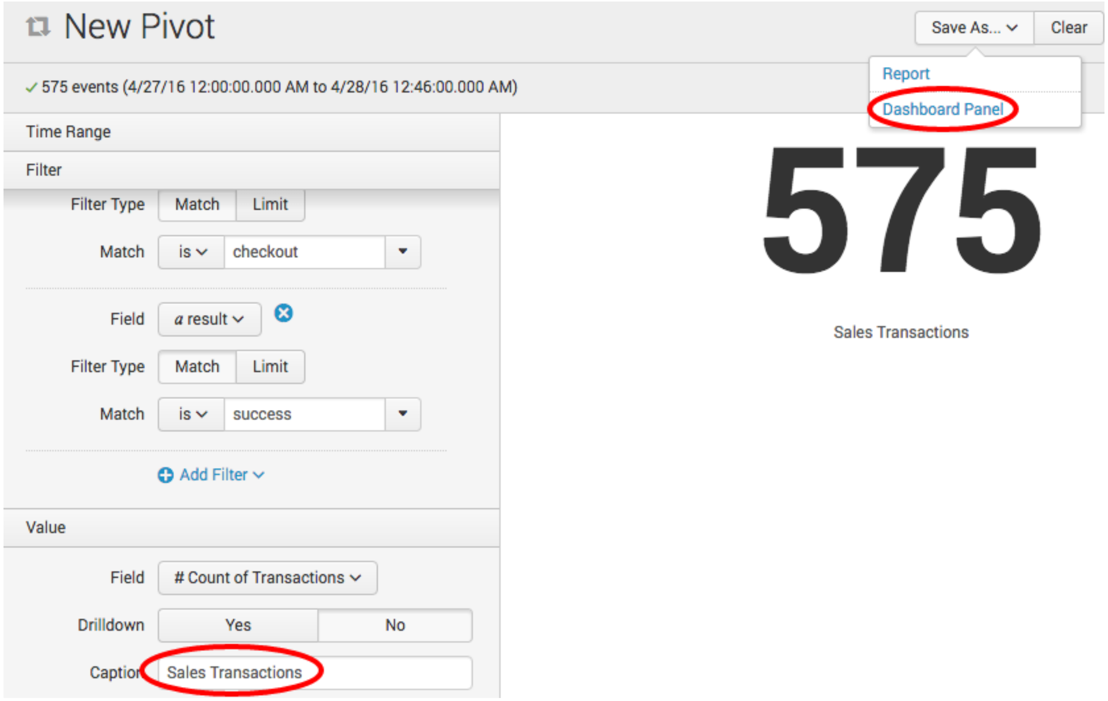
Dashboard: New [✓ Existing]

[✓ Product Monitoring]

Panel Title: [✓ Sales Transactions]

Panel Powered By: Inline Search

Panel Content: Statistics | 42 Single Value



New Pivot

✓ 575 events (4/27/16 12:00:00.000 AM to 4/28/16 12:46:00.000 AM)

Time Range

Filter

Filter Type: Match | Limit

Match: is checkout

Field: a result

Filter Type: Match | Limit

Match: is success

Value

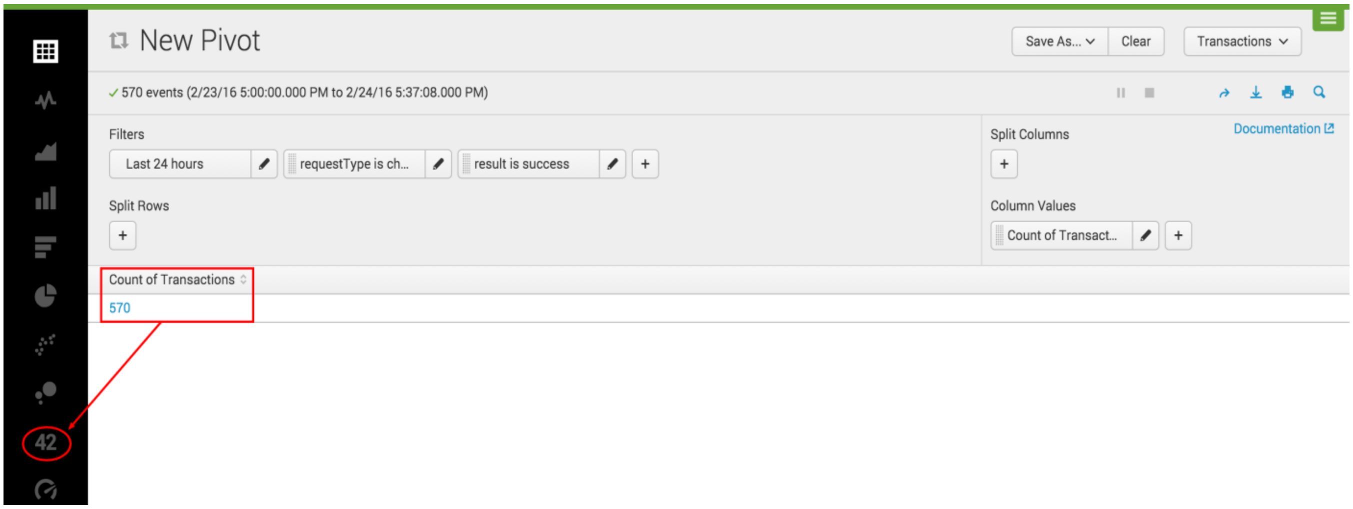
Field: # Count of Transactions

Drilldown: Yes | No

Caption: [✓ Sales Transactions]

575

Sales Transactions



New Pivot

✓ 570 events (2/23/16 5:00:00.000 PM to 2/24/16 5:37:08.000 PM)

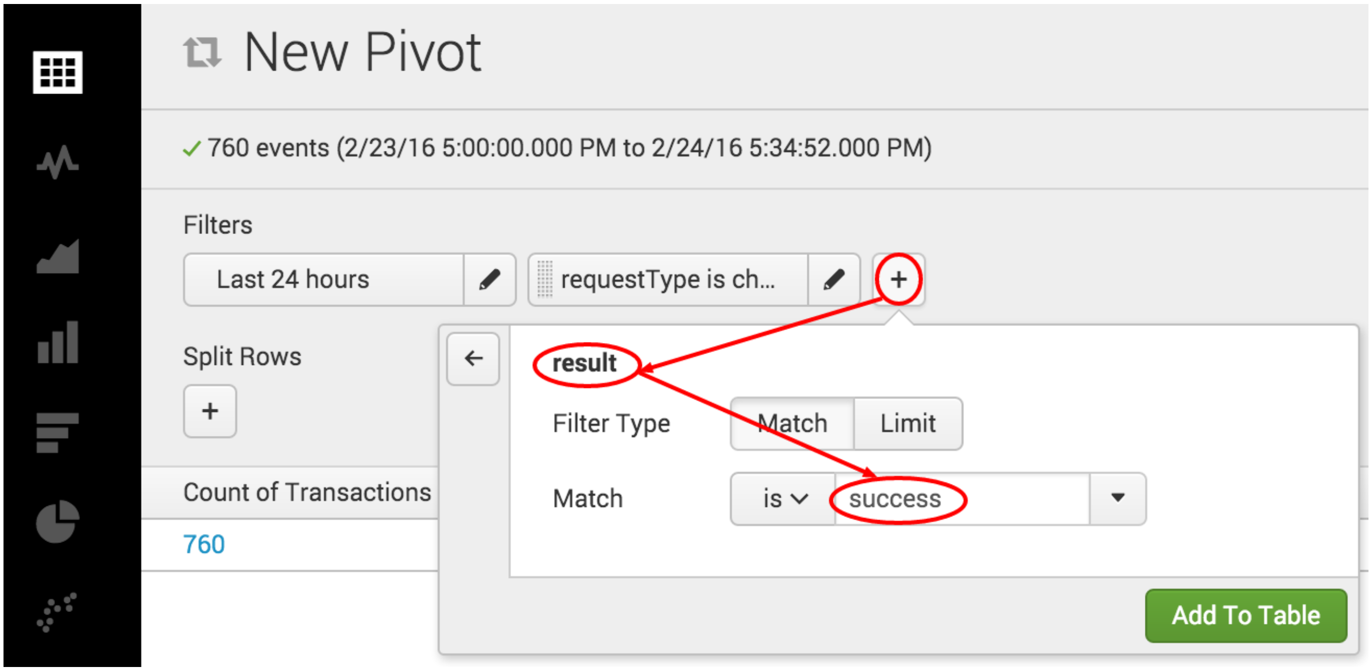
Filters: Last 24 hours | requestType is ch... | result is success

Split Rows

Split Columns

Column Values: Count of Transact...

Count of Transactions
570



New Pivot

✓ 760 events (2/23/16 5:00:00.000 PM to 2/24/16 5:34:52.000 PM)

Filters: Last 24 hours | requestType is ch...

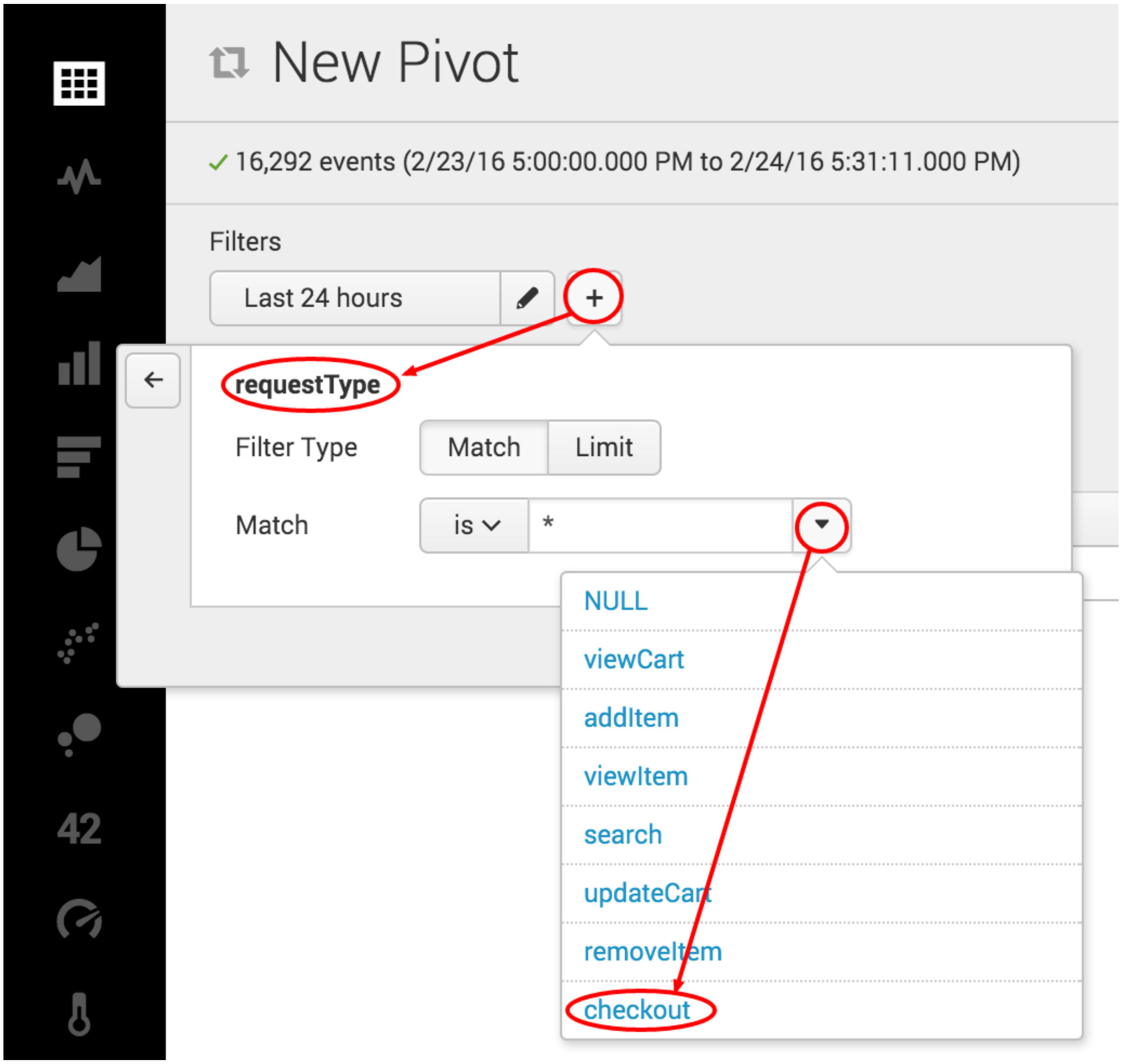
Split Rows

Count of Transactions
760

result

Filter Type: Match | Limit

Match: is success



New Pivot

✓ 16,292 events (2/23/16 5:00:00.000 PM to 2/24/16 5:31:11.000 PM)

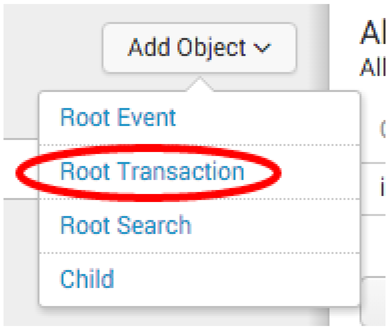
Filters

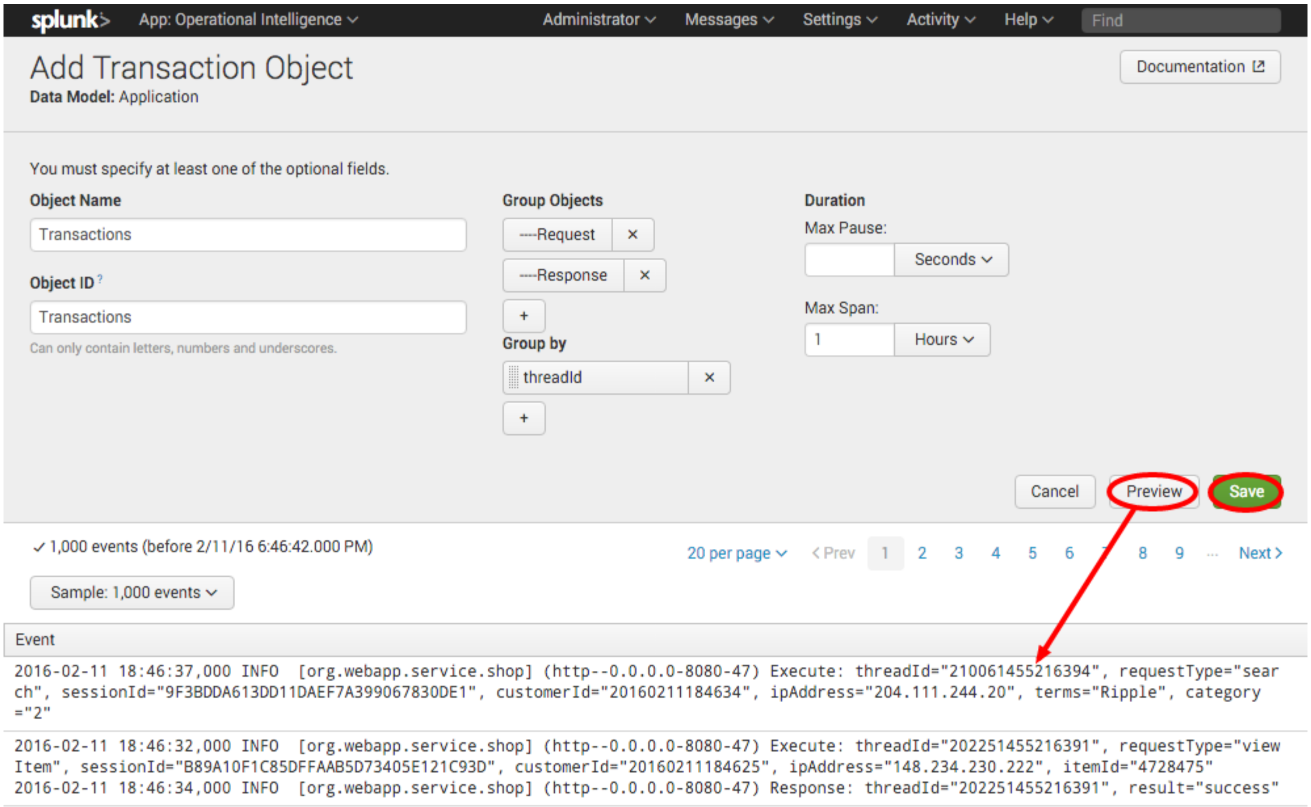
Last 24 hours

requestType

Filter Type: Match

Match: is *





Add Transaction Object

Data Model: Application

You must specify at least one of the optional fields.

Object Name

Transactions

Object ID ?

Transactions

Can only contain letters, numbers and underscores.

Group Objects

---Request ×

---Response ×

+

Group by

threadId ×

+

Duration

Max Pause:

Seconds

Max Span:

1 Hours

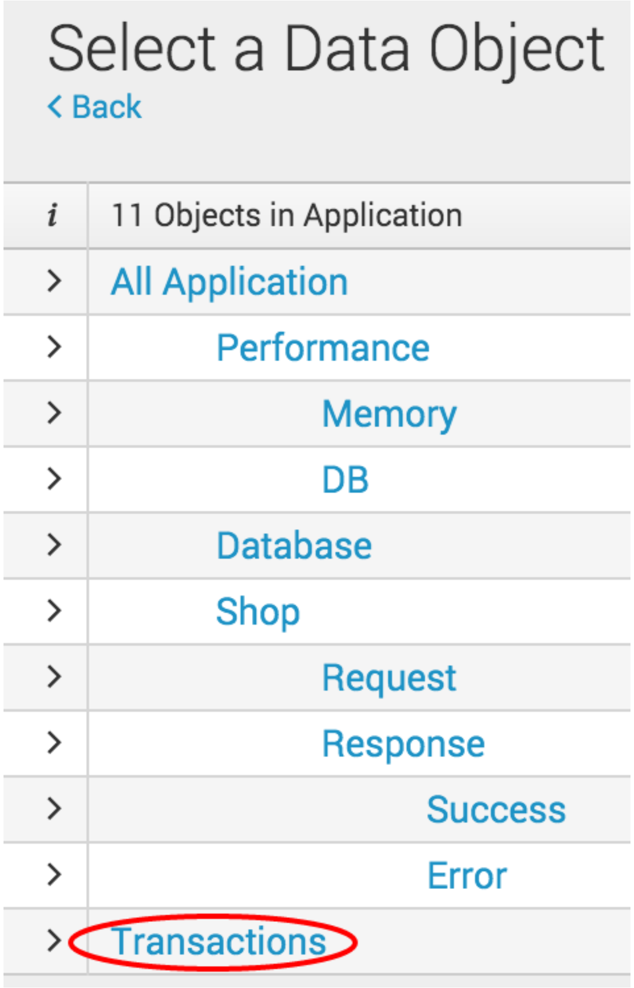
✓ 1,000 events (before 2/11/16 6:46:42.000 PM)

Sample: 1,000 events

Event

```
2016-02-11 18:46:37,000 INFO  [org.webapp.service.shop] (http--0.0.0.0-8080-47) Execute: threadId="210061455216394", requestType="sear
ch", sessionId="9F3BDDA613DD11DAEF7A399067830DE1", customerId="20160211184634", ipAddress="204.111.244.20", terms="Ripple", category
="2"
```

```
2016-02-11 18:46:32,000 INFO  [org.webapp.service.shop] (http--0.0.0.0-8080-47) Execute: threadId="202251455216391", requestType="view
Item", sessionId="B89A10F1C85DFFAAB5D73405E121C93D", customerId="20160211184625", ipAddress="148.234.230.222", itemId="4728475"
2016-02-11 18:46:34,000 INFO  [org.webapp.service.shop] (http--0.0.0.0-8080-47) Response: threadId="202251455216391", result="success"
```

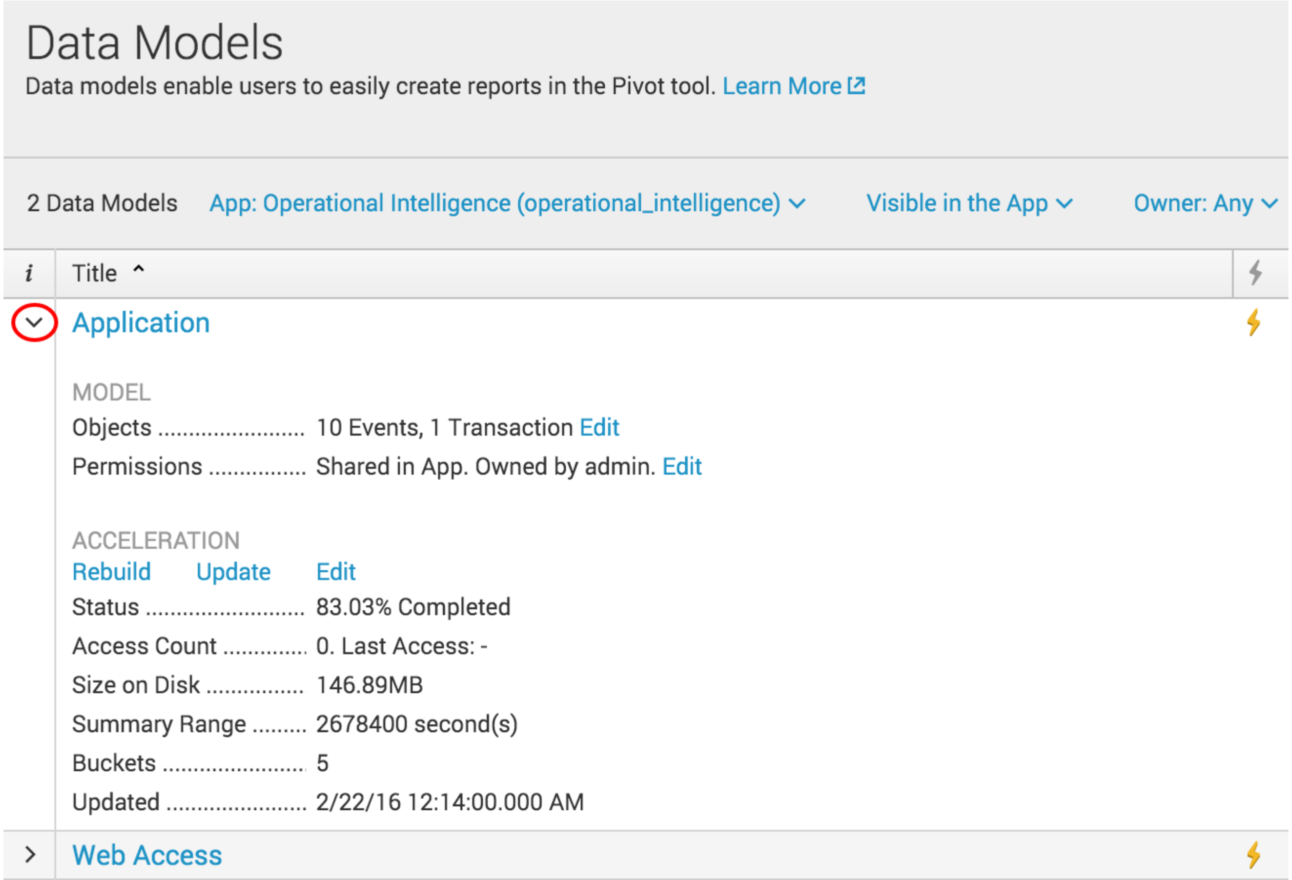


Select a Data Object

‹ Back

i 11 Objects in Application

- All Application
    - Performance
        - Memory
        - DB
    - Database
    - Shop
        - Request
        - Response
            - Success
            - Error
- Transactions



Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More

2 Data Models App: Operational Intelligence (operational_intelligence) Visible in the App Owner: Any

i	Title ^	⚡
⌄	Application	⚡
›	Web Access	⚡

Application

MODEL

Objects .... 10 Events, 1 Transaction Edit

Permissions .... Shared in App. Owned by admin. Edit

ACCELERATION

Rebuild Update Edit

Status .... 83.03% Completed

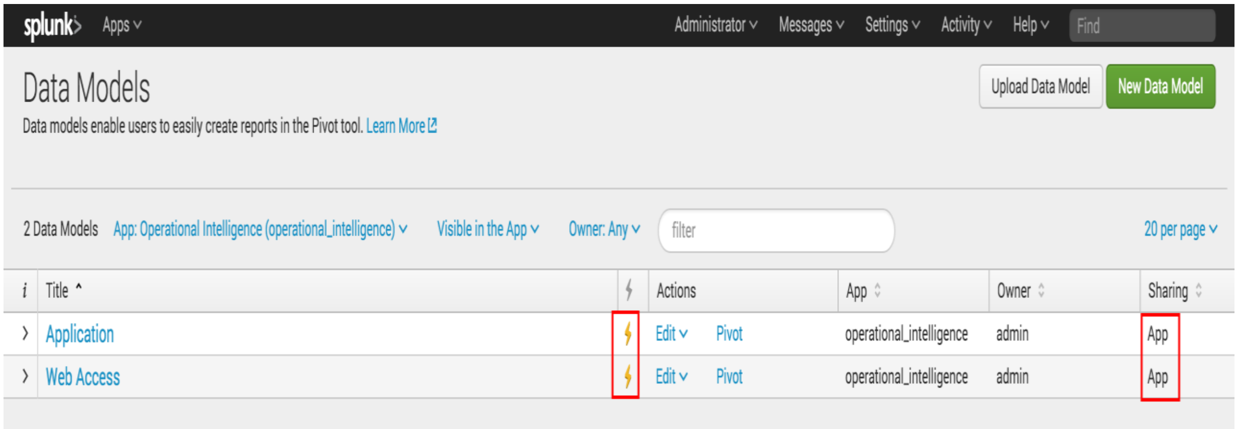
Access Count .... 0. Last Access: -

Size on Disk 146.89MB

Summary Range .... 2678400 second(s)

Buckets 5

Updated .... 2/22/16 12:14:00.000 AM

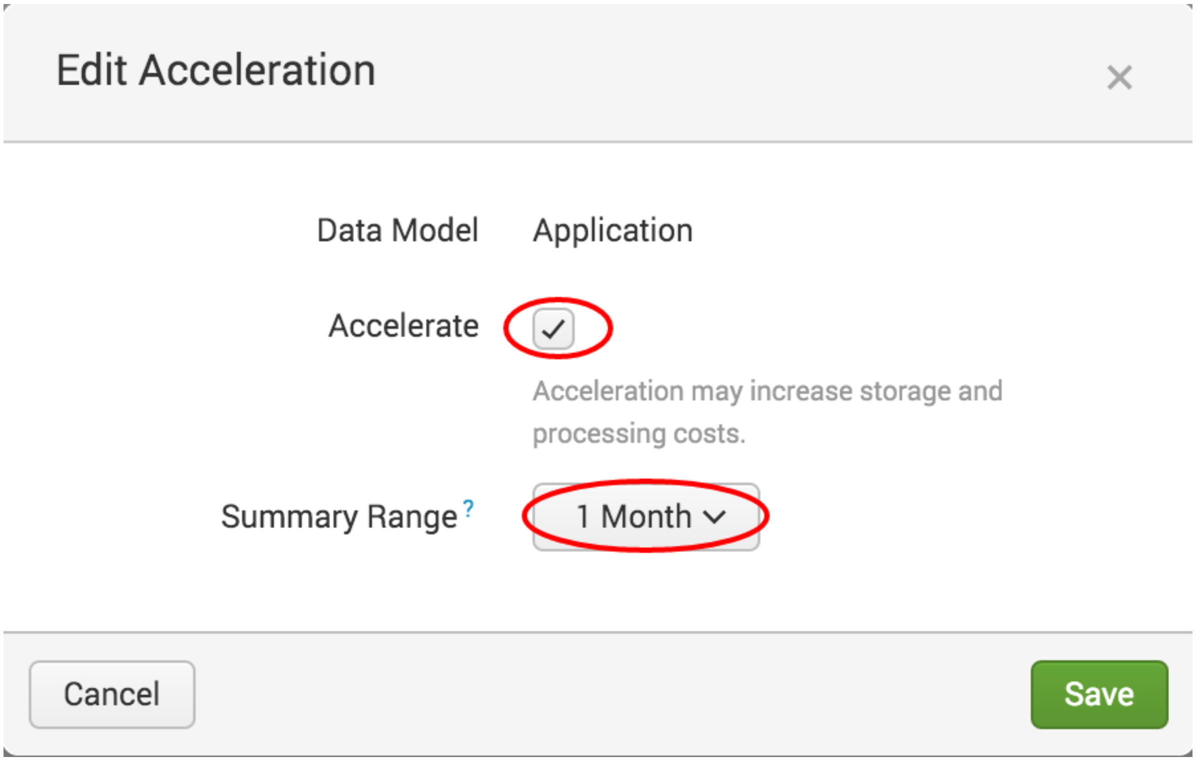


Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More

2 Data Models App: Operational Intelligence (operational_intelligence) Visible in the App Owner: Any filter 20 per page

i	Title ^	⚡	Actions		App	Owner	Sharing
›	Application	⚡	Edit	Pivot	operational_intelligence	admin	App
›	Web Access	⚡	Edit	Pivot	operational_intelligence	admin	App



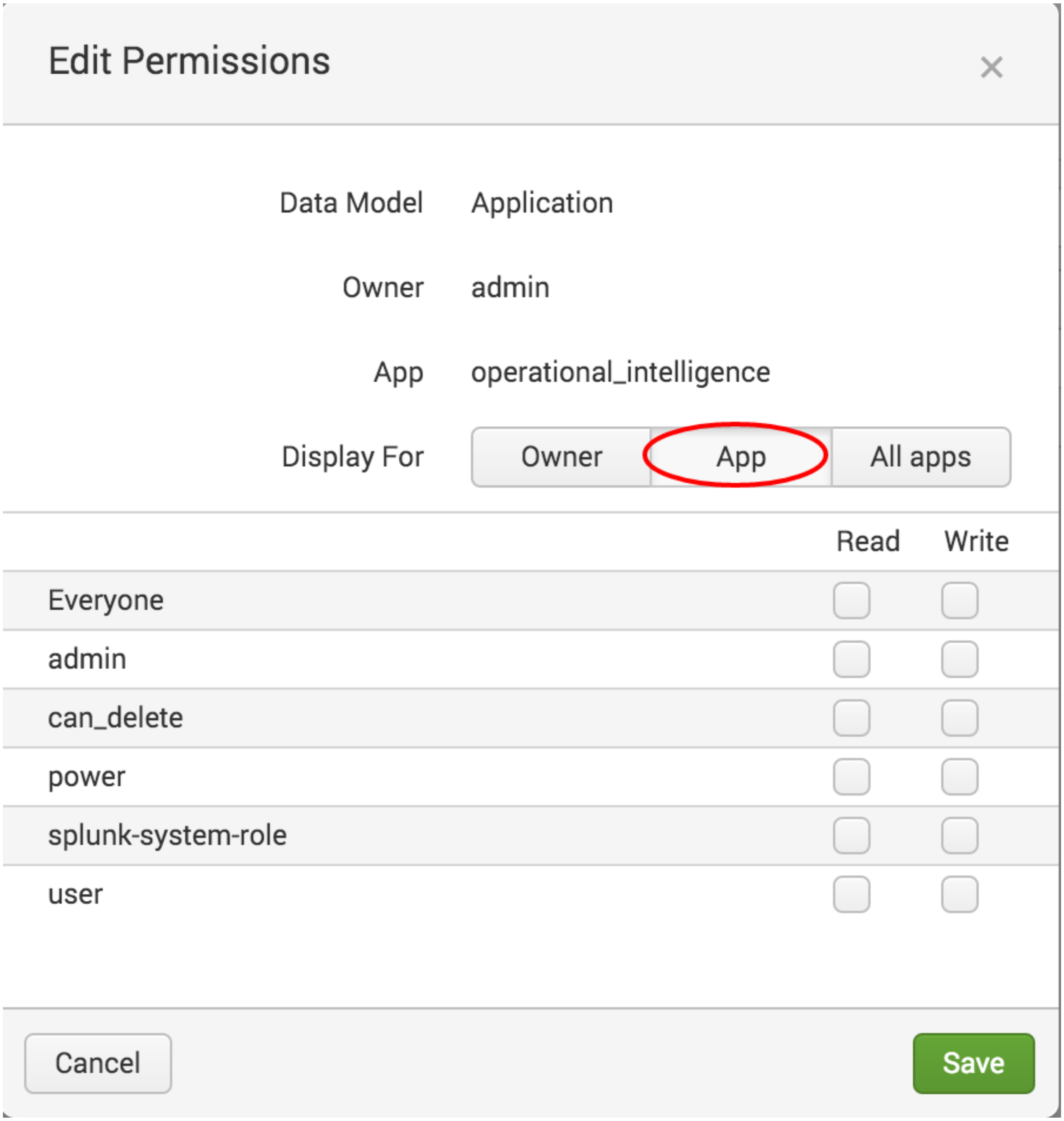
Edit Acceleration

Data Model: Application

Accelerate: ☑

Acceleration may increase storage and processing costs.

Summary Range: 1 Month



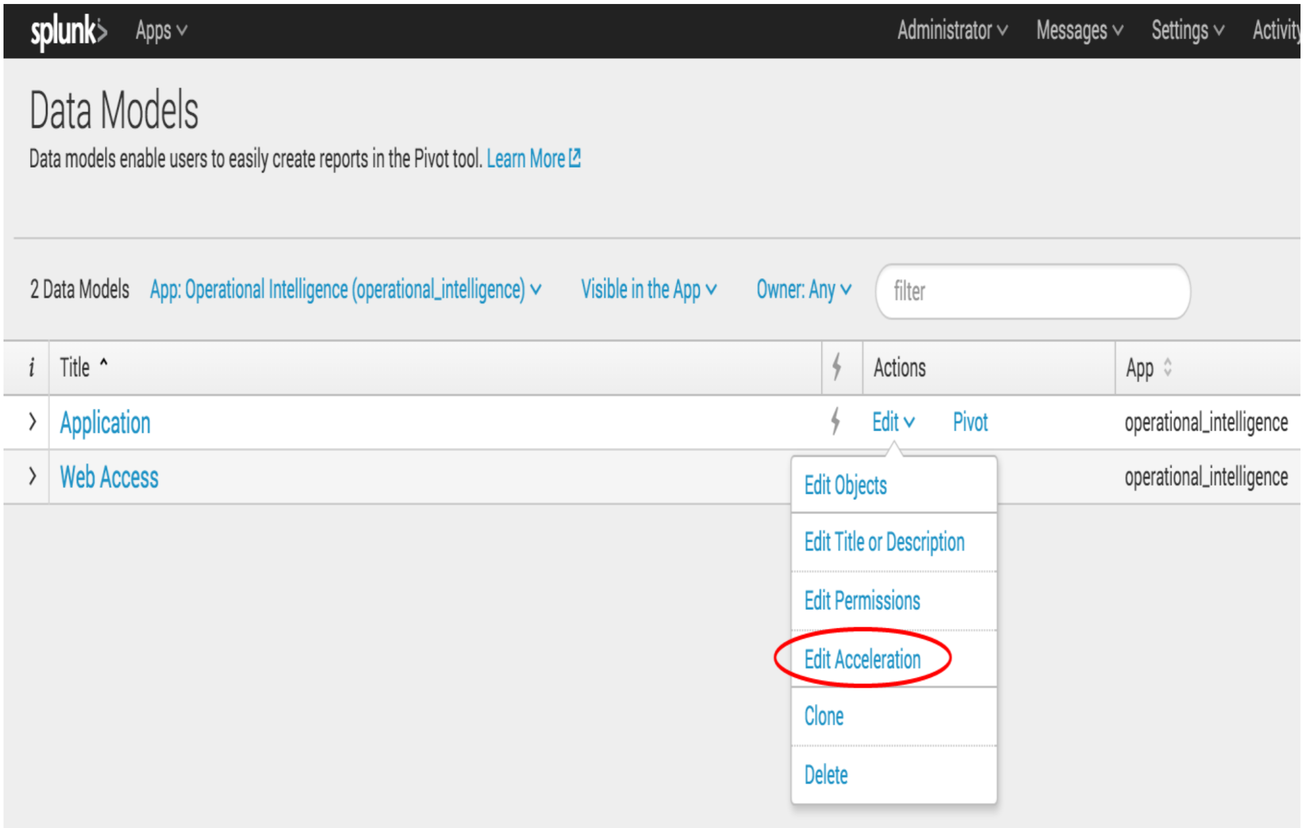
Data Model Application

Owner admin

App operational_intelligence

Display For Owner [✓ App] All apps

	Read	Write
Everyone	□	□
admin	□	□
can_delete	□	□
power	□	□
splunk-system-role	□	□
user	□	□

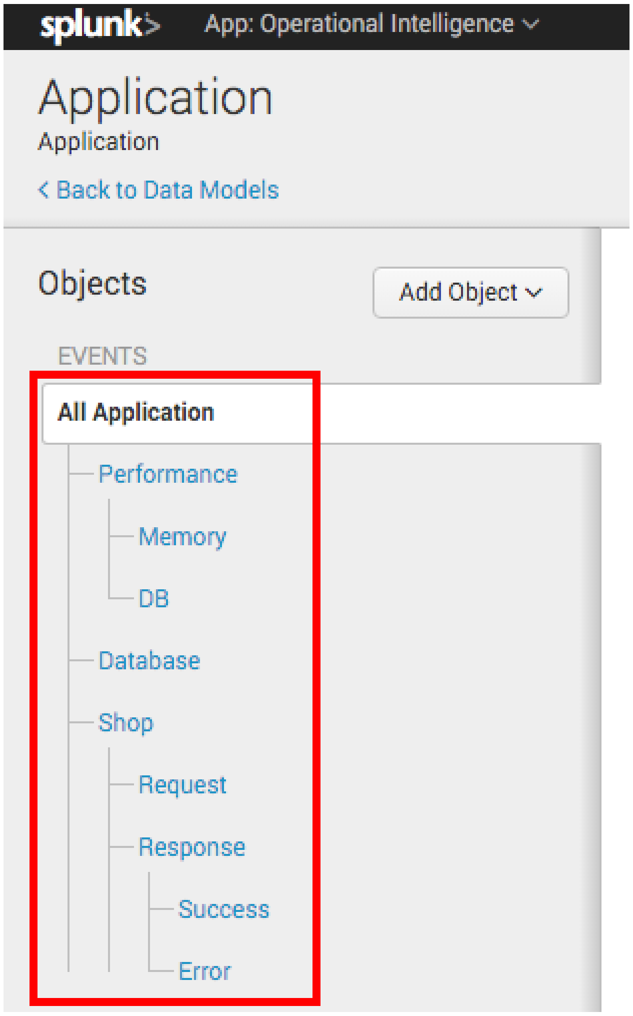


Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More

2 Data Models App: Operational Intelligence (operational_intelligence) Visible in the App Owner: Any filter

i	Title		Actions		App
›	Application	ϟ	Edit	Pivot	operational_intelligence
›	Web Access				operational_intelligence



Application

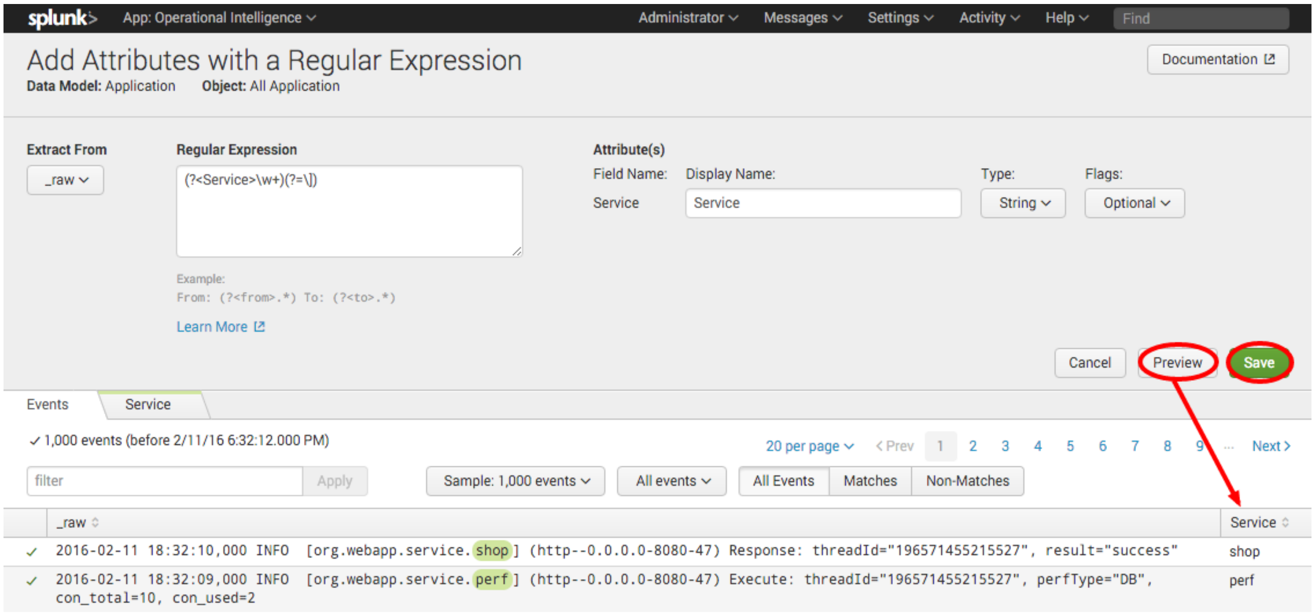
Application

< Back to Data Models

Objects

EVENTS

- All Application
  - Performance
    - Memory
    - DB
  - Database
  - Shop
    - Request
    - Response
      - Success
      - Error



Add Attributes with a Regular Expression

Data Model: Application **Object:** All Application

Extract From: _raw

Regular Expression

```
(?<Service>\w+)(?=\])
```

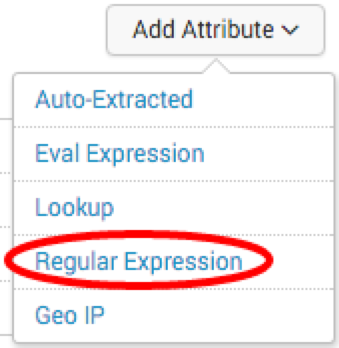
Example:
From: (?<from>.*) To: (?<to>.*)

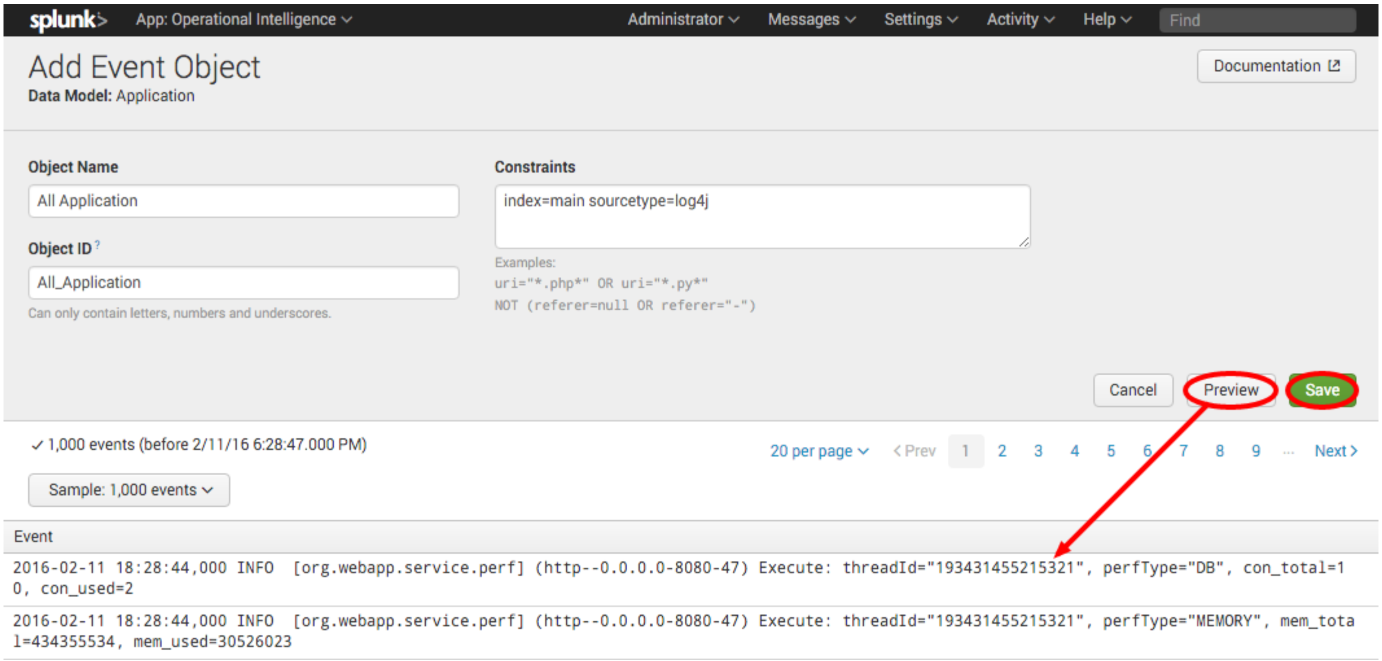
Attribute(s)

Field Name:	Display Name:	Type:	Flags:
Service	Service	String	Optional

✓ 1,000 events (before 2/11/16 6:32:12.000 PM)

	_raw	Service
✓	2016-02-11 18:32:10,000 INFO [org.webapp.service.shop] (http--0.0.0.0-8080-47) Response: threadId="196571455215527", result="success"	shop
✓	2016-02-11 18:32:09,000 INFO [org.webapp.service.perf] (http--0.0.0.0-8080-47) Execute: threadId="196571455215527", perfType="DB", con_total=10, con_used=2	perf





Add Event Object

Data Model: Application

Object Name

All Application

Object ID ?

All_Application

Can only contain letters, numbers and underscores.

Constraints

index=main sourcetype=log4j

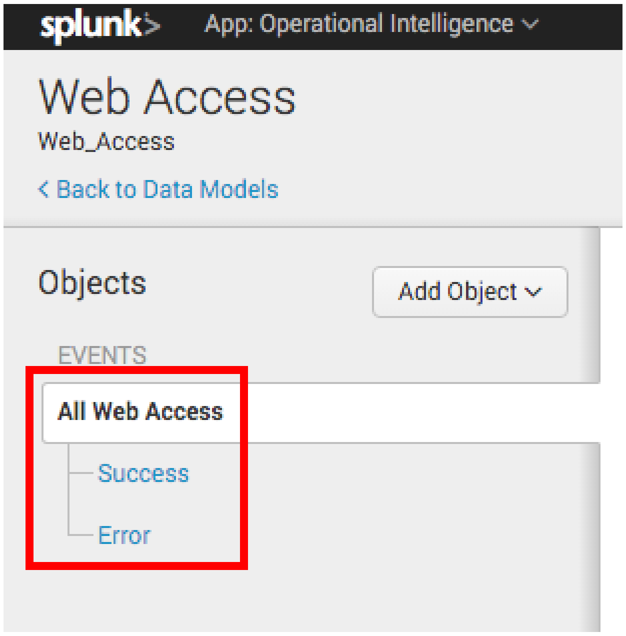
Examples:

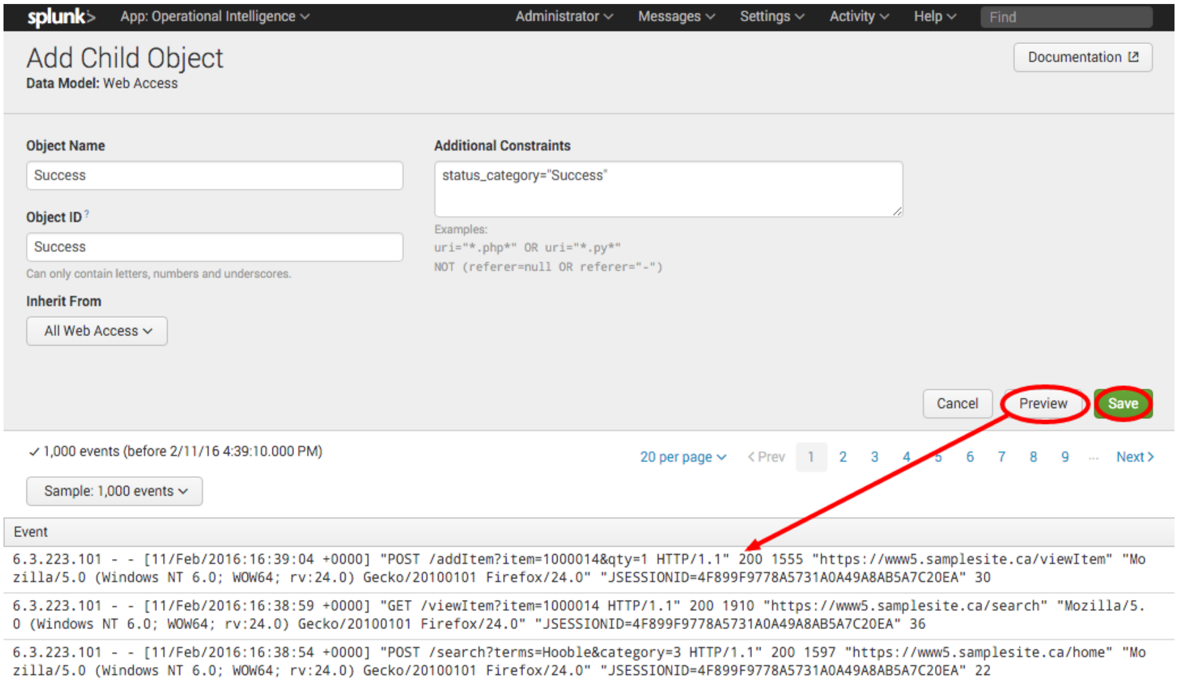
```
uri="*.php*" OR uri="*.py*"
NOT (referer=null OR referer="-")
```

✓ 1,000 events (before 2/11/16 6:28:47.000 PM)

Event

```
2016-02-11 18:28:44,000 INFO  [org.webapp.service.perf] (http--0.0.0.0-8080-47) Execute: threadId="193431455215321", perfType="DB", con_total=1
0, con_used=2
2016-02-11 18:28:44,000 INFO  [org.webapp.service.perf] (http--0.0.0.0-8080-47) Execute: threadId="193431455215321", perfType="MEMORY", mem_tota
l=434355534, mem_used=30526023
```





Add Child Object

Data Model: Web Access

Object Name

Success

Object ID

Success

Can only contain letters, numbers and underscores.

Inherit From

All Web Access

Additional Constraints

status_category="Success"

Examples:

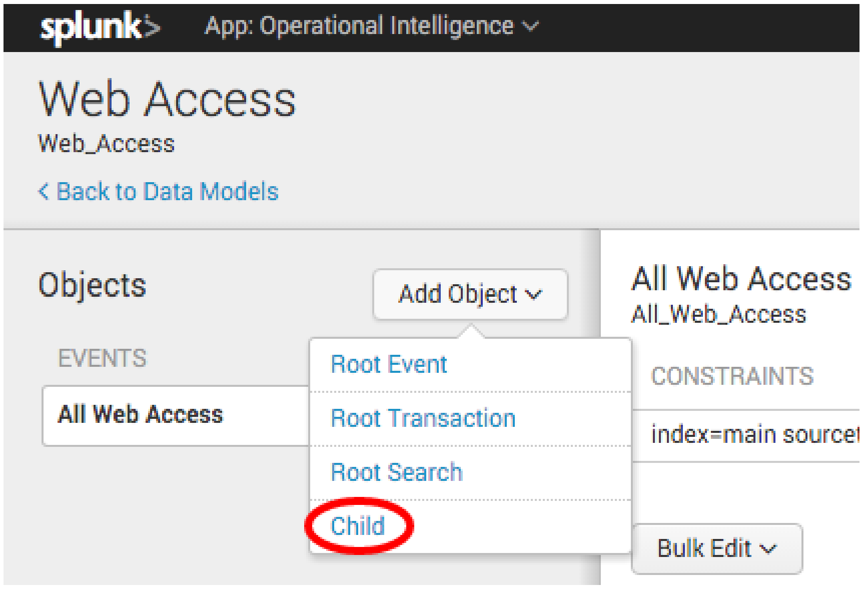
```
uri="*.php*" OR uri="*.py*"
NOT (referer=null OR referer="-")
```

✓ 1,000 events (before 2/11/16 4:39:10.000 PM)

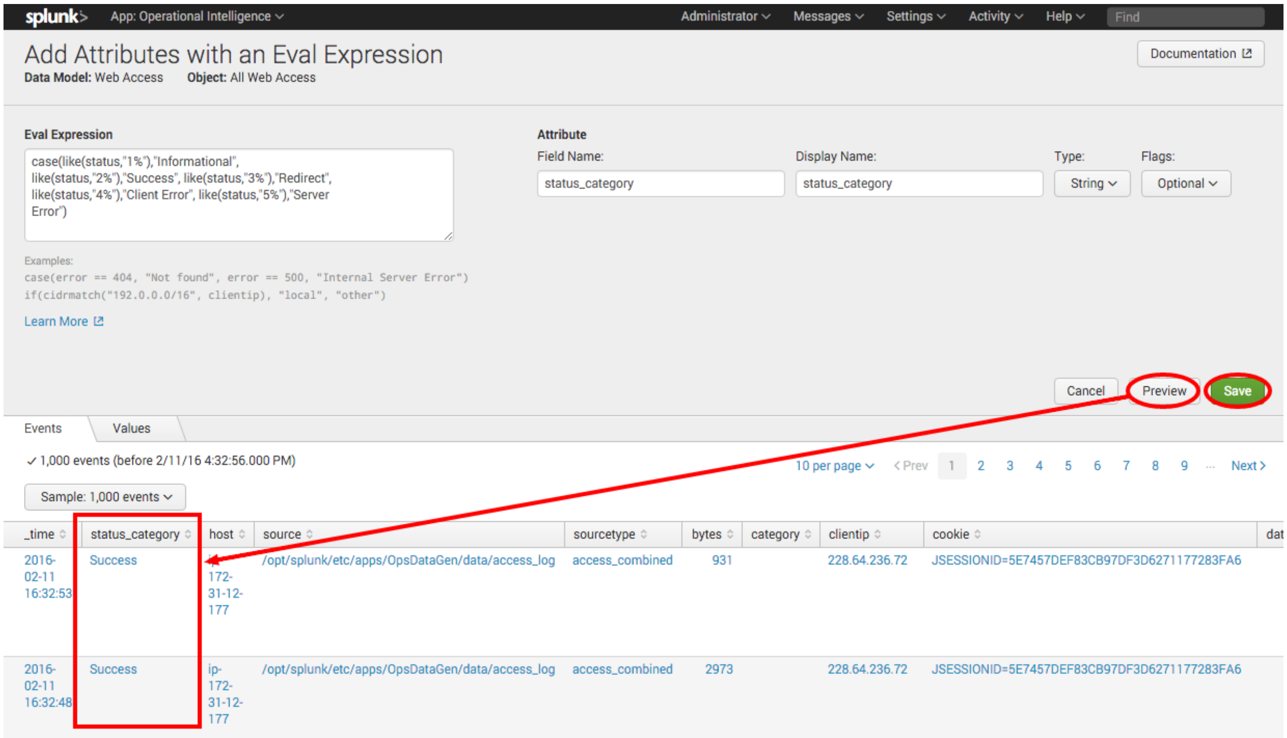
Sample: 1,000 events

Event

```
6.3.223.101 - - [11/Feb/2016:16:39:04 +0000] "POST /addItem?item=1000014&qty=1 HTTP/1.1" 200 1555 "https://www5.samplesite.ca/viewItem" "Mo
zilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" "JSESSIONID=4F899F9778A5731A0A49A8AB5A7C20EA" 30
6.3.223.101 - - [11/Feb/2016:16:38:59 +0000] "GET /viewItem?item=1000014 HTTP/1.1" 200 1910 "https://www5.samplesite.ca/search" "Mozilla/5.
0 (Windows NT 6.0; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" "JSESSIONID=4F899F9778A5731A0A49A8AB5A7C20EA" 36
6.3.223.101 - - [11/Feb/2016:16:38:54 +0000] "POST /search?terms=Hooble&category=3 HTTP/1.1" 200 1597 "https://www5.samplesite.ca/home" "Mo
zilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" "JSESSIONID=4F899F9778A5731A0A49A8AB5A7C20EA" 22
```



index=main sourcet



Add Attributes with an Eval Expression

Data Model: Web Access **Object:** All Web Access

Eval Expression

```
case(like(status,"1%"),"Informational",
like(status,"2%"),"Success", like(status,"3%"),"Redirect",
like(status,"4%"),"Client Error", like(status,"5%"),"Server
Error")
```

Examples:

```
case(error == 404, "Not found", error == 500, "Internal Server Error")
if(cidrmatch("192.0.0.0/16", clientip), "local", "other")
```

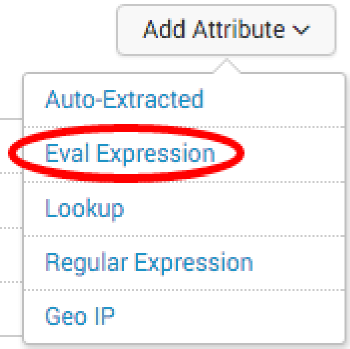
Attribute

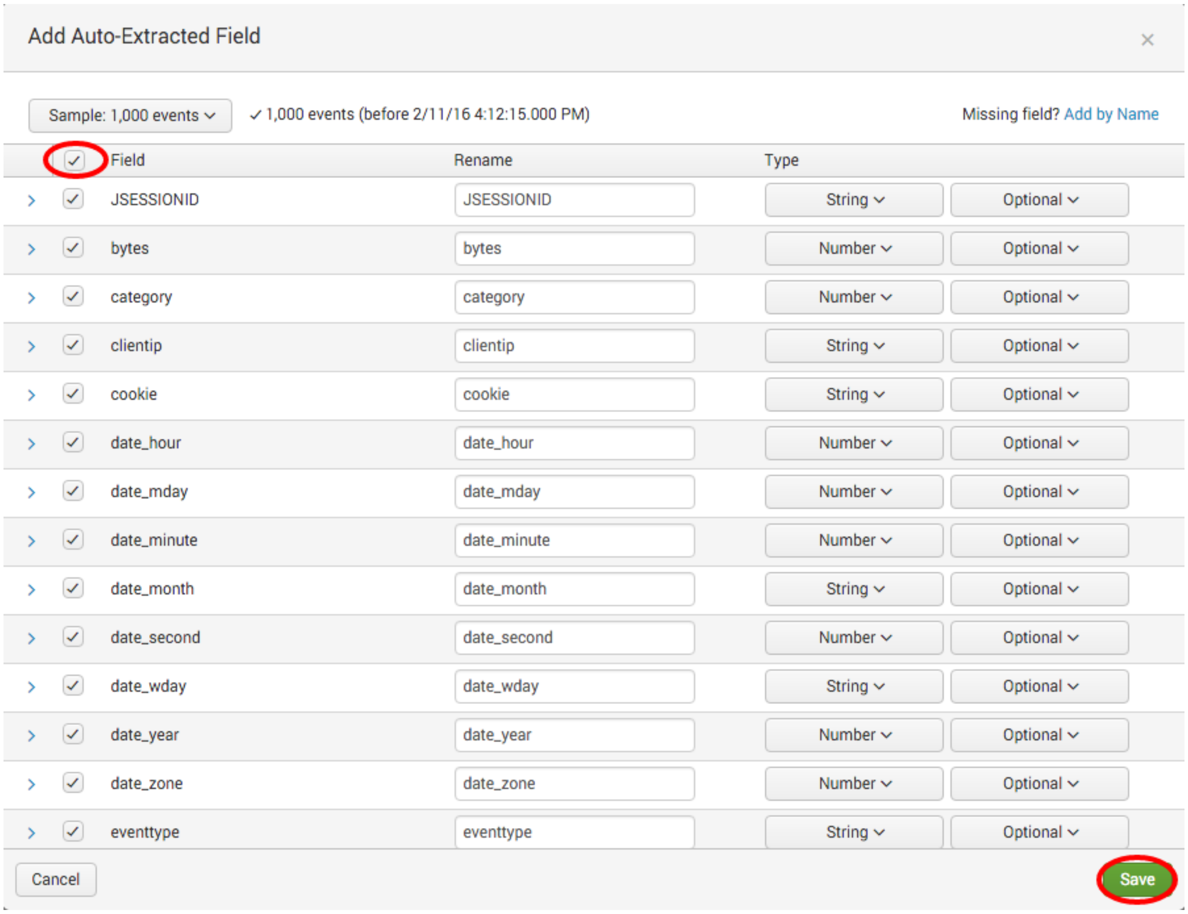
Field Name:	Display Name:	Type:	Flags:
status_category	status_category	String	Optional

✓ 1,000 events (before 2/11/16 4:32:56.000 PM)

Sample: 1,000 events

_time	status_category	host	source	sourcetype	bytes	category	clientip	cookie	dat
2016-02-11 16:32:53	Success	ip-172-31-12-177	/opt/splunk/etc/apps/OpsDataGen/data/access_log	access_combined	931		228.64.236.72	JSESSIONID=5E7457DEF83CB97DF3D6271177283FA6	
2016-02-11 16:32:48	Success	ip-172-31-12-177	/opt/splunk/etc/apps/OpsDataGen/data/access_log	access_combined	2973		228.64.236.72	JSESSIONID=5E7457DEF83CB97DF3D6271177283FA6	



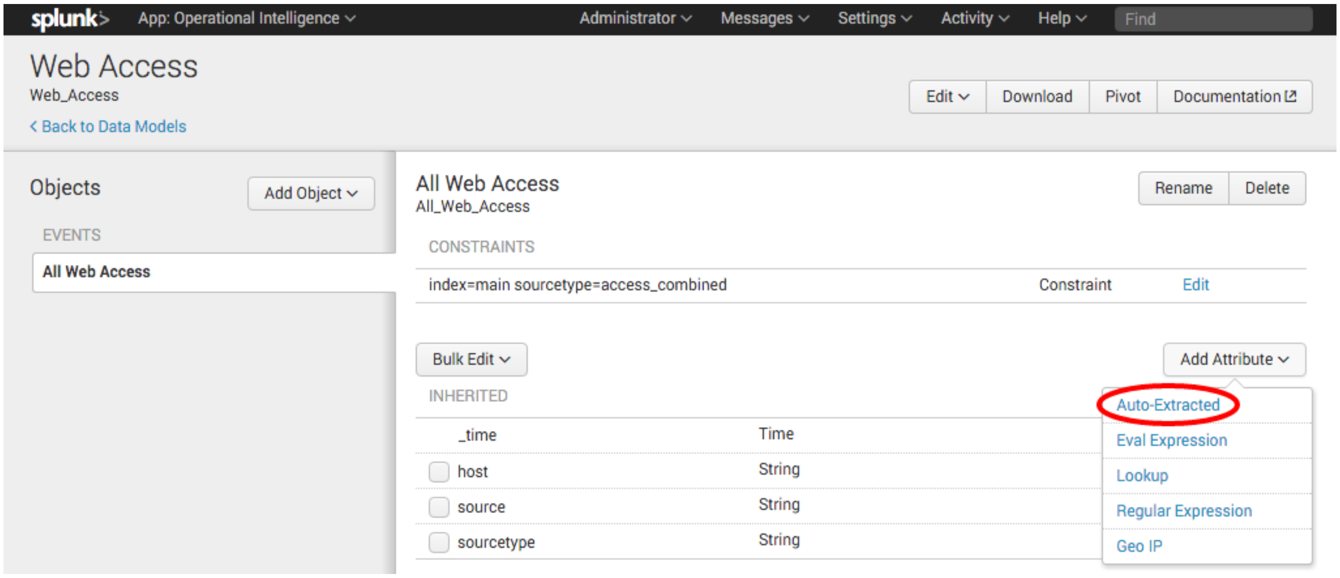


Add Auto-Extracted Field ×

Sample: 1,000 events ✓ 1,000 events (before 2/11/16 4:12:15.000 PM) Missing field? Add by Name

	☑ Field	Rename	Type	
›	☑ JSESSIONID	JSESSIONID	String	Optional
›	☑ bytes	bytes	Number	Optional
›	☑ category	category	Number	Optional
›	☑ clientip	clientip	String	Optional
›	☑ cookie	cookie	String	Optional
›	☑ date_hour	date_hour	Number	Optional
›	☑ date_mday	date_mday	Number	Optional
›	☑ date_minute	date_minute	Number	Optional
›	☑ date_month	date_month	String	Optional
›	☑ date_second	date_second	Number	Optional
›	☑ date_wday	date_wday	String	Optional
›	☑ date_year	date_year	Number	Optional
›	☑ date_zone	date_zone	Number	Optional
›	☑ eventtype	eventtype	String	Optional

Cancel Save



Web Access

Web_Access

Objects

EVENTS

All Web Access

All Web Access

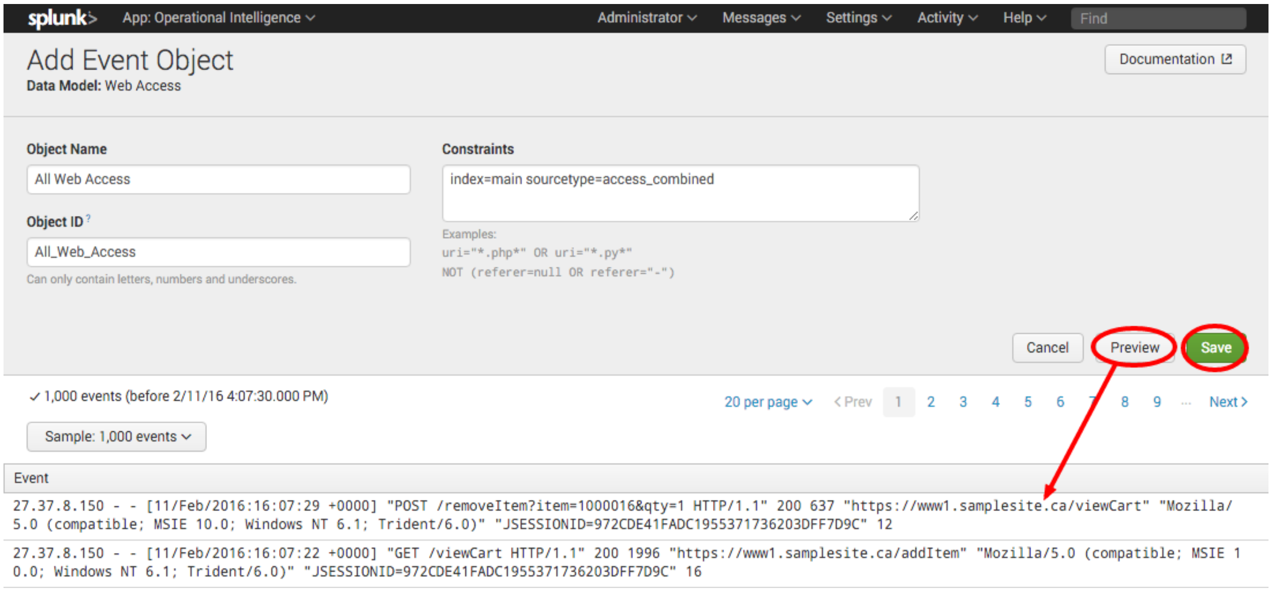
All_Web_Access

CONSTRAINTS

index=main sourcetype=access_combined	Constraint	Edit

INHERITED

_time	Time
□ host	String
□ source	String
□ sourcetype	String



Add Event Object

Data Model: Web Access

Object Name

All Web Access

Object ID ?

All_Web_Access

Can only contain letters, numbers and underscores.

Constraints

index=main sourcetype=access_combined

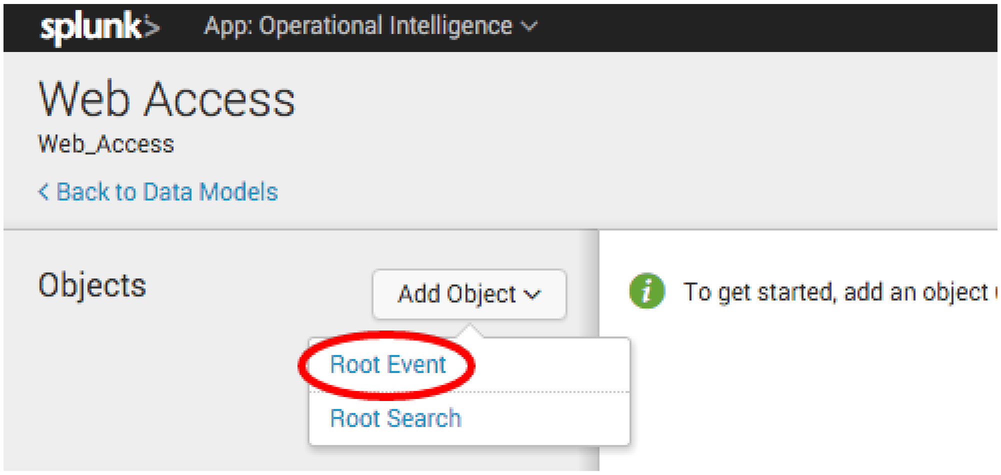
Examples:

```
uri="*.php*" OR uri="*.py*"
NOT (referer=null OR referer="-")
```

✓ 1,000 events (before 2/11/16 4:07:30.000 PM)

Event

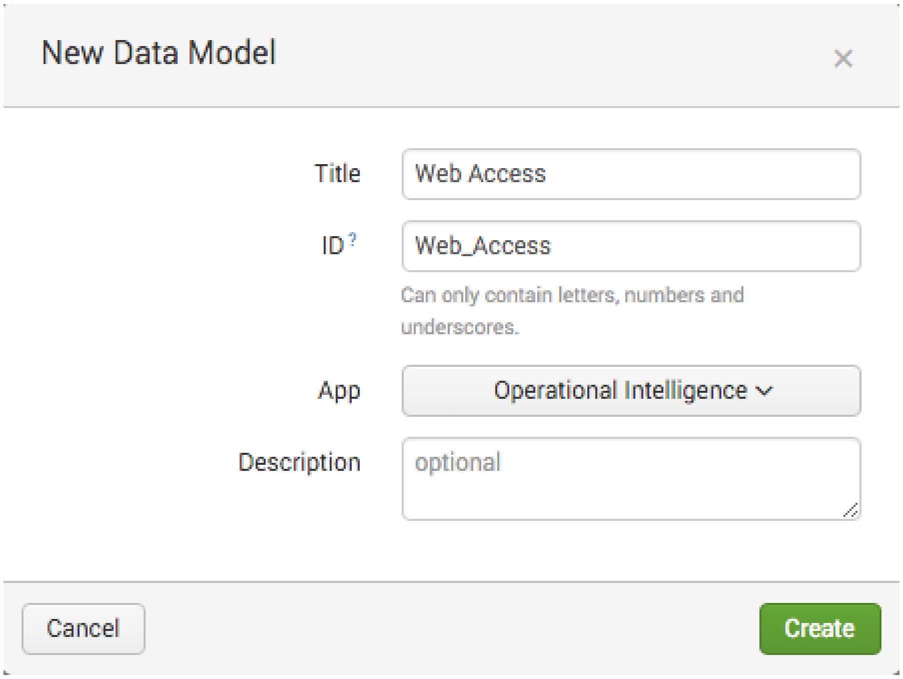
```
27.37.8.150 - - [11/Feb/2016:16:07:29 +0000] "POST /removeItem?item=1000016&qty=1 HTTP/1.1" 200 637 "https://www1.samplesite.ca/viewCart" "Mozilla/
5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)" "JSESSIONID=972CDE41FADC1955371736203DFF7D9C" 12
27.37.8.150 - - [11/Feb/2016:16:07:22 +0000] "GET /viewCart HTTP/1.1" 200 1996 "https://www1.samplesite.ca/addItem" "Mozilla/5.0 (compatible; MSIE 1
0.0; Windows NT 6.1; Trident/6.0)" "JSESSIONID=972CDE41FADC1955371736203DFF7D9C" 16
```



Web Access

Web_Access

To get started, add an object


New Data Model

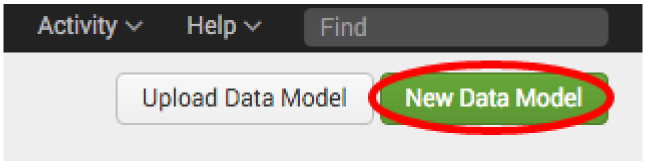
Title: Web Access

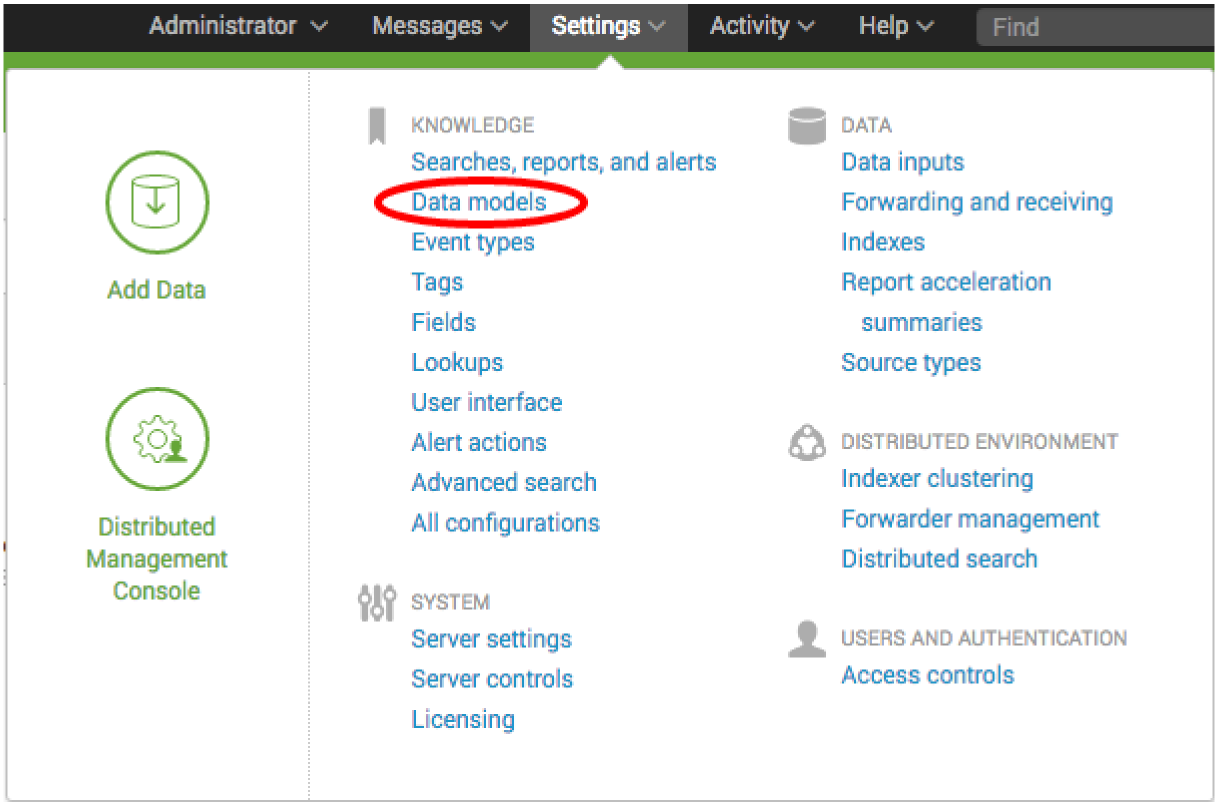
ID: Web_Access

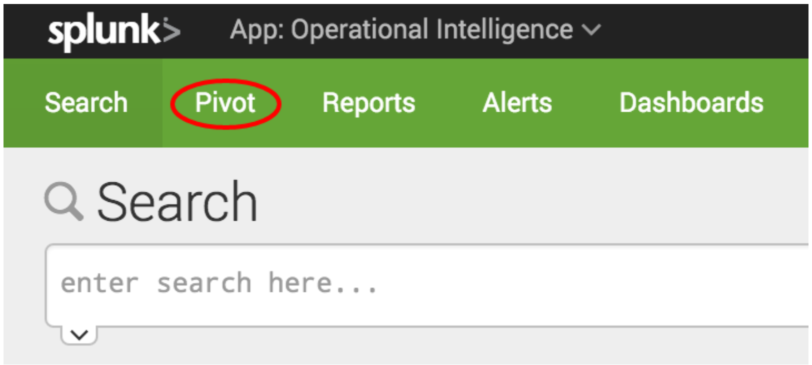
Can only contain letters, numbers and underscores.

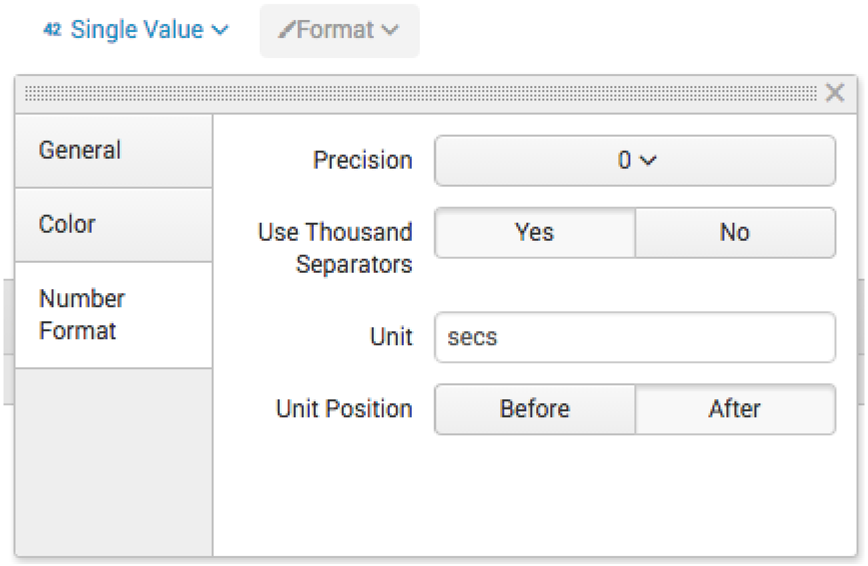
App: Operational Intelligence

Description: optional




Administrator
Messages
Settings
Activity
Help
Find
Add Data
Distributed Management Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Licensing
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
USERS AND AUTHENTICATION
Access controls


splunk>
App: Operational Intelligence
Search
Pivot
Reports
Alerts
Dashboards
Search
enter search here...

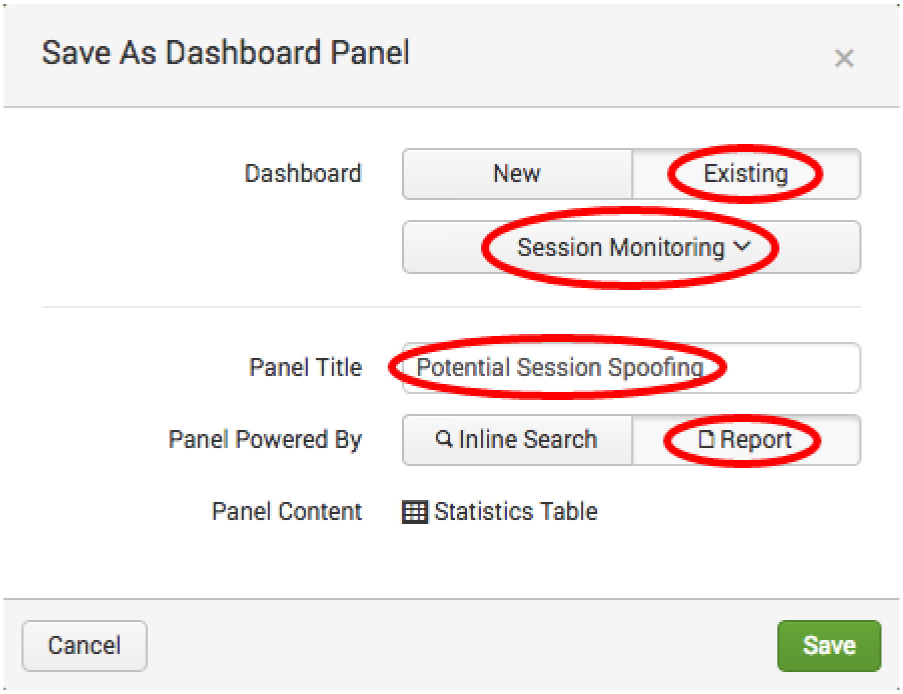


Precision: 0

Use Thousand Separators: Yes No

Unit: secs

Unit Position: Before After



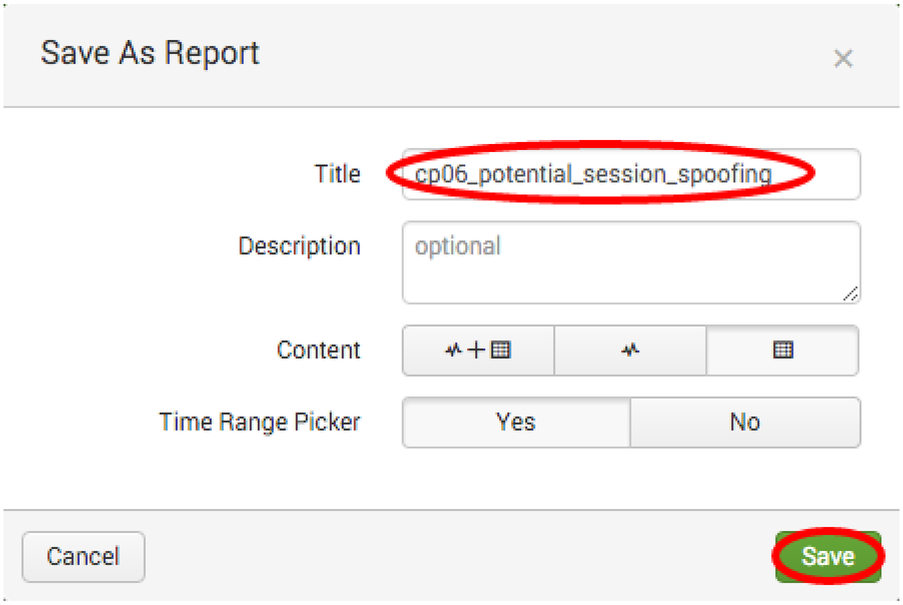
Dashboard: New [✓ Existing]

[✓ Session Monitoring]

Panel Title: [✓ Potential Session Spoofing]

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics Table



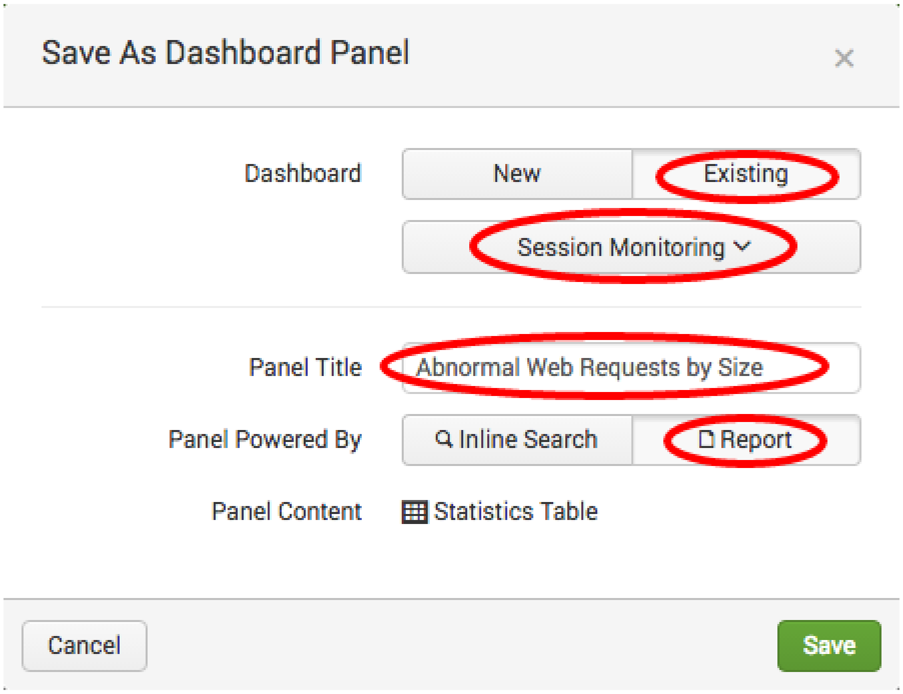
Save As Report

Title [✓ cp06_potential_session_spoofing]

Description optional

Content

Time Range Picker Yes No



Save As Dashboard Panel

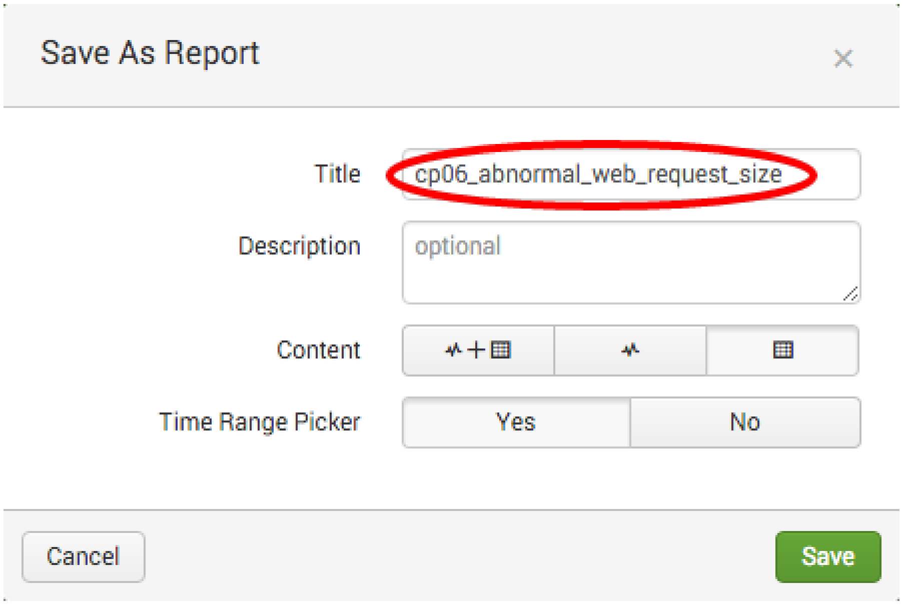
Dashboard New [✓ Existing]

[✓ Session Monitoring]

Panel Title [✓ Abnormal Web Requests by Size]

Panel Powered By Inline Search [✓ Report]

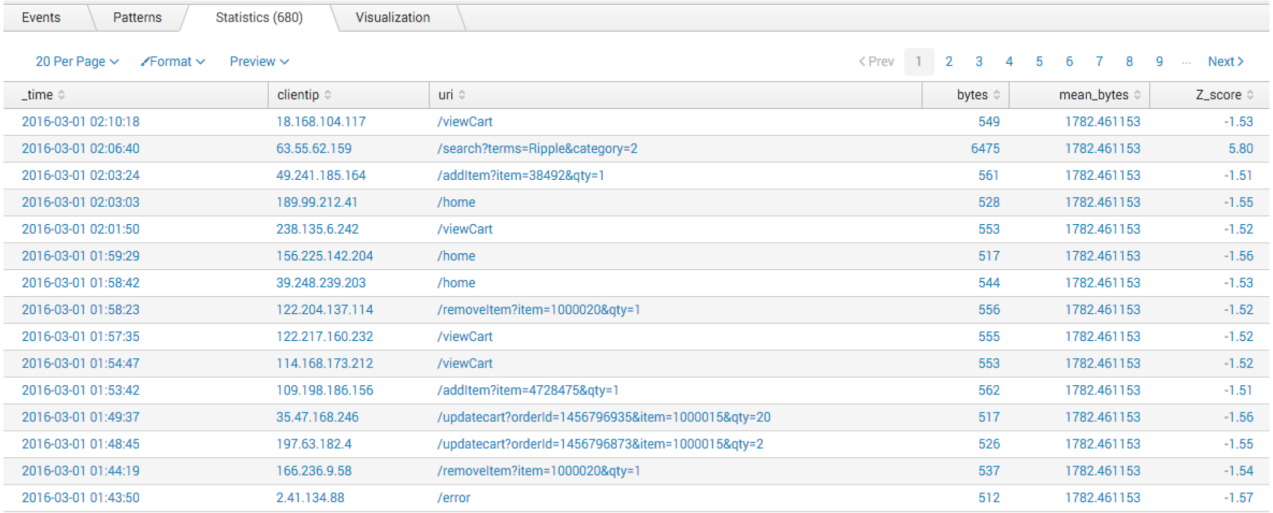
Panel Content Statistics Table



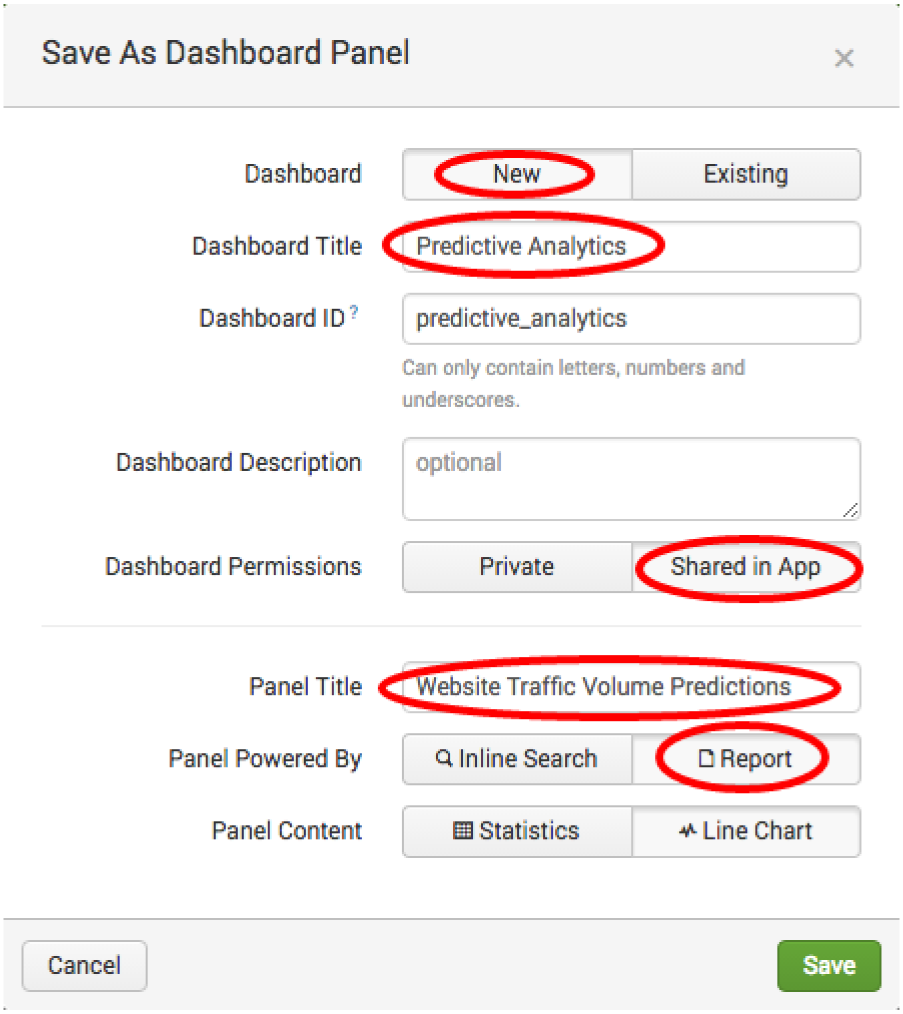
Save As Report

Title: cp06_abnormal_web_request_size

Description: optional



_time	clientip	uri	bytes	mean_bytes	Z_score
2016-03-01 02:10:18	18.168.104.117	/viewCart	549	1782.461153	-1.53
2016-03-01 02:06:40	63.55.62.159	/search?terms=Ripple&category=2	6475	1782.461153	5.80
2016-03-01 02:03:24	49.241.185.164	/addItem?item=38492&qty=1	561	1782.461153	-1.51
2016-03-01 02:03:03	189.99.212.41	/home	528	1782.461153	-1.55
2016-03-01 02:01:50	238.135.6.242	/viewCart	553	1782.461153	-1.52
2016-03-01 01:59:29	156.225.142.204	/home	517	1782.461153	-1.56
2016-03-01 01:58:42	39.248.239.203	/home	544	1782.461153	-1.53
2016-03-01 01:58:23	122.204.137.114	/removeItem?item=1000020&qty=1	556	1782.461153	-1.52
2016-03-01 01:57:35	122.217.160.232	/viewCart	555	1782.461153	-1.52
2016-03-01 01:54:47	114.168.173.212	/viewCart	553	1782.461153	-1.52
2016-03-01 01:53:42	109.198.186.156	/addItem?item=4728475&qty=1	562	1782.461153	-1.51
2016-03-01 01:49:37	35.47.168.246	/updatecart?orderId=1456796935&item=1000015&qty=20	517	1782.461153	-1.56
2016-03-01 01:48:45	197.63.182.4	/updatecart?orderId=1456796873&item=1000015&qty=2	526	1782.461153	-1.55
2016-03-01 01:44:19	166.236.9.58	/removeItem?item=1000020&qty=1	537	1782.461153	-1.54
2016-03-01 01:43:50	2.41.134.88	/error	512	1782.461153	-1.57



Save As Dashboard Panel ×

Dashboard: [✓ New] Existing

Dashboard Title: Predictive Analytics

Dashboard ID ?: predictive_analytics

Can only contain letters, numbers and underscores.

Dashboard Description: optional

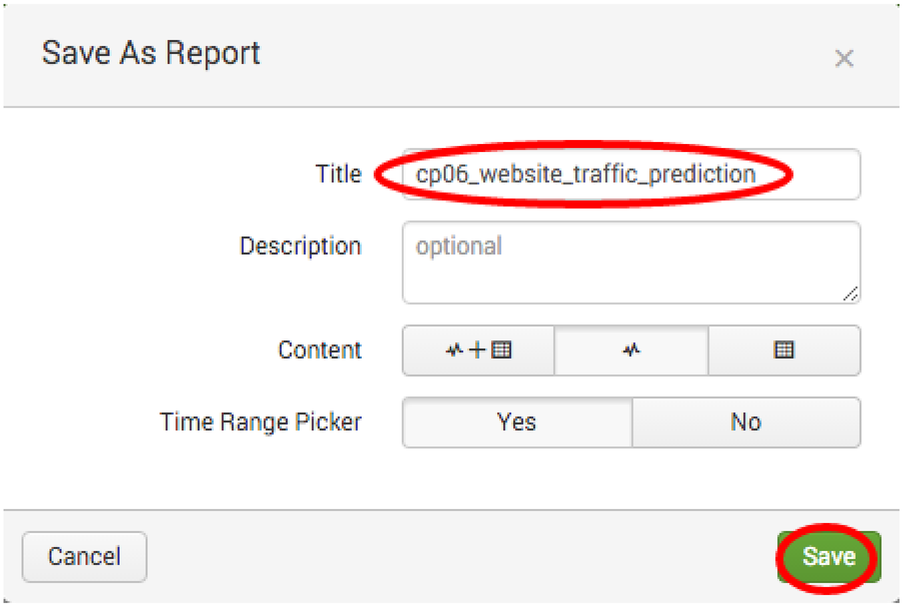
Dashboard Permissions: Private [✓ Shared in App]

Panel Title: Website Traffic Volume Predictions

Panel Powered By: 🔍 Inline Search [✓ 🗋 Report]

Panel Content: ▦ Statistics ∿ Line Chart

Cancel Save



Save As Report ×

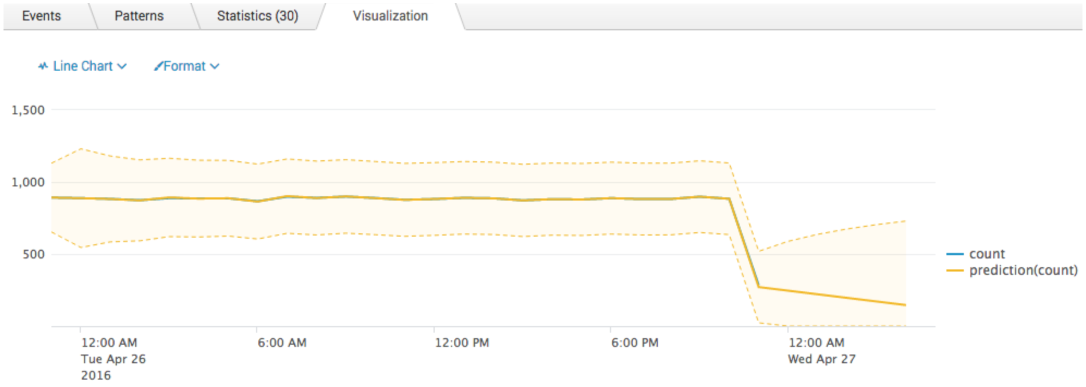
Title: cp06_website_traffic_prediction

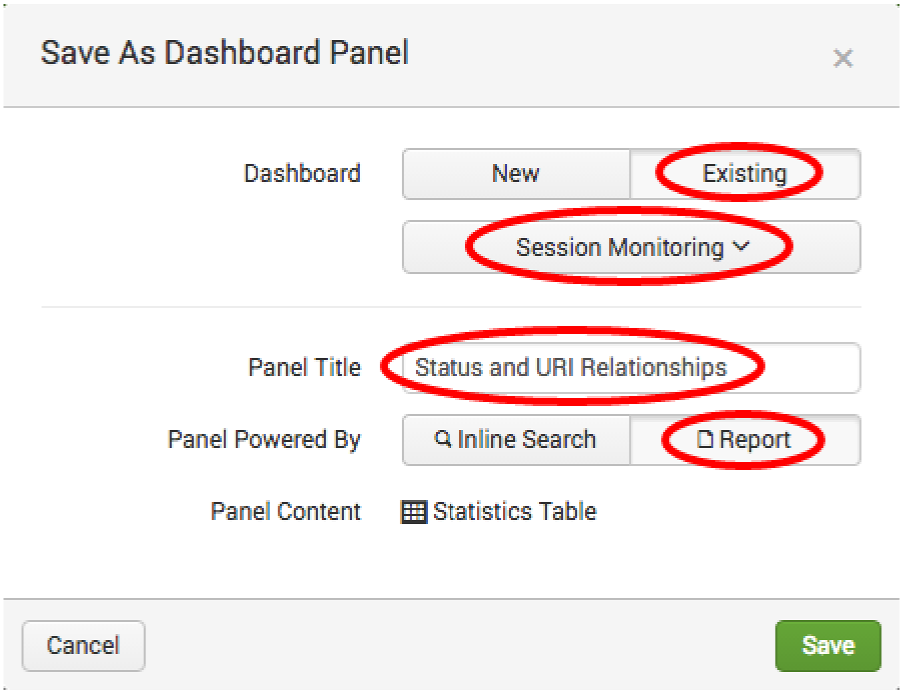
Description: optional

Content: ∿ + ▦ ∿ ▦

Time Range Picker: Yes No

Cancel [✓ Save]





Save As Dashboard Panel

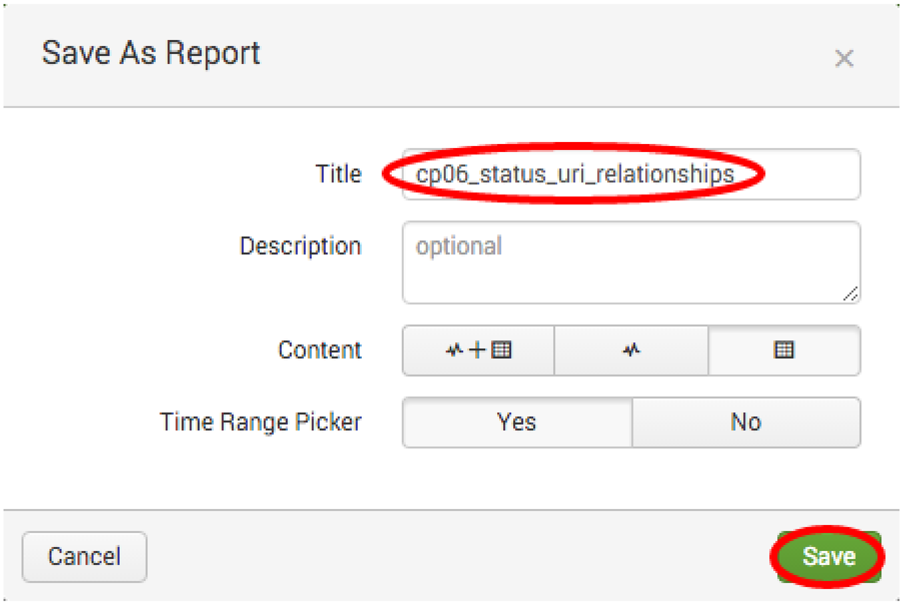
Dashboard: New [✓ Existing]

[✓ Session Monitoring]

Panel Title: [✓ Status and URI Relationships]

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics Table

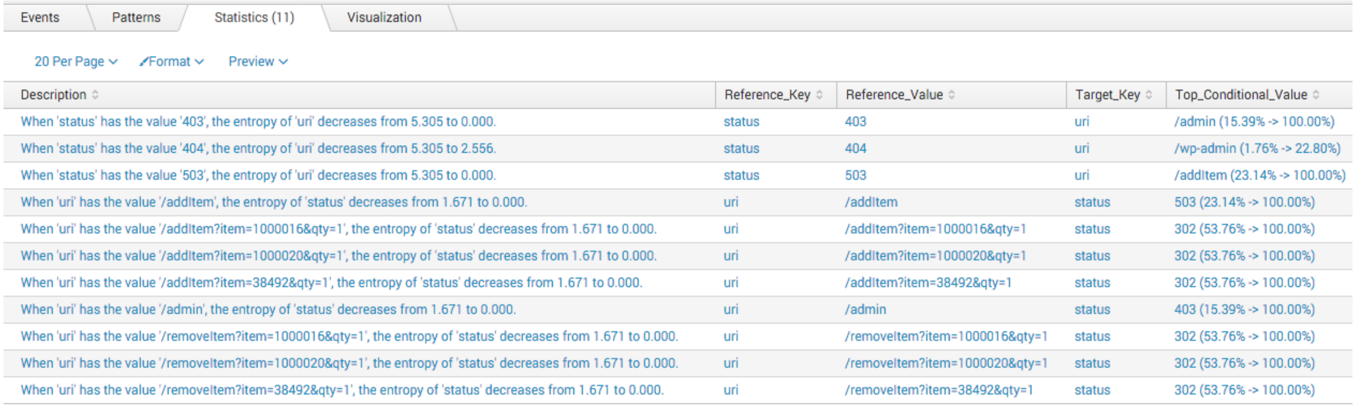


Title: cp06_status_uri_relationships

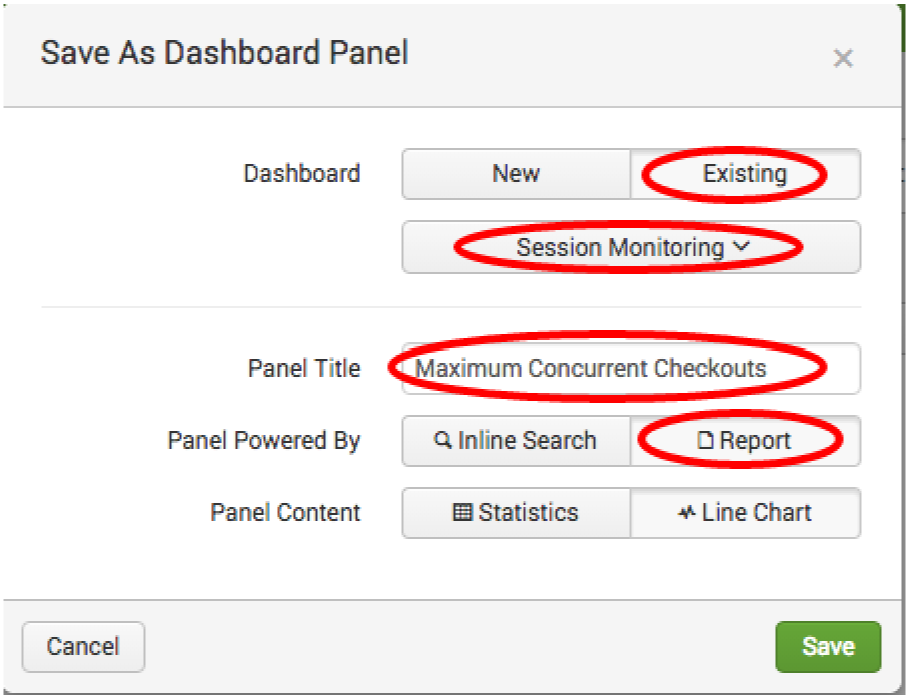
Description: optional

Content

Time Range Picker: Yes | No



Description	Reference_Key	Reference_Value	Target_Key	Top_Conditional_Value
When 'status' has the value '403', the entropy of 'uri' decreases from 5.305 to 0.000.	status	403	uri	/admin (15.39% -> 100.00%)
When 'status' has the value '404', the entropy of 'uri' decreases from 5.305 to 2.556.	status	404	uri	/wp-admin (1.76% -> 22.80%)
When 'status' has the value '503', the entropy of 'uri' decreases from 5.305 to 0.000.	status	503	uri	/addItem (23.14% -> 100.00%)
When 'uri' has the value '/addItem', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/addItem	status	503 (23.14% -> 100.00%)
When 'uri' has the value '/addItem?item=1000016&qty=1', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/addItem?item=1000016&qty=1	status	302 (53.76% -> 100.00%)
When 'uri' has the value '/addItem?item=1000020&qty=1', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/addItem?item=1000020&qty=1	status	302 (53.76% -> 100.00%)
When 'uri' has the value '/addItem?item=38492&qty=1', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/addItem?item=38492&qty=1	status	302 (53.76% -> 100.00%)
When 'uri' has the value '/admin', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/admin	status	403 (15.39% -> 100.00%)
When 'uri' has the value '/removeItem?item=1000016&qty=1', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/removeItem?item=1000016&qty=1	status	302 (53.76% -> 100.00%)
When 'uri' has the value '/removeItem?item=1000020&qty=1', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/removeItem?item=1000020&qty=1	status	302 (53.76% -> 100.00%)
When 'uri' has the value '/removeItem?item=38492&qty=1', the entropy of 'status' decreases from 1.671 to 0.000.	uri	/removeItem?item=38492&qty=1	status	302 (53.76% -> 100.00%)



Save As Dashboard Panel

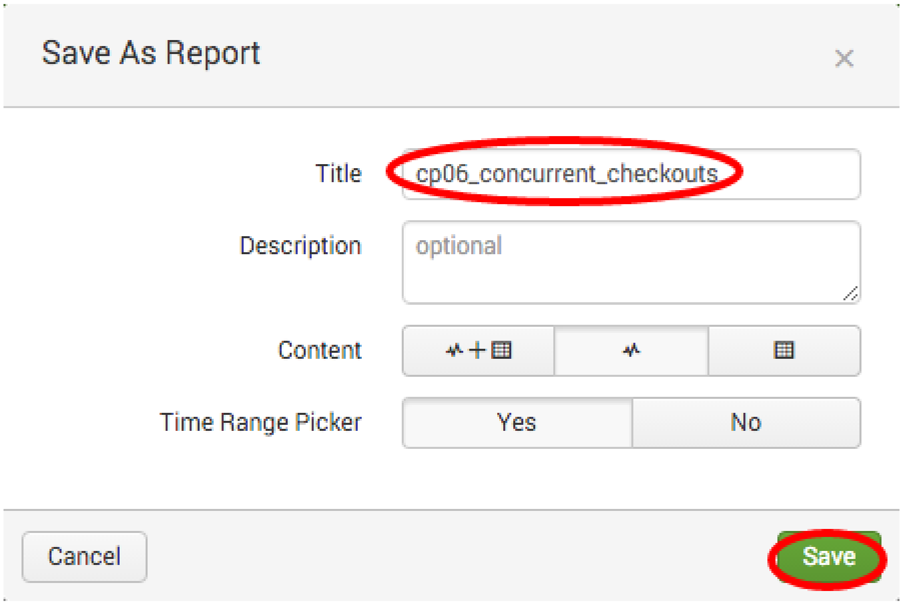
Dashboard: New [✓ Existing]

[✓ Session Monitoring]

Panel Title: [✓ Maximum Concurrent Checkouts]

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics Line Chart



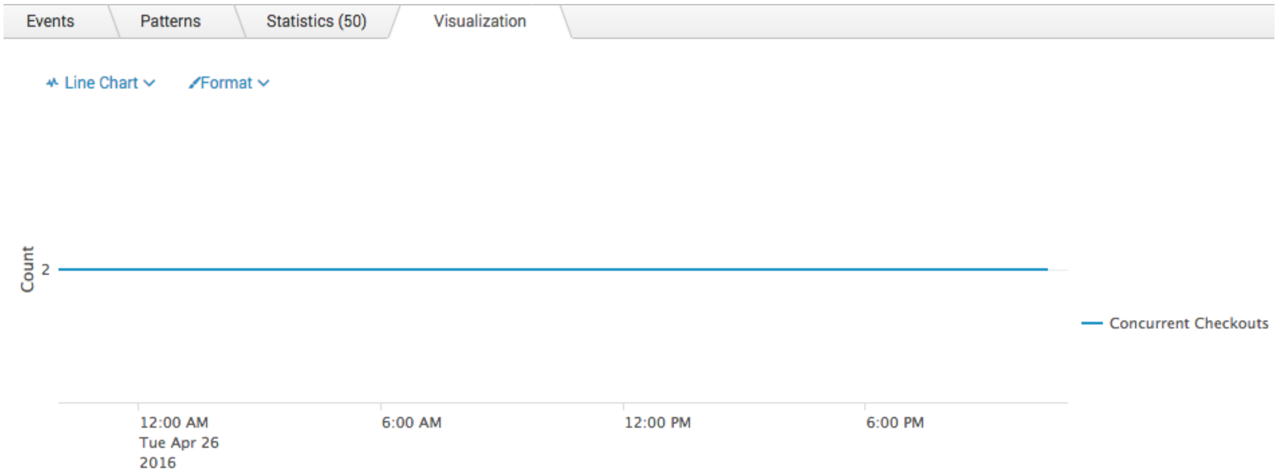
Save As Report

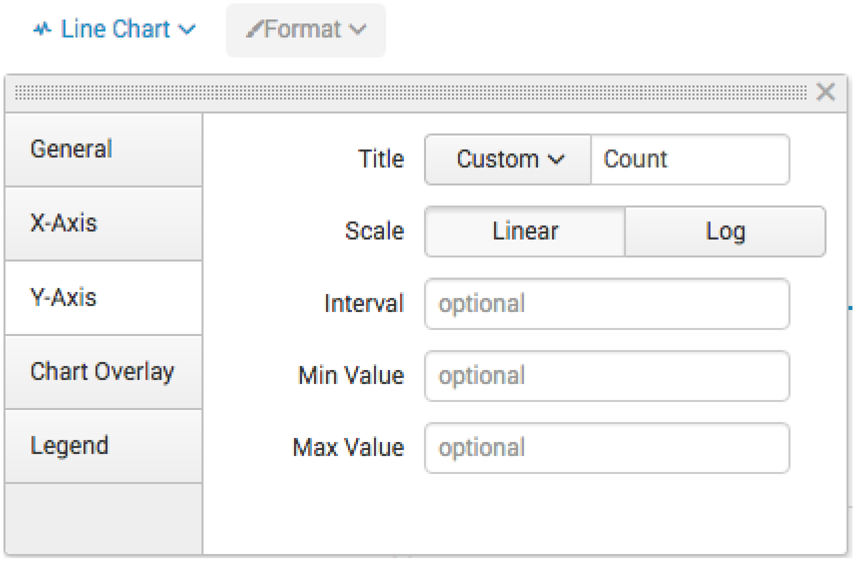
Title: [✓ cp06_concurrent_checkouts]

Description: optional

Time Range Picker: Yes No

[✓ Save]





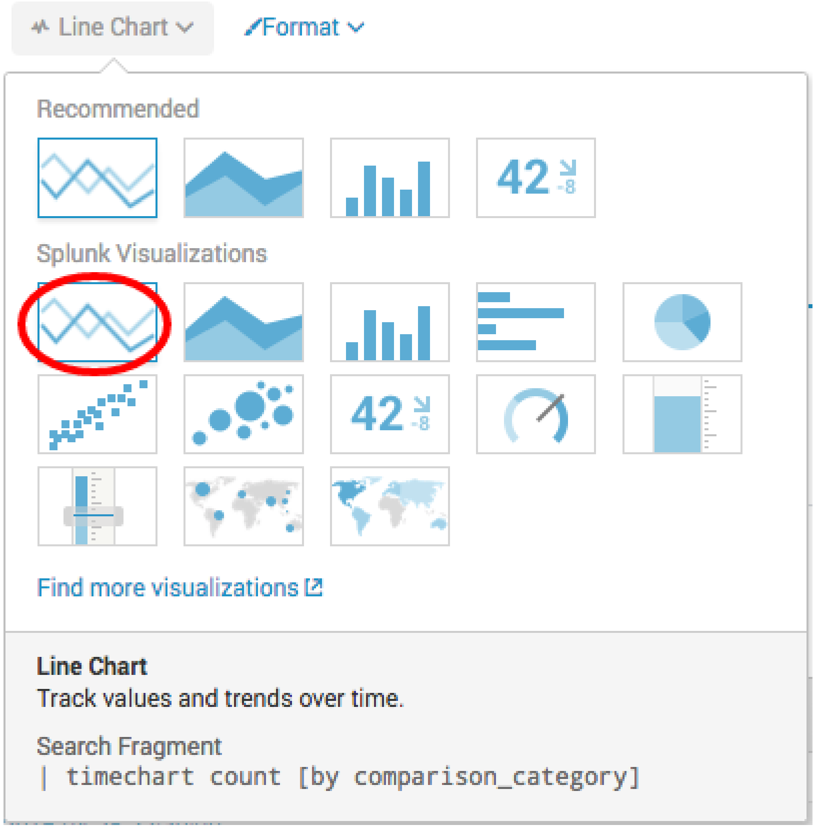
Title Custom Count

Scale Linear Log

Interval optional

Min Value optional

Max Value optional

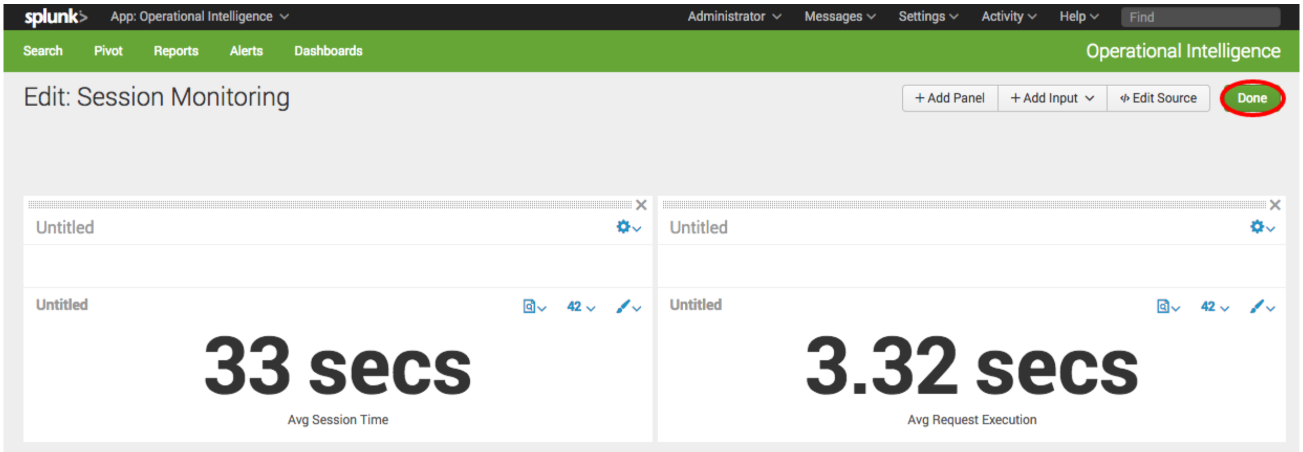


Line Chart

Track values and trends over time.

Search Fragment

```
| timechart count [by comparison_category]
```



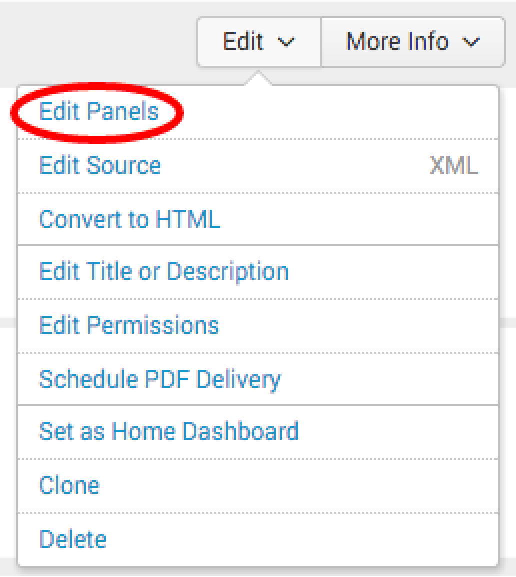
Edit: Session Monitoring

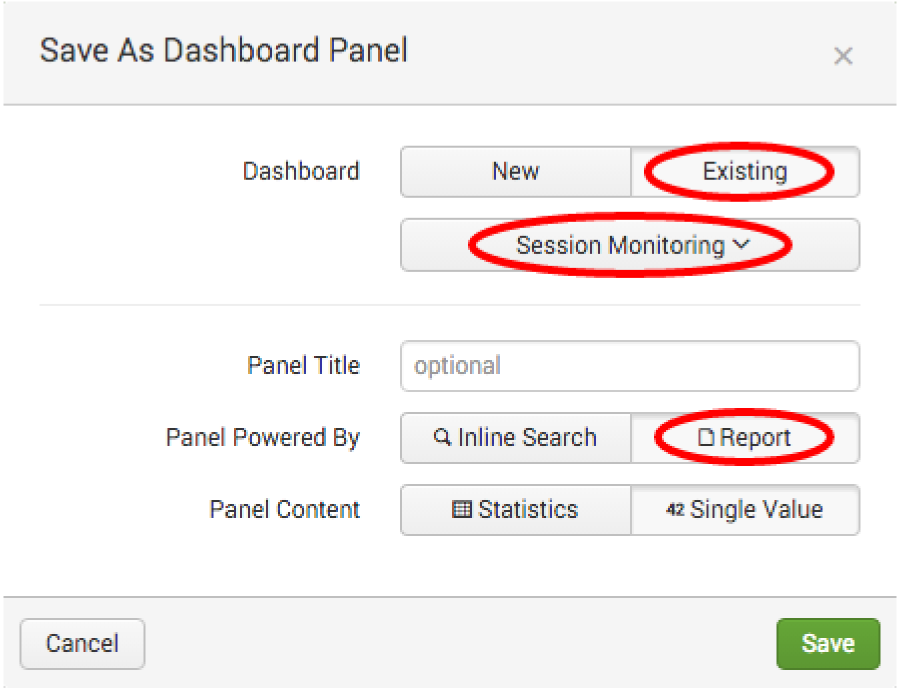
33 secs

Avg Session Time

3.32 secs

Avg Request Execution





Save As Dashboard Panel

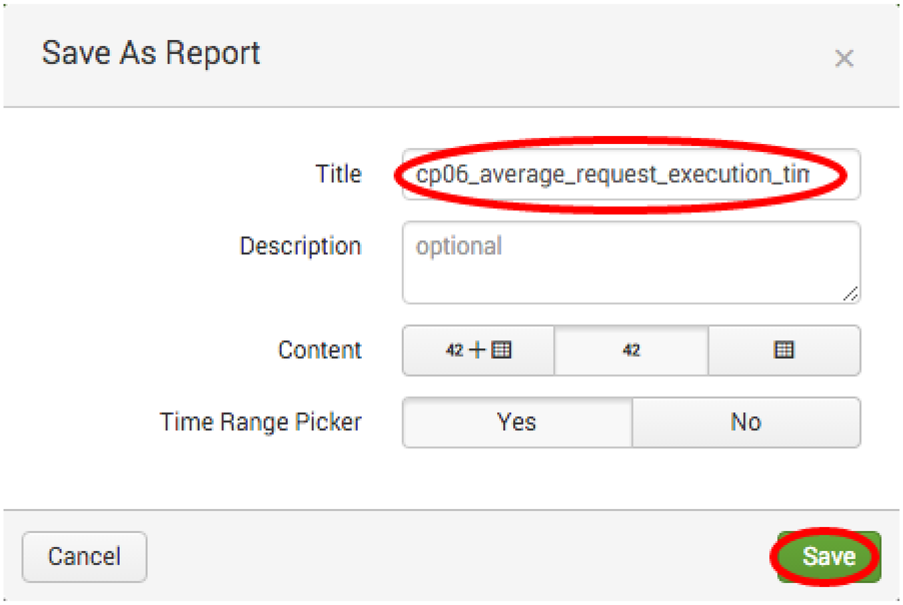
Dashboard: New [✓ Existing]

[✓ Session Monitoring]

Panel Title: optional

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics | 42 Single Value



Save As Report ×

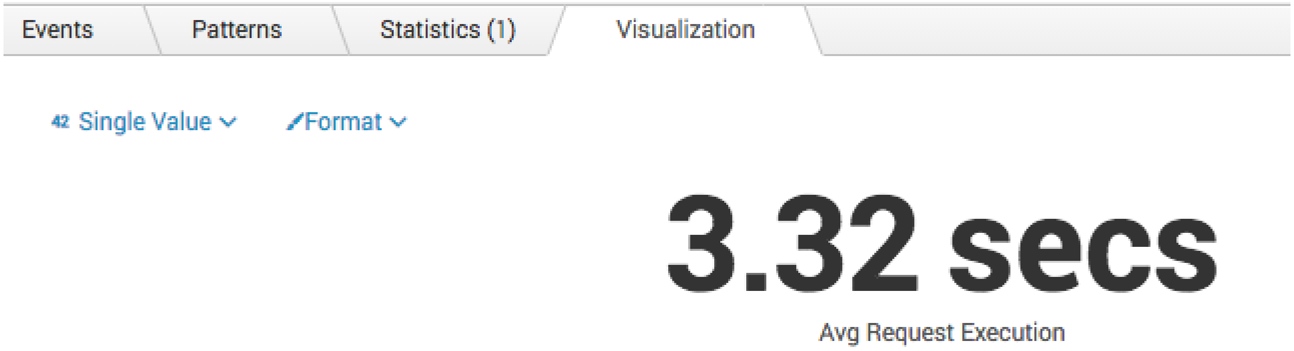
Title: cp06_average_request_execution_tin

Description: optional

Content: 42 + ▦ | 42 | ▦

Time Range Picker: Yes | No

Cancel | Save

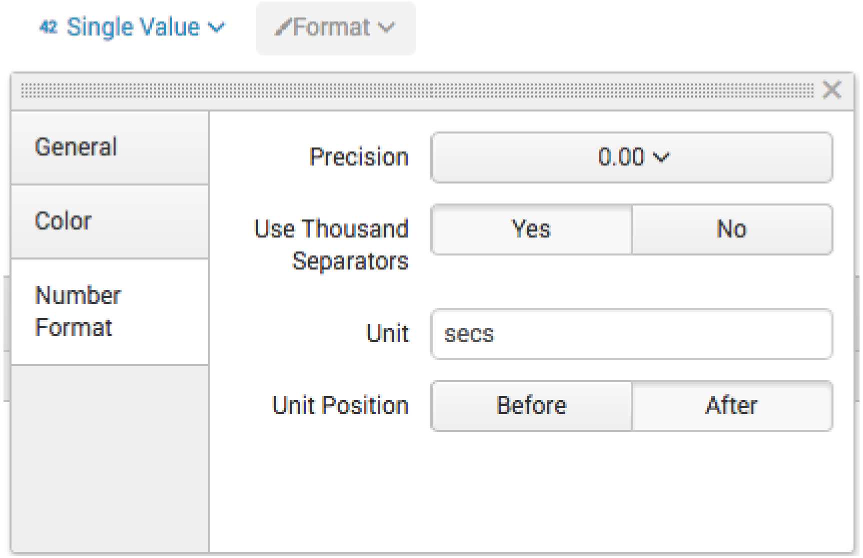


Events | Patterns | Statistics (1) | Visualization

42 Single Value ⌄ | Format ⌄

3.32 secs

Avg Request Execution



42 Single Value ⌄ | Format ⌄

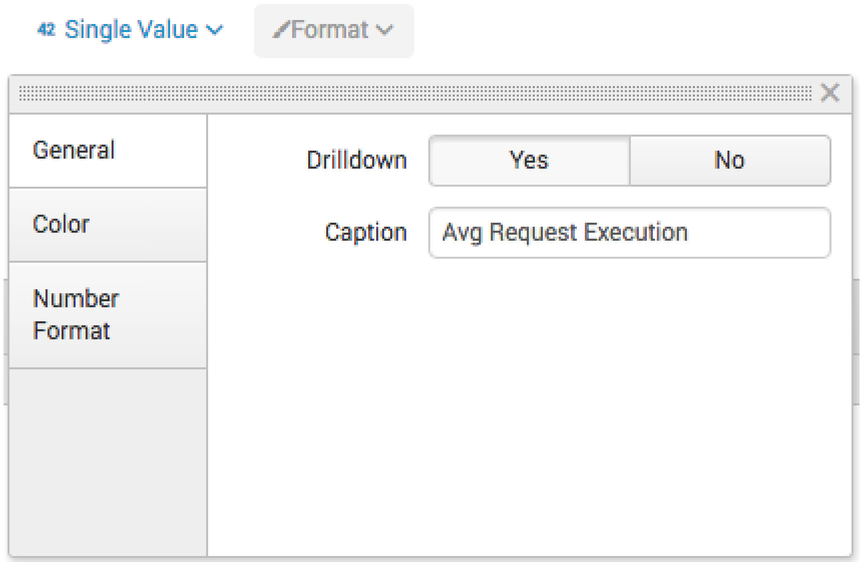
General | Color | Number Format

Precision: 0.00 ⌄

Use Thousand Separators: Yes | No

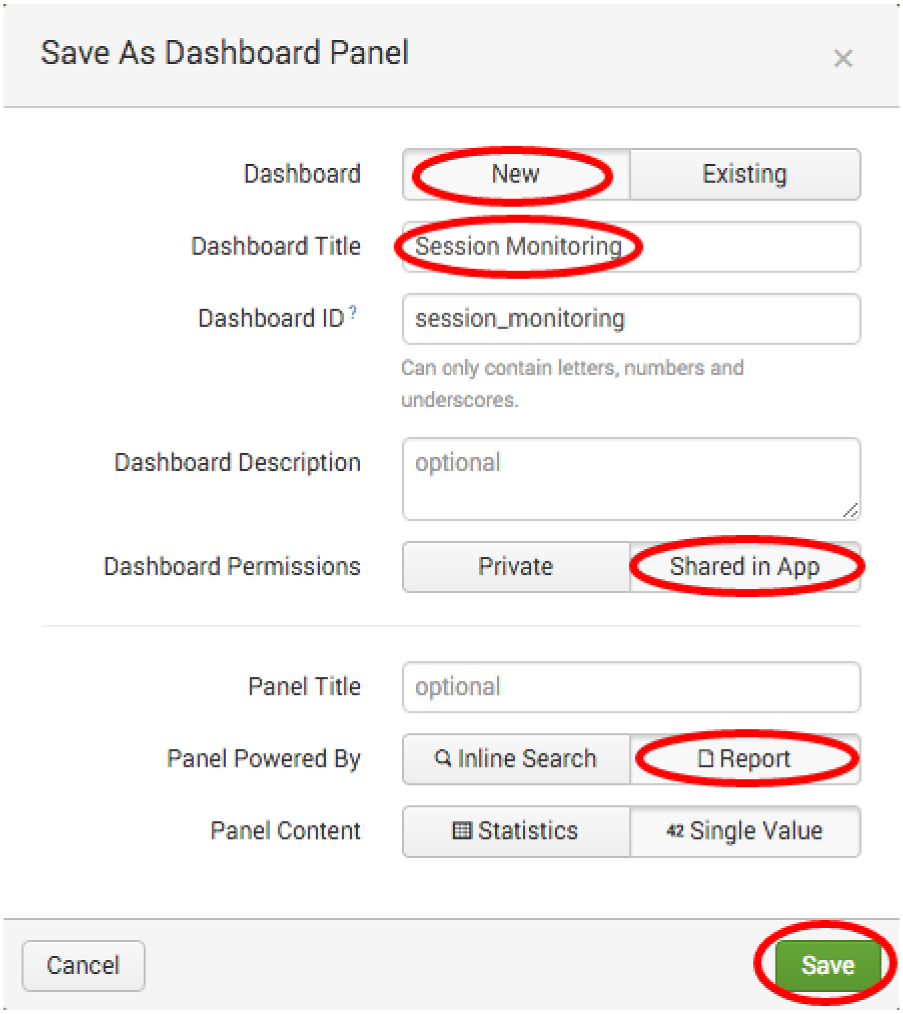
Unit: secs

Unit Position: Before | After



Drilldown: Yes No

Caption: Avg Request Execution



Save As Dashboard Panel

Dashboard: [✓ New] Existing

Dashboard Title: Session Monitoring

Dashboard ID: session_monitoring

Can only contain letters, numbers and underscores.

Dashboard Description: optional

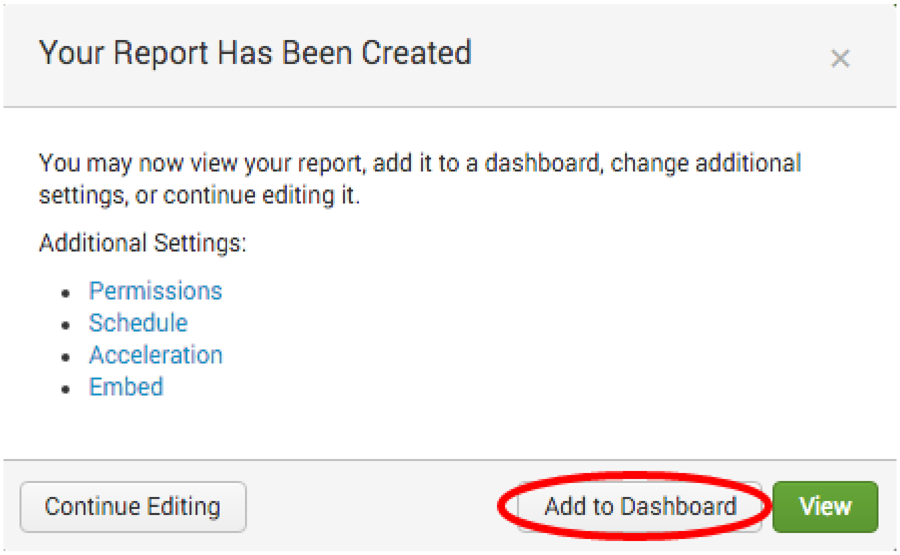
Dashboard Permissions: Private [✓ Shared in App]

Panel Title: optional

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics 42 Single Value

Cancel [✓ Save]

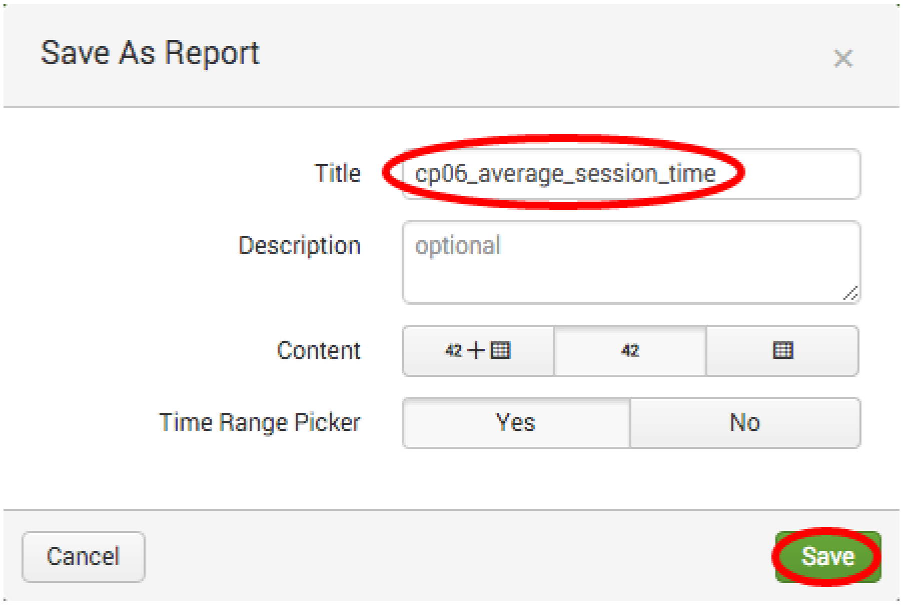


Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed



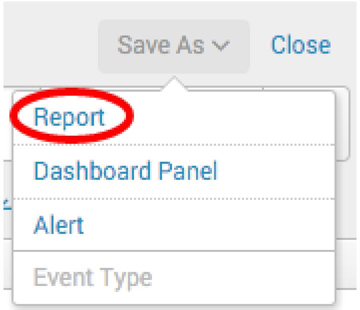
Save As Report

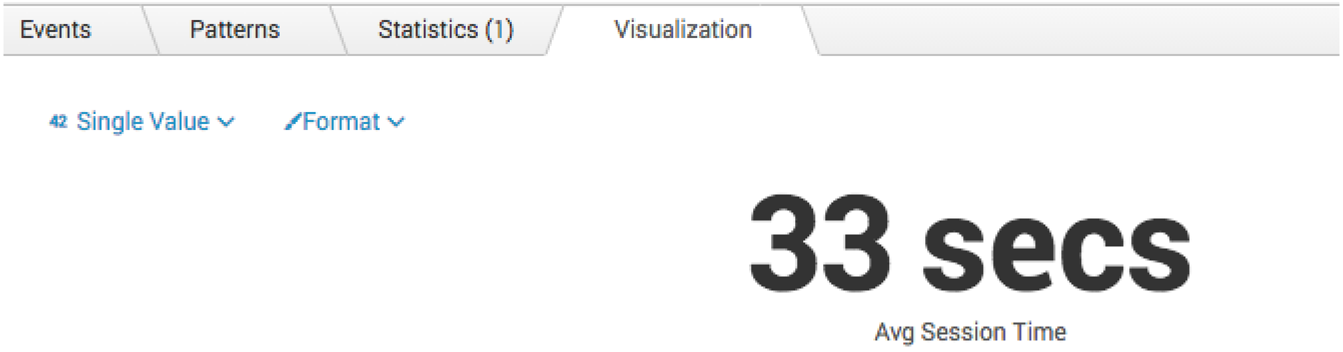
Title: cp06_average_session_time

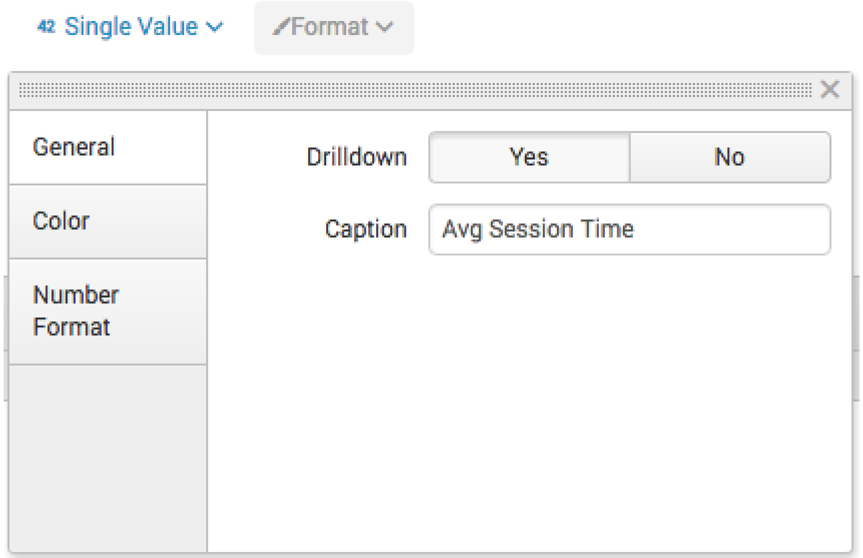
Description: optional

Content: 42 + ▦ | 42 | ▦

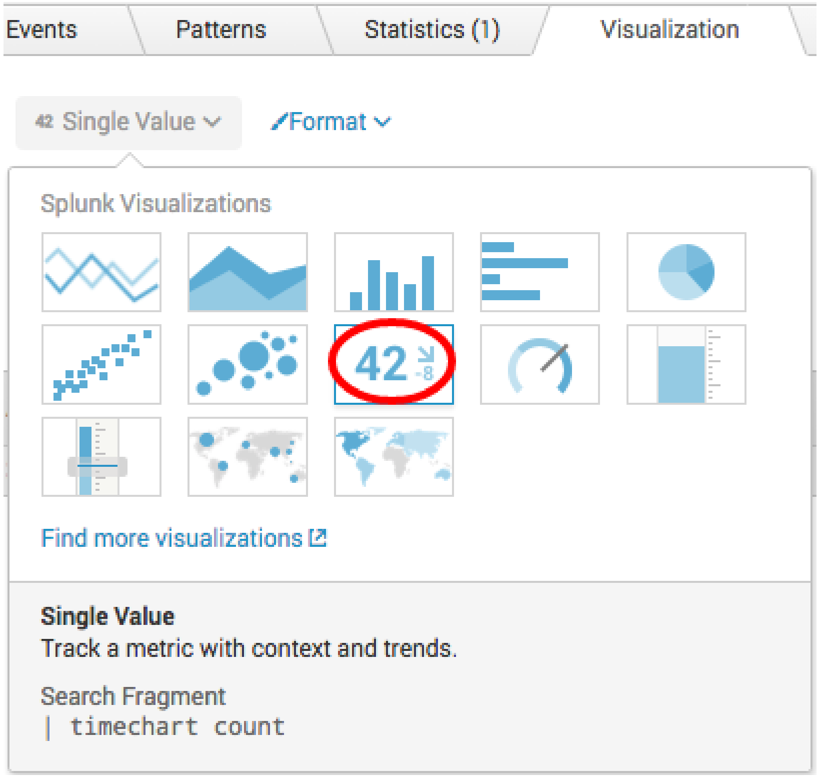
Time Range Picker: Yes | No







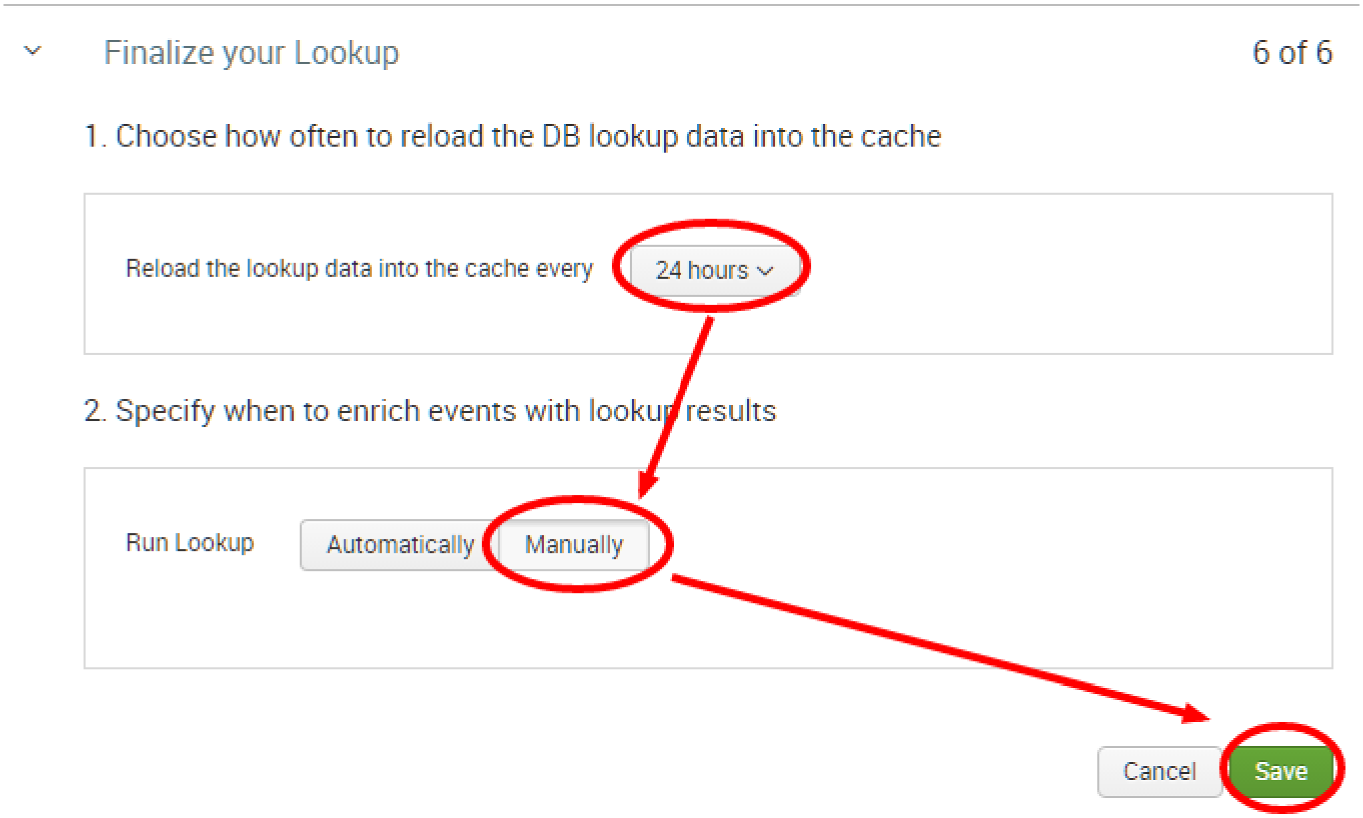
Caption: Avg Session Time



Single Value
Track a metric with context and trends.

Search Fragment

```
| timechart count
```



Finalize your Lookup

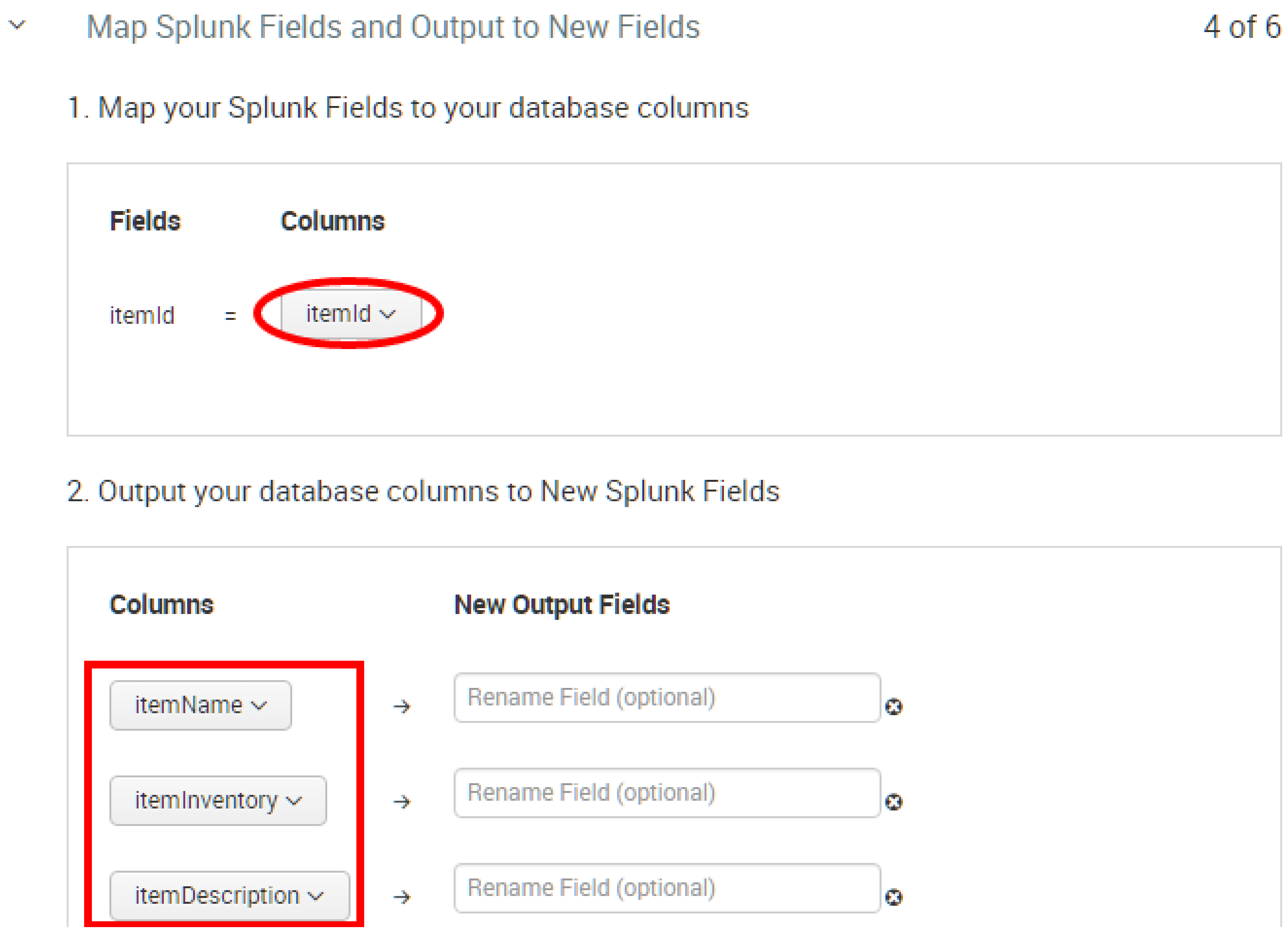
6 of 6

1. Choose how often to reload the DB lookup data into the cache

Reload the lookup data into the cache every [✓ 24 hours]

2. Specify when to enrich events with lookup results

Run Lookup: Automatically [✓ Manually]



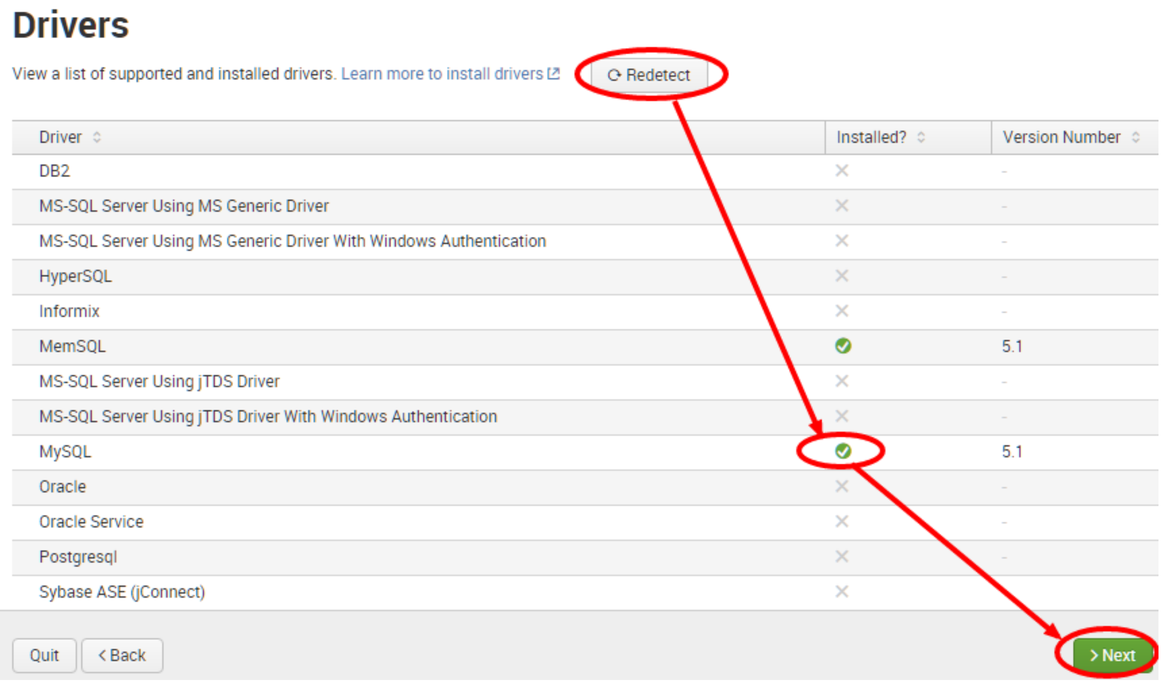
Map Splunk Fields and Output to New Fields — 4 of 6

1. Map your Splunk Fields to your database columns

Fields		Columns
itemId	=	itemId

2. Output your database columns to New Splunk Fields

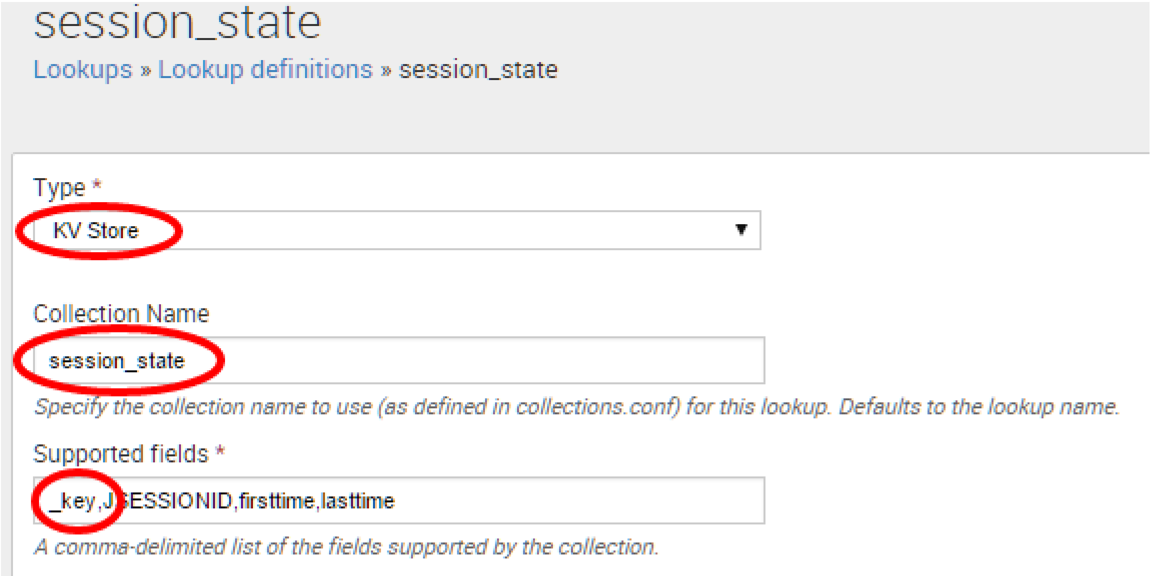
Columns		New Output Fields
itemName	→	Rename Field (optional)
itemInventory	→	Rename Field (optional)
itemDescription	→	Rename Field (optional)



Drivers

View a list of supported and installed drivers. Learn more to install drivers

Driver	Installed?	Version Number
DB2	✗	-
MS-SQL Server Using MS Generic Driver	✗	-
MS-SQL Server Using MS Generic Driver With Windows Authentication	✗	-
HyperSQL	✗	-
Informix	✗	-
MemSQL	✓	5.1
MS-SQL Server Using jTDS Driver	✗	-
MS-SQL Server Using jTDS Driver With Windows Authentication	✗	-
MySQL	✓	5.1
Oracle	✗	-
Oracle Service	✗	-
Postgresql	✗	-
Sybase ASE (jConnect)	✗	



session_state

Lookups » Lookup definitions » session_state

Type *

KV Store ▾

Collection Name

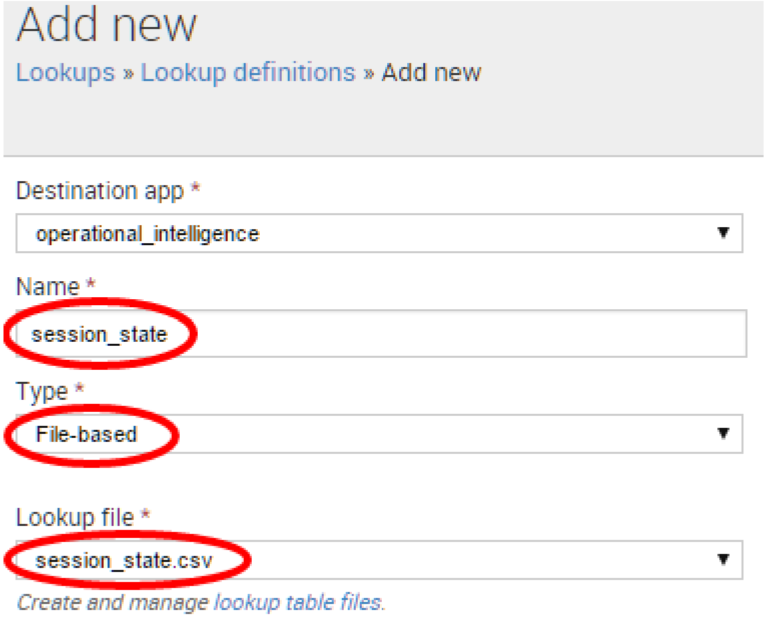
session_state

Specify the collection name to use (as defined in collections.conf) for this lookup. Defaults to the lookup name.

Supported fields *

_key,JSESSIONID,firsttime,lasttime

A comma-delimited list of the fields supported by the collection.



Add new

Lookups » Lookup definitions » Add new

Destination app *

operational_intelligence ▾

Name *

session_state

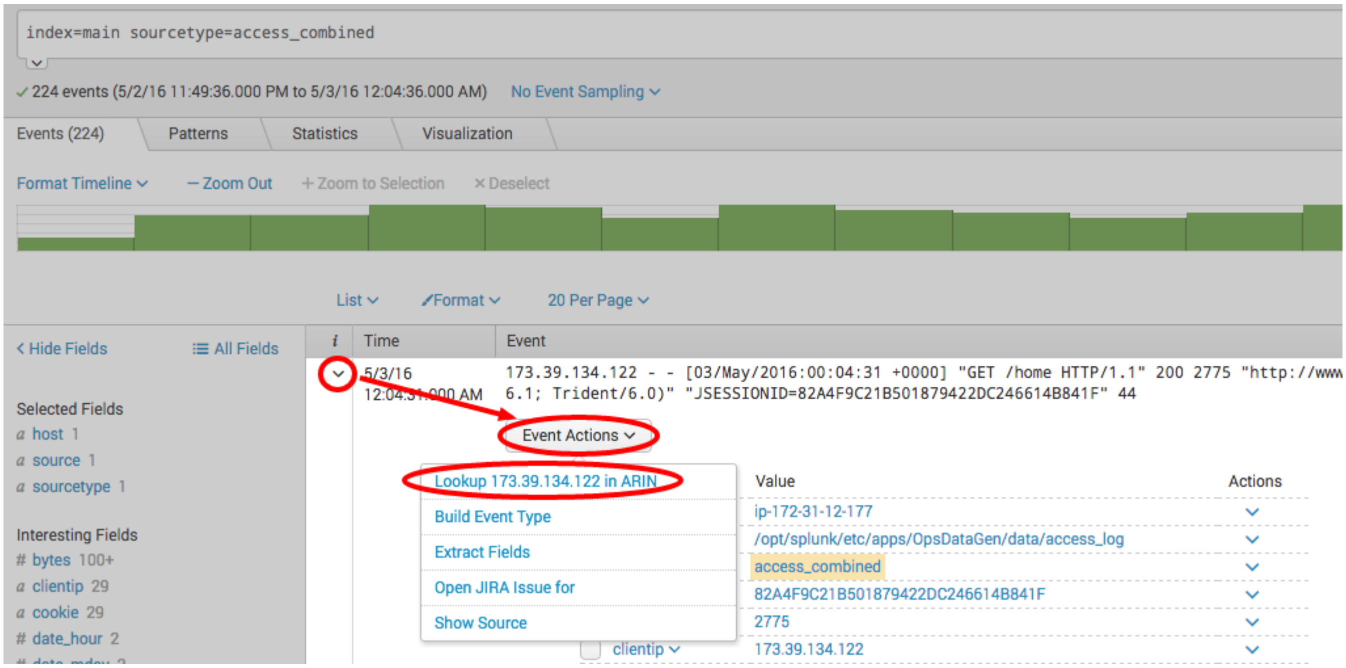
Type *

File-based ▾

Lookup file *

session_state.csv ▾

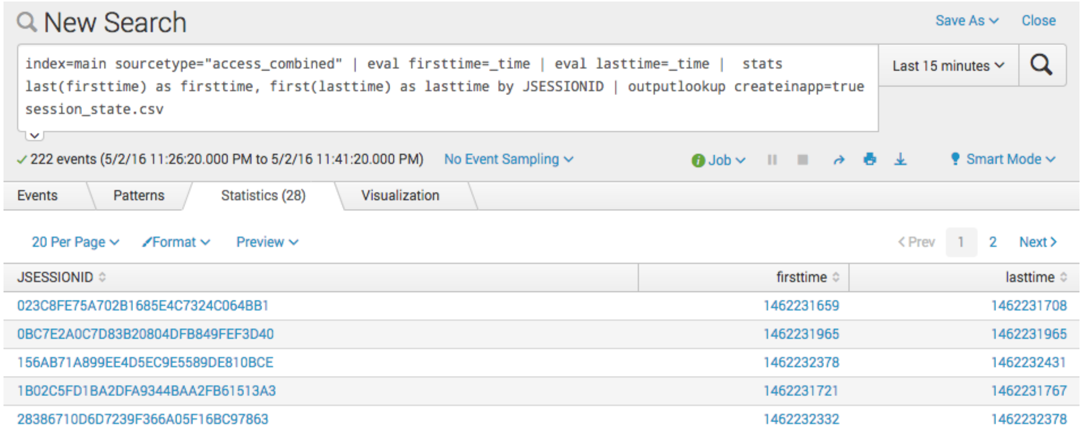
Create and manage lookup table files.



```
index=main sourcetype=access_combined
```

✓ 224 events (5/2/16 11:49:36.000 PM to 5/3/16 12:04:36.000 AM)

```
5/3/16
12:04:31.000 AM   173.39.134.122 - - [03/May/2016:00:04:31 +0000] "GET /home HTTP/1.1" 200 2775 "http://www
                  6.1; Trident/6.0)" "JSESSIONID=82A4F9C21B501879422DC246614B841F" 44
```

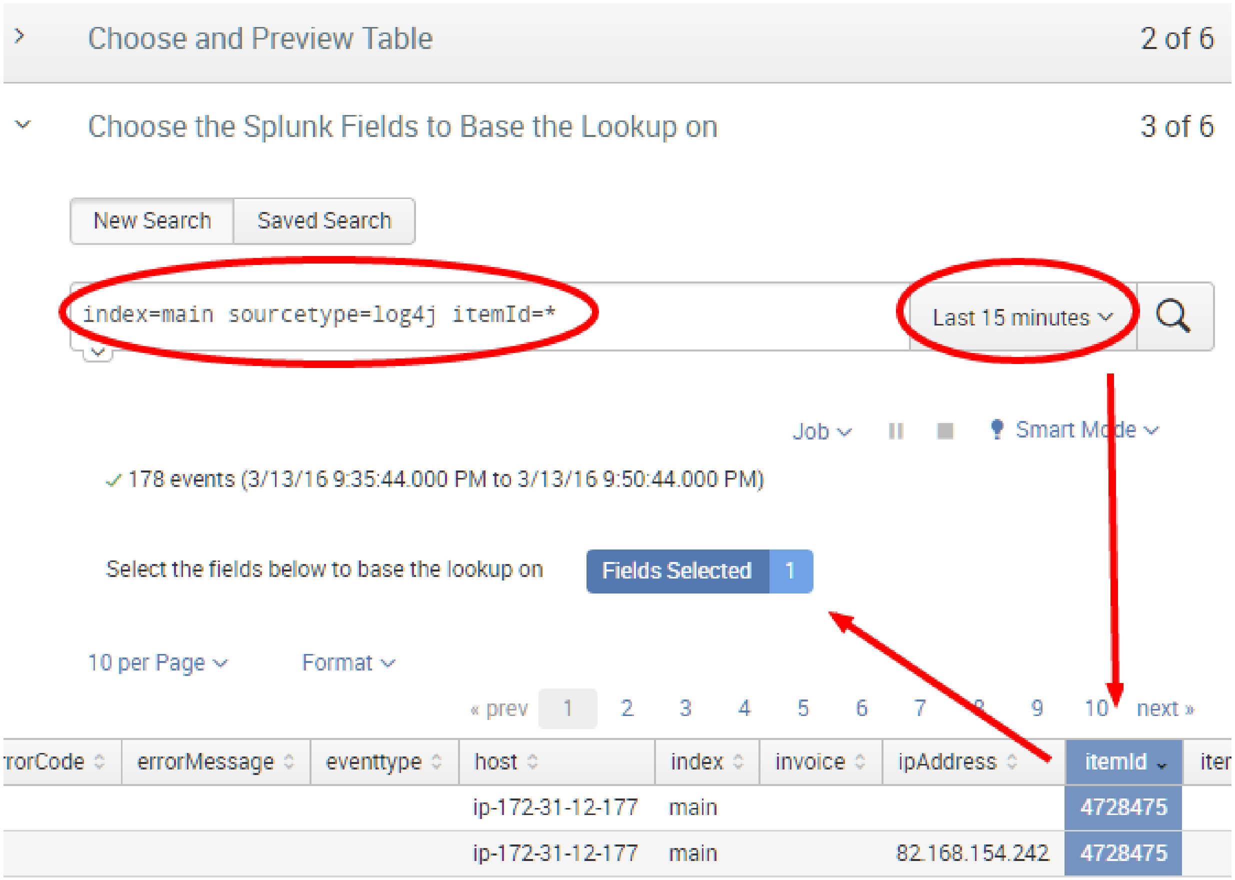


New Search

```
index=main sourcetype="access_combined" | eval firsttime=_time | eval lasttime=_time |  stats
last(firsttime) as firsttime, first(lasttime) as lasttime by JSESSIONID | outputlookup createinapp=true
session_state.csv
```

✓ 222 events (5/2/16 11:26:20.000 PM to 5/2/16 11:41:20.000 PM)

JSESSIONID	firsttime	lasttime
023C8FE75A702B1685E4C7324C064BB1	1462231659	1462231708
0BC7E2A0C7D83B20804DFB849FEF3D40	1462231965	1462231965
156AB71A899EE4D5EC9E5589DE810BCE	1462232378	1462232431
1B02C5FD1BA2DFA9344BAA2FB61513A3	1462231721	1462231767
28386710D6D7239F366A05F16BC97863	1462232332	1462232378



Choose and Preview Table 2 of 6

Choose the Splunk Fields to Base the Lookup on 3 of 6

```
index=main sourcetype=log4j itemId=*
```

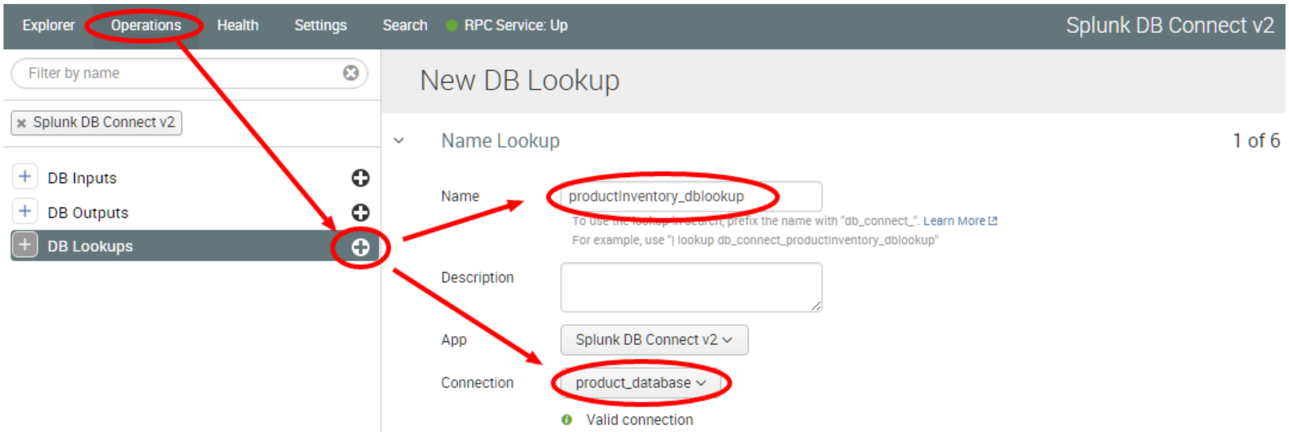
Last 15 minutes

✓ 178 events (3/13/16 9:35:44.000 PM to 3/13/16 9:50:44.000 PM)

Select the fields below to base the lookup on

Fields Selected 1

rorCode	errorMessage	eventtype	host	index	invoice	ipAddress	itemId	iter
			ip-172-31-12-177	main			4728475	
			ip-172-31-12-177	main		82.168.154.242	4728475	



New DB Lookup

Name Lookup 1 of 6

Name: productInventory_dblookup

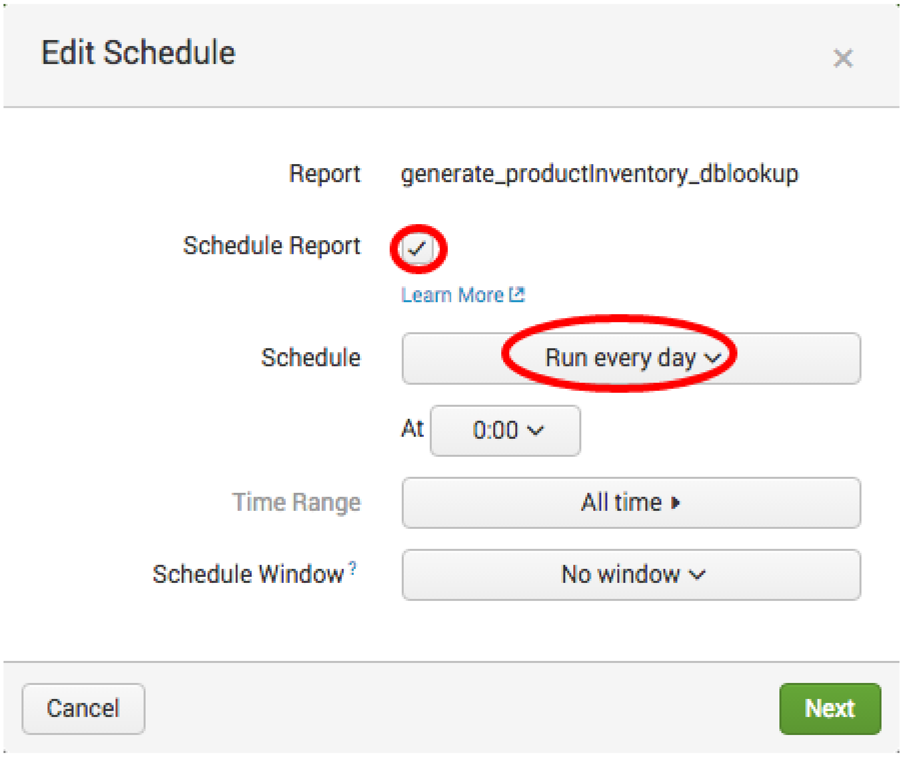
To use the lookup in search, prefix the name with "db_connect_". Learn More
For example, use "| lookup db_connect_productInventory_dblookup"

Description:

App: Splunk DB Connect v2

Connection: product_database

Valid connection



Edit Schedule

Report generate_productInventory_dblookup

Schedule Report ☑

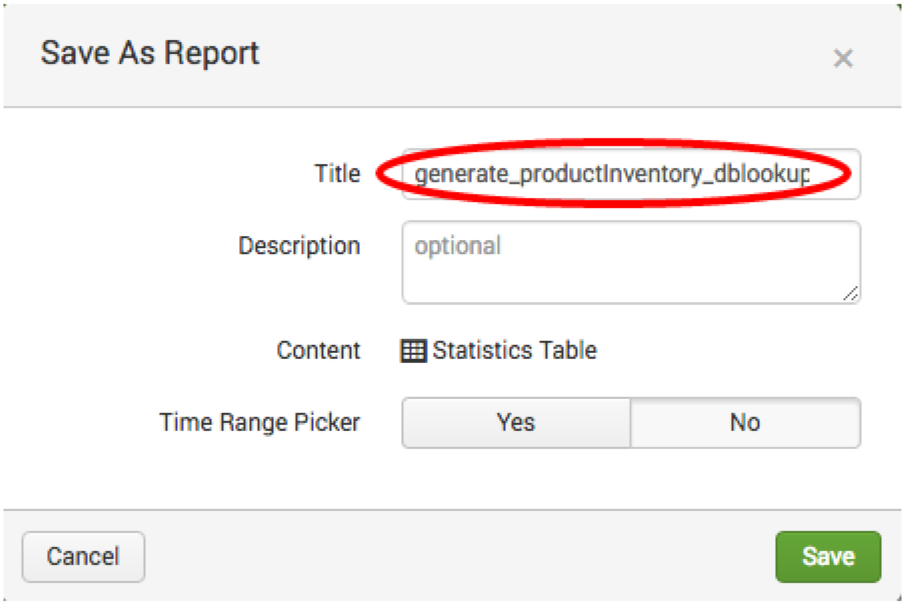
Learn More

Schedule Run every day

At 0:00

Time Range All time

Schedule Window No window



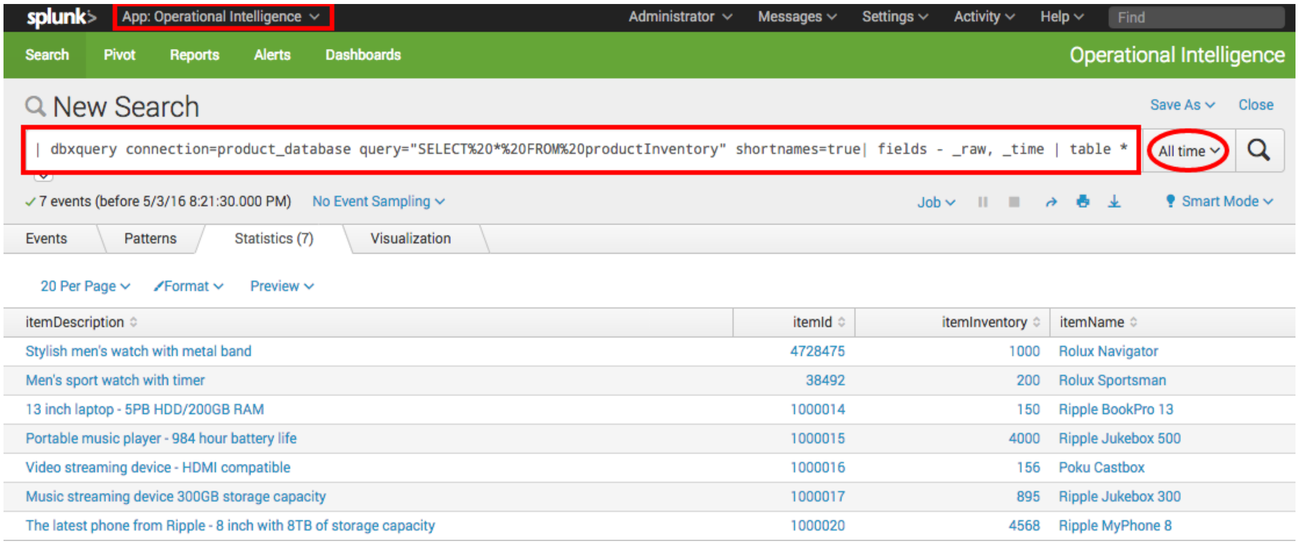
Save As Report

Title generate_productInventory_dblookup

Description optional

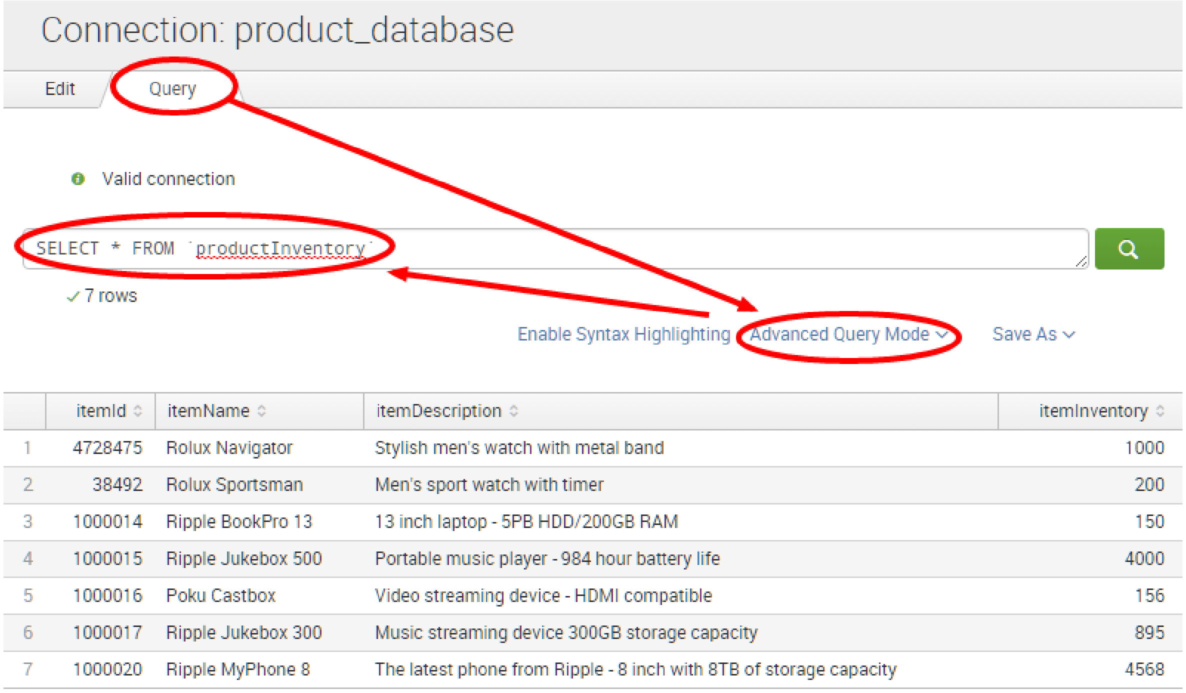
Content Statistics Table

Time Range Picker Yes No



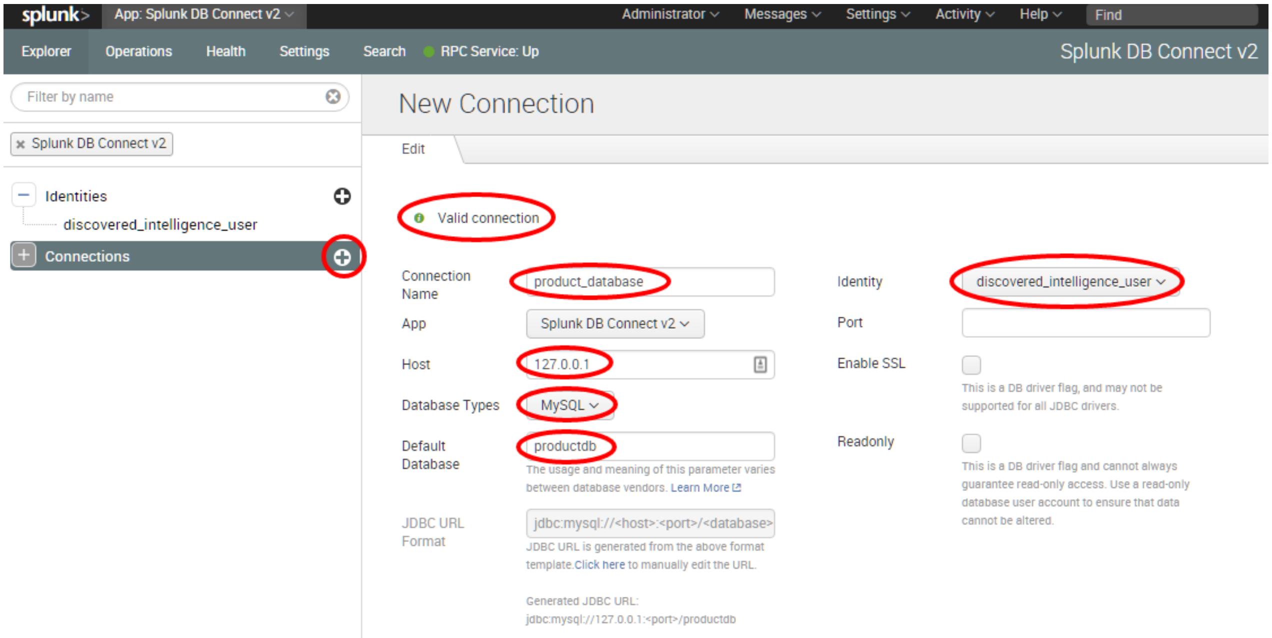
```
| dbxquery connection=product_database query="SELECT%20*%20FROM%20productInventory" shortnames=true| fields - _raw, _time | table *
```

itemDescription	itemId	itemInventory	itemName
Stylish men's watch with metal band	4728475	1000	Rolux Navigator
Men's sport watch with timer	38492	200	Rolux Sportsman
13 inch laptop - 5PB HDD/200GB RAM	1000014	150	Ripple BookPro 13
Portable music player - 984 hour battery life	1000015	4000	Ripple Jukebox 500
Video streaming device - HDMI compatible	1000016	156	Poku Castbox
Music streaming device 300GB storage capacity	1000017	895	Ripple Jukebox 300
The latest phone from Ripple - 8 inch with 8TB of storage capacity	1000020	4568	Ripple MyPhone 8



```
SELECT * FROM `productInventory`
```

	itemId	itemName	itemDescription	itemInventory
1	4728475	Rolux Navigator	Stylish men's watch with metal band	1000
2	38492	Rolux Sportsman	Men's sport watch with timer	200
3	1000014	Ripple BookPro 13	13 inch laptop - 5PB HDD/200GB RAM	150
4	1000015	Ripple Jukebox 500	Portable music player - 984 hour battery life	4000
5	1000016	Poku Castbox	Video streaming device - HDMI compatible	156
6	1000017	Ripple Jukebox 300	Music streaming device 300GB storage capacity	895
7	1000020	Ripple MyPhone 8	The latest phone from Ripple - 8 inch with 8TB of storage capacity	4568



New Connection

Valid connection

Connection Name: product_database

App: Splunk DB Connect v2

Host: 127.0.0.1

Database Types: MySQL

Default Database: productdb

The usage and meaning of this parameter varies between database vendors. Learn More

JDBC URL Format: jdbc:mysql://<host>:<port>/<database>

JDBC URL is generated from the above format template.Click here to manually edit the URL.

Generated JDBC URL:
jdbc:mysql://127.0.0.1:<port>/productdb

Identity: discovered_intelligence_user

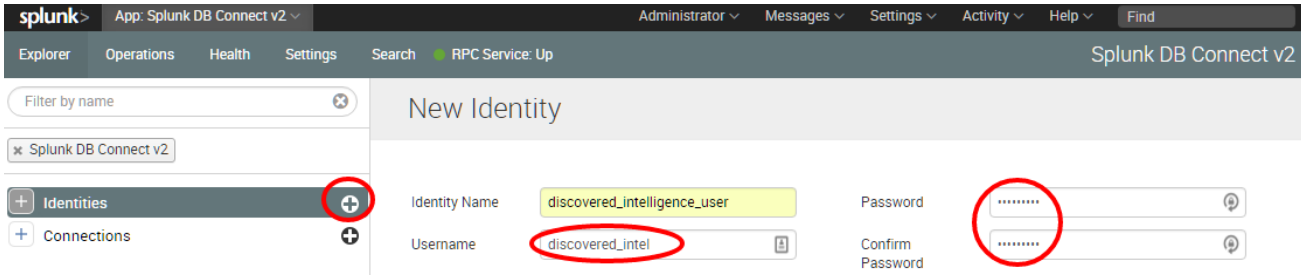
Port:

Enable SSL: □

This is a DB driver flag, and may not be supported for all JDBC drivers.

Readonly: □

This is a DB driver flag and cannot always guarantee read-only access. Use a read-only database user account to ensure that data cannot be altered.



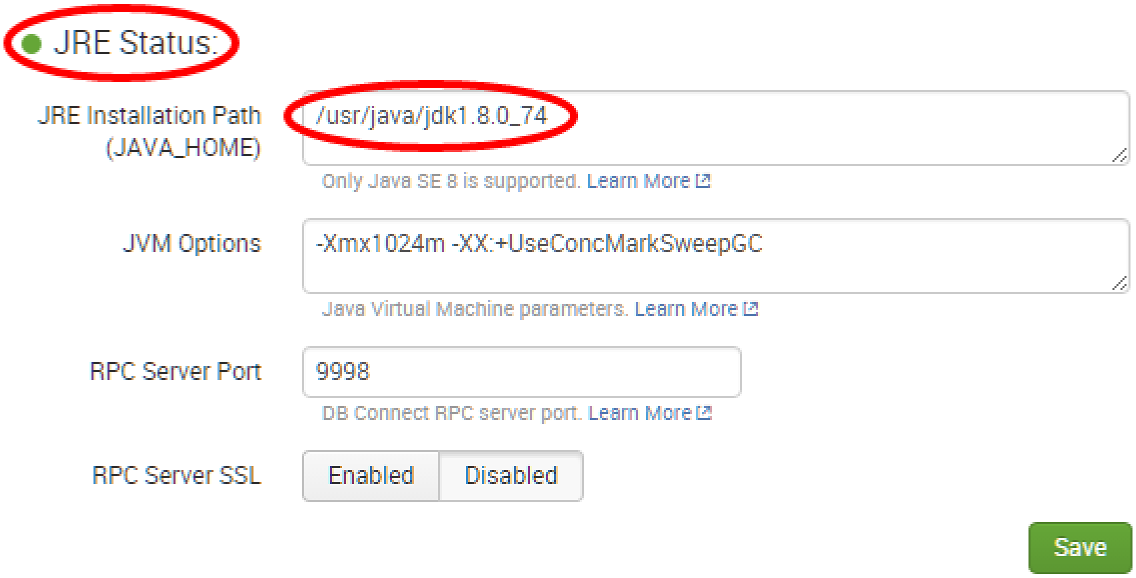
New Identity

Identity Name: discovered_intelligence_user

Username: discovered_intel

Password: ••••••••

Confirm Password: ••••••••


● JRE Status:

JRE Installation Path (JAVA_HOME): /usr/java/jdk1.8.0_74

Only Java SE 8 is supported. Learn More

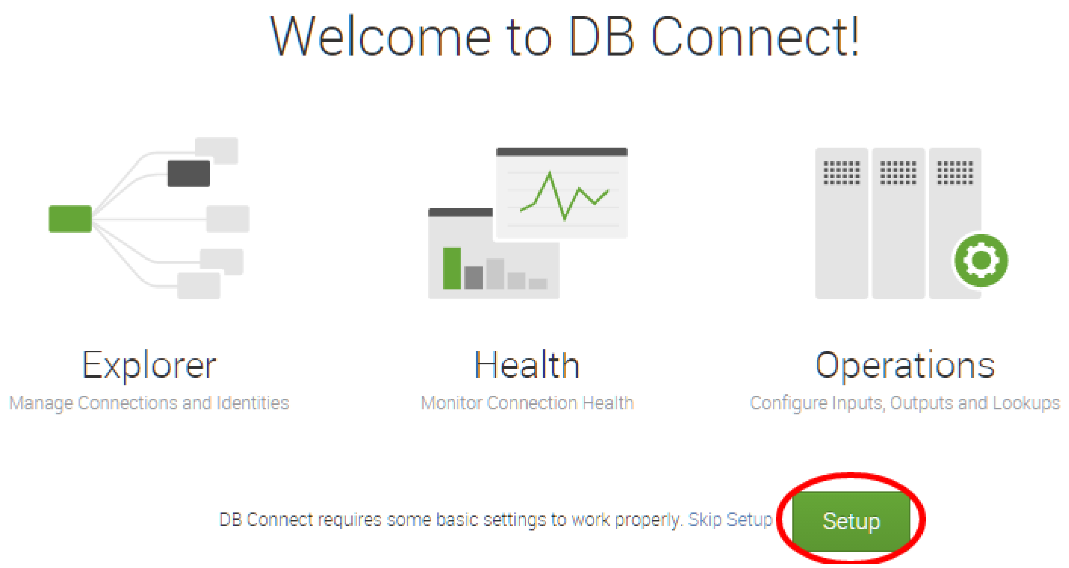
JVM Options: -Xmx1024m -XX:+UseConcMarkSweepGC

Java Virtual Machine parameters. Learn More

RPC Server Port: 9998

DB Connect RPC server port. Learn More

RPC Server SSL: Enabled Disabled



Welcome to DB Connect!

Explorer

Manage Connections and Identities

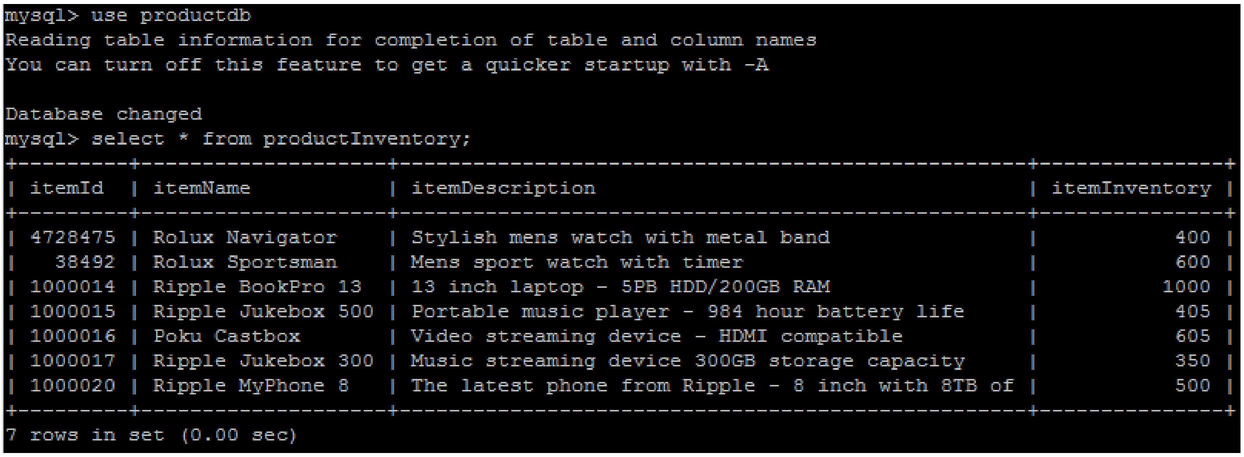
Health

Monitor Connection Health

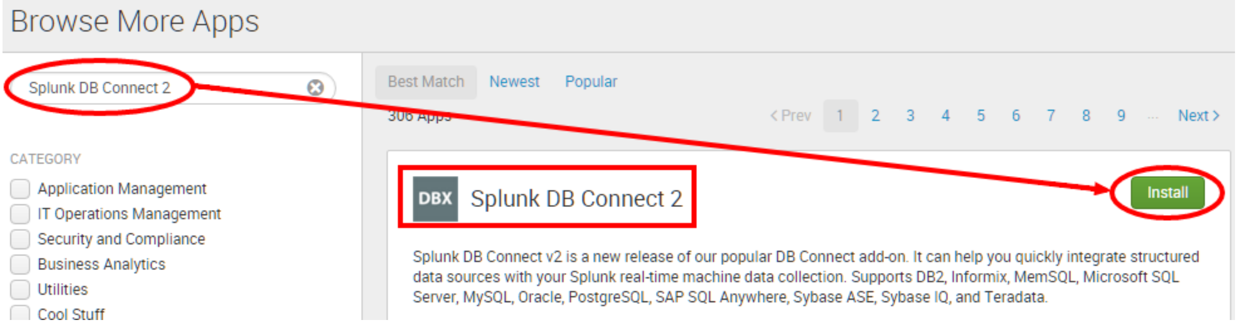
Operations

Configure Inputs, Outputs and Lookups

DB Connect requires some basic settings to work properly. Skip Setup



```
mysql> use productdb
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from productInventory;
+---------+--------------------+---------------------------------------------------+---------------+
| itemId  | itemName           | itemDescription                                   | itemInventory |
+---------+--------------------+---------------------------------------------------+---------------+
| 4728475 | Rolux Navigator    | Stylish mens watch with metal band                |           400 |
|   38492 | Rolux Sportsman    | Mens sport watch with timer                       |           600 |
| 1000014 | Ripple BookPro 13  | 13 inch laptop - 5PB HDD/200GB RAM                |          1000 |
| 1000015 | Ripple Jukebox 500 | Portable music player - 984 hour battery life     |           405 |
| 1000016 | Poku Castbox       | Video streaming device - HDMI compatible          |           605 |
| 1000017 | Ripple Jukebox 300 | Music streaming device 300GB storage capacity     |           350 |
| 1000020 | Ripple MyPhone 8   | The latest phone from Ripple - 8 inch with 8TB of |           500 |
+---------+--------------------+---------------------------------------------------+---------------+
7 rows in set (0.00 sec)
```



Browse More Apps

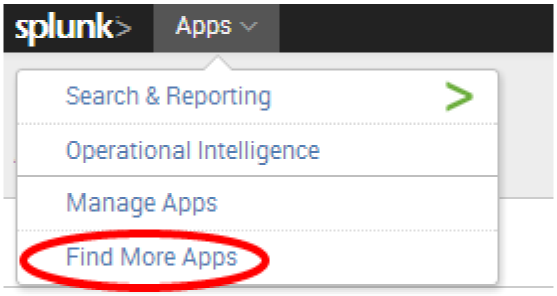
Splunk DB Connect 2

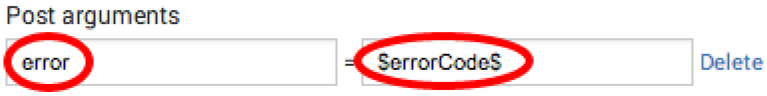
CATEGORY

- □ Application Management
- □ IT Operations Management
- □ Security and Compliance
- □ Business Analytics
- □ Utilities
- □ Cool Stuff

Splunk DB Connect 2

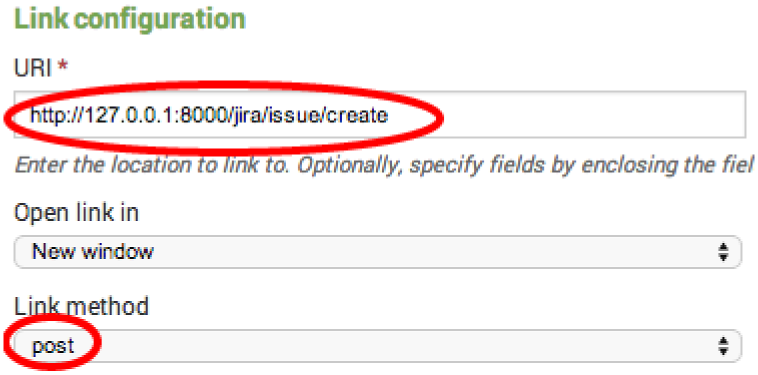
Splunk DB Connect v2 is a new release of our popular DB Connect add-on. It can help you quickly integrate structured data sources with your Splunk real-time machine data collection. Supports DB2, Informix, MemSQL, Microsoft SQL Server, MySQL, Oracle, PostgreSQL, SAP SQL Anywhere, Sybase ASE, Sybase IQ, and Teradata.





Post arguments

error = $errorCode$ Delete



Link configuration

URI *

http://127.0.0.1:8000/jira/issue/create

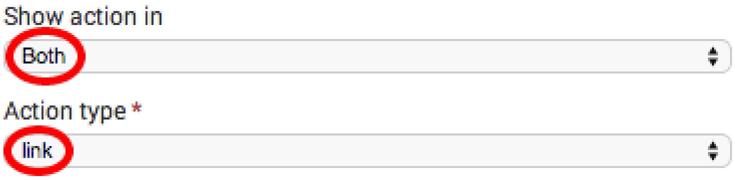
Enter the location to link to. Optionally, specify fields by enclosing the fiel

Open link in

New window

Link method

post

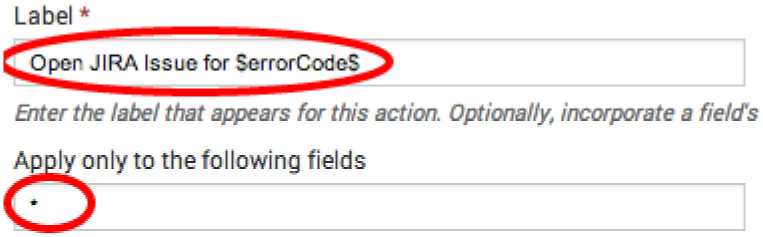


Show action in

Both

Action type *

link



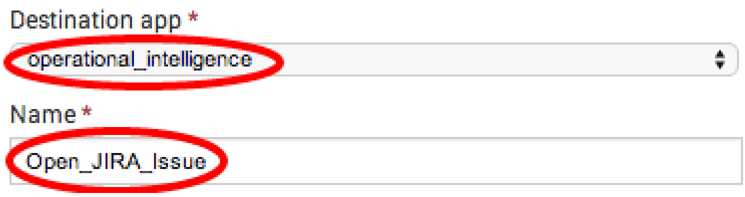
Label *

Open JIRA Issue for $errorCode$

Enter the label that appears for this action. Optionally, incorporate a field's

Apply only to the following fields

*

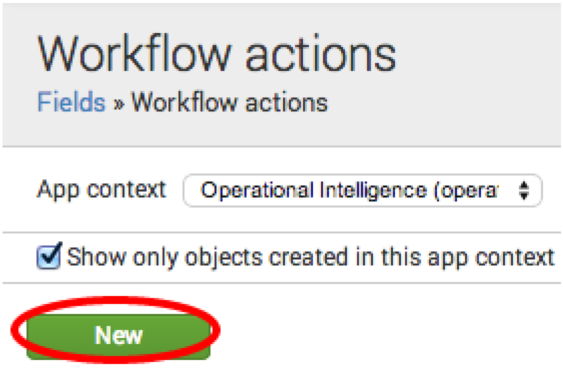


Destination app *

operational_intelligence

Name *

Open_JIRA_Issue

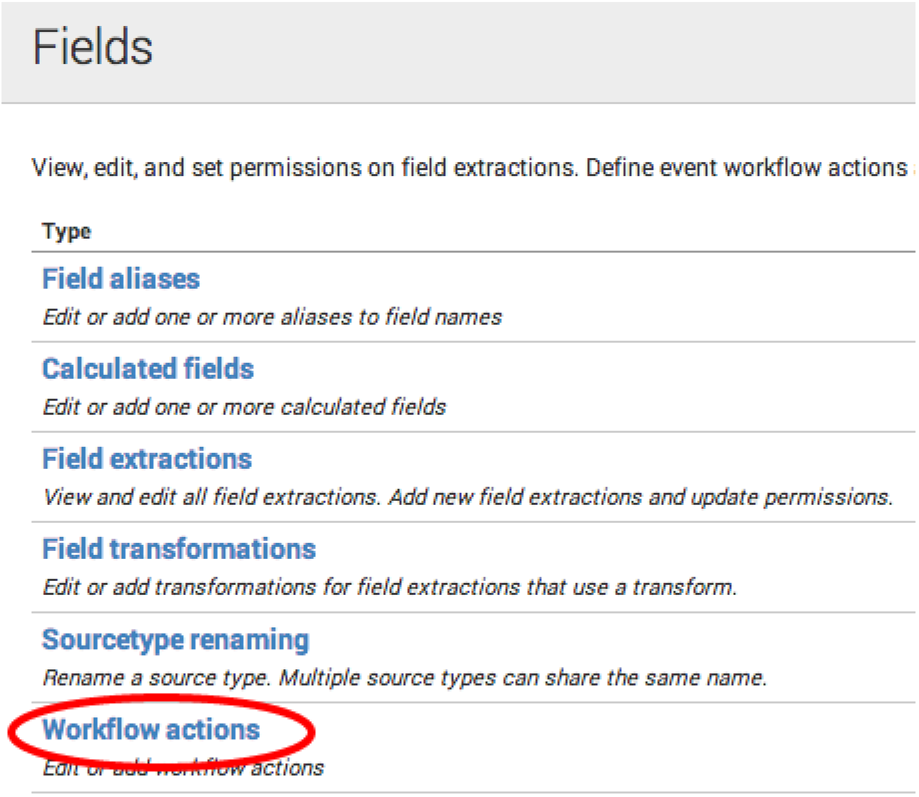


Workflow actions

Fields » Workflow actions

App context: Operational Intelligence (opera

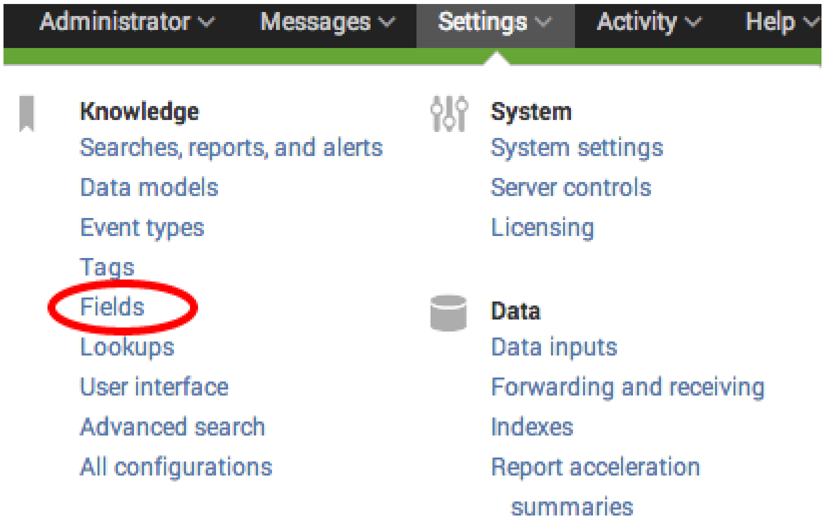
☑ Show only objects created in this app context

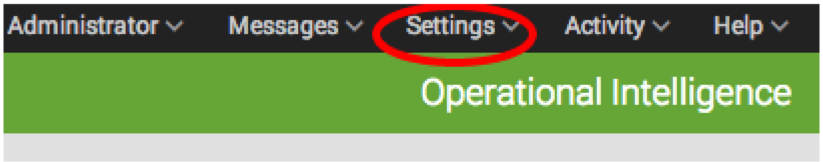


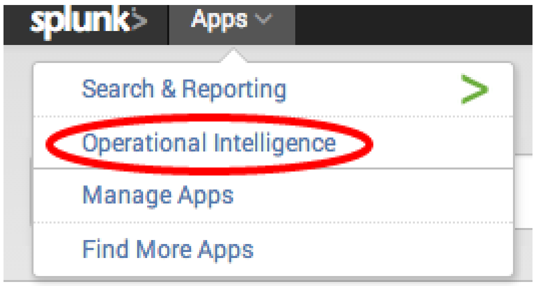
Fields

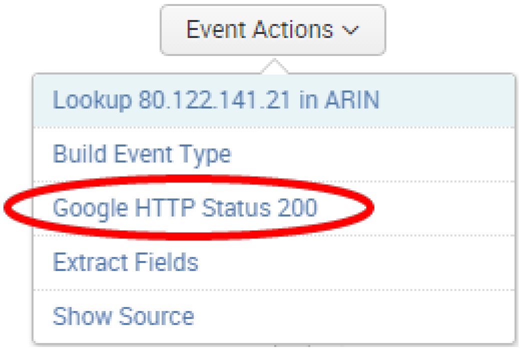
View, edit, and set permissions on field extractions. Define event workflow actions

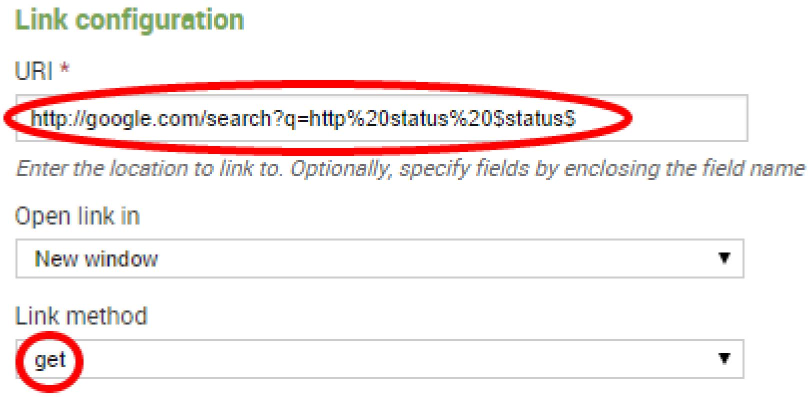
Type
Field aliases *Edit or add one or more aliases to field names*
Calculated fields *Edit or add one or more calculated fields*
Field extractions *View and edit all field extractions. Add new field extractions and update permissions.*
Field transformations *Edit or add transformations for field extractions that use a transform.*
Sourcetype renaming *Rename a source type. Multiple source types can share the same name.*
Workflow actions *Edit or add workflow actions*











Link configuration

URI *

http://google.com/search?q=http%20status%20$status$

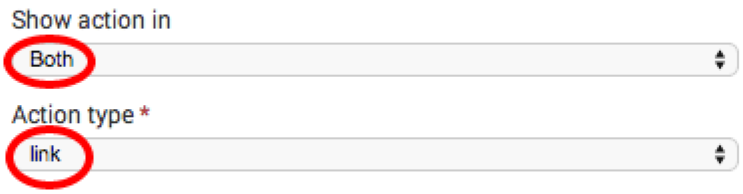
Enter the location to link to. Optionally, specify fields by enclosing the field name

Open link in

New window ▼

Link method

get ▼

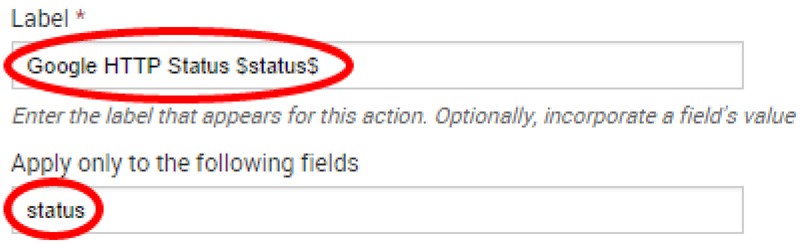


Show action in

Both

Action type *

link



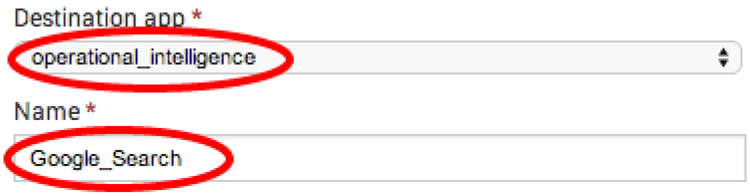
Label *

Google HTTP Status $status$

Enter the label that appears for this action. Optionally, incorporate a field's value

Apply only to the following fields

status

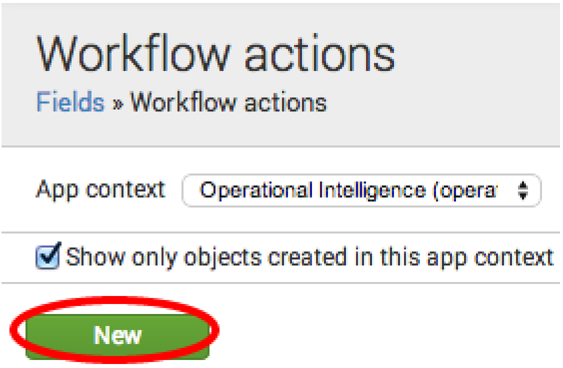


Destination app *

operational_intelligence

Name *

Google_Search

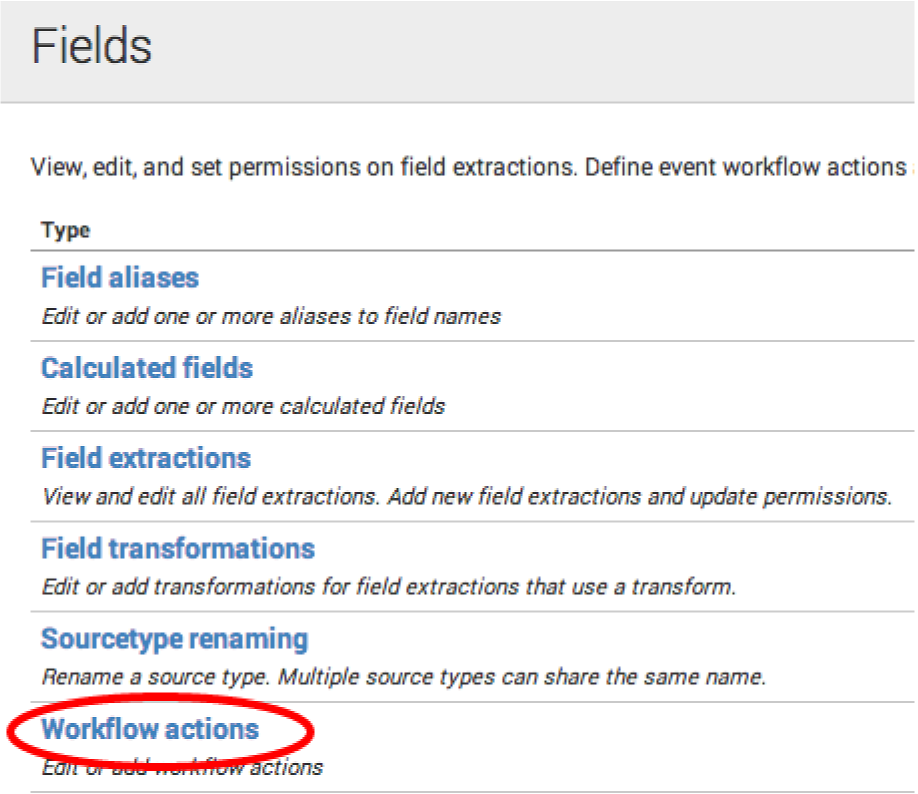


Workflow actions

Fields » Workflow actions

App context: Operational Intelligence (opera

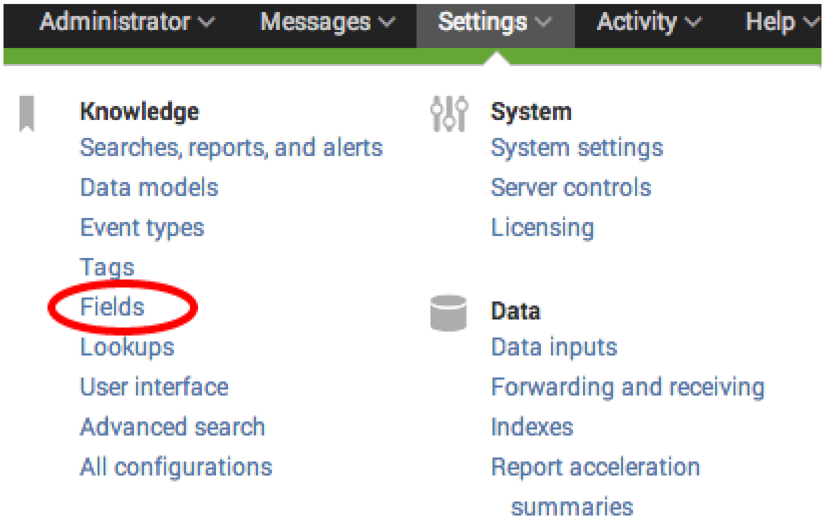
☑ Show only objects created in this app context



Fields

View, edit, and set permissions on field extractions. Define event workflow actions

Type
Field aliases *Edit or add one or more aliases to field names*
Calculated fields *Edit or add one or more calculated fields*
Field extractions *View and edit all field extractions. Add new field extractions and update permissions.*
Field transformations *Edit or add transformations for field extractions that use a transform.*
Sourcetype renaming *Rename a source type. Multiple source types can share the same name.*
Workflow actions *Edit or add workflow actions*

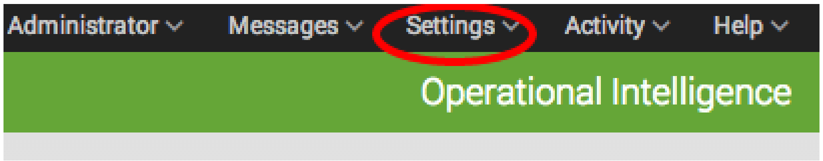


Administrator ⌄ Messages ⌄ Settings ⌄ Activity ⌄ Help ⌄

Knowledge
- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Advanced search
- All configurations

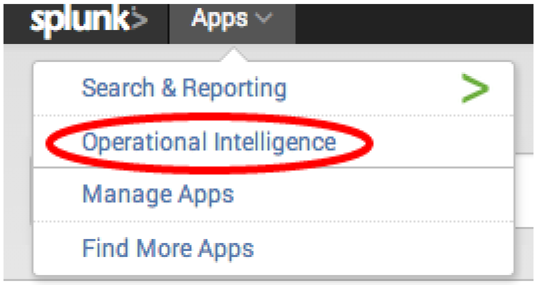
System
- System settings
- Server controls
- Licensing

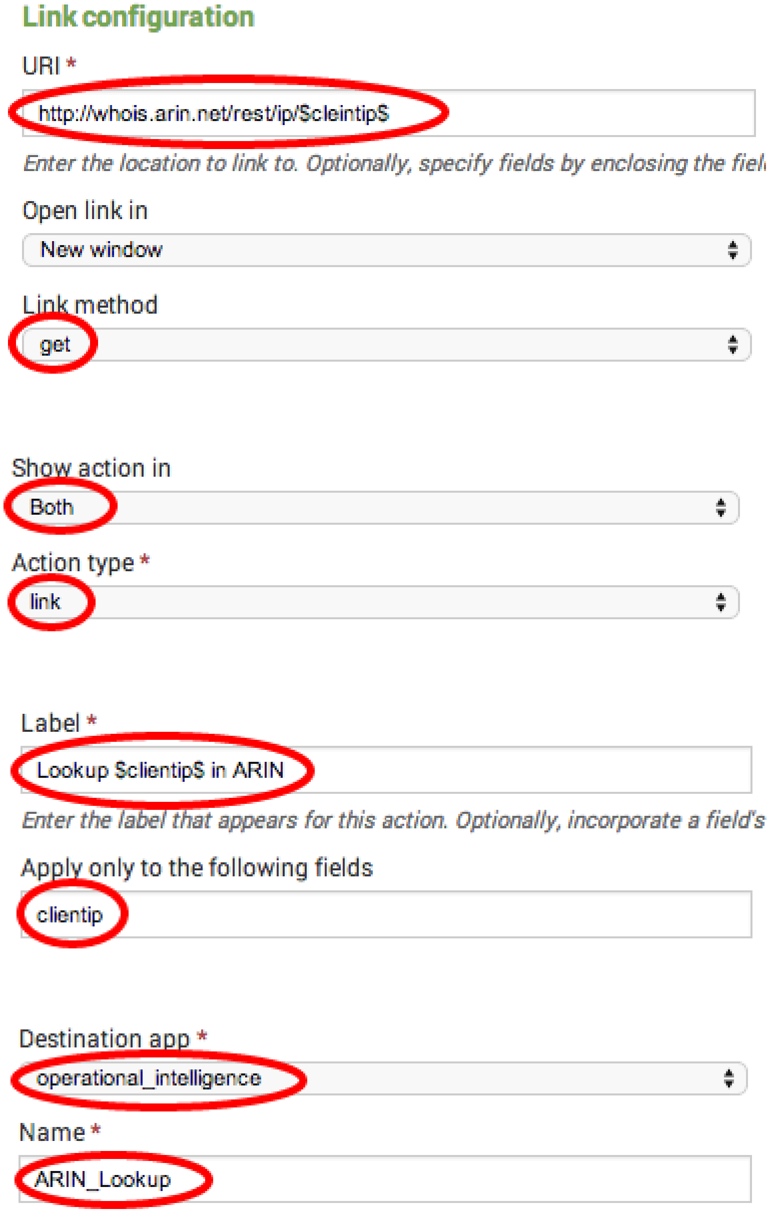
Data
- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries



Administrator ⌄ Messages ⌄ Settings ⌄ Activity ⌄ Help ⌄

Operational Intelligence





Link configuration

URI *

http://whois.arin.net/rest/ip/$cleintip$

Enter the location to link to. Optionally, specify fields by enclosing the fiel

Open link in

New window

Link method

get

Show action in

Both

Action type *

link

Label *

Lookup $clientip$ in ARIN

Enter the label that appears for this action. Optionally, incorporate a field's

Apply only to the following fields

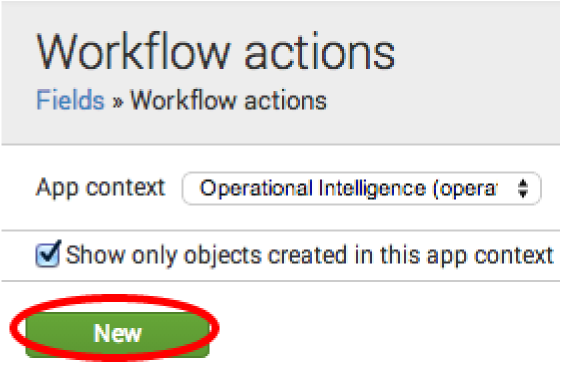
clientip

Destination app *

operational_intelligence

Name *

ARIN_Lookup

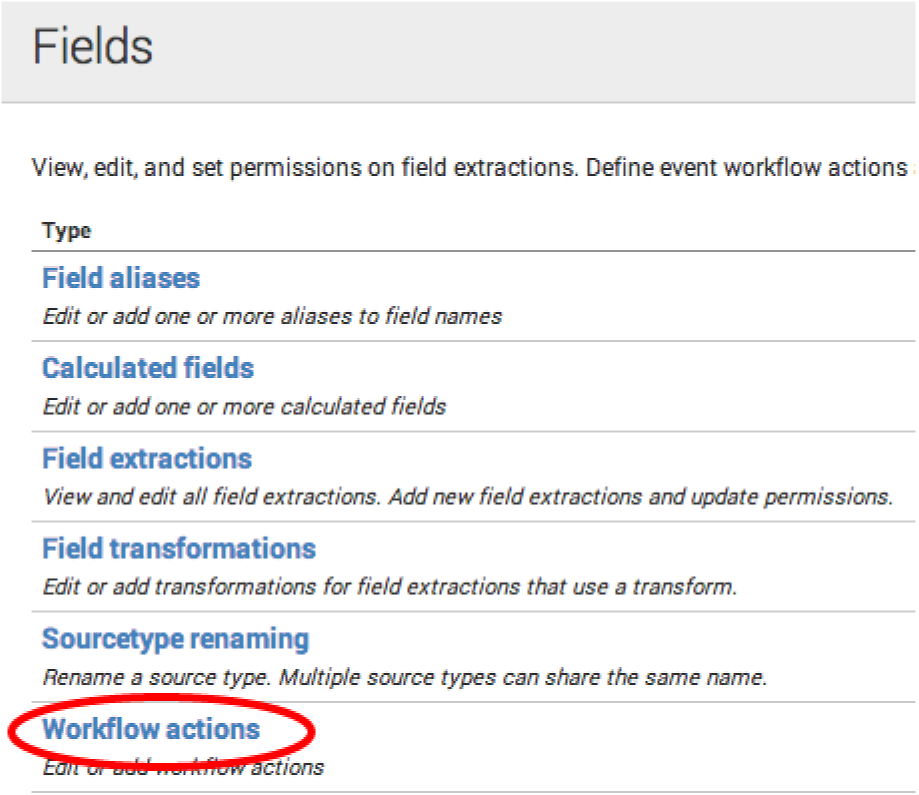


Workflow actions

Fields » Workflow actions

App context: Operational Intelligence (opera

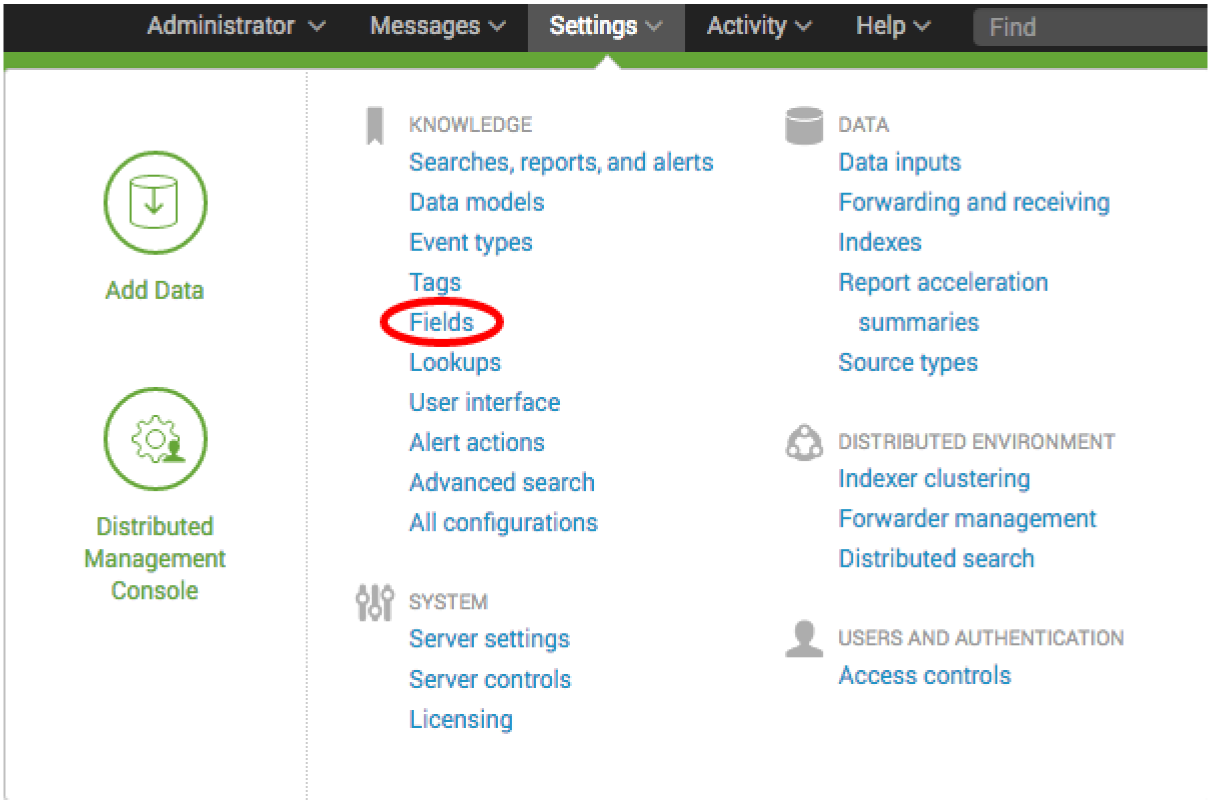
☑ Show only objects created in this app context

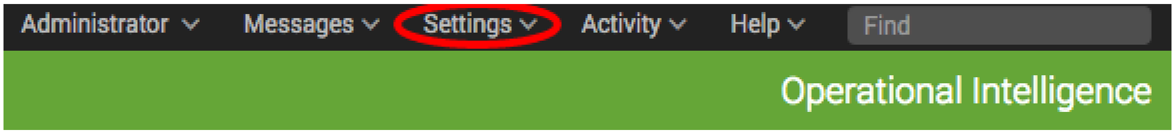


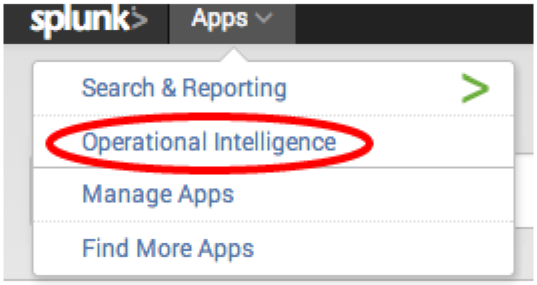
Fields

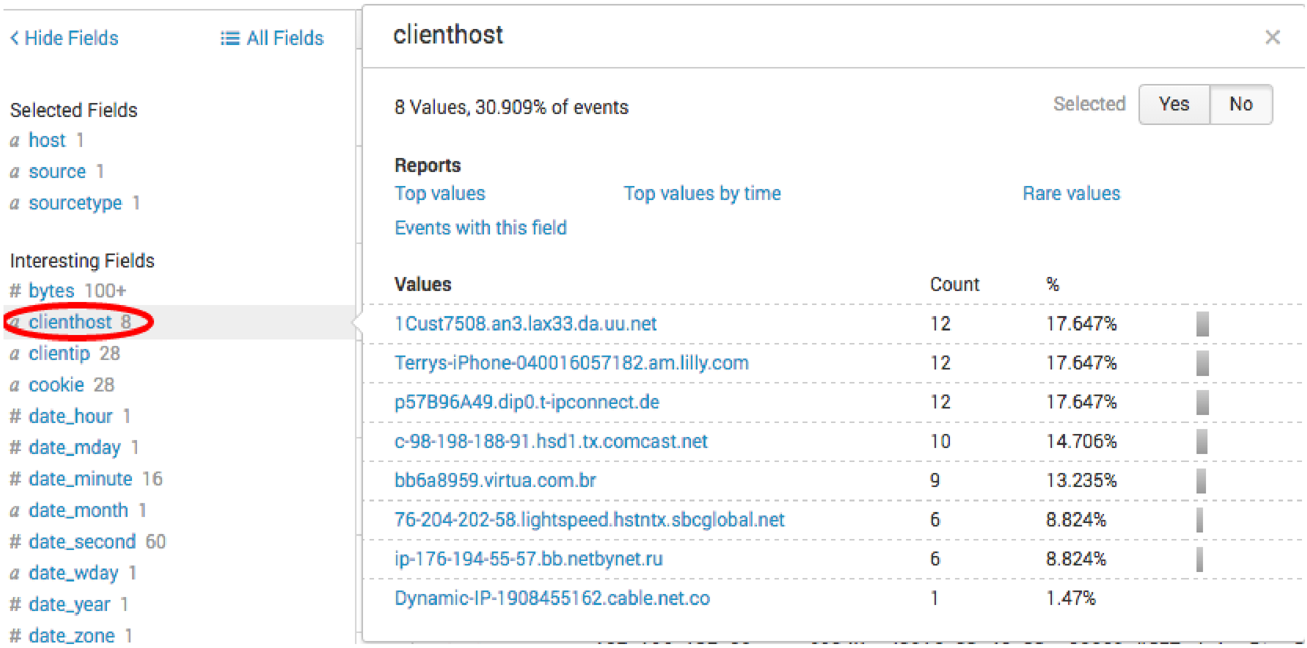
View, edit, and set permissions on field extractions. Define event workflow actions

Type
Field aliases *Edit or add one or more aliases to field names*
Calculated fields *Edit or add one or more calculated fields*
Field extractions *View and edit all field extractions. Add new field extractions and update permissions.*
Field transformations *Edit or add transformations for field extractions that use a transform.*
Sourcetype renaming *Rename a source type. Multiple source types can share the same name.*
Workflow actions *Edit or add workflow actions*


Administrator
Messages
Settings
Activity
Help
Find
Add Data
Distributed Management Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Licensing
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
USERS AND AUTHENTICATION
Access controls


Administrator
Messages
Settings
Activity
Help
Find
Operational Intelligence


splunk>
Apps
Search & Reporting
Operational Intelligence
Manage Apps
Find More Apps



Selected Fields
a host 1
a source 1
a sourcetype 1

Interesting Fields
# bytes 100+
a clienthost 8
a clientip 28
a cookie 28
# date_hour 1
# date_mday 1
# date_minute 16
a date_month 1
# date_second 60
a date_wday 1
# date_year 1
# date_zone 1

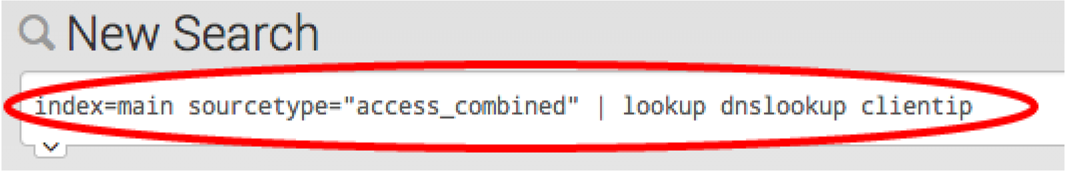
clienthost

8 Values, 30.909% of events

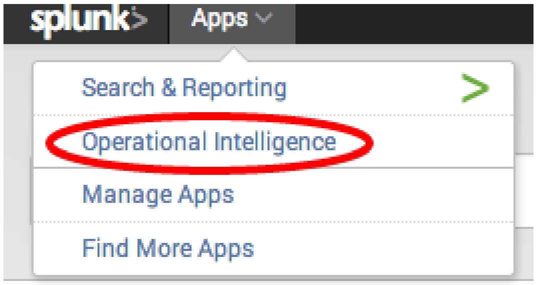
Selected Yes No

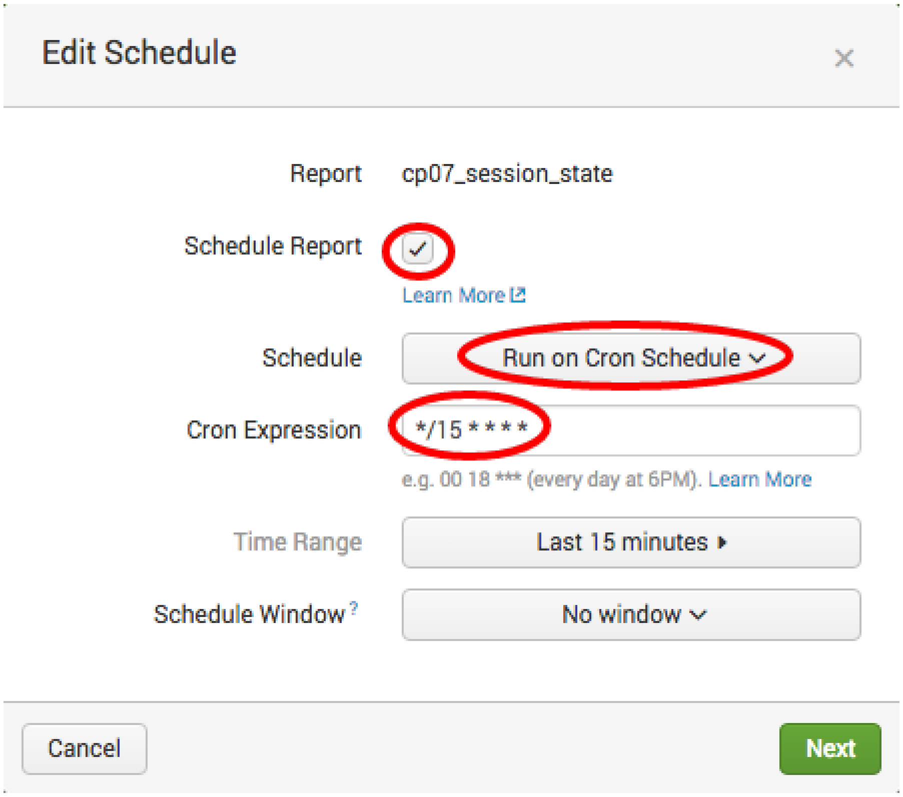
Reports

Values	Count	%
1Cust7508.an3.lax33.da.uu.net	12	17.647%
Terrys-iPhone-040016057182.am.lilly.com	12	17.647%
p57B96A49.dip0.t-ipconnect.de	12	17.647%
c-98-198-188-91.hsd1.tx.comcast.net	10	14.706%
bb6a8959.virtua.com.br	9	13.235%
76-204-202-58.lightspeed.hstntx.sbcglobal.net	6	8.824%
ip-176-194-55-57.bb.netbynet.ru	6	8.824%
Dynamic-IP-1908455162.cable.net.co	1	1.47%


New Search

```
index=main sourcetype="access_combined" | lookup dnslookup clientip
```





Edit Schedule

Report cp07_session_state

Schedule Report ☑

Learn More

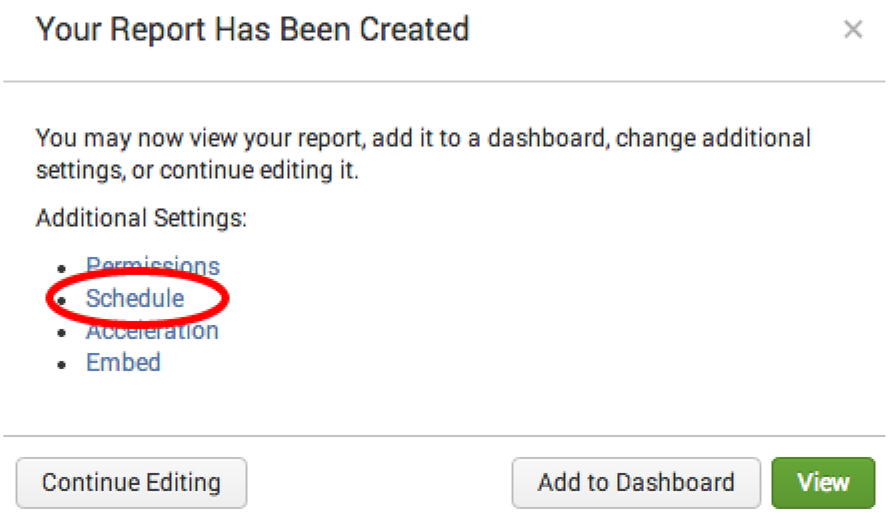
Schedule: Run on Cron Schedule

Cron Expression: */15 * * * *

e.g. 00 18 *** (every day at 6PM). Learn More

Time Range: Last 15 minutes

Schedule Window: No window

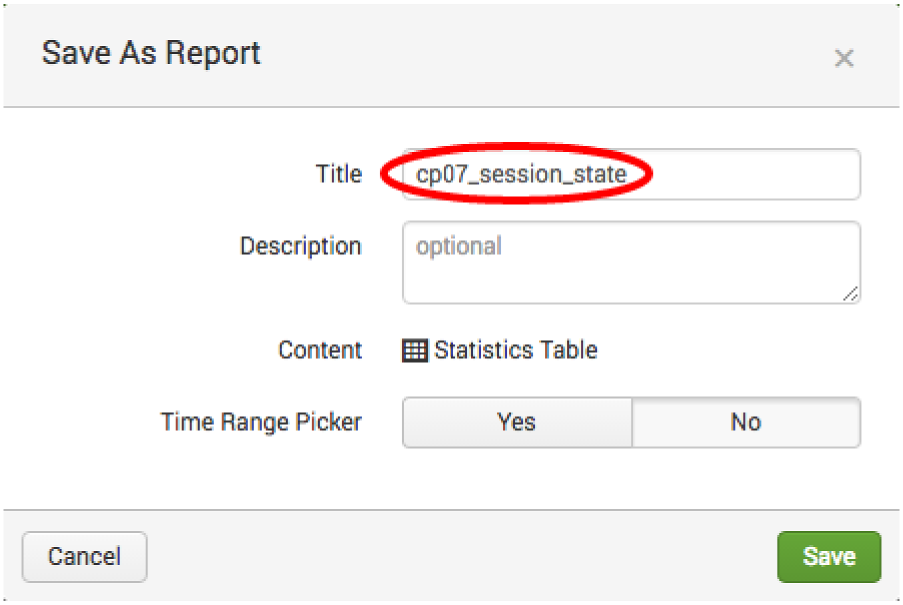


Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed

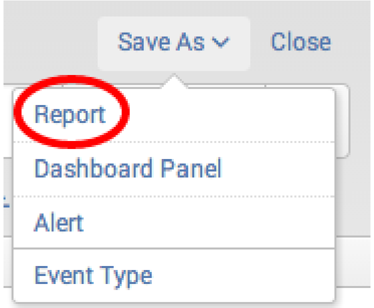


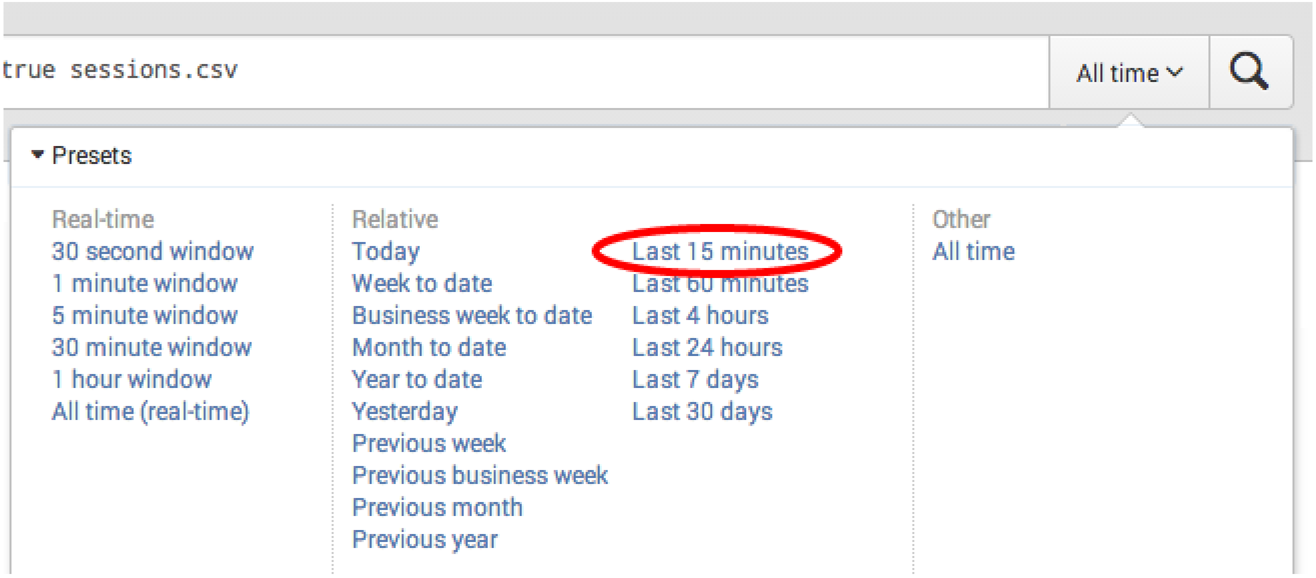
Title [✓ cp07_session_state]

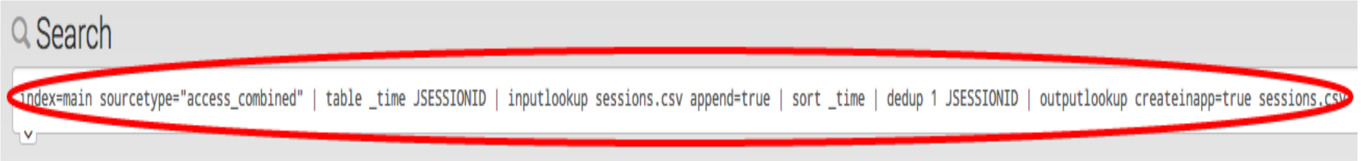
Description optional

Content ▦ Statistics Table

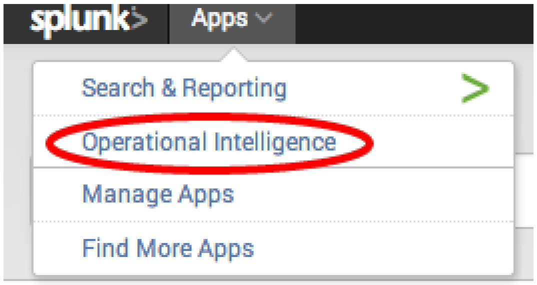
Time Range Picker Yes No

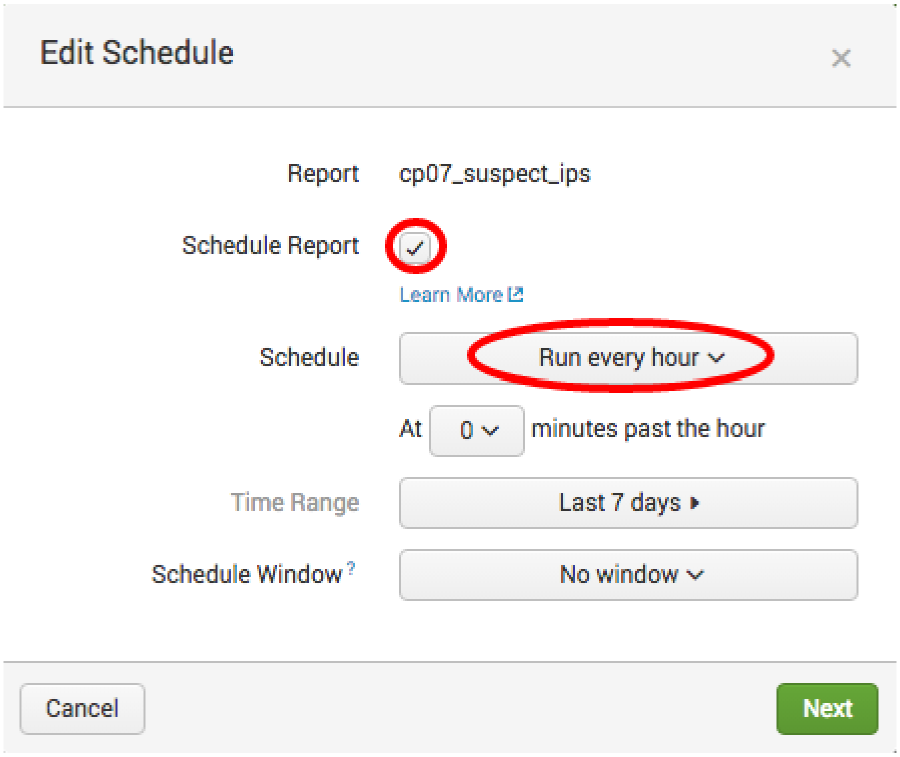



```
true sessions.csv
```

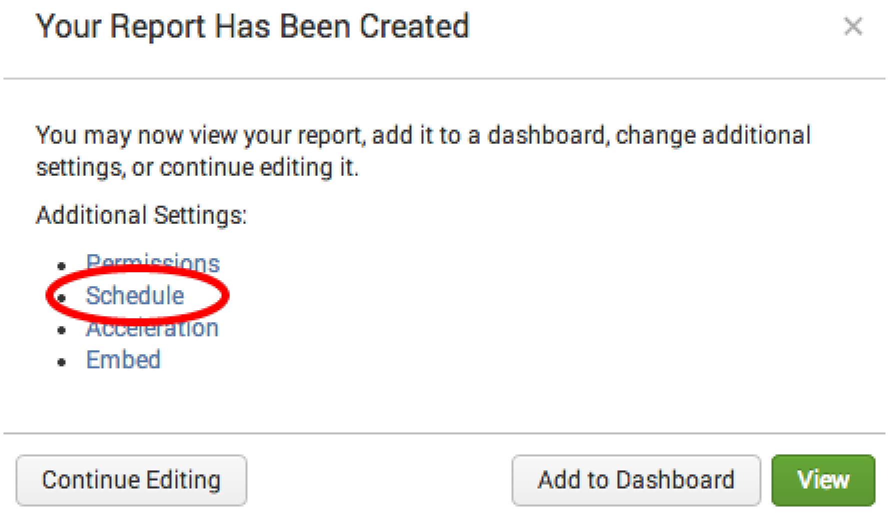


```
index=main sourcetype="access_combined" | table _time JSESSIONID | inputlookup sessions.csv append=true | sort _time | dedup 1 JSESSIONID | outputlookup createinapp=true sessions.csv
```




Edit Schedule

Report	cp07_suspect_ips
Schedule Report	☑
	Learn More
Schedule	Run every hour
	At 0 minutes past the hour
Time Range	Last 7 days
Schedule Window?	No window

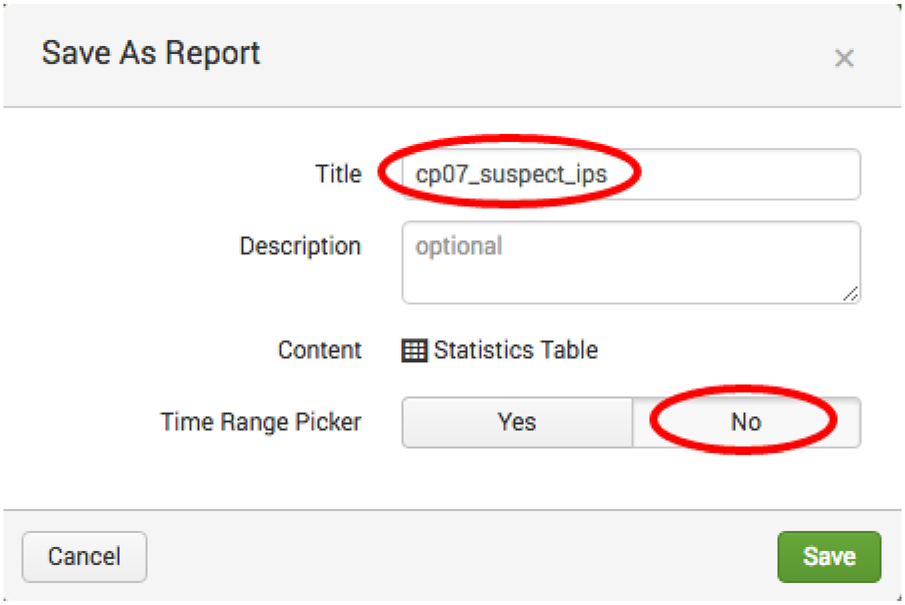


Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- [✓ Schedule]
- Acceleration
- Embed



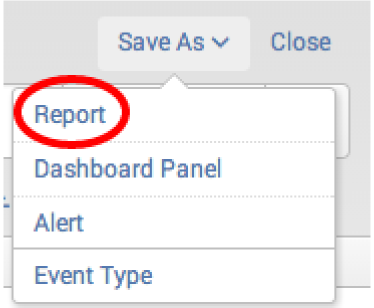
Save As Report

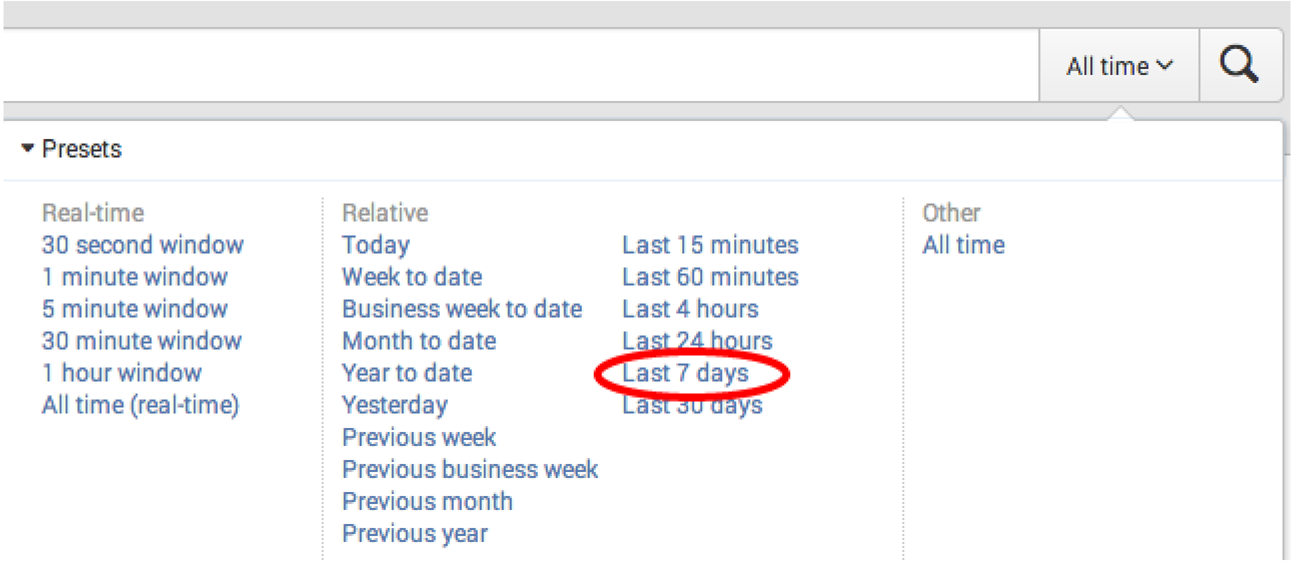
Title [✓ cp07_suspect_ips]

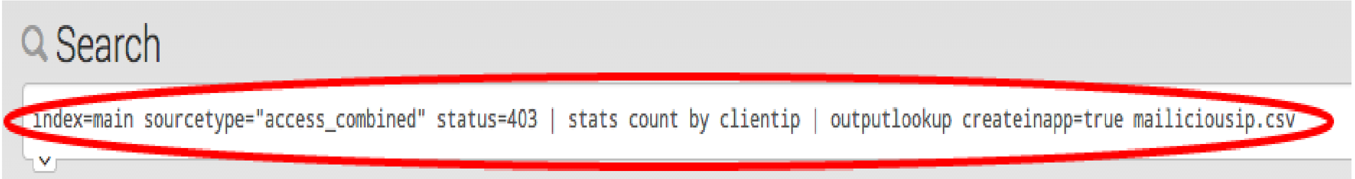
Description optional

Content Statistics Table

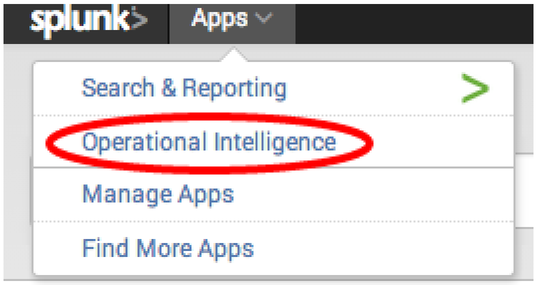
Time Range Picker Yes [✓ No]

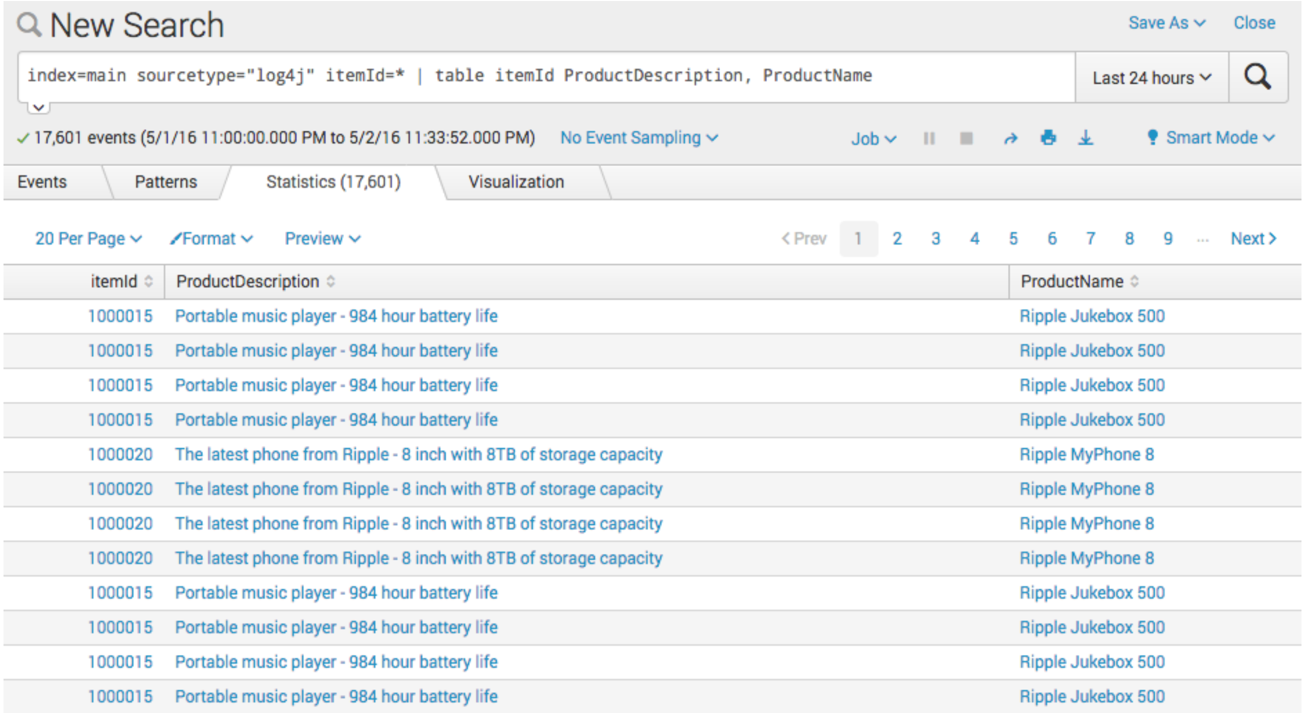






```
index=main sourcetype="access_combined" status=403 | stats count by clientip | outputlookup createinapp=true mailiciousip.csv
```

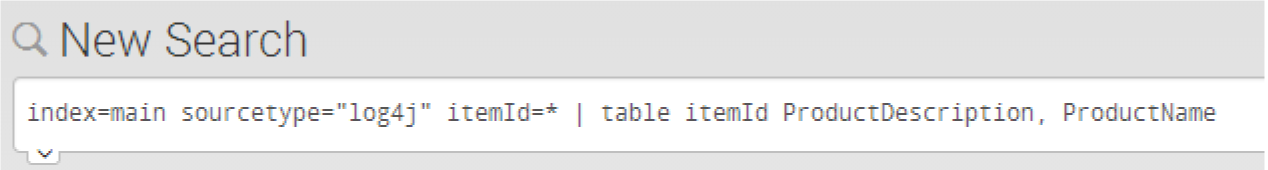




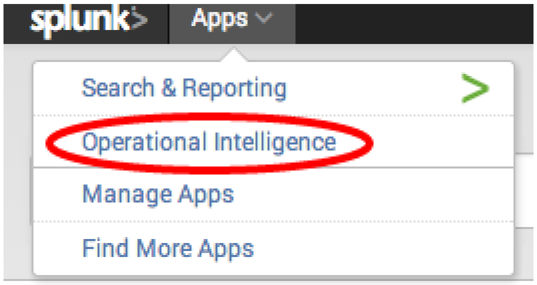
```
index=main sourcetype="log4j" itemId=* | table itemId ProductDescription, ProductName
```

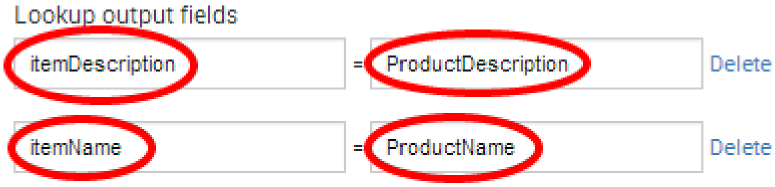
✓ 17,601 events (5/1/16 11:00:00.000 PM to 5/2/16 11:33:52.000 PM)

itemId	ProductDescription	ProductName
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500
1000020	The latest phone from Ripple - 8 inch with 8TB of storage capacity	Ripple MyPhone 8
1000020	The latest phone from Ripple - 8 inch with 8TB of storage capacity	Ripple MyPhone 8
1000020	The latest phone from Ripple - 8 inch with 8TB of storage capacity	Ripple MyPhone 8
1000020	The latest phone from Ripple - 8 inch with 8TB of storage capacity	Ripple MyPhone 8
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500
1000015	Portable music player - 984 hour battery life	Ripple Jukebox 500



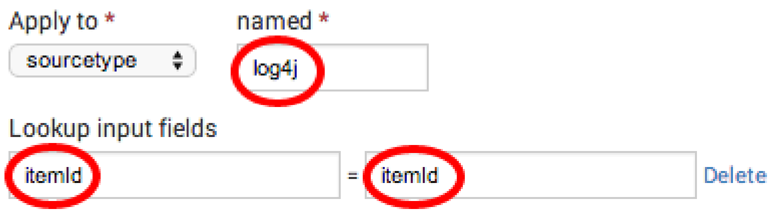
```
index=main sourcetype="log4j" itemId=* | table itemId ProductDescription, ProductName
```





Lookup output fields

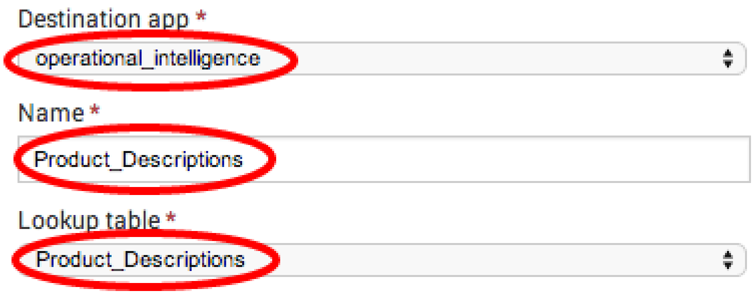
itemDescription	=	ProductDescription	Delete
itemName	=	ProductName	Delete



Apply to * sourcetype named * log4j

Lookup input fields

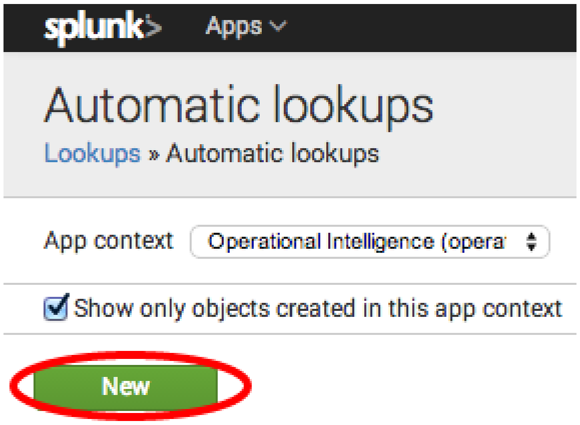
itemId = itemId



Destination app * operational_intelligence

Name * Product_Descriptions

Lookup table * Product_Descriptions

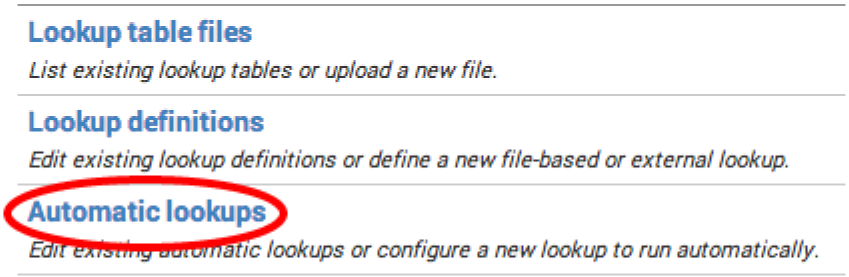


Automatic lookups

Lookups » Automatic lookups

App context Operational Intelligence (opera

☑ Show only objects created in this app context



Lookup table files

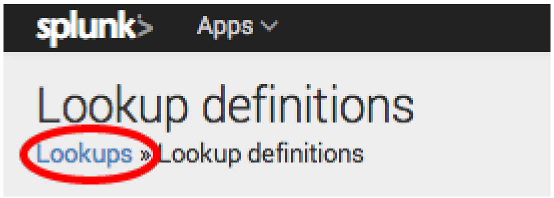
List existing lookup tables or upload a new file.

Lookup definitions

Edit existing lookup definitions or define a new file-based or external lookup.

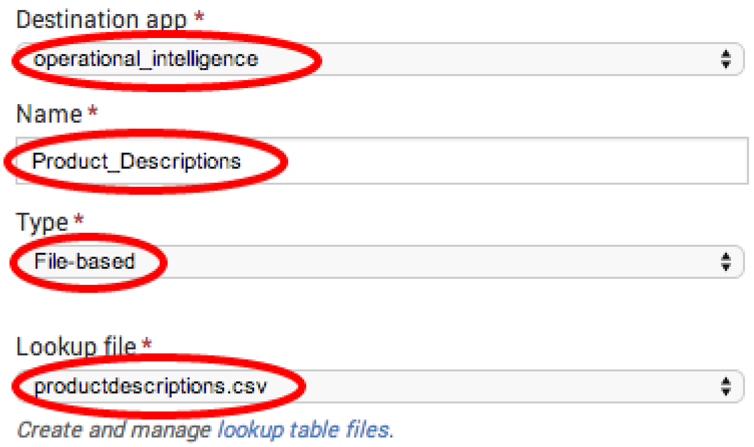
Automatic lookups

Edit existing automatic lookups or configure a new lookup to run automatically.



Lookup definitions

Lookups » Lookup definitions



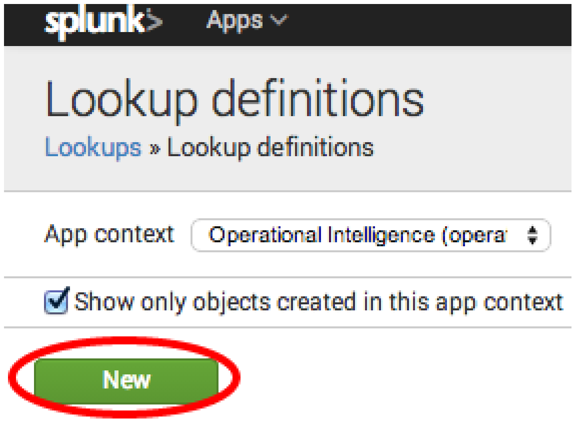
Destination app * operational_intelligence

Name * Product_Descriptions

Type * File-based

Lookup file * productdescriptions.csv

Create and manage lookup table files.

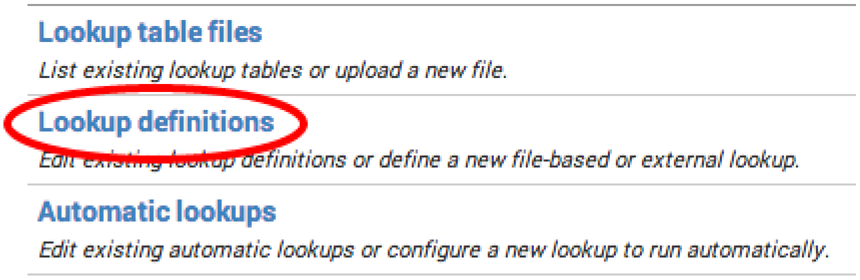


Lookup definitions

Lookups » Lookup definitions

App context: Operational Intelligence (opera

☑ Show only objects created in this app context



Lookup table files

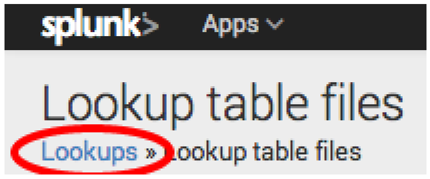
List existing lookup tables or upload a new file.

Lookup definitions

Edit existing lookup definitions or define a new file-based or external lookup.

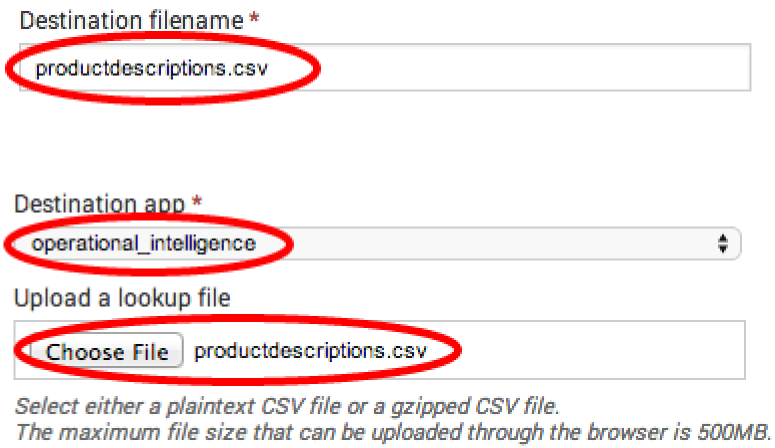
Automatic lookups

Edit existing automatic lookups or configure a new lookup to run automatically.



Lookup table files

Lookups » Lookup table files



Destination filename *

productdescriptions.csv

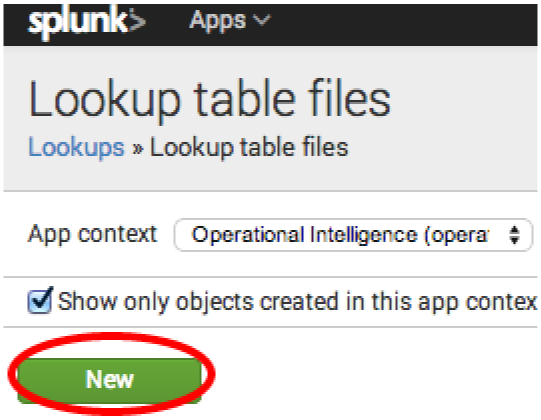
Destination app *

operational_intelligence

Upload a lookup file

Choose File productdescriptions.csv

Select either a plaintext CSV file or a gzipped CSV file.
The maximum file size that can be uploaded through the browser is 500MB.



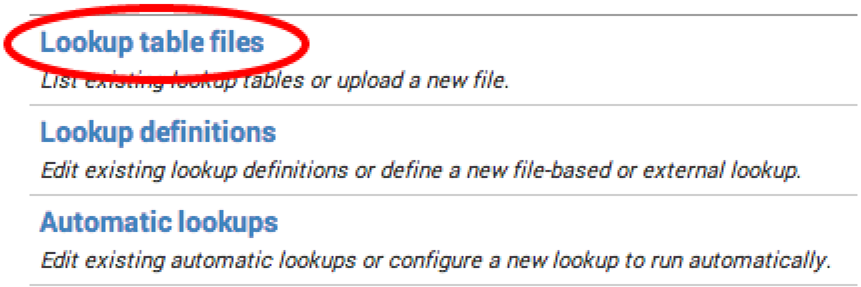
Lookup table files

Lookups » Lookup table files

App context: Operational Intelligence (opera

☑ Show only objects created in this app contex

New



Lookup table files

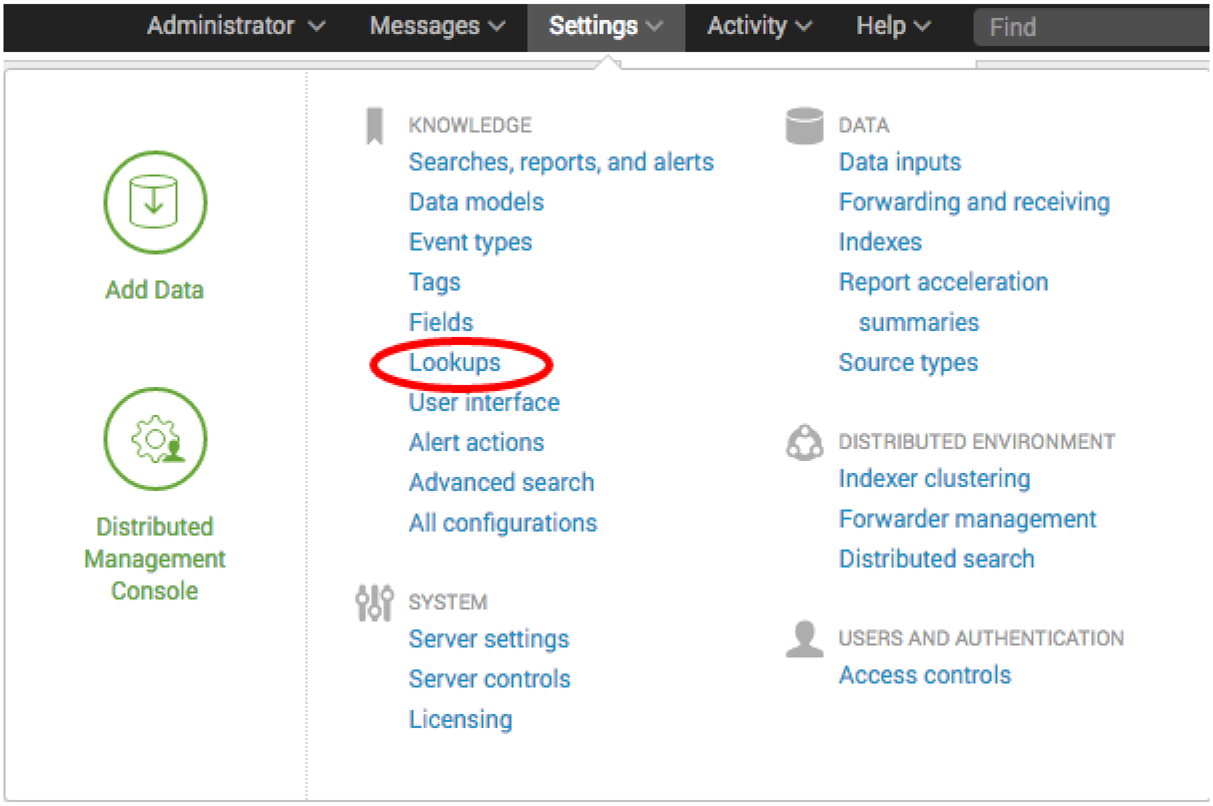
List existing lookup tables or upload a new file.

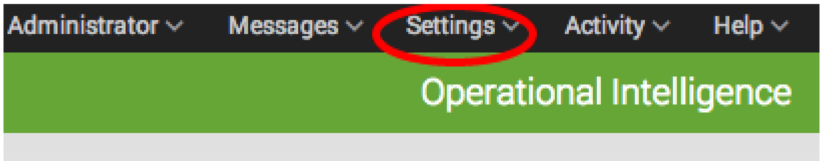
Lookup definitions

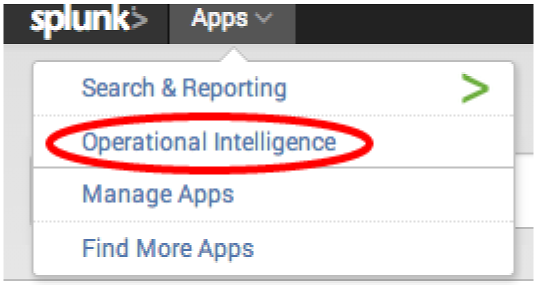
Edit existing lookup definitions or define a new file-based or external lookup.

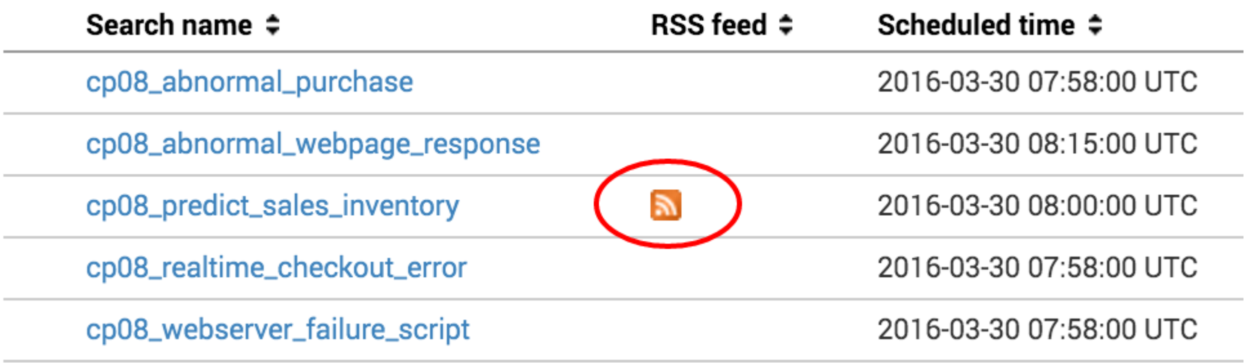
Automatic lookups

Edit existing automatic lookups or configure a new lookup to run automatically.

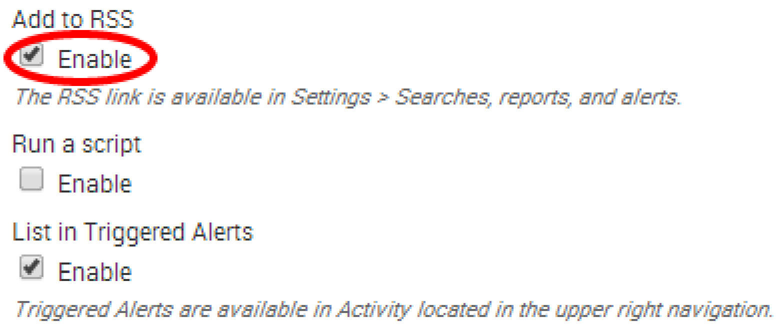

Administrator
Messages
Settings
Activity
Help
Find
Add Data
Distributed Management Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Licensing
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
USERS AND AUTHENTICATION
Access controls


Administrator
Messages
Settings
Activity
Help
Operational Intelligence


splunk>
Apps
Search & Reporting
>
Operational Intelligence
Manage Apps
Find More Apps



Search name ⬍	RSS feed ⬍	Scheduled time ⬍
cp08_abnormal_purchase		2016-03-30 07:58:00 UTC
cp08_abnormal_webpage_response		2016-03-30 08:15:00 UTC
cp08_predict_sales_inventory	■	2016-03-30 08:00:00 UTC
cp08_realtime_checkout_error		2016-03-30 07:58:00 UTC
cp08_webserver_failure_script		2016-03-30 07:58:00 UTC



Add to RSS

☑ Enable

The RSS link is available in Settings > Searches, reports, and alerts.

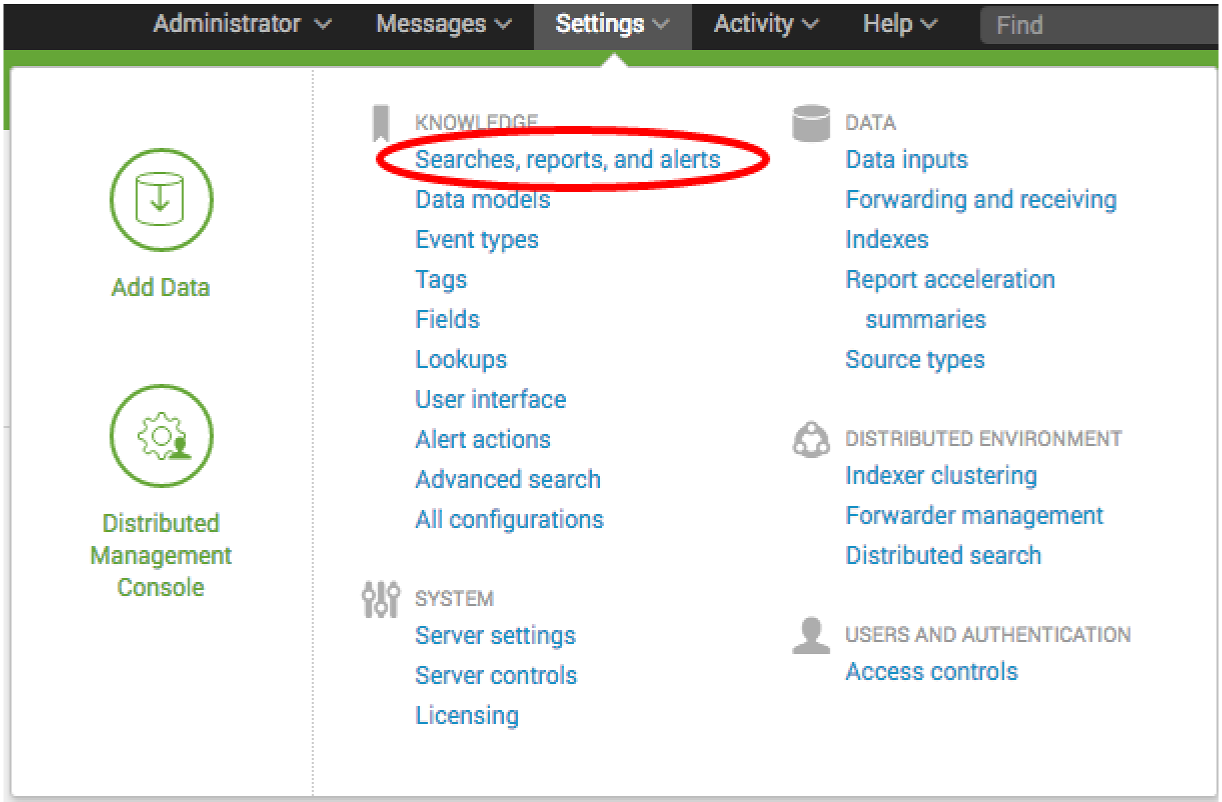
Run a script

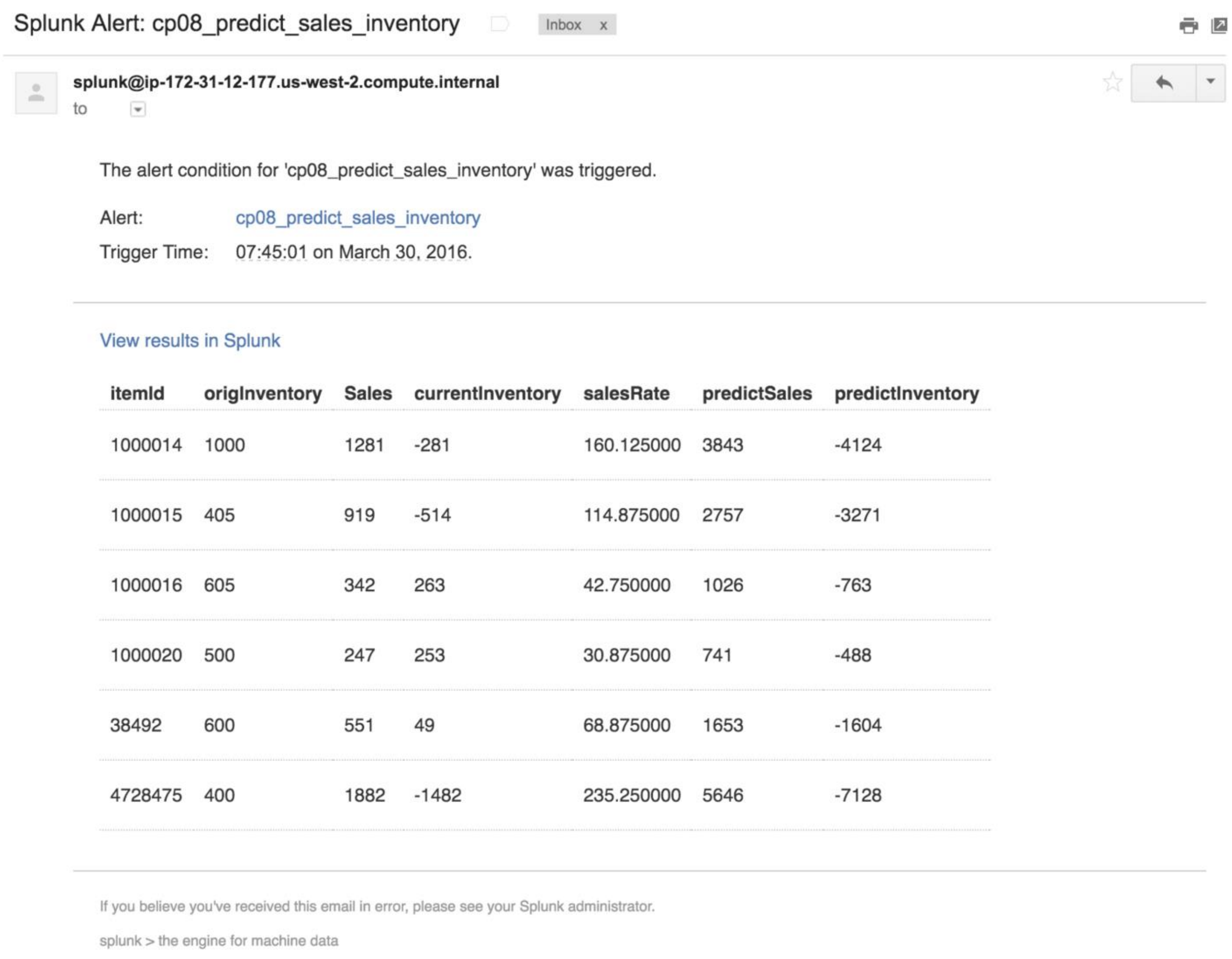
□ Enable

List in Triggered Alerts

☑ Enable

Triggered Alerts are available in Activity located in the upper right navigation.


Administrator
Messages
Settings
Activity
Help
Find
Add Data
Distributed Management Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Licensing
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
USERS AND AUTHENTICATION
Access controls



Splunk Alert: cp08_predict_sales_inventory

splunk@ip-172-31-12-177.us-west-2.compute.internal
to

The alert condition for 'cp08_predict_sales_inventory' was triggered.

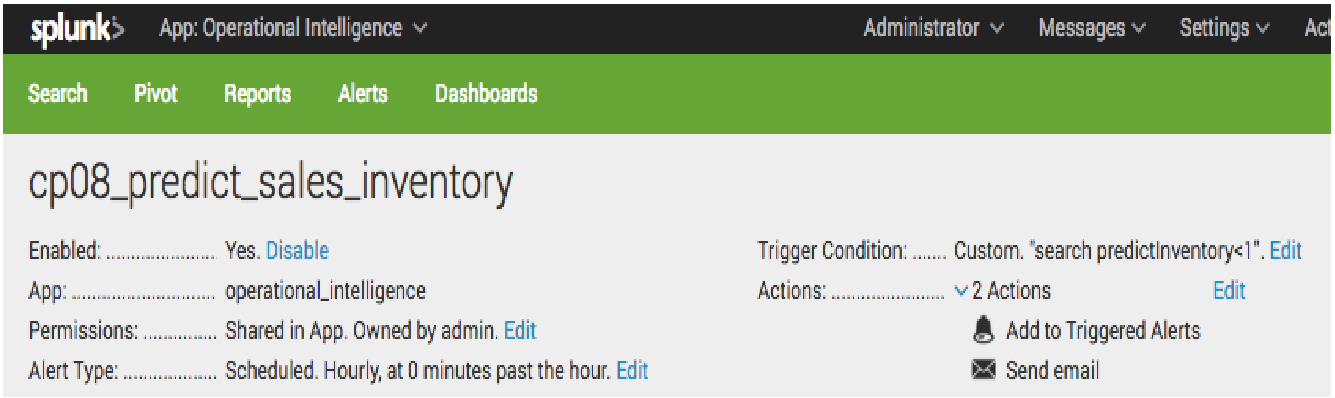
Alert: cp08_predict_sales_inventory
Trigger Time: 07:45:01 on March 30, 2016.

View results in Splunk

itemId	origInventory	Sales	currentInventory	salesRate	predictSales	predictInventory
1000014	1000	1281	-281	160.125000	3843	-4124
1000015	405	919	-514	114.875000	2757	-3271
1000016	605	342	263	42.750000	1026	-763
1000020	500	247	253	30.875000	741	-488
38492	600	551	49	68.875000	1653	-1604
4728475	400	1882	-1482	235.250000	5646	-7128

If you believe you've received this email in error, please see your Splunk administrator.

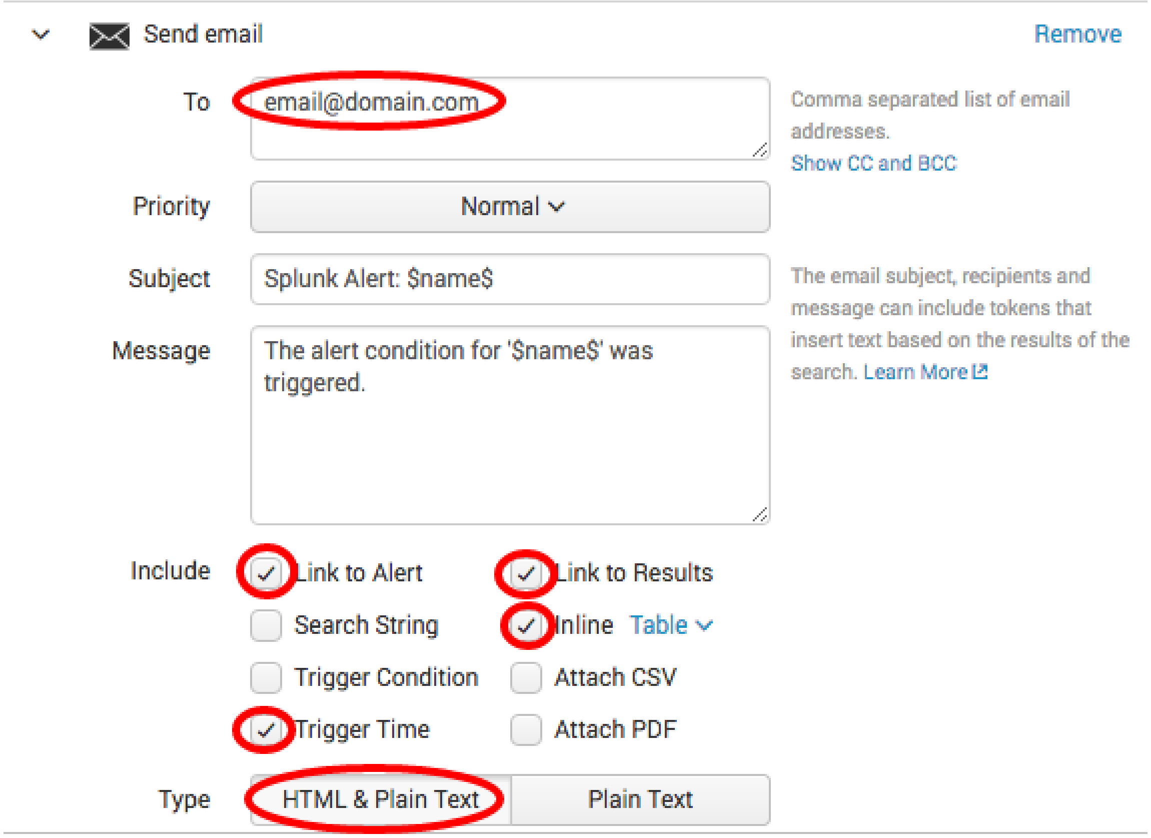
splunk > the engine for machine data



cp08_predict_sales_inventory

Enabled: .... Yes. Disable
App: .... operational_intelligence
Permissions: .... Shared in App. Owned by admin. Edit
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .... Custom. "search predictInventory<1". Edit
Actions: .... 2 Actions Edit
Add to Triggered Alerts
Send email



Send email

To: email@domain.com

Comma separated list of email addresses.

Show CC and BCC

Priority: Normal

Subject: Splunk Alert: $name$

Message: The alert condition for '$name$' was triggered.

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Include:

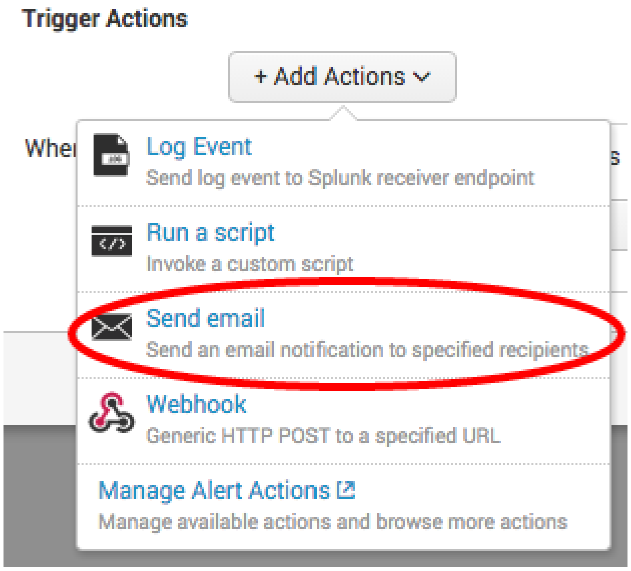
☑ Link to Alert ☑ Link to Results

☐ Search String ☑ Inline Table

☐ Trigger Condition ☐ Attach CSV

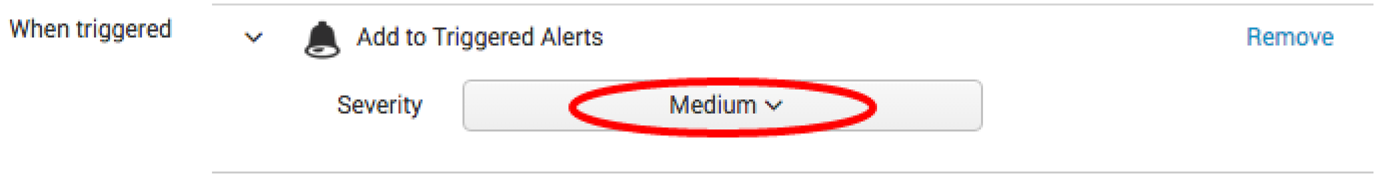
☑ Trigger Time ☐ Attach PDF

Type: [✓ HTML & Plain Text] Plain Text



Trigger Actions

+ Add Actions
Whe
Log Event
Send log event to Splunk receiver endpoint
Run a script
Invoke a custom script
Send email
Send an email notification to specified recipients
Webhook
Generic HTTP POST to a specified URL
Manage Alert Actions
Manage available actions and browse more actions

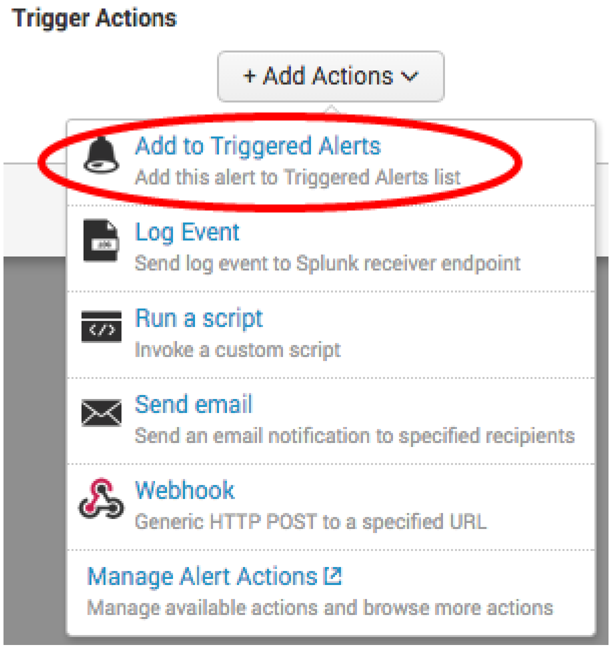


When triggered

Add to Triggered Alerts

Remove

Severity: Medium



Trigger Actions

+ Add Actions

Add to Triggered Alerts
Add this alert to Triggered Alerts list

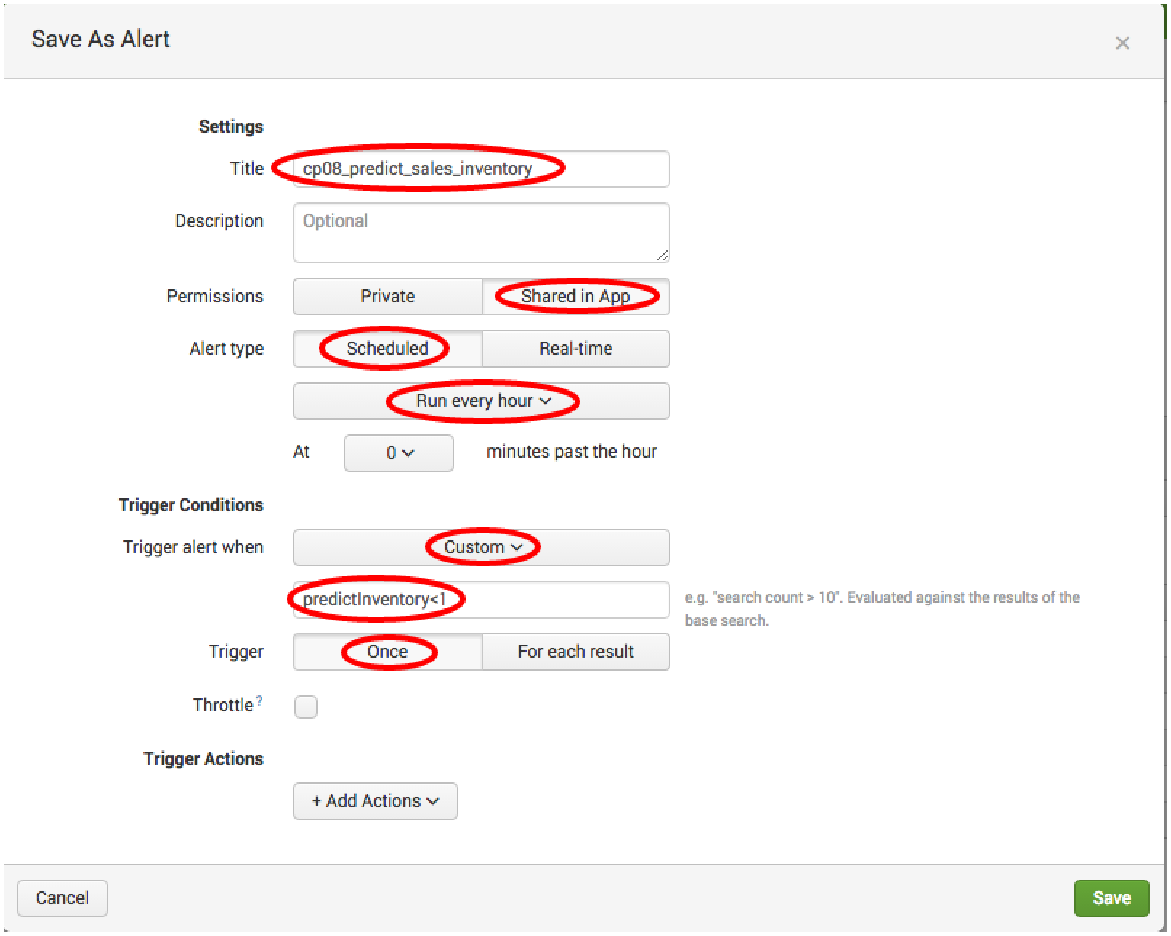
Log Event
Send log event to Splunk receiver endpoint

Run a script
Invoke a custom script

Send email
Send an email notification to specified recipients

Webhook
Generic HTTP POST to a specified URL

Manage Alert Actions
Manage available actions and browse more actions



Save As Alert

Settings

Title: cp08_predict_sales_inventory

Description: Optional

Permissions: Private [✓ Shared in App]

Alert type: [✓ Scheduled] Real-time

Run every hour

At 0 minutes past the hour

Trigger Conditions

Trigger alert when: Custom

predictInventory<1

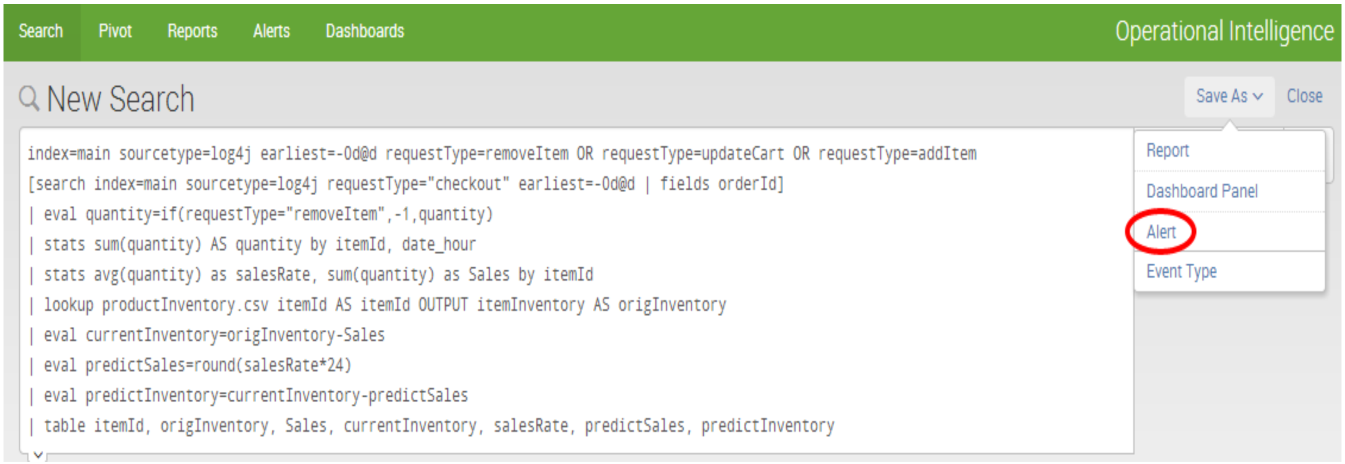
e.g. "search count > 10". Evaluated against the results of the base search.

Trigger: [✓ Once] For each result

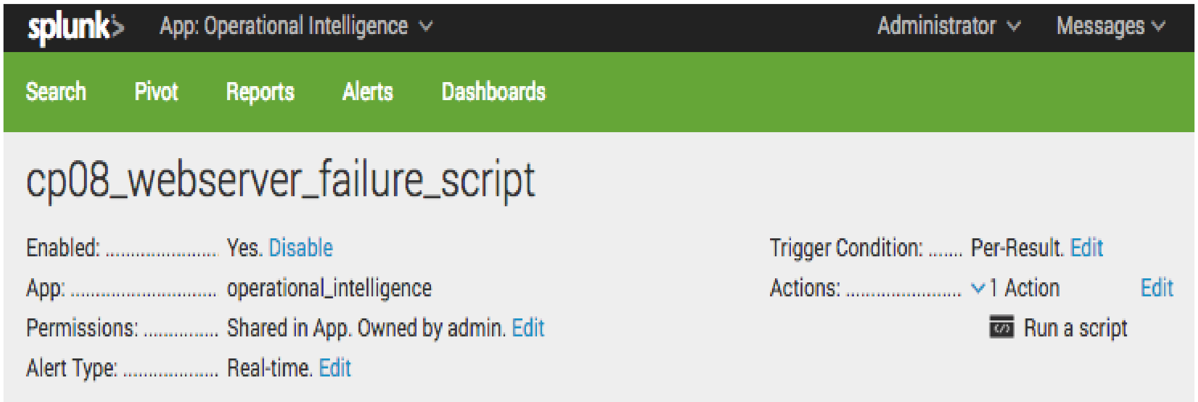
Throttle? □

Trigger Actions

+ Add Actions



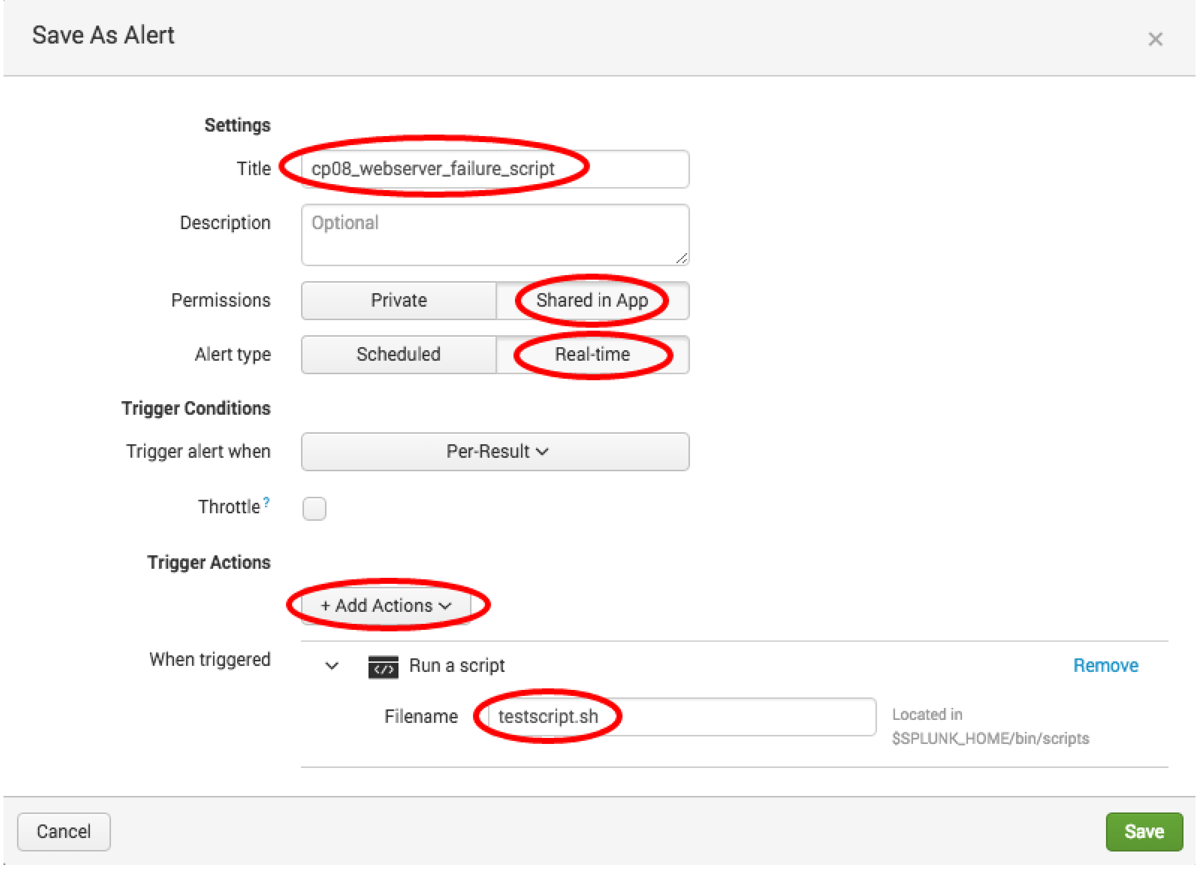
```
index=main sourcetype=log4j earliest=-0d@d requestType=removeItem OR requestType=updateCart OR requestType=addItem
[search index=main sourcetype=log4j requestType="checkout" earliest=-0d@d | fields orderId]
| eval quantity=if(requestType="removeItem",-1,quantity)
| stats sum(quantity) AS quantity by itemId, date_hour
| stats avg(quantity) as salesRate, sum(quantity) as Sales by itemId
| lookup productInventory.csv itemId AS itemId OUTPUT itemInventory AS origInventory
| eval currentInventory=origInventory-Sales
| eval predictSales=round(salesRate*24)
| eval predictInventory=currentInventory-predictSales
| table itemId, origInventory, Sales, currentInventory, salesRate, predictSales, predictInventory
```



cp08_webserver_failure_script

Enabled: .... Yes. Disable
App: .... operational_intelligence
Permissions: .... Shared in App. Owned by admin. Edit
Alert Type: .... Real-time. Edit

Trigger Condition: .... Per-Result. Edit
Actions: .... 1 Action Edit
Run a script



Save As Alert

Settings

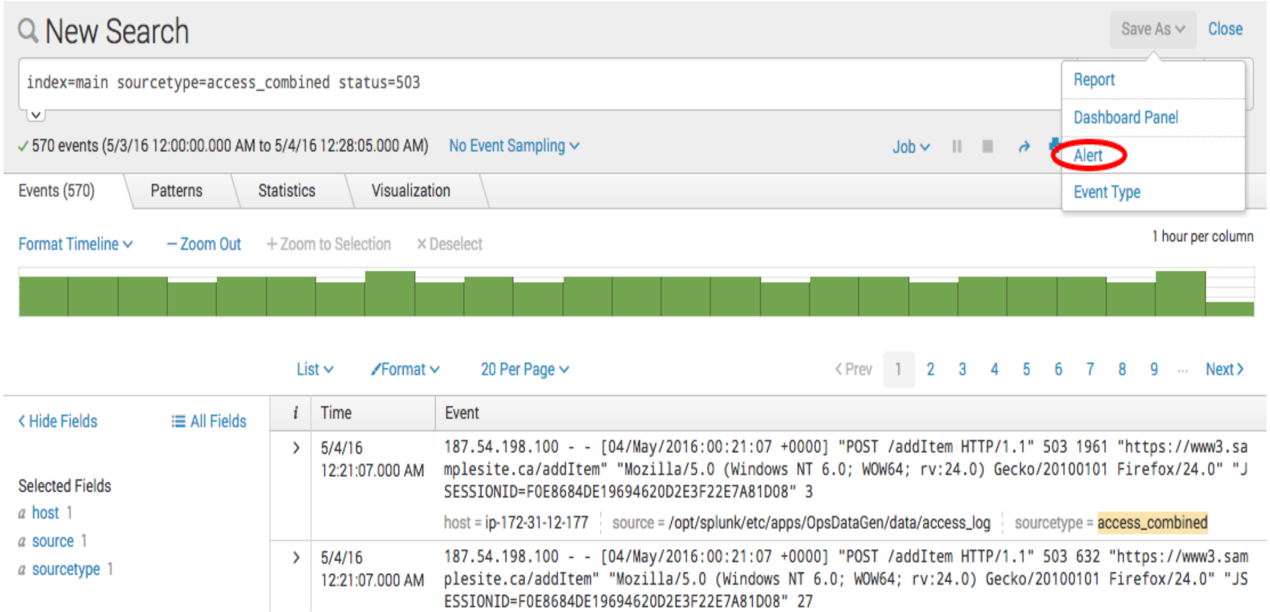
Title: cp08_webserver_failure_script
Description: Optional
Permissions: Private [✓ Shared in App]
Alert type: Scheduled [✓ Real-time]

Trigger Conditions

Trigger alert when: Per-Result
Throttle? □

Trigger Actions

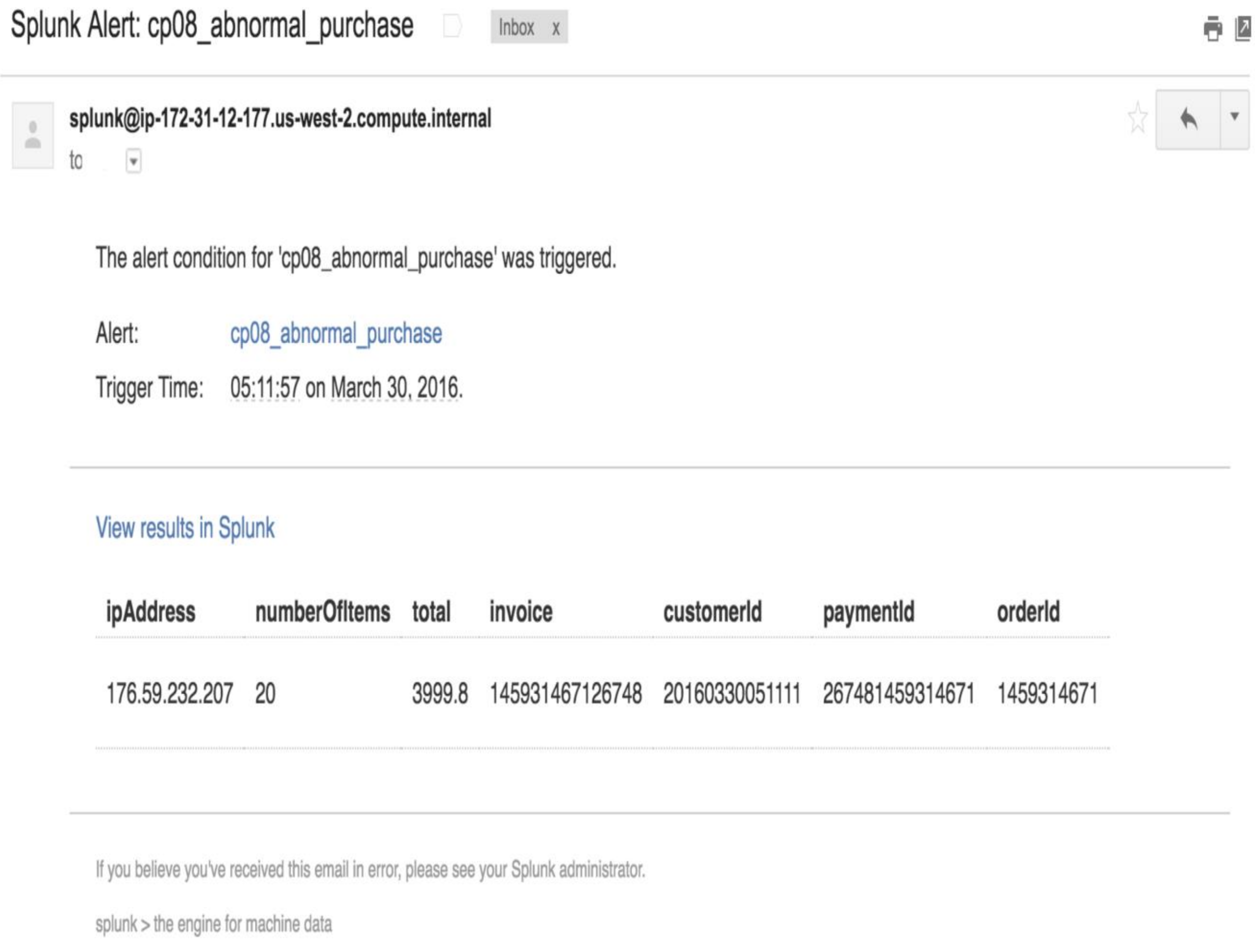
When triggered: Run a script
Filename: testscript.sh
Located in $SPLUNK_HOME/bin/scripts



```
index=main sourcetype=access_combined status=503
```

✓ 570 events (5/3/16 12:00:00.000 AM to 5/4/16 12:28:05.000 AM)

i	Time	Event
>	5/4/16 12:21:07.000 AM	187.54.198.100 - - [04/May/2016:00:21:07 +0000] "POST /addItem HTTP/1.1" 503 1961 "https://www3.samplesite.ca/addItem" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" "JSESSIONID=F0E8684DE19694620D2E3F22E7A81D08" 3 host = ip-172-31-12-177 source = /opt/splunk/etc/apps/OpsDataGen/data/access_log sourcetype = access_combined
>	5/4/16 12:21:07.000 AM	187.54.198.100 - - [04/May/2016:00:21:07 +0000] "POST /addItem HTTP/1.1" 503 632 "https://www3.samplesite.ca/addItem" "Mozilla/5.0 (Windows NT 6.0; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" "JSESSIONID=F0E8684DE19694620D2E3F22E7A81D08" 27



Splunk Alert: cp08_abnormal_purchase

splunk@ip-172-31-12-177.us-west-2.compute.internal

to

The alert condition for 'cp08_abnormal_purchase' was triggered.

Alert: cp08_abnormal_purchase

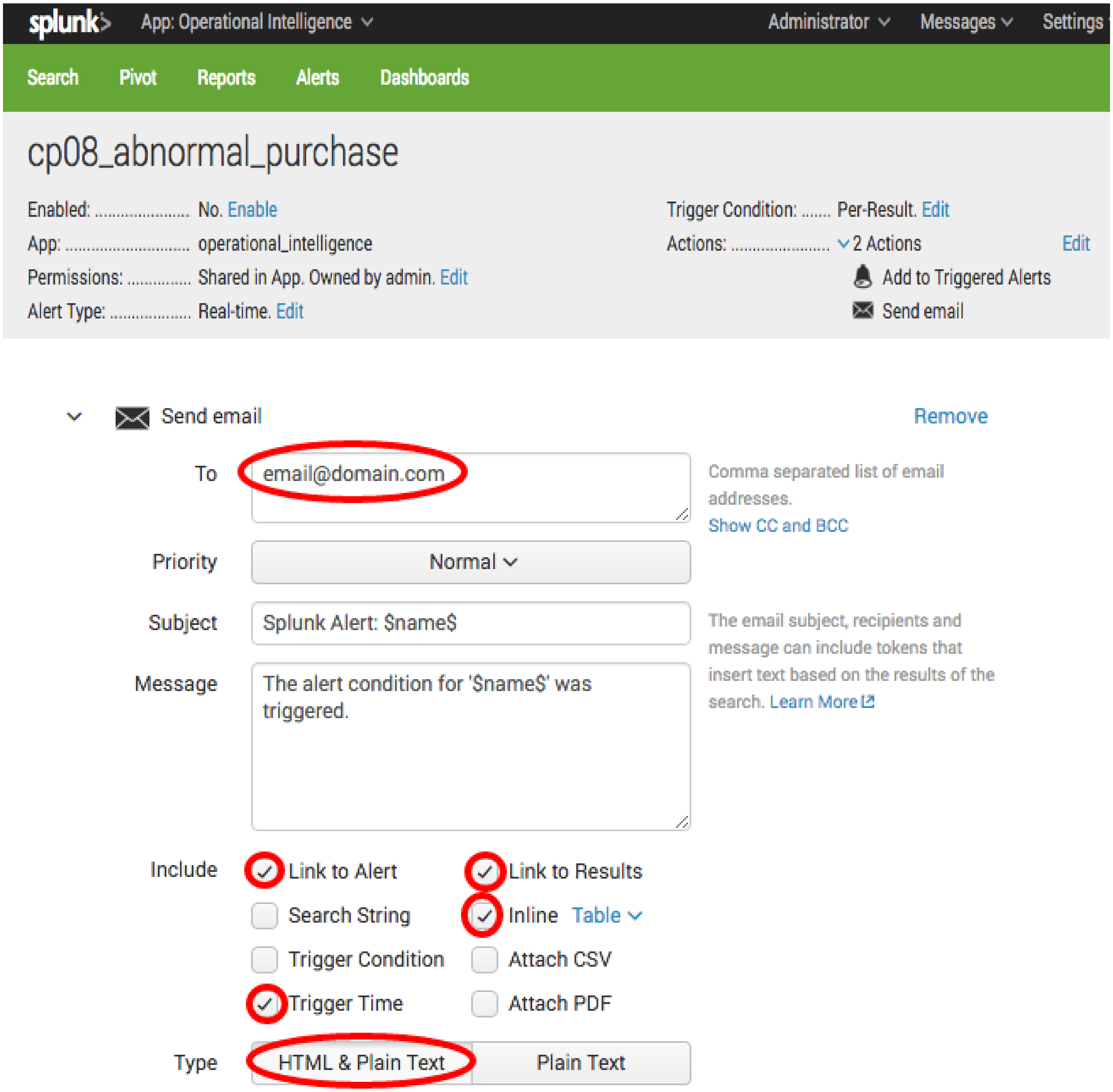
Trigger Time: 05:11:57 on March 30, 2016.

View results in Splunk

ipAddress	numberOfItems	total	invoice	customerId	paymentId	orderId
176.59.232.207	20	3999.8	145931467126748	20160330051111	267481459314671	1459314671

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data



cp08_abnormal_purchase

Enabled: .... No. Enable
App: .... operational_intelligence
Permissions: .... Shared in App. Owned by admin. Edit
Alert Type: .... Real-time. Edit

Trigger Condition: .... Per-Result. Edit
Actions: .... 2 Actions Edit
Add to Triggered Alerts
Send email

Send email Remove

To: email@domain.com

Comma separated list of email addresses.
Show CC and BCC

Priority: Normal

Subject: Splunk Alert: $name$

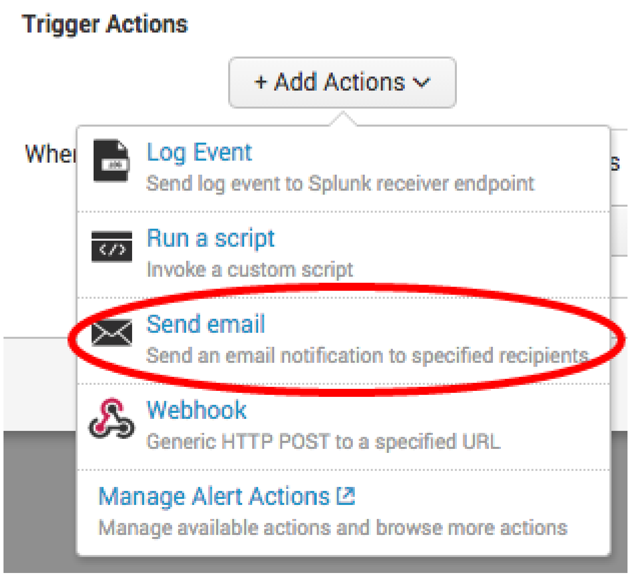
Message: The alert condition for '$name$' was triggered.

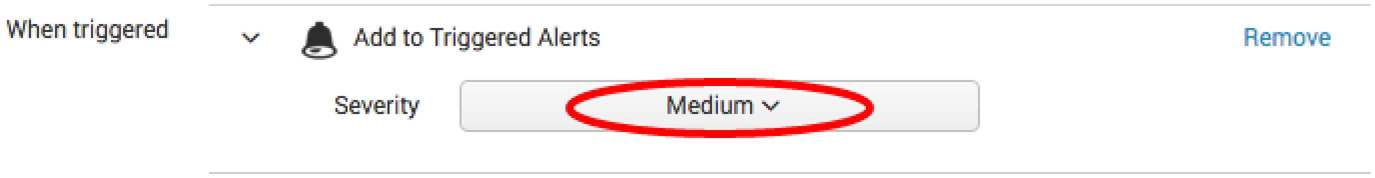
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Include:

☑ Link to Alert ☑ Link to Results
□ Search String ☑ Inline Table
□ Trigger Condition □ Attach CSV
☑ Trigger Time □ Attach PDF

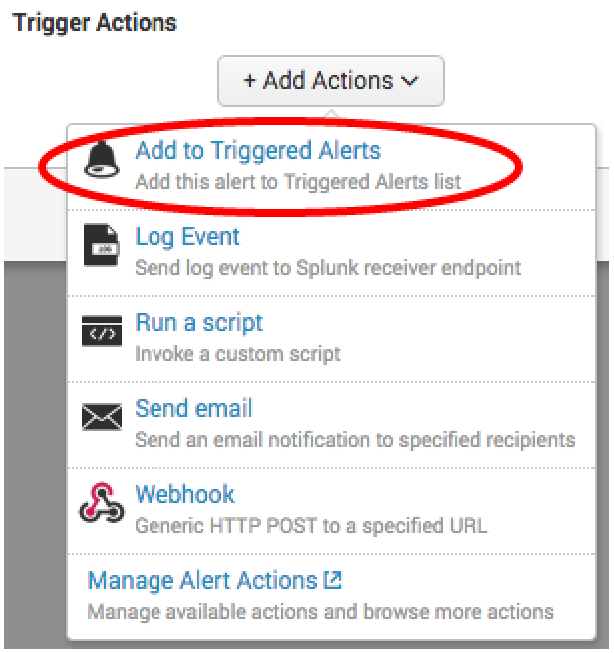
Type: [✓ HTML & Plain Text] Plain Text

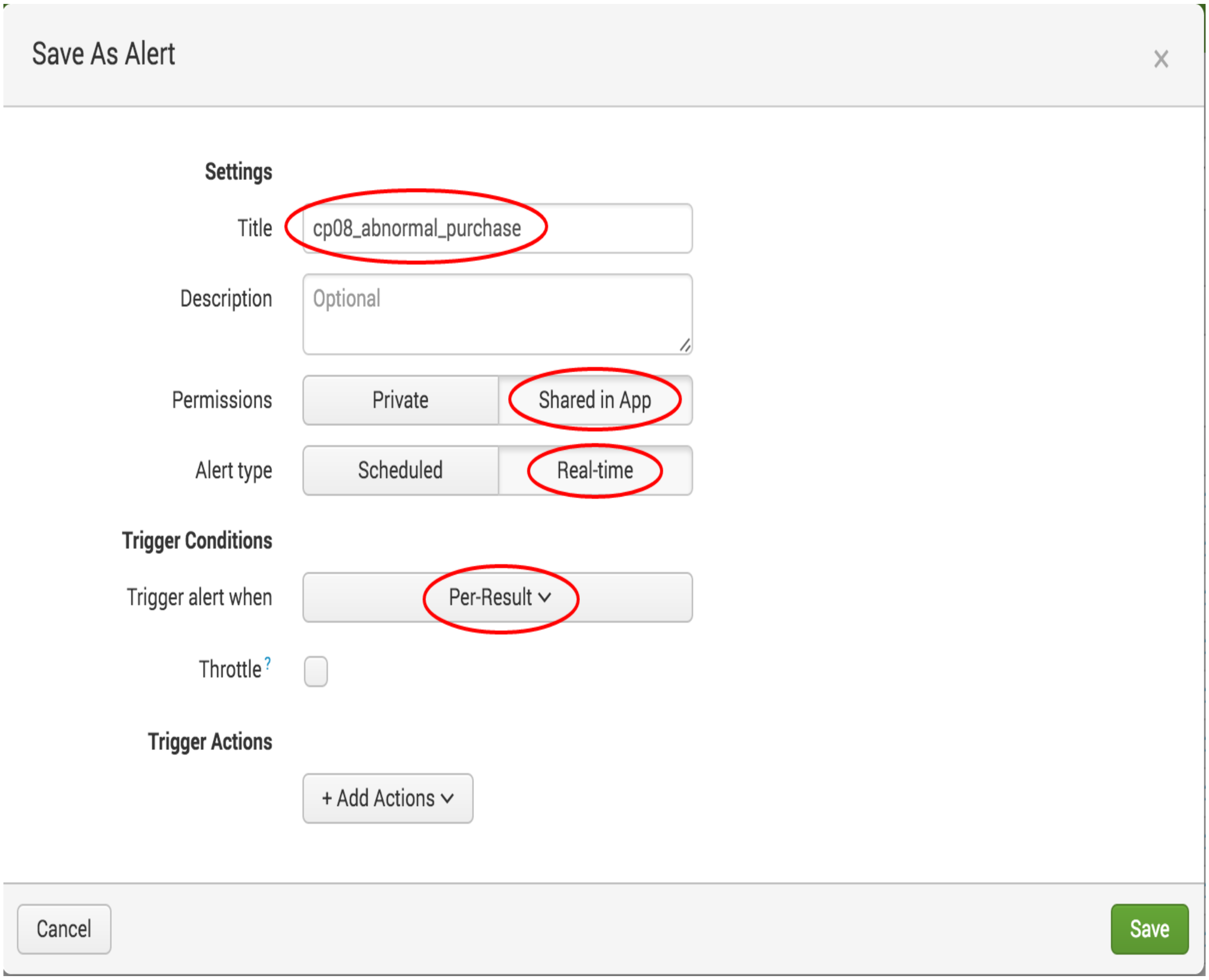

Trigger Actions
+ Add Actions
Whe
s
Log Event
Send log event to Splunk receiver endpoint
Run a script
Invoke a custom script
Send email
Send an email notification to specified recipients
Webhook
Generic HTTP POST to a specified URL
Manage Alert Actions
Manage available actions and browse more actions


When triggered

Add to Triggered Alerts

Severity: Medium


Trigger Actions
+ Add Actions
Add to Triggered Alerts
Add this alert to Triggered Alerts list
Log Event
Send log event to Splunk receiver endpoint
Run a script
Invoke a custom script
Send email
Send an email notification to specified recipients
Webhook
Generic HTTP POST to a specified URL
Manage Alert Actions
Manage available actions and browse more actions



Save As Alert ×

Settings

Title: cp08_abnormal_purchase

Description: Optional

Permissions: Private [✓ Shared in App]

Alert type: Scheduled [✓ Real-time]

Trigger Conditions

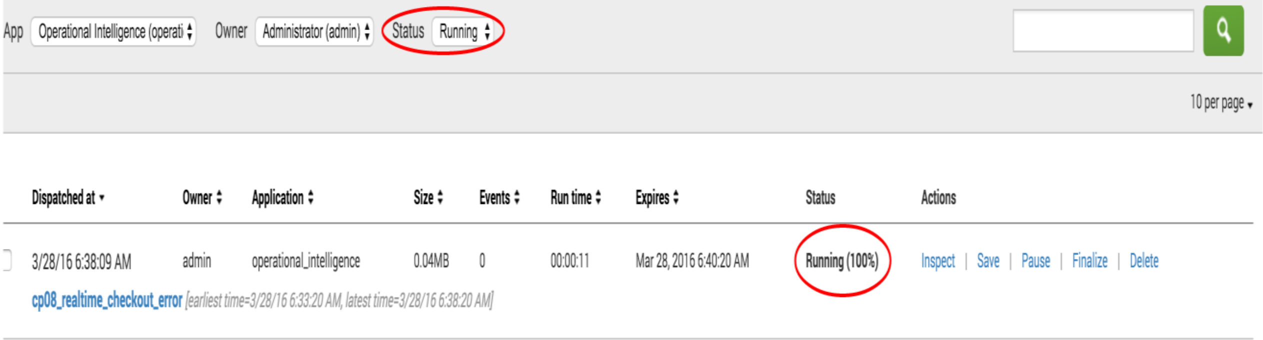
Trigger alert when: [✓ Per-Result]

Throttle? □

Trigger Actions

+ Add Actions

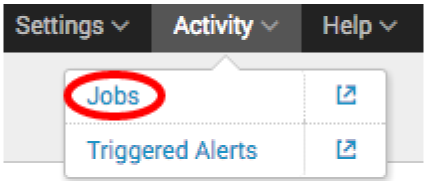
Cancel   Save

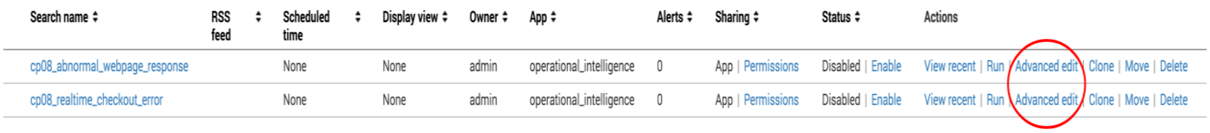


App: Operational Intelligence (operati   Owner: Administrator (admin)   Status: [✓ Running]

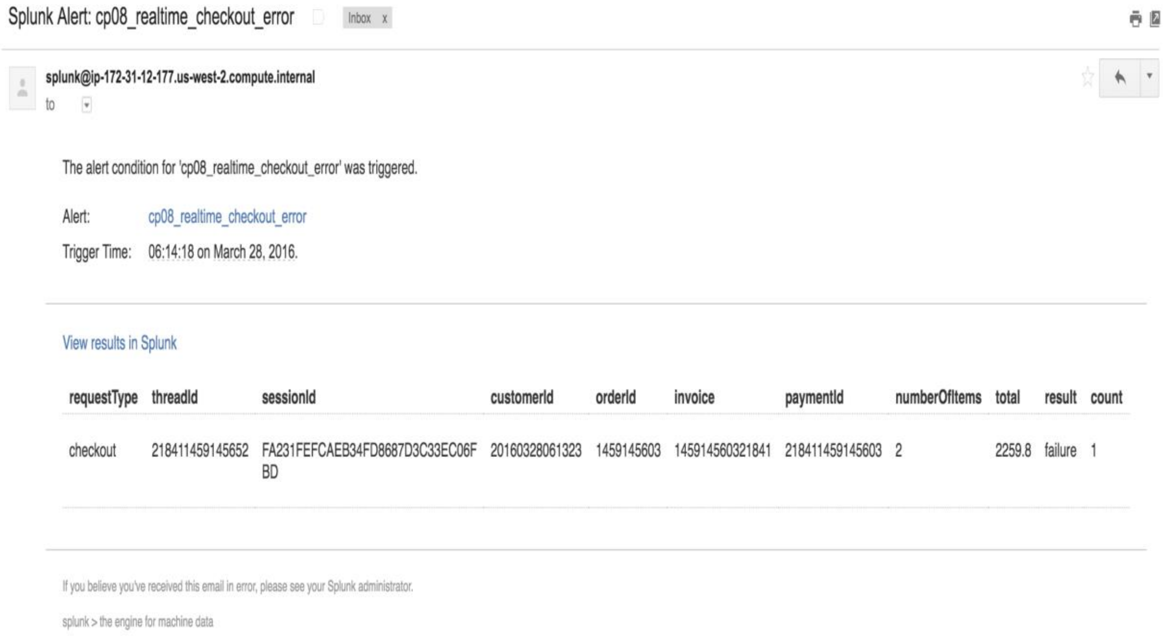
10 per page

	Dispatched at	Owner	Application	Size	Events	Run time	Expires	Status	Actions
□	3/28/16 6:38:09 AM cp08_realtime_checkout_error *[earliest time=3/28/16 6:33:20 AM, latest time=3/28/16 6:38:20 AM]*	admin	operational_intelligence	0.04MB	0	00:00:11	Mar 28, 2016 6:40:20 AM	[✓ Running (100%)]	Inspect | Save | Pause | Finalize | Delete





Search name ⇕	RSS feed ⇕	Scheduled time ⇕	Display view ⇕	Owner ⇕	App ⇕	Alerts ⇕	Sharing ⇕	Status ⇕	Actions
cp08_abnormal_webpage_response		None	None	admin	operational_intelligence	0	App | Permissions	Disabled | Enable	View recent | Run | Advanced edit | Clone | Move | Delete
cp08_realtime_checkout_error		None	None	admin	operational_intelligence	0	App | Permissions	Disabled | Enable	View recent | Run | Advanced edit | Clone | Move | Delete



Splunk Alert: cp08_realtime_checkout_error Inbox x

splunk@ip-172-31-12-177.us-west-2.compute.internal
to

The alert condition for 'cp08_realtime_checkout_error' was triggered.

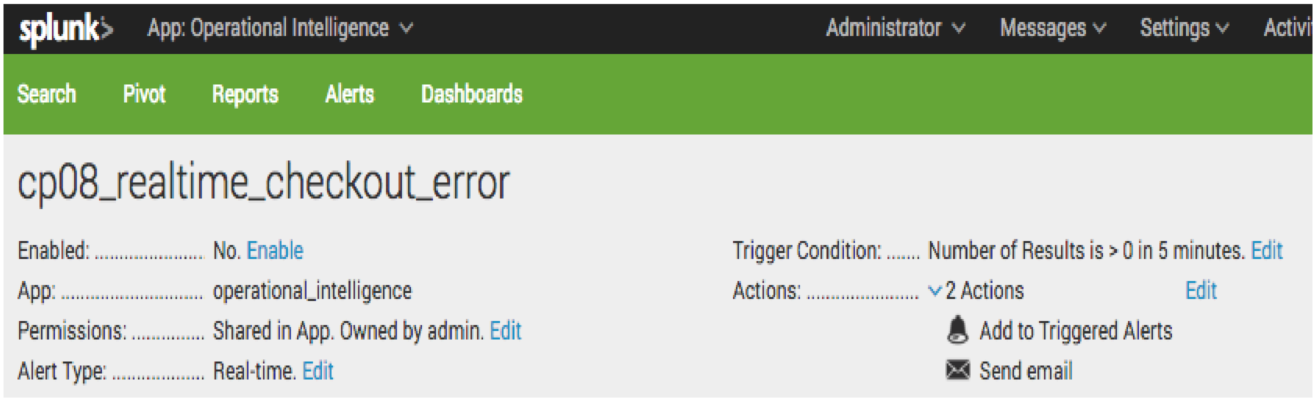
Alert: cp08_realtime_checkout_error
Trigger Time: 06:14:18 on March 28, 2016.

View results in Splunk

requestType	threadId	sessionId	customerId	orderId	invoice	paymentId	numberOfItems	total	result	count
checkout	218411459145652	FA231FEFCAEB34FD8687D3C33EC06FBD	20160328061323	1459145603	145914560321841	218411459145603	2	2259.8	failure	1

If you believe you've received this email in error, please see your Splunk administrator.

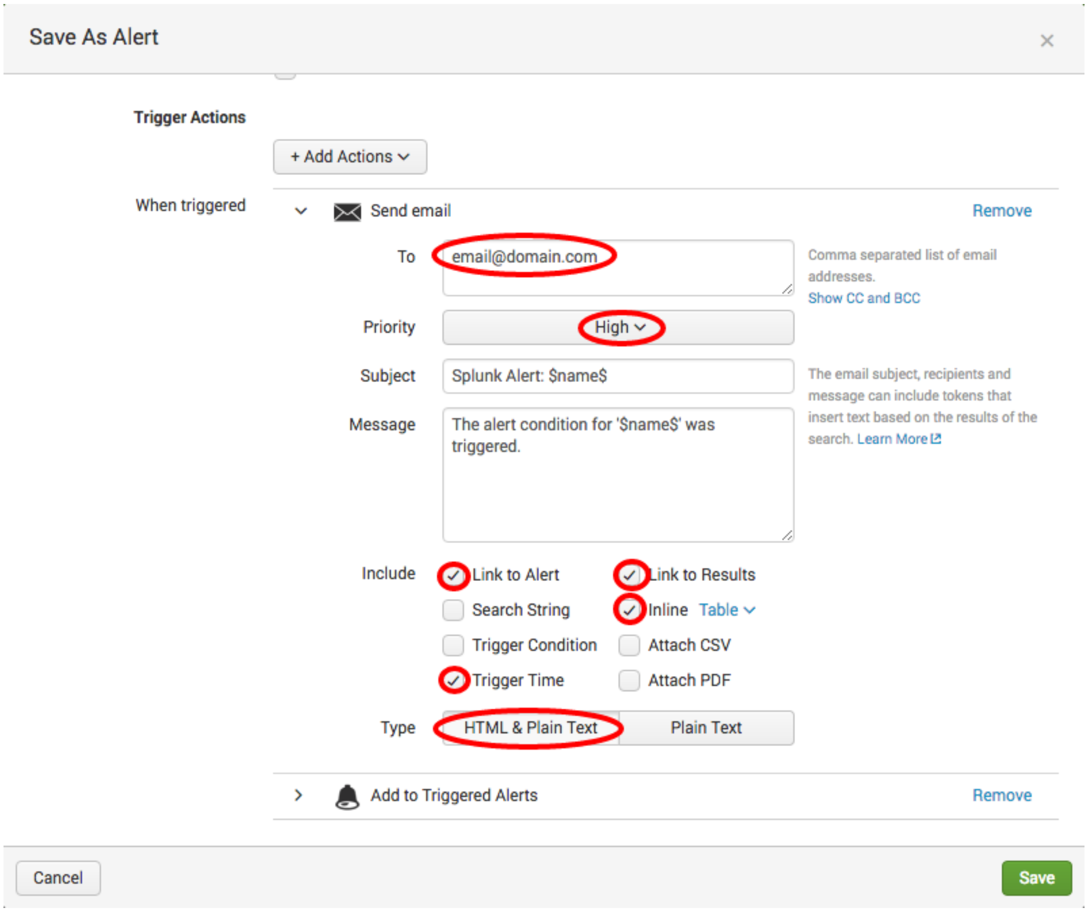
splunk > the engine for machine data



cp08_realtime_checkout_error

Enabled: .... No. Enable
App: .... operational_intelligence
Permissions: .... Shared in App. Owned by admin. Edit
Alert Type: .... Real-time. Edit

Trigger Condition: .... Number of Results is > 0 in 5 minutes. Edit
Actions: .... 2 Actions Edit
Add to Triggered Alerts
Send email



Save As Alert

Trigger Actions

+ Add Actions

When triggered

Send email

To: email@domain.com

Comma separated list of email addresses.
Show CC and BCC

Priority: High

Subject: Splunk Alert: $name$

Message: The alert condition for '$name$' was triggered.

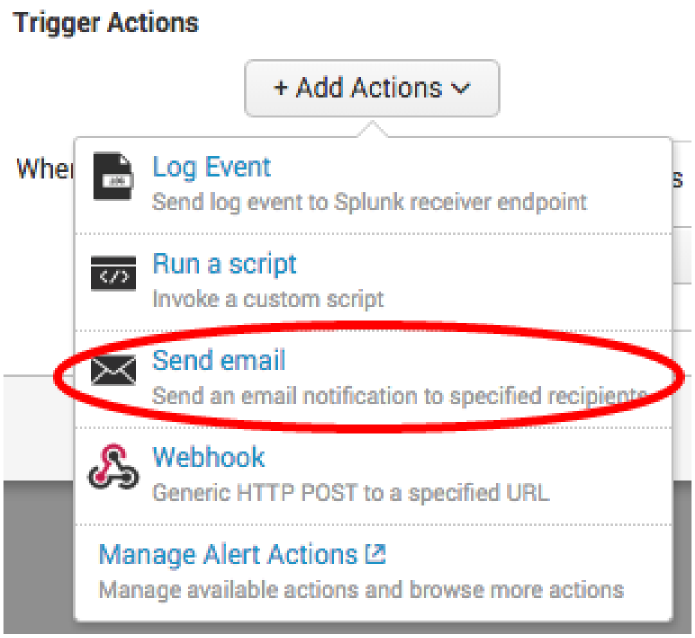
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Include:

☑ Link to Alert ☑ Link to Results
☐ Search String ☑ Inline Table
☐ Trigger Condition ☐ Attach CSV
☑ Trigger Time ☐ Attach PDF

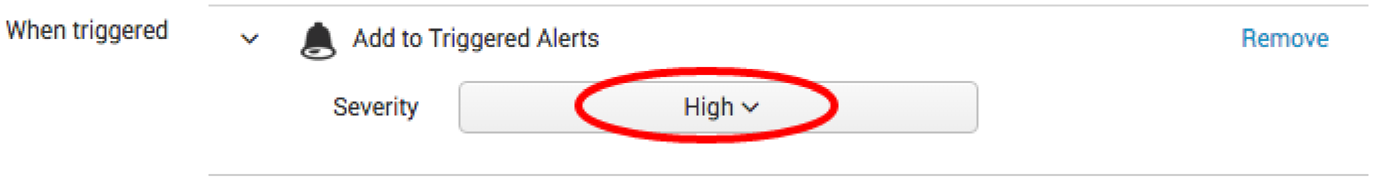
Type: [✓ HTML & Plain Text] Plain Text

Remove
Add to Triggered Alerts
Remove
Cancel
Save



Trigger Actions

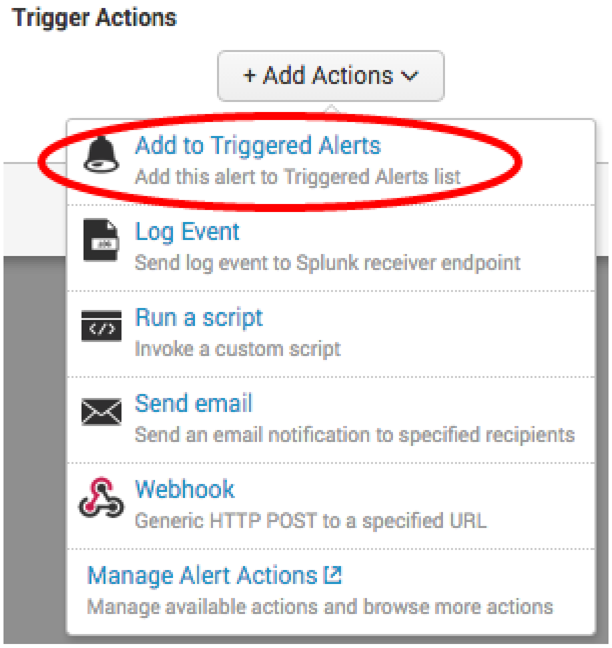
+ Add Actions
Log Event
Send log event to Splunk receiver endpoint
Run a script
Invoke a custom script
Send email
Send an email notification to specified recipients
Webhook
Generic HTTP POST to a specified URL
Manage Alert Actions
Manage available actions and browse more actions



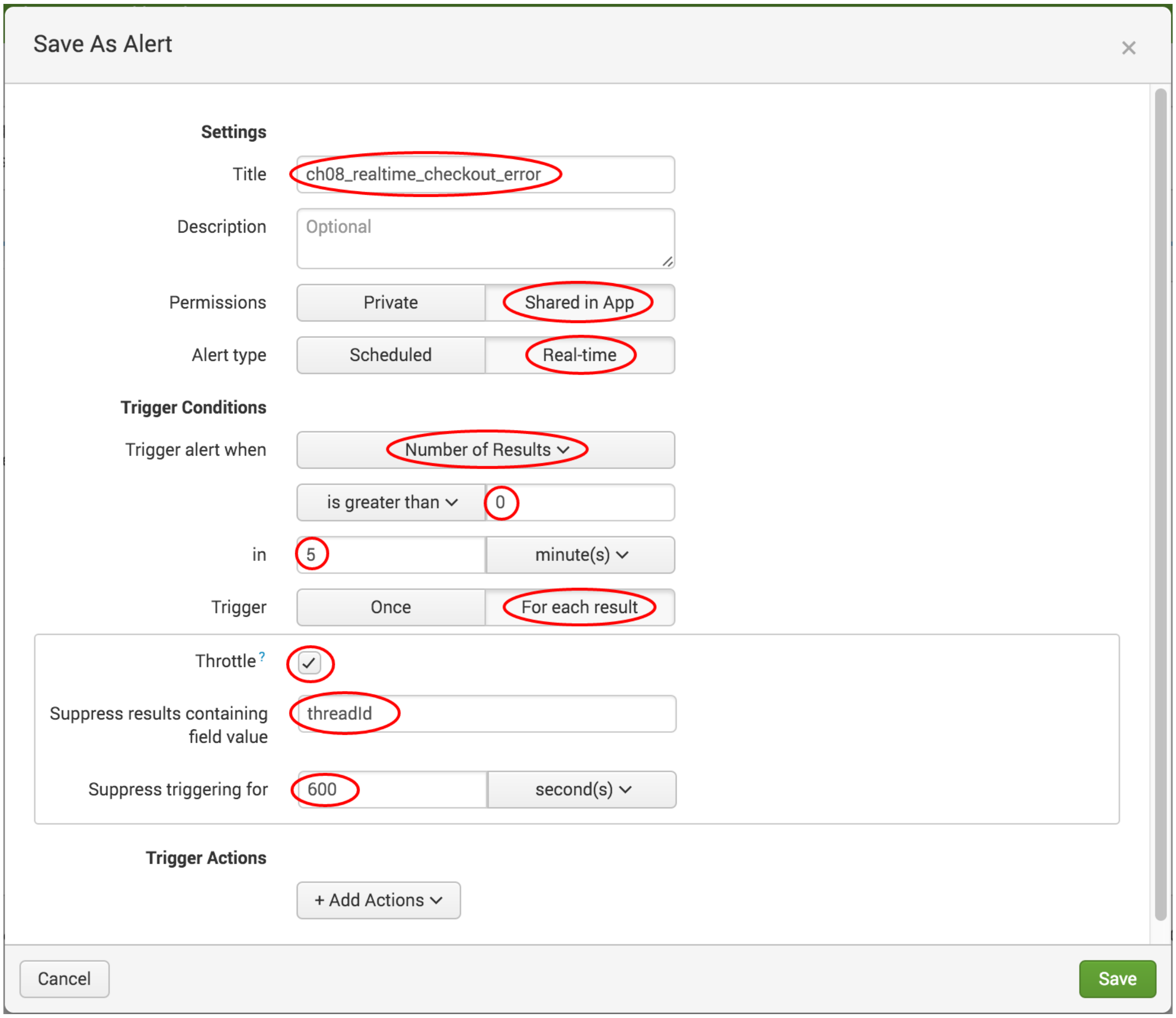
When triggered

Add to Triggered Alerts

Severity: High



Trigger Actions
+ Add Actions
Add to Triggered Alerts
Add this alert to Triggered Alerts list
Log Event
Send log event to Splunk receiver endpoint
Run a script
Invoke a custom script
Send email
Send an email notification to specified recipients
Webhook
Generic HTTP POST to a specified URL
Manage Alert Actions
Manage available actions and browse more actions



Save As Alert

Settings

Title: ch08_realtime_checkout_error

Description: Optional

Permissions: Private [✓ Shared in App]

Alert type: Scheduled [✓ Real-time]

Trigger Conditions

Trigger alert when: Number of Results

is greater than 0

in 5 minute(s)

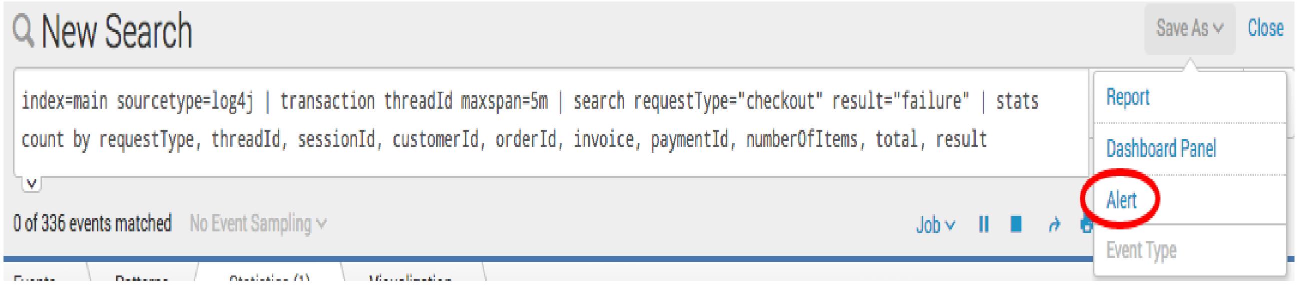
Trigger: Once [✓ For each result]

Throttle ☑

Suppress results containing field value: threadId

Suppress triggering for: 600 second(s)

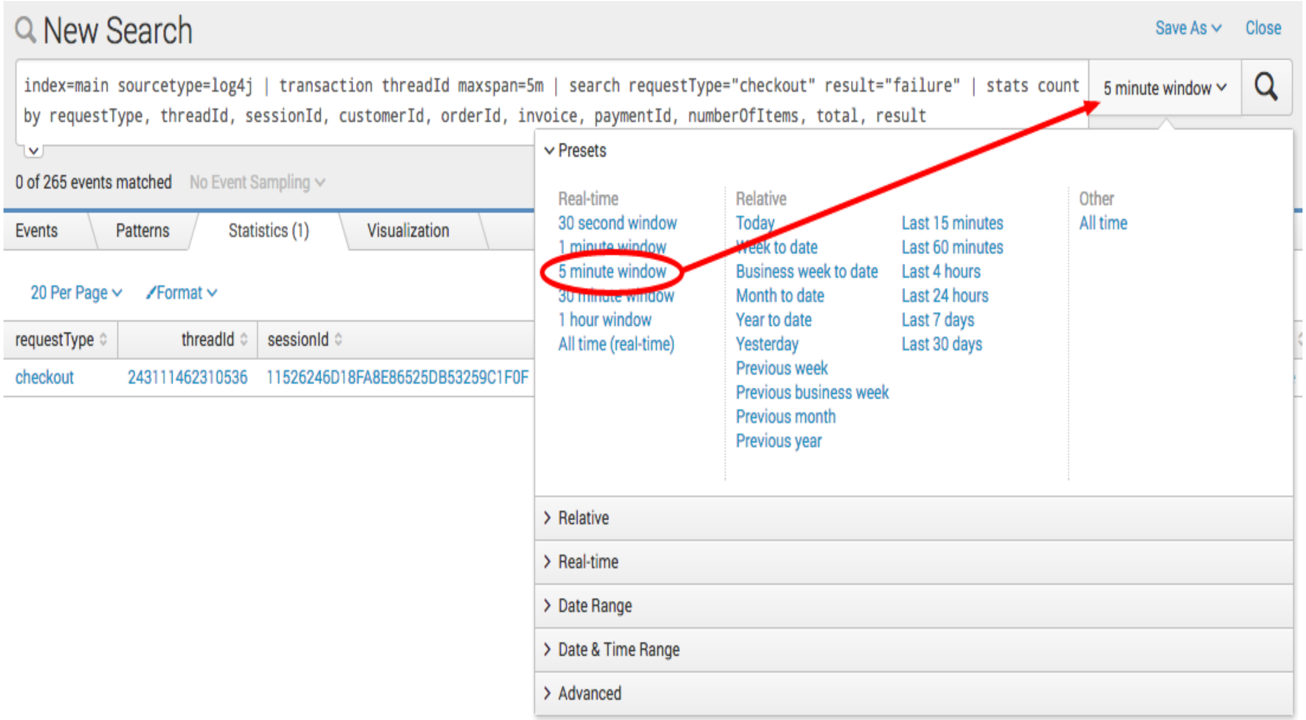
Trigger Actions



New Search

```
index=main sourcetype=log4j | transaction threadId maxspan=5m | search requestType="checkout" result="failure" | stats
count by requestType, threadId, sessionId, customerId, orderId, invoice, paymentId, numberOfItems, total, result
```

0 of 336 events matched



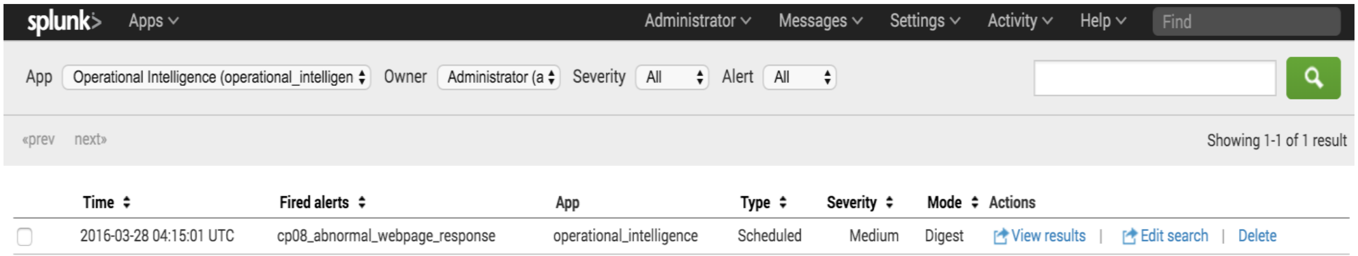
New Search

```
index=main sourcetype=log4j | transaction threadId maxspan=5m | search requestType="checkout" result="failure" | stats count
by requestType, threadId, sessionId, customerId, orderId, invoice, paymentId, numberOfItems, total, result
```

5 minute window

0 of 265 events matched

requestType	threadId	sessionId
checkout	243111462310536	11526246D18FA8E86525DB53259C1F0F

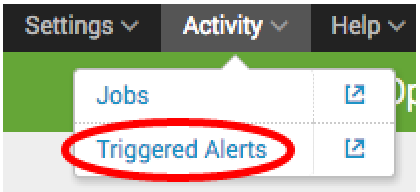


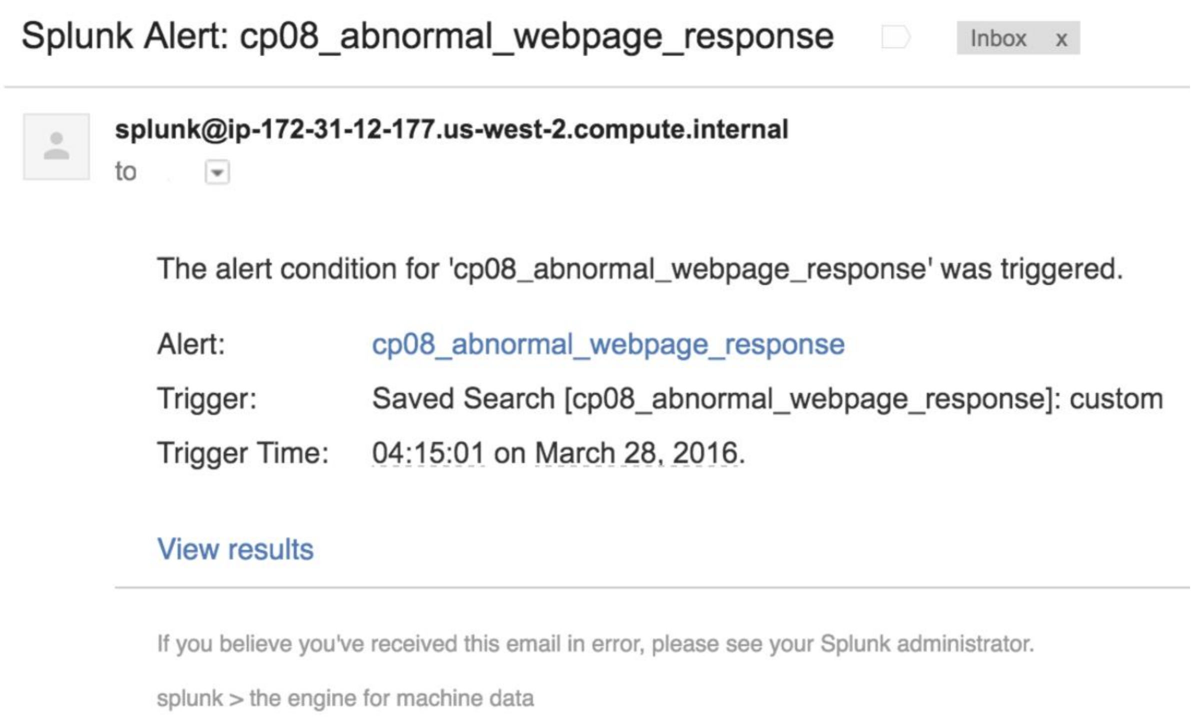
App: Operational Intelligence (operational_intelligen | Owner: Administrator (a | Severity: All | Alert: All

«prev next»

Showing 1-1 of 1 result

	Time	Fired alerts	App	Type	Severity	Mode	Actions
□	2016-03-28 04:15:01 UTC	cp08_abnormal_webpage_response	operational_intelligence	Scheduled	Medium	Digest	View results | Edit search | Delete





Splunk Alert: cp08_abnormal_webpage_response

splunk@ip-172-31-12-177.us-west-2.compute.internal

to

The alert condition for 'cp08_abnormal_webpage_response' was triggered.

Alert: cp08_abnormal_webpage_response

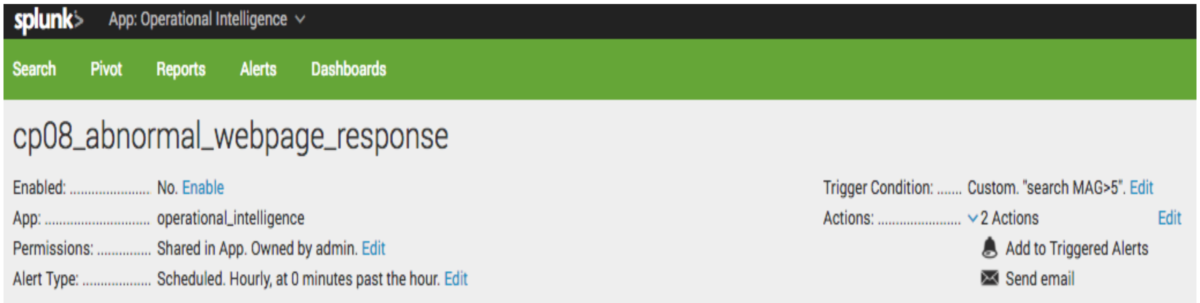
Trigger: Saved Search [cp08_abnormal_webpage_response]: custom

Trigger Time: 04:15:01 on March 28, 2016.

View results

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data



cp08_abnormal_webpage_response

Enabled: .... No. Enable

App: .... operational_intelligence

Permissions: .... Shared in App. Owned by admin. Edit

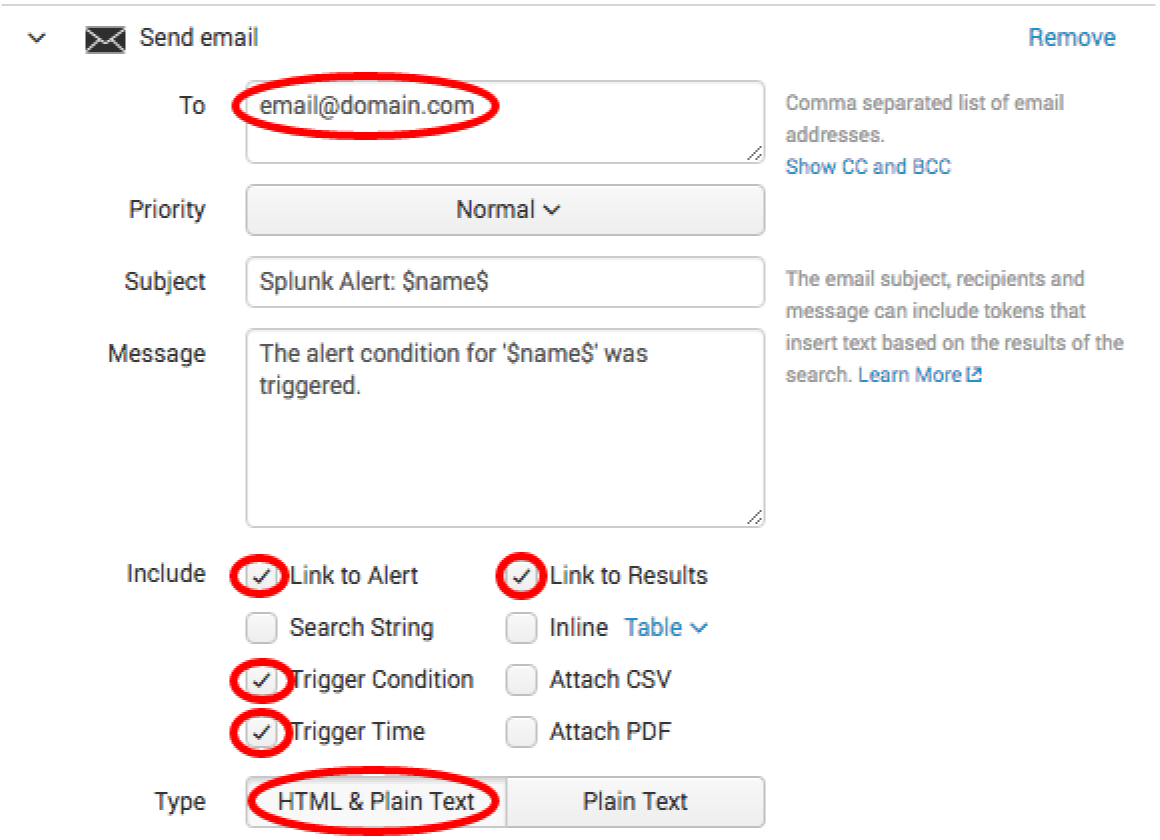
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .... Custom. "search MAG>5". Edit

Actions: .... 2 Actions Edit

Add to Triggered Alerts

Send email



Send email Remove

To: email@domain.com

Comma separated list of email addresses.
Show CC and BCC

Priority: Normal

Subject: Splunk Alert: $name$

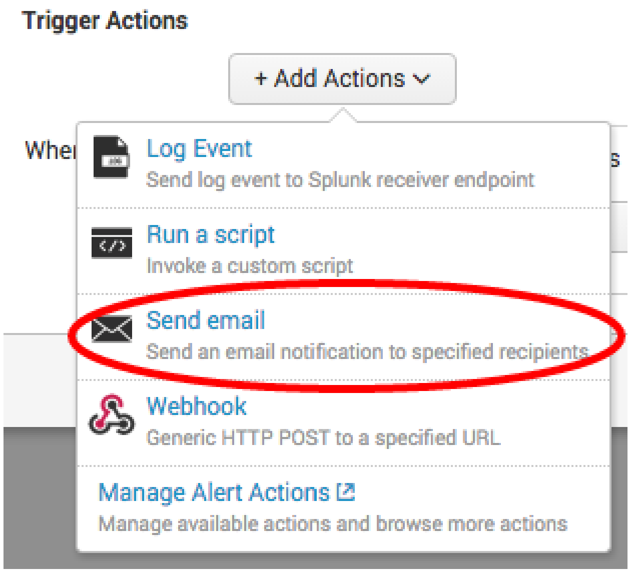
Message: The alert condition for '$name$' was triggered.

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Include:

- ☑ Link to Alert
- ☑ Link to Results
- □ Search String
- □ Inline Table
- ☑ Trigger Condition
- □ Attach CSV
- ☑ Trigger Time
- □ Attach PDF

Type: [✓ HTML & Plain Text] Plain Text

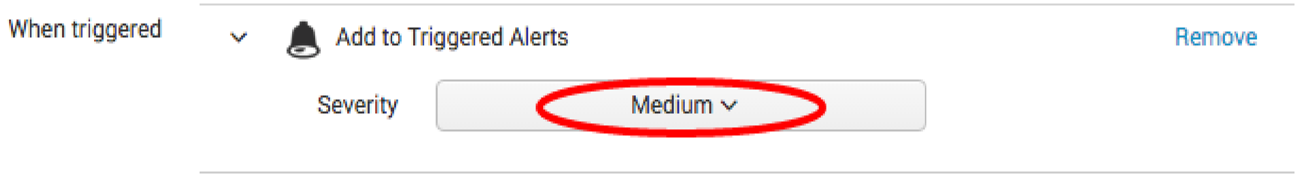


Trigger Actions

+ Add Actions

Whe

- Log Event
  Send log event to Splunk receiver endpoint
- Run a script
  Invoke a custom script
- [✓ Send email
  Send an email notification to specified recipients]
- Webhook
  Generic HTTP POST to a specified URL
- Manage Alert Actions
  Manage available actions and browse more actions

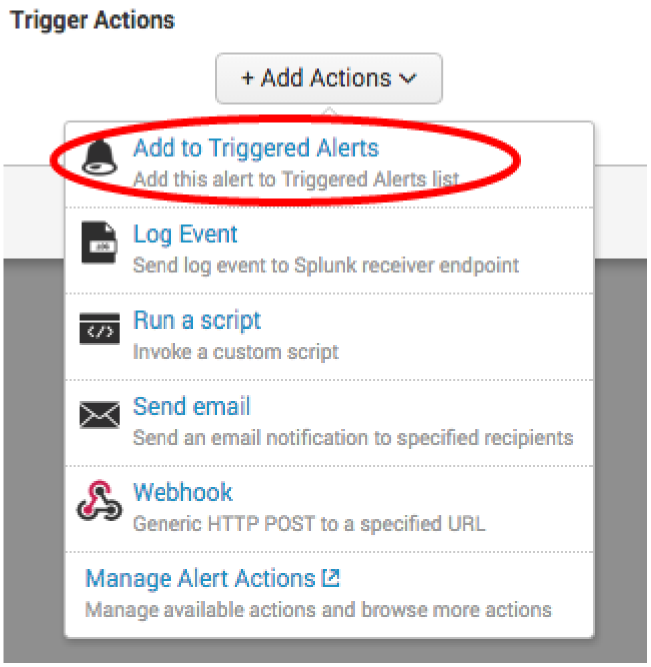


When triggered

Add to Triggered Alerts

Remove

Severity [✓ Medium]



Trigger Actions

+ Add Actions

[✓ Add to Triggered Alerts]
Add this alert to Triggered Alerts list

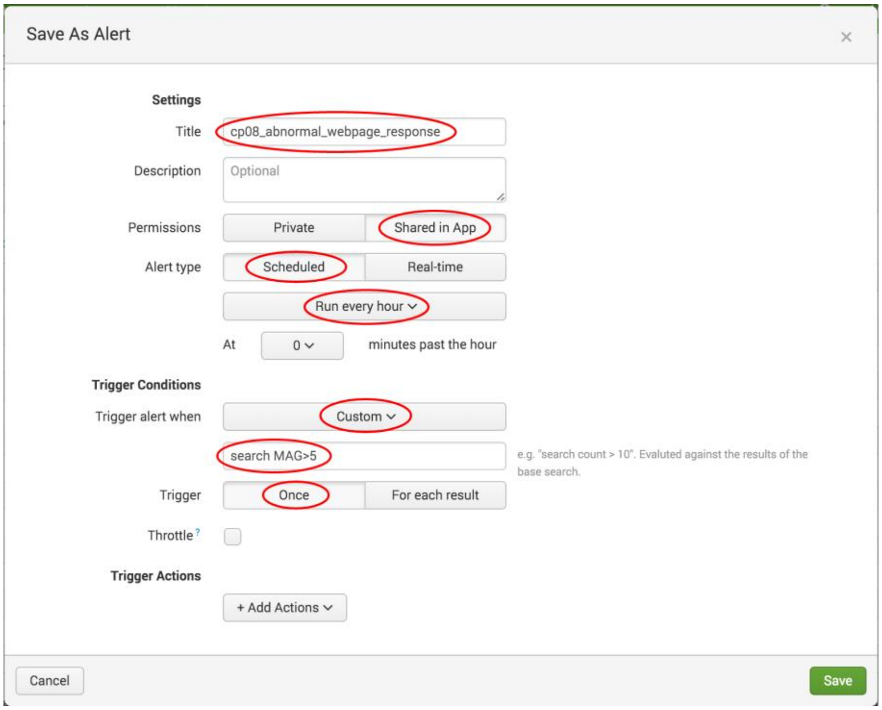
Log Event
Send log event to Splunk receiver endpoint

Run a script
Invoke a custom script

Send email
Send an email notification to specified recipients

Webhook
Generic HTTP POST to a specified URL

Manage Alert Actions
Manage available actions and browse more actions



Save As Alert

Settings

Title: cp08_abnormal_webpage_response

Description: Optional

Permissions: Private [✓ Shared in App]

Alert type: [✓ Scheduled] Real-time

Run every hour

At 0 minutes past the hour

Trigger Conditions

Trigger alert when: Custom

search MAG>5

e.g. "search count > 10". Evaluated against the results of the base search.

Trigger: [✓ Once] For each result

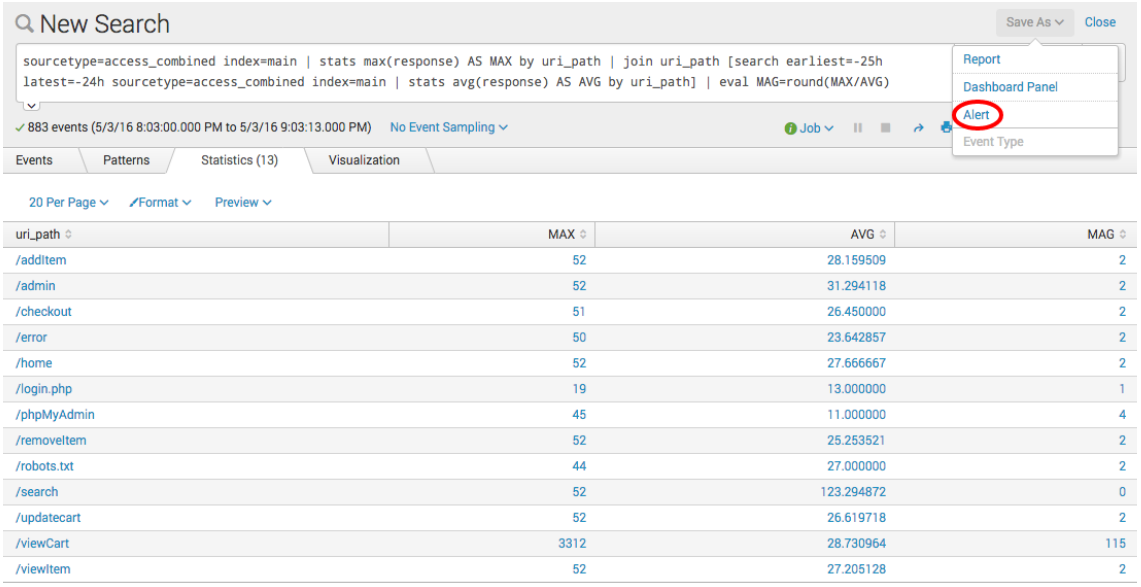
Throttle ? □

Trigger Actions

+ Add Actions

Cancel

Save



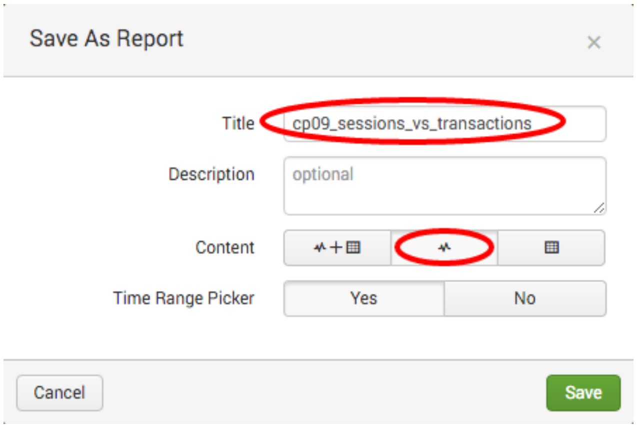
```
sourcetype=access_combined index=main | stats max(response) AS MAX by uri_path | join uri_path [search earliest=-25h
latest=-24h sourcetype=access_combined index=main | stats avg(response) AS AVG by uri_path] | eval MAG=round(MAX/AVG)
```

✓ 883 events (5/3/16 8:03:00.000 PM to 5/3/16 9:03:13.000 PM)

uri_path	MAX	AVG	MAG
/addItem	52	28.159509	2
/admin	52	31.294118	2
/checkout	51	26.450000	2
/error	50	23.642857	2
/home	52	27.666667	2
/login.php	19	13.000000	1
/phpMyAdmin	45	11.000000	4
/removeItem	52	25.253521	2
/robots.txt	44	27.000000	2
/search	52	123.294872	0
/updatecart	52	26.619718	2
/viewCart	3312	28.730964	115
/viewItem	52	27.205128	2

Graphics.zip

Chapter 9: Chapter 9: Speeding Up Intelligence – Data Summarization



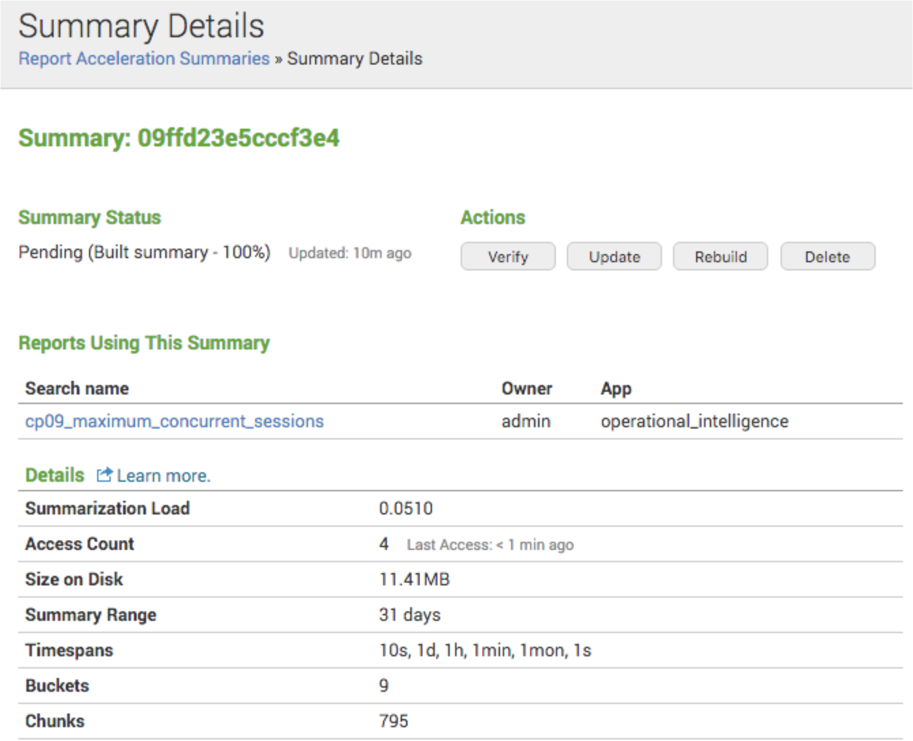
Save As Report

Title: cp09_sessions_vs_transactions

Description: optional

Content: ⩘+▦ | [✓ ⩘] | ▦

Time Range Picker: Yes | No



Summary Details

Report Acceleration Summaries » Summary Details

Summary: 09ffd23e5cccf3e4

Summary Status

Pending (Built summary - 100%) Updated: 10m ago

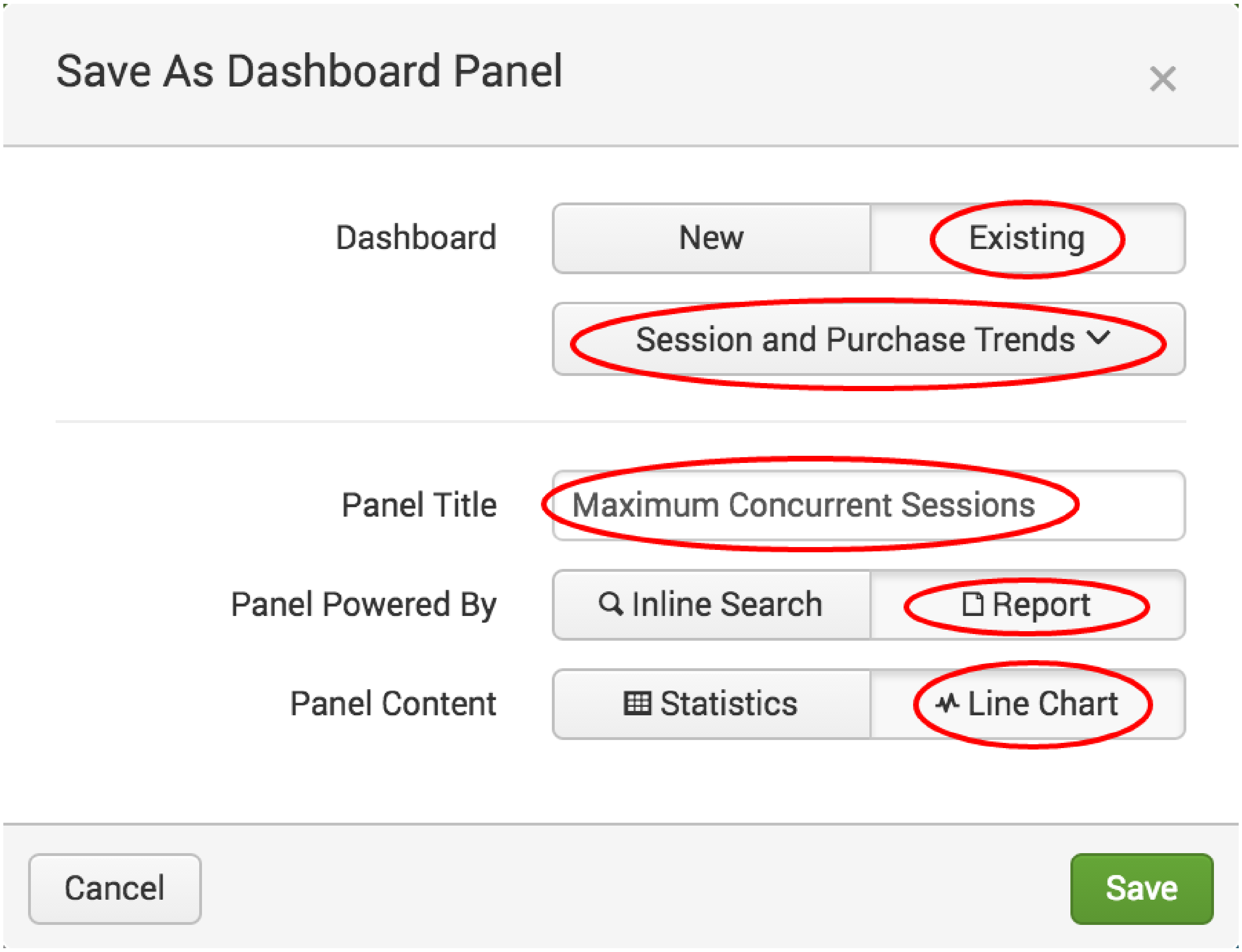
Actions

Reports Using This Summary

Search name	Owner	App
cp09_maximum_concurrent_sessions	admin	operational_intelligence

Details Learn more.

Summarization Load	0.0510
Access Count	4 Last Access: < 1 min ago
Size on Disk	11.41MB
Summary Range	31 days
Timespans	10s, 1d, 1h, 1min, 1mon, 1s
Buckets	9
Chunks	795



Save As Dashboard Panel

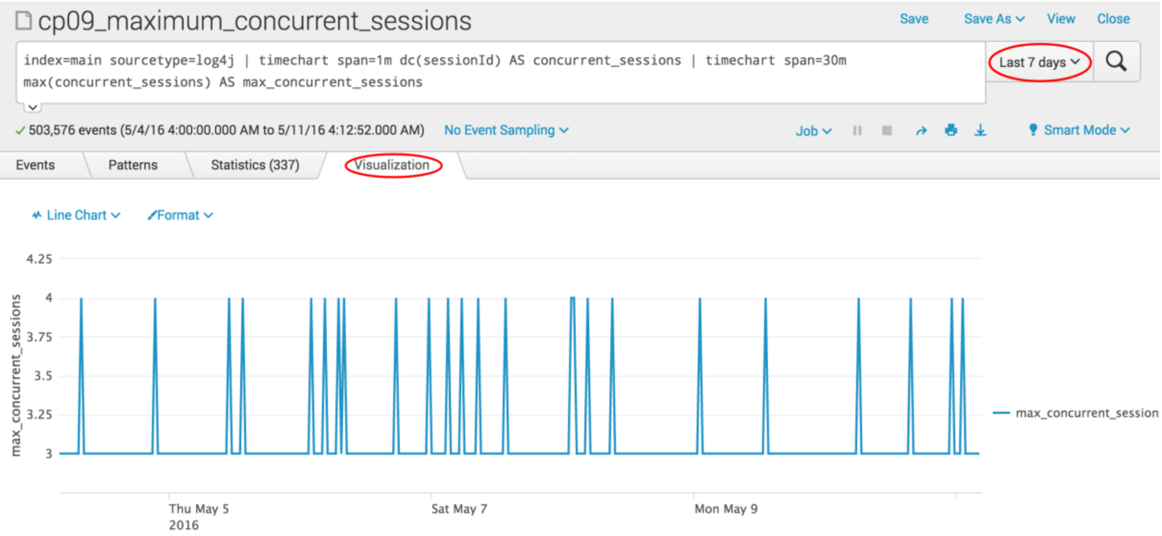
Dashboard New [✓ Existing]

[✓ Session and Purchase Trends]

Panel Title [✓ Maximum Concurrent Sessions]

Panel Powered By Inline Search [✓ Report]

Panel Content Statistics [✓ Line Chart]



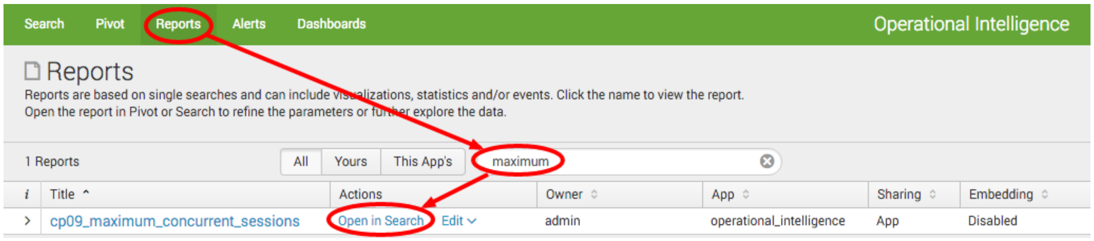
cp09_maximum_concurrent_sessions

```
index=main sourcetype=log4j | timechart span=1m dc(sessionId) AS concurrent_sessions | timechart span=30m
max(concurrent_sessions) AS max_concurrent_sessions
```

[✓ Last 7 days]

✓ 503,576 events (5/4/16 4:00:00.000 AM to 5/11/16 4:12:52.000 AM) No Event Sampling

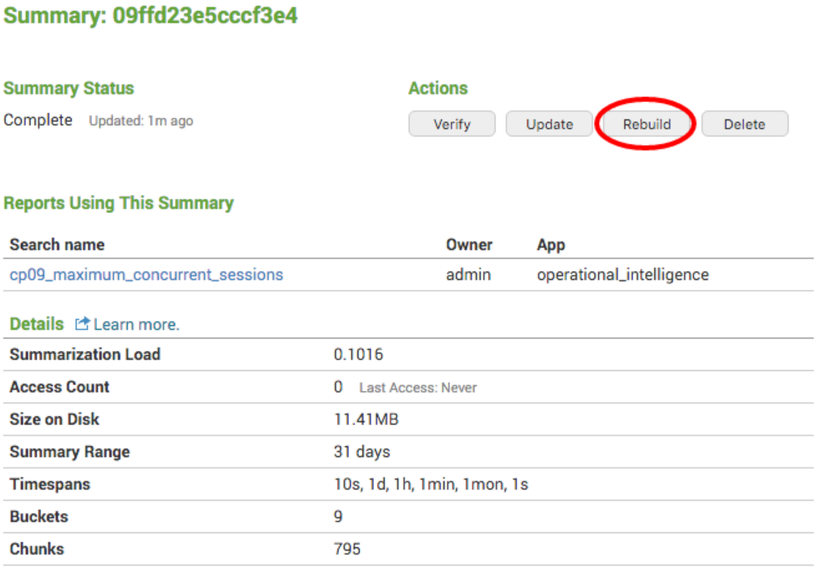
Events Patterns Statistics (337) [✓ Visualization]



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report.
Open the report in Pivot or Search to refine the parameters or further explore the data.

i	Title ^	Actions	Owner	App	Sharing	Embedding
>	cp09_maximum_concurrent_sessions	Open in Search Edit ˅	admin	operational_intelligence	App	Disabled



Summary: 09ffd23e5cccf3e4

Summary Status

Complete Updated: 1m ago

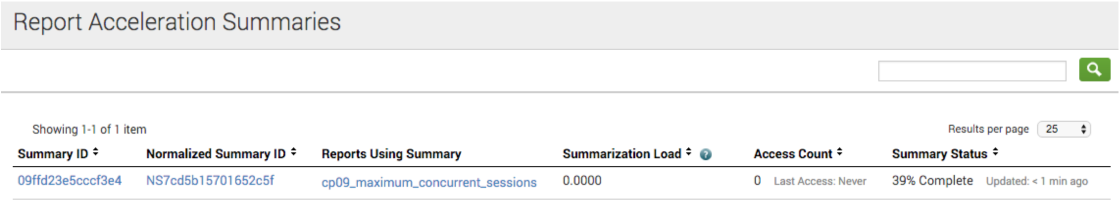
Actions

Reports Using This Summary

Search name	Owner	App
cp09_maximum_concurrent_sessions	admin	operational_intelligence

Details Learn more.

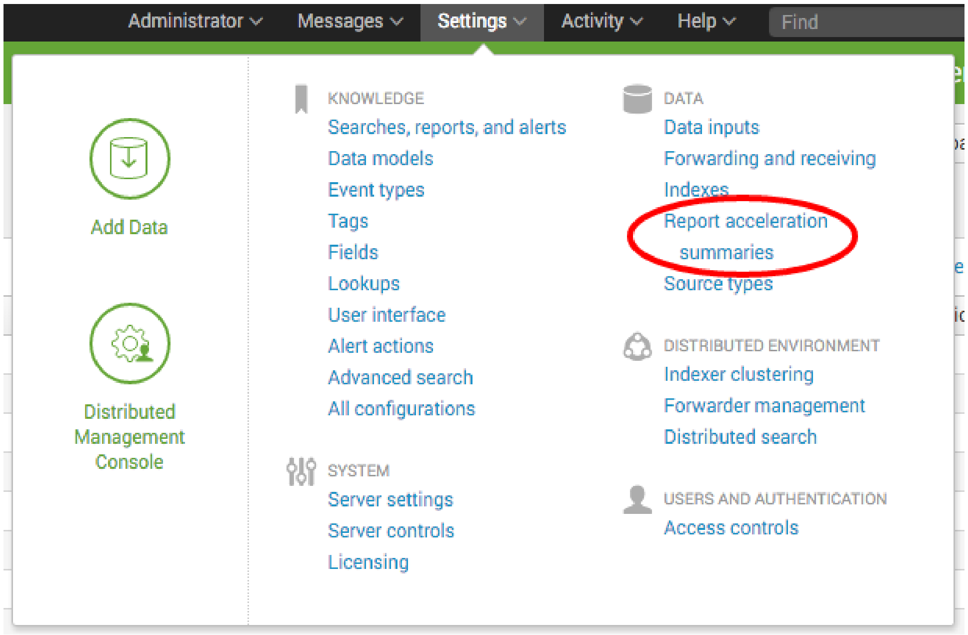
Summarization Load	0.1016
Access Count	0 Last Access: Never
Size on Disk	11.41MB
Summary Range	31 days
Timespans	10s, 1d, 1h, 1min, 1mon, 1s
Buckets	9
Chunks	795

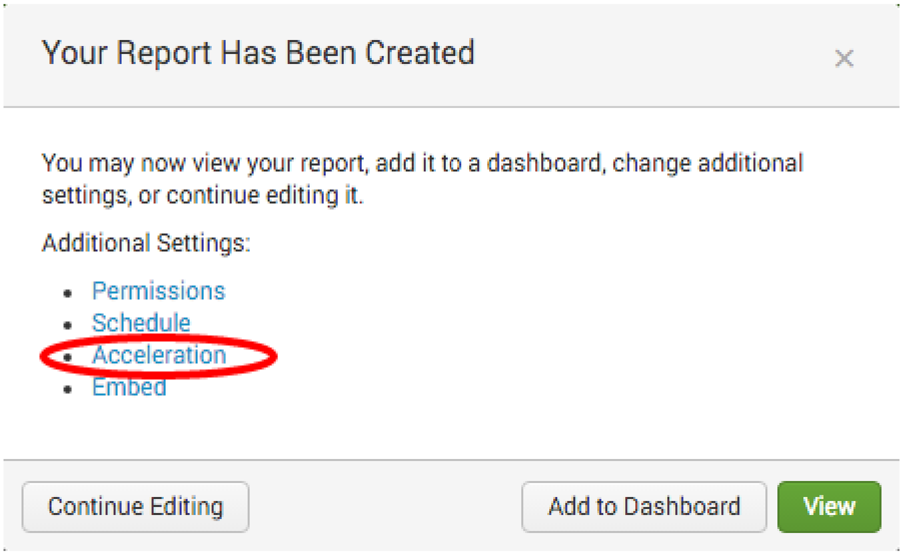


Report Acceleration Summaries

Showing 1-1 of 1 item

Summary ID	Normalized Summary ID	Reports Using Summary	Summarization Load	Access Count	Summary Status
09ffd23e5cccf3e4	NS7cd5b15701652c5f	cp09_maximum_concurrent_sessions	0.0000	0 Last Access: Never	39% Complete Updated: < 1 min ago



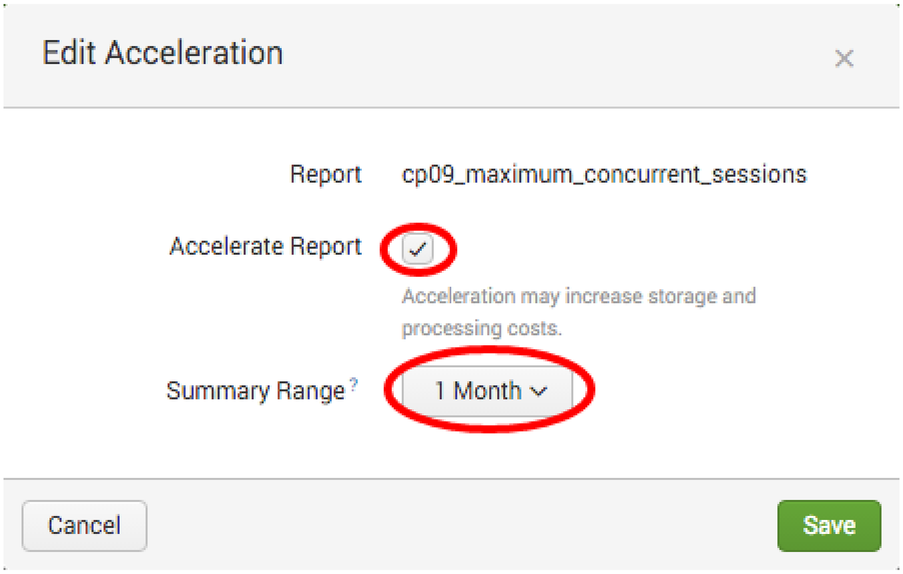


Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed



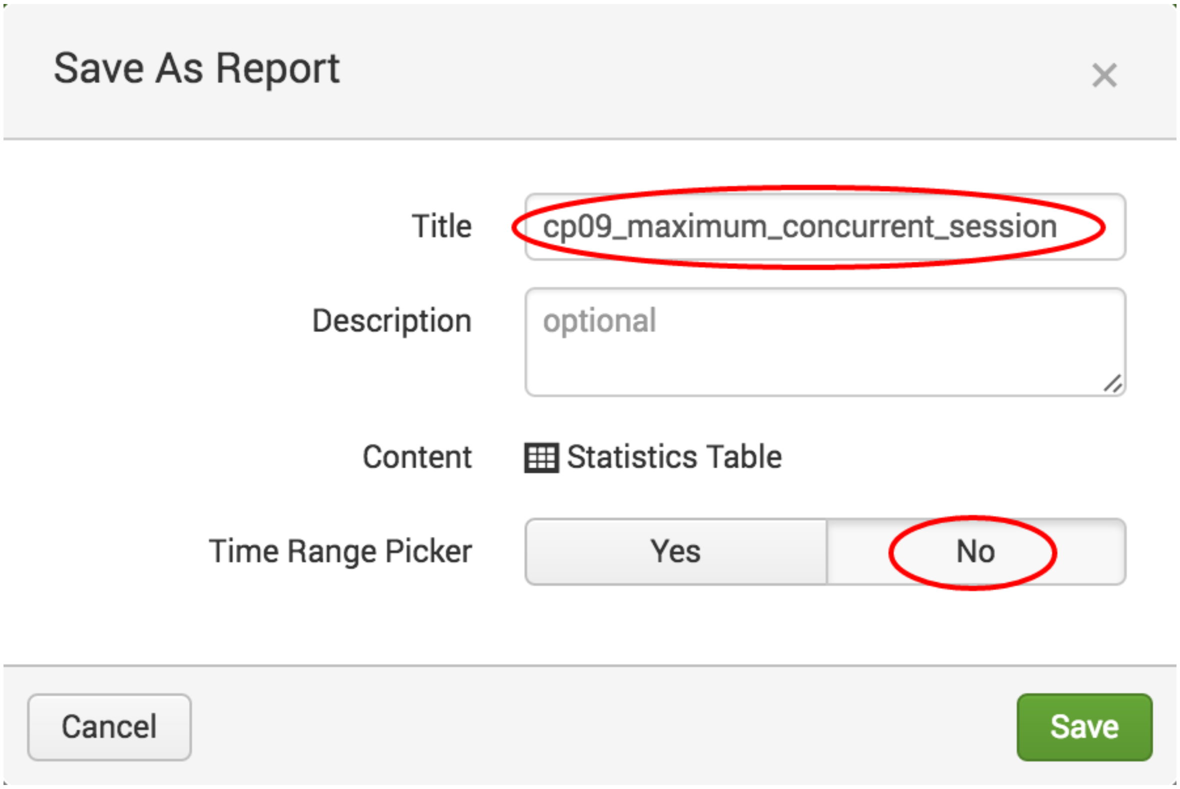
Edit Acceleration

Report cp09_maximum_concurrent_sessions

Accelerate Report ☑

Acceleration may increase storage and processing costs.

Summary Range? [✓ 1 Month]



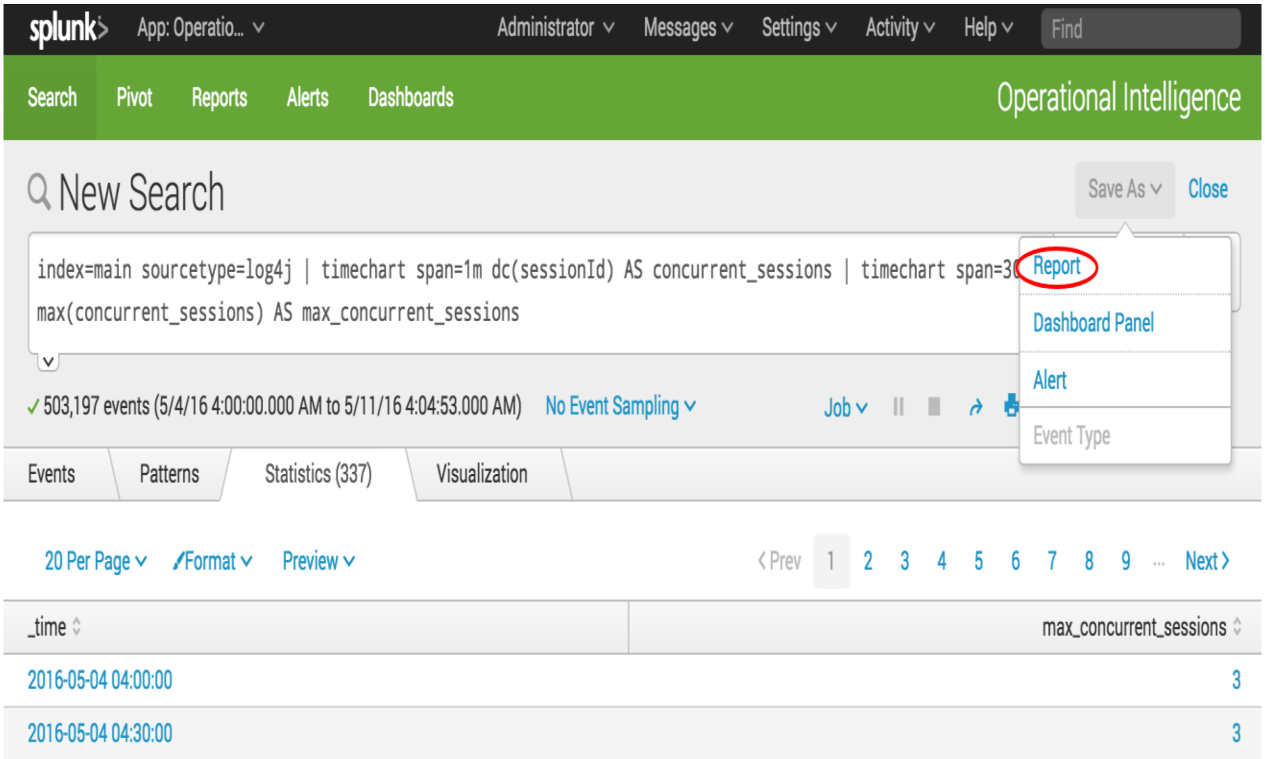
Save As Report

Title [✓ cp09_maximum_concurrent_session]

Description optional

Content Statistics Table

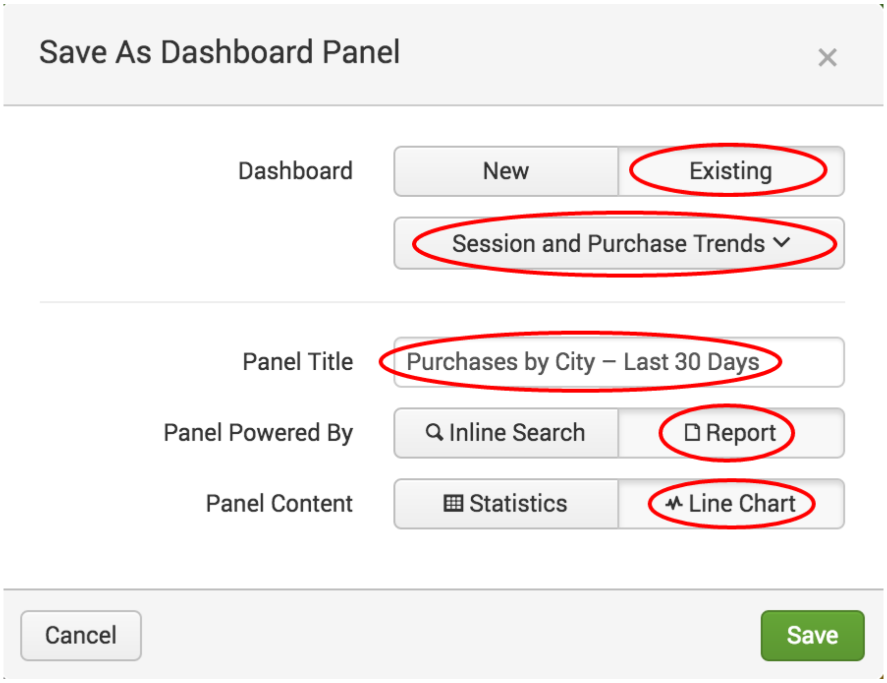
Time Range Picker Yes [✓ No]



```
index=main sourcetype=log4j | timechart span=1m dc(sessionId) AS concurrent_sessions | timechart span=3(
max(concurrent_sessions) AS max_concurrent_sessions
```

✓ 503,197 events (5/4/16 4:00:00.000 AM to 5/11/16 4:04:53.000 AM)

_time	max_concurrent_sessions
2016-05-04 04:00:00	3
2016-05-04 04:30:00	3



Save As Dashboard Panel

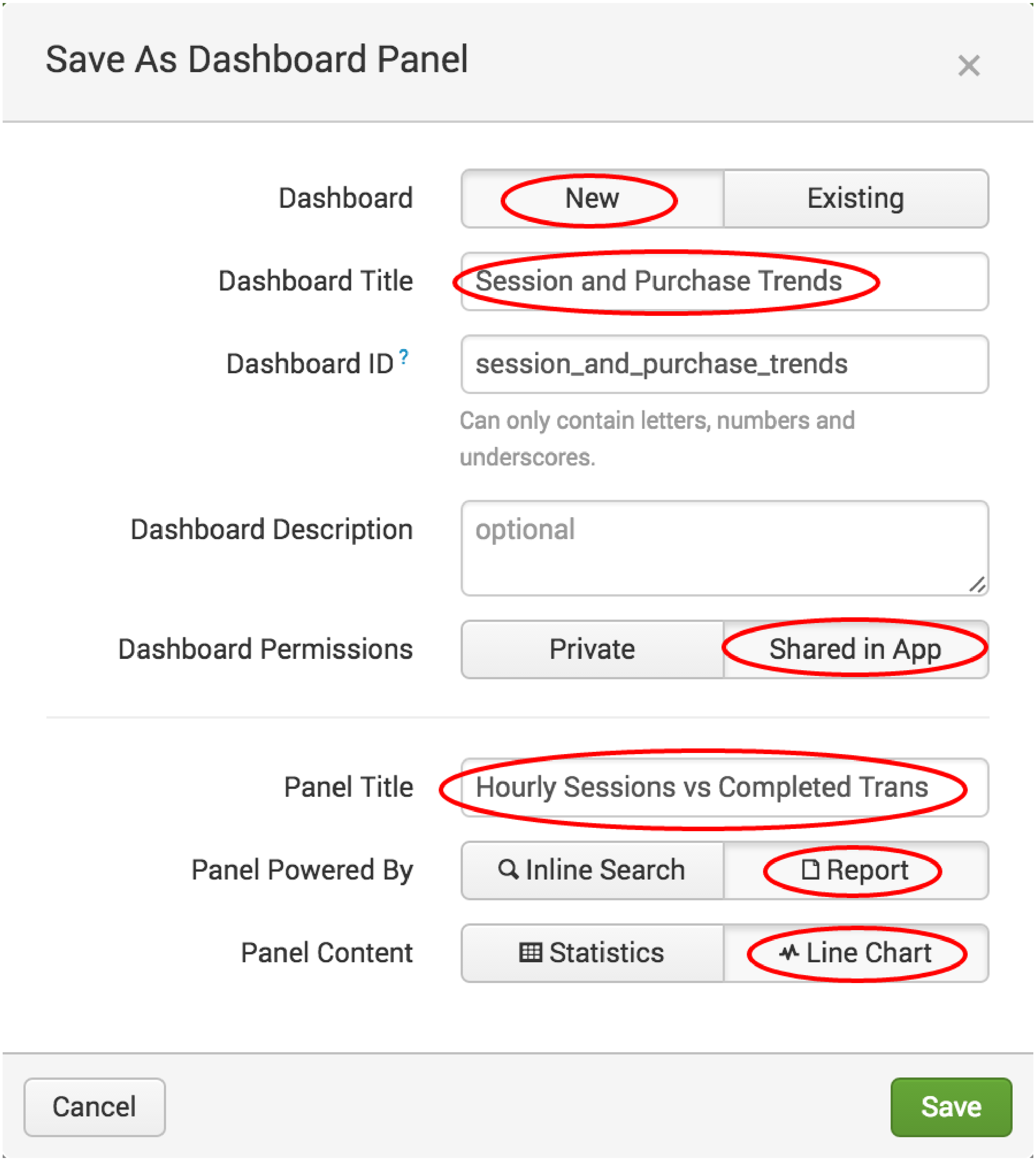
Dashboard: New [✓ Existing]

[✓ Session and Purchase Trends]

Panel Title: [✓ Purchases by City – Last 30 Days]

Panel Powered By: Inline Search [✓ Report]

Panel Content: Statistics [✓ Line Chart]



Save As Dashboard Panel

Dashboard: [✓ New] Existing

Dashboard Title: Session and Purchase Trends

Dashboard ID ?: session_and_purchase_trends

Can only contain letters, numbers and underscores.

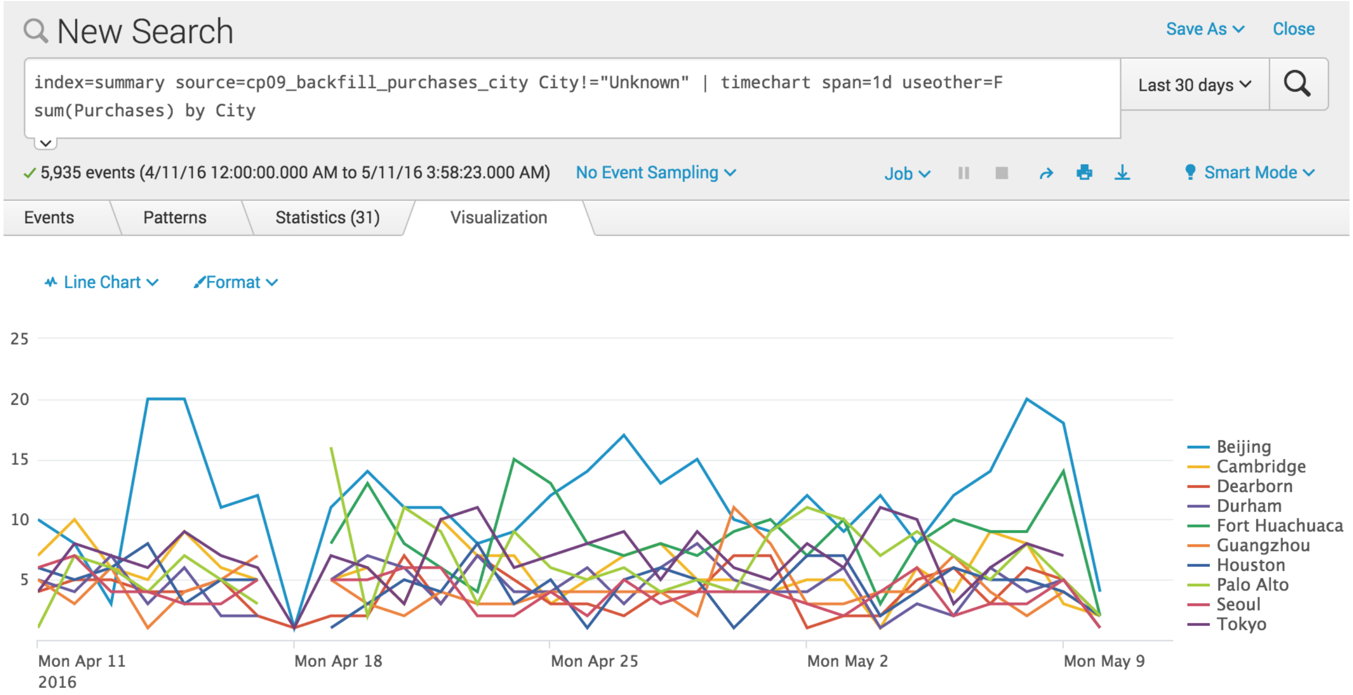
Dashboard Description: optional

Dashboard Permissions: Private [✓ Shared in App]

Panel Title: Hourly Sessions vs Completed Trans

Panel Powered By: Inline Search [✓ Report]

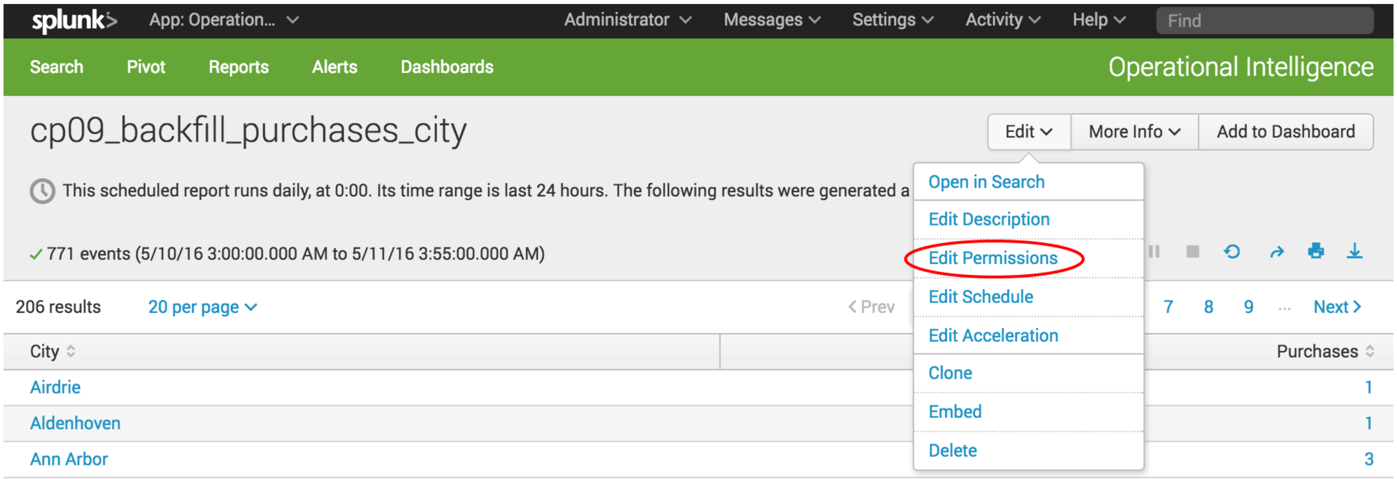
Panel Content: Statistics [✓ Line Chart]



New Search

```
index=summary source=cp09_backfill_purchases_city City!="Unknown" | timechart span=1d useother=F
sum(Purchases) by City
```

✓ 5,935 events (4/11/16 12:00:00.000 AM to 5/11/16 3:58:23.000 AM)



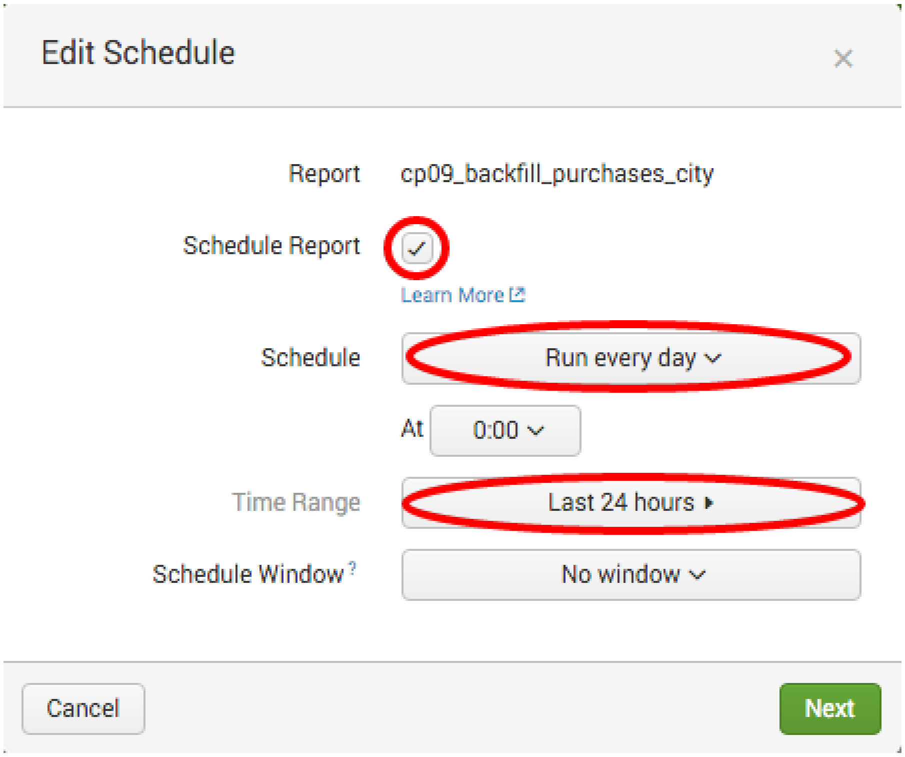
cp09_backfill_purchases_city

This scheduled report runs daily, at 0:00. Its time range is last 24 hours. The following results were generated a

✓ 771 events (5/10/16 3:00:00.000 AM to 5/11/16 3:55:00.000 AM)

206 results

City	Purchases
Airdrie	1
Aldenhoven	1
Ann Arbor	3



Edit Schedule

Report: cp09_backfill_purchases_city

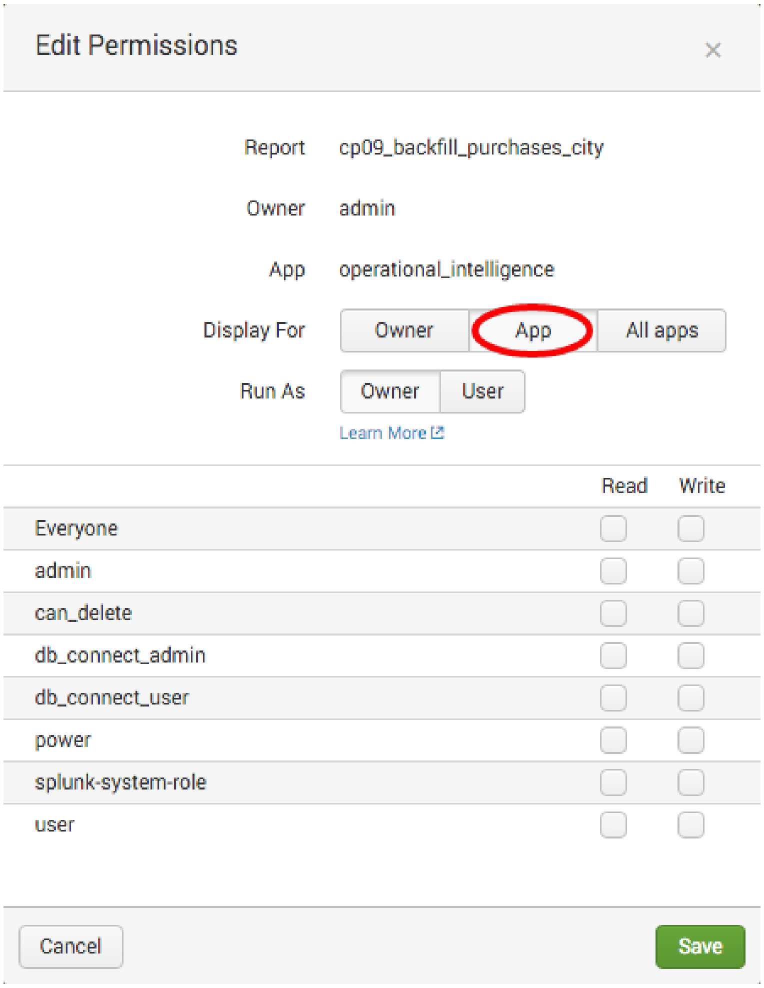
Schedule Report: ☑

Schedule: Run every day

At: 0:00

Time Range: Last 24 hours

Schedule Window: No window



Edit Permissions

Report cp09_backfill_purchases_city

Owner admin

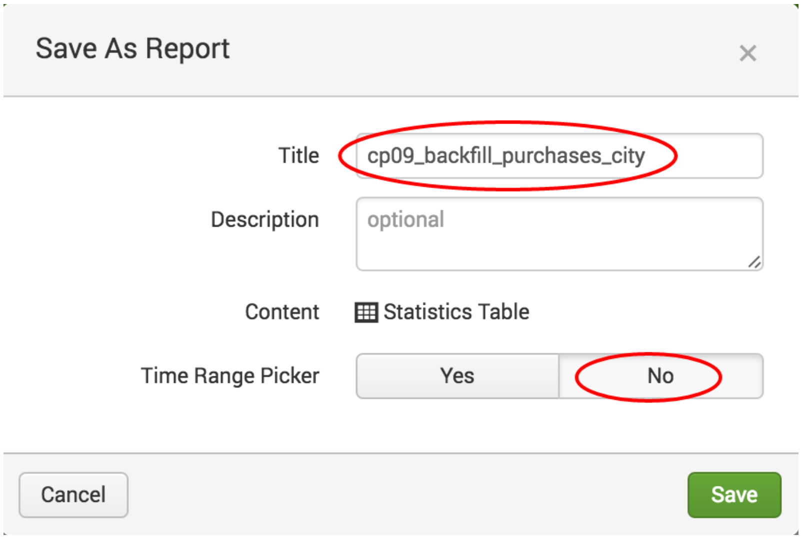
App operational_intelligence

Display For Owner [✓ App] All apps

Run As Owner User

Learn More

	Read	Write
Everyone	□	□
admin	□	□
can_delete	□	□
db_connect_admin	□	□
db_connect_user	□	□
power	□	□
splunk-system-role	□	□
user	□	□



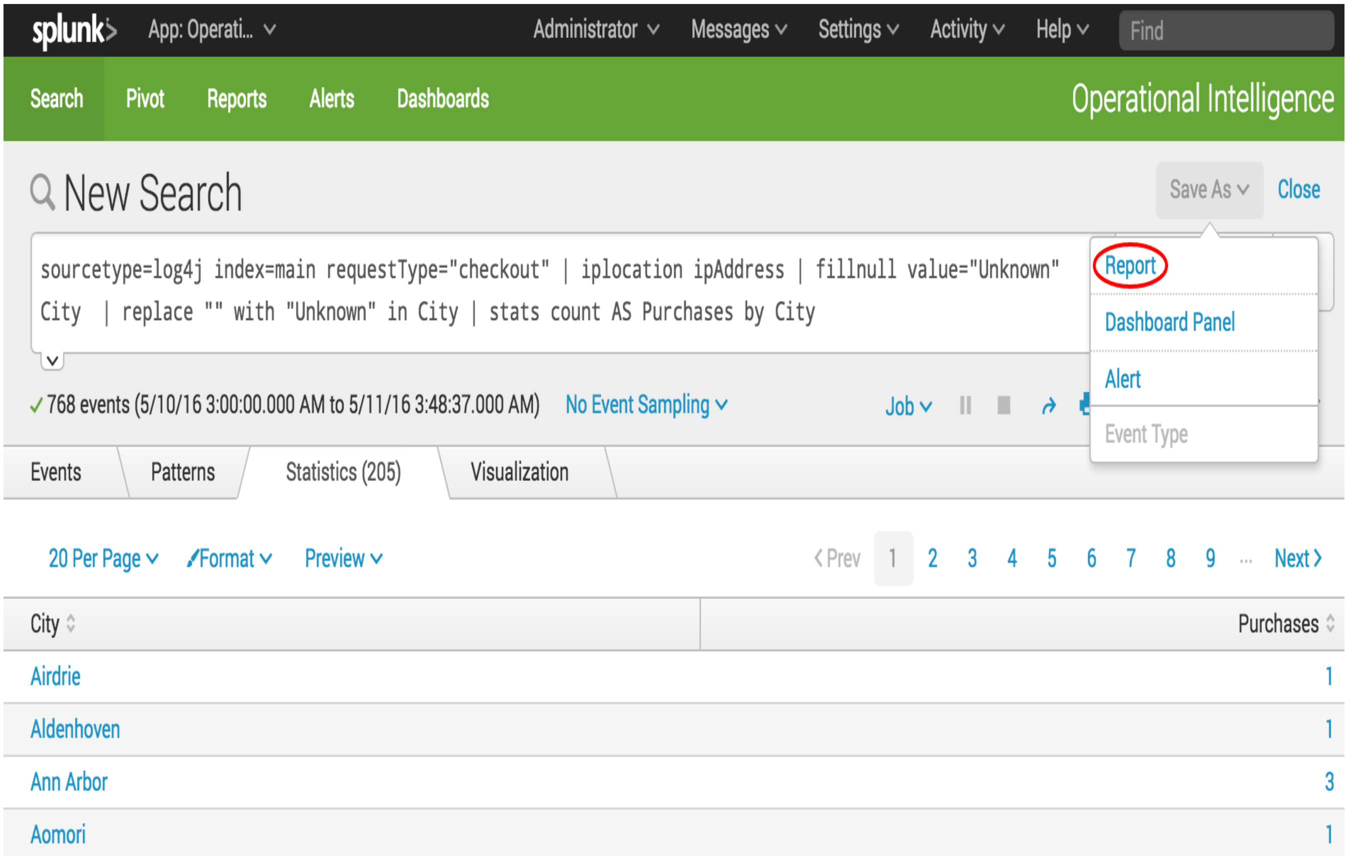
Save As Report

Title [✓ cp09_backfill_purchases_city]

Description optional

Content Statistics Table

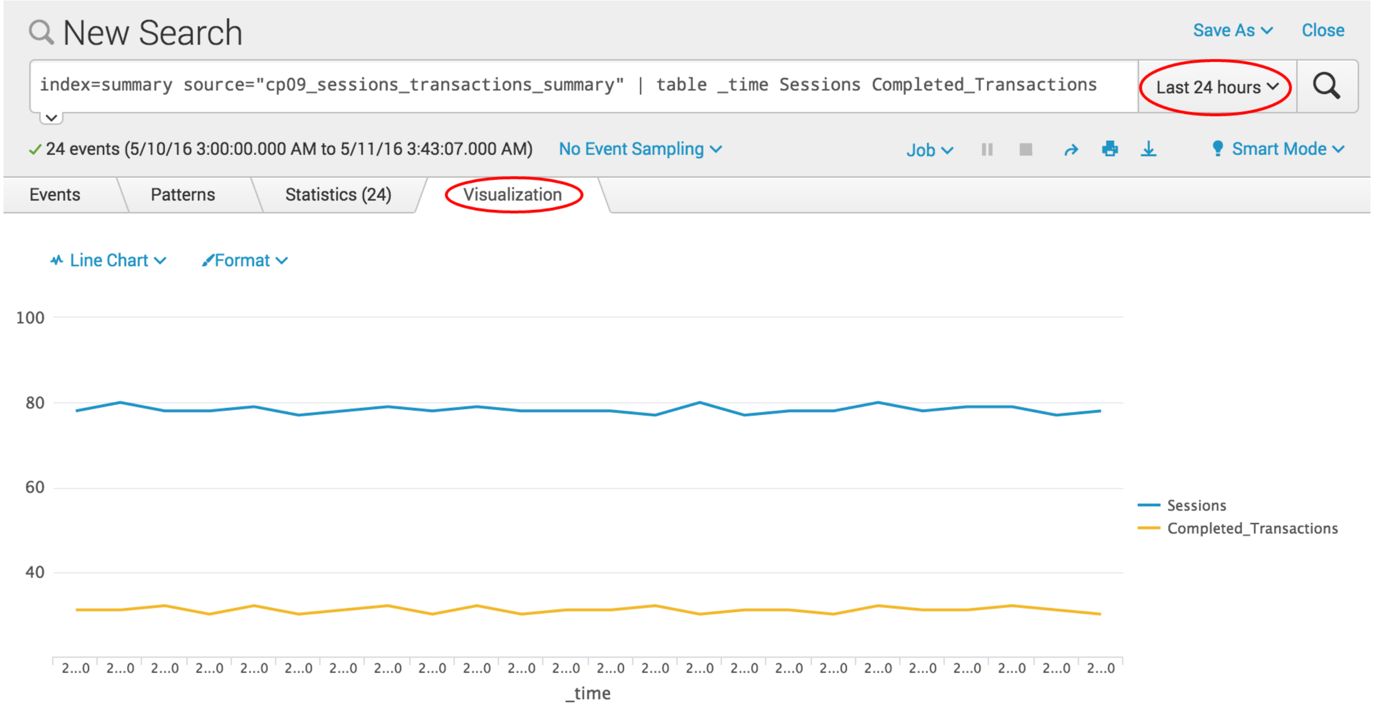
Time Range Picker Yes [✓ No]



```
sourcetype=log4j index=main requestType="checkout" | iplocation ipAddress | fillnull value="Unknown"
City  | replace "" with "Unknown" in City | stats count AS Purchases by City
```

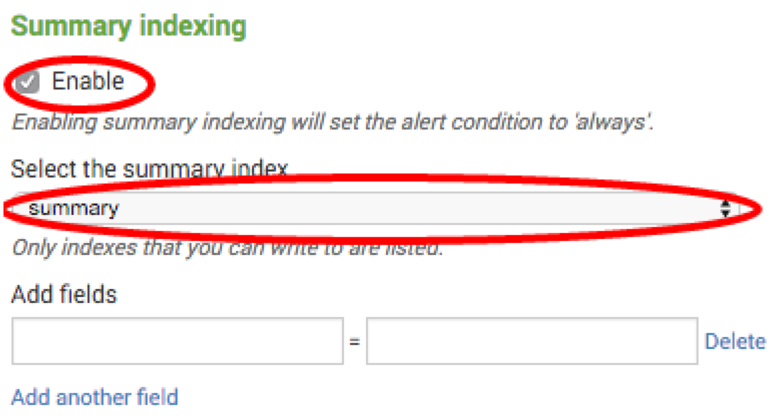
✓ 768 events (5/10/16 3:00:00.000 AM to 5/11/16 3:48:37.000 AM) No Event Sampling

City	Purchases
Airdrie	1
Aldenhoven	1
Ann Arbor	3
Aomori	1



```
index=summary source="cp09_sessions_transactions_summary" | table _time Sessions Completed_Transactions
```

✓ 24 events (5/10/16 3:00:00.000 AM to 5/11/16 3:43:07.000 AM) No Event Sampling



Summary indexing

☑ Enable

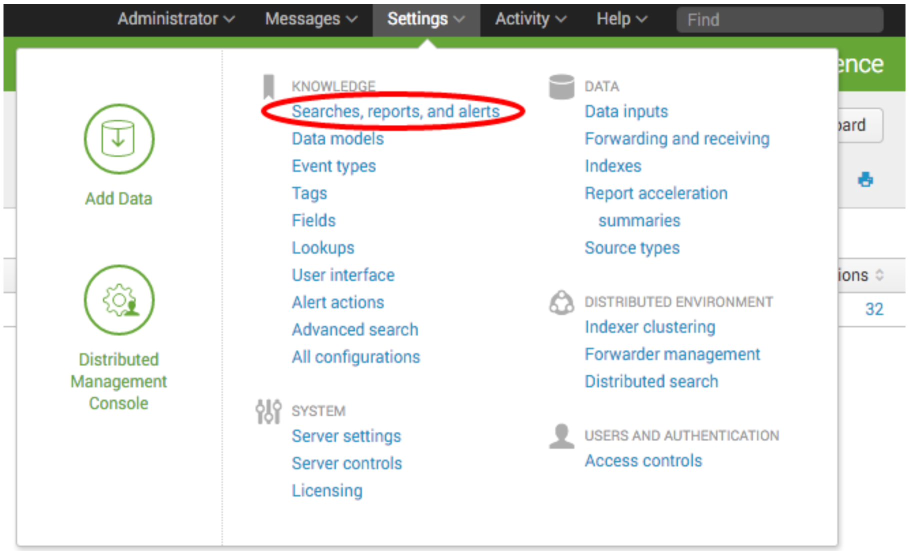
Enabling summary indexing will set the alert condition to 'always'.

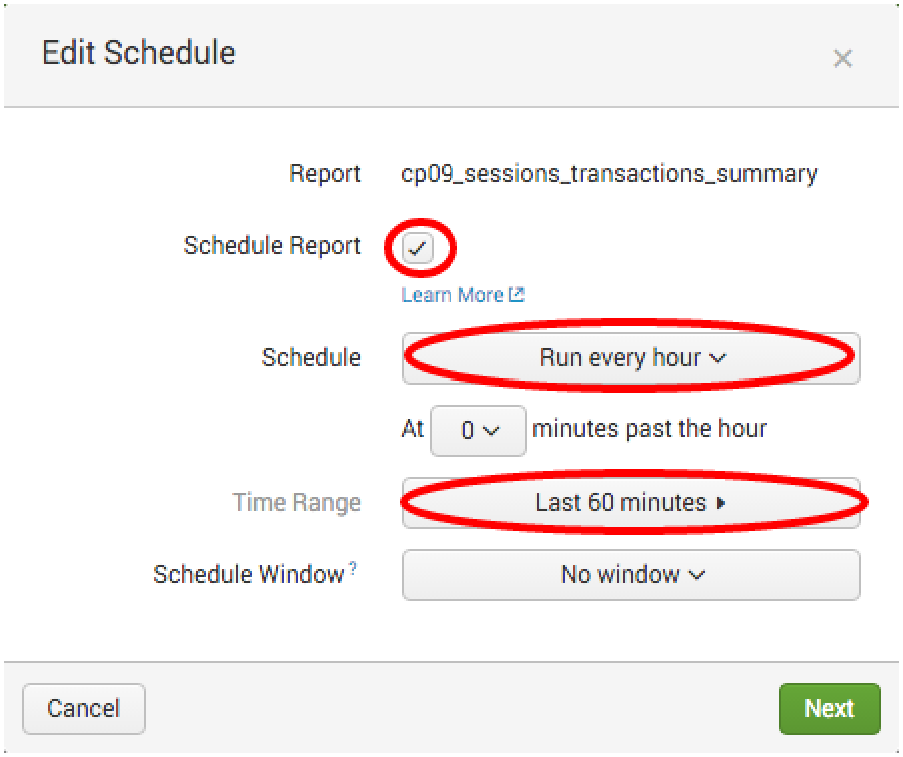
Select the summary index

summary

Only indexes that you can write to are listed.

Add fields





Edit Schedule

Report cp09_sessions_transactions_summary

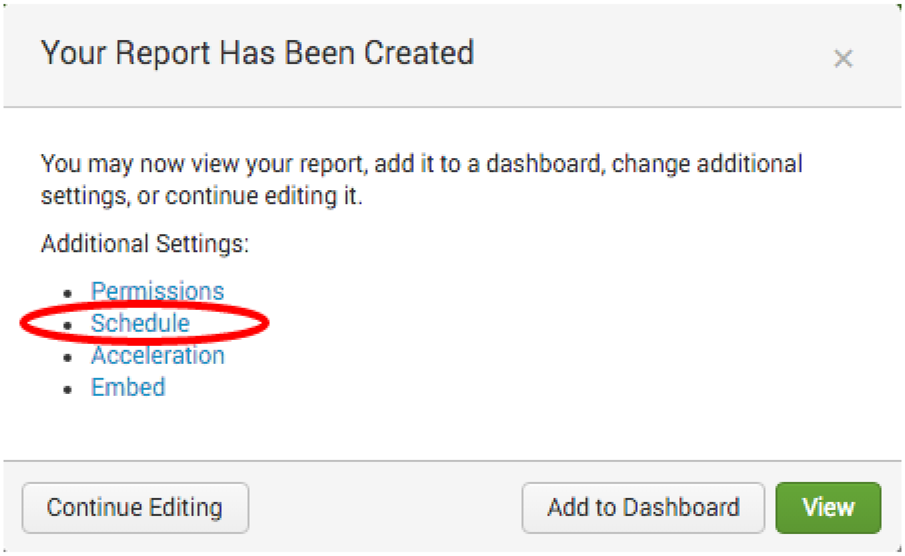
Schedule Report ☑

Schedule: Run every hour

At 0 minutes past the hour

Time Range: Last 60 minutes

Schedule Window: No window

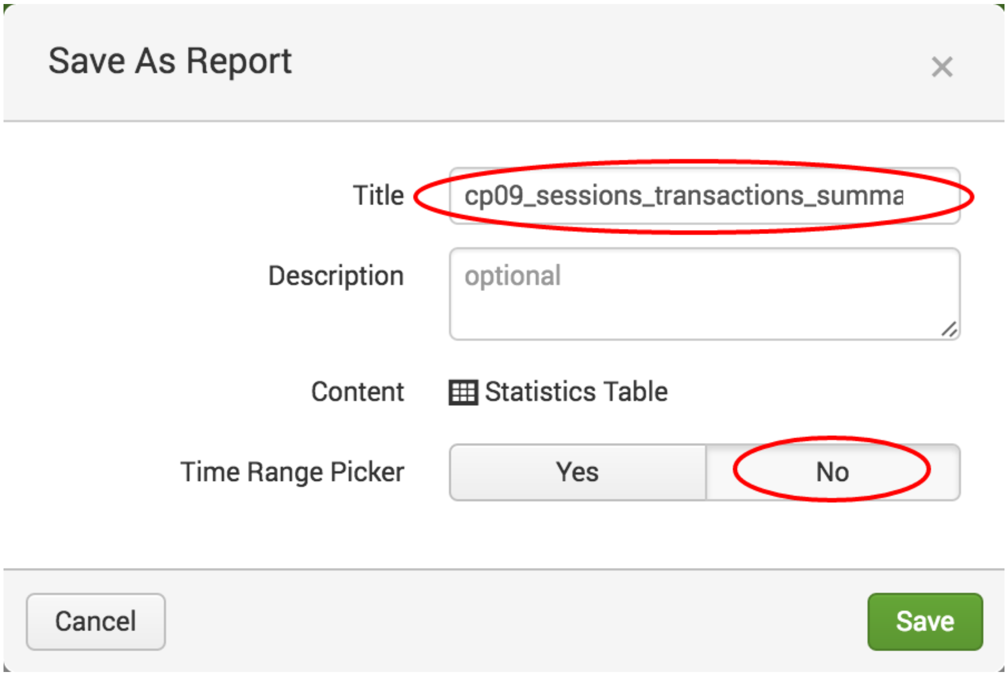


Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed



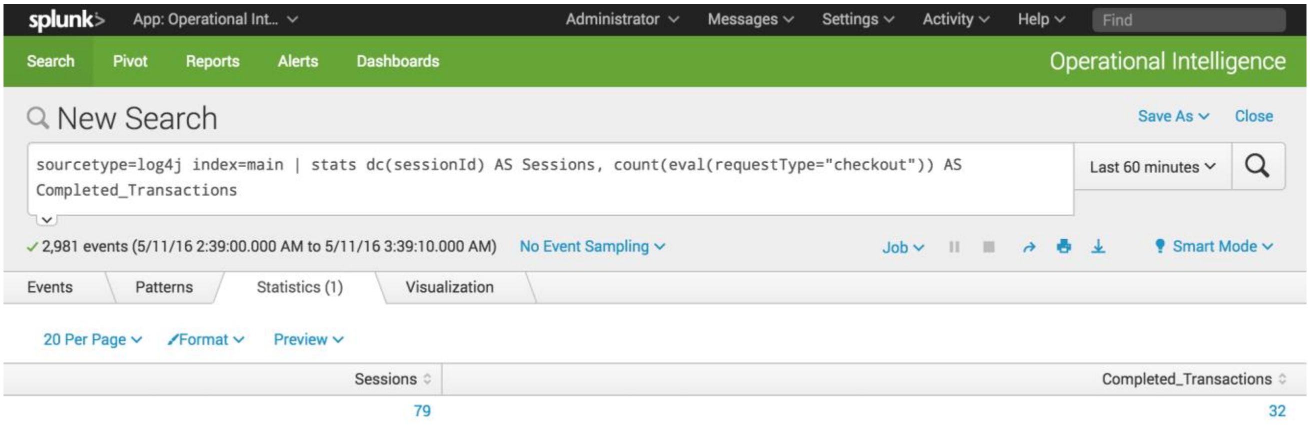
Save As Report

Title: cp09_sessions_transactions_summa

Description: optional

Content: Statistics Table

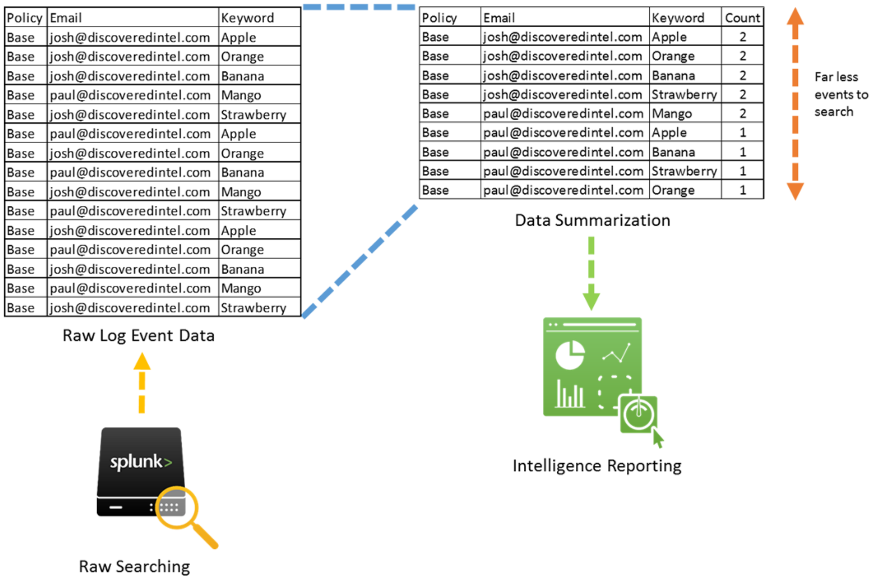
Time Range Picker: Yes [✓ No]



```
sourcetype=log4j index=main | stats dc(sessionId) AS Sessions, count(eval(requestType="checkout")) AS
Completed_Transactions
```

✓ 2,981 events (5/11/16 2:39:00.000 AM to 5/11/16 3:39:10.000 AM)

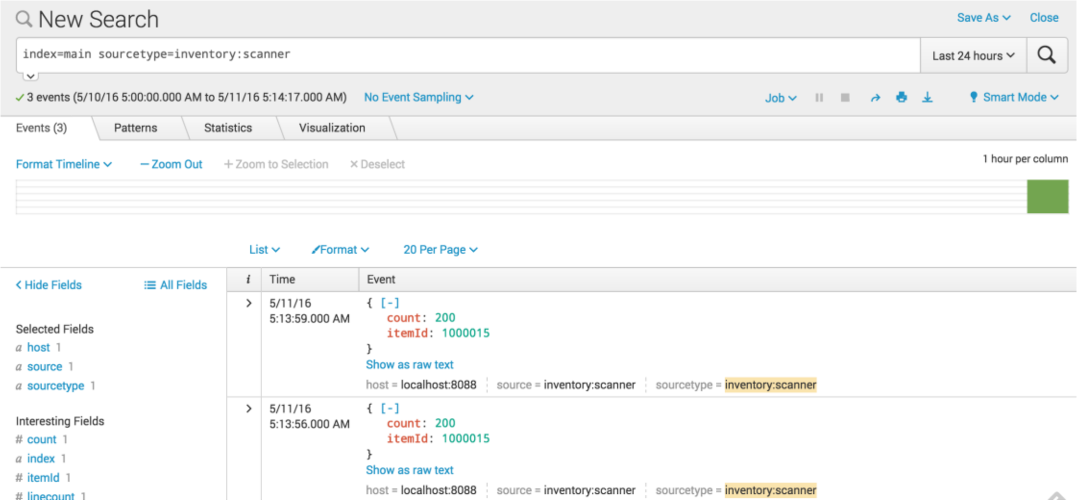
Sessions	Completed_Transactions
79	32



Policy	Email	Keyword
Base	josh@discoveredintel.com	Apple
Base	josh@discoveredintel.com	Orange
Base	josh@discoveredintel.com	Banana
Base	paul@discoveredintel.com	Mango
Base	josh@discoveredintel.com	Strawberry
Base	paul@discoveredintel.com	Apple
Base	josh@discoveredintel.com	Orange
Base	paul@discoveredintel.com	Banana
Base	josh@discoveredintel.com	Mango
Base	paul@discoveredintel.com	Strawberry
Base	josh@discoveredintel.com	Apple
Base	paul@discoveredintel.com	Orange
Base	josh@discoveredintel.com	Banana
Base	paul@discoveredintel.com	Mango
Base	josh@discoveredintel.com	Strawberry

Policy	Email	Keyword	Count
Base	josh@discoveredintel.com	Apple	2
Base	josh@discoveredintel.com	Orange	2
Base	josh@discoveredintel.com	Banana	2
Base	josh@discoveredintel.com	Strawberry	2
Base	paul@discoveredintel.com	Mango	2
Base	paul@discoveredintel.com	Apple	1
Base	paul@discoveredintel.com	Banana	1
Base	paul@discoveredintel.com	Strawberry	1
Base	paul@discoveredintel.com	Orange	1

Chapter 10: Above and Beyond – Customization, Web Framework, REST API, HTTP Event Collector, and SDKs

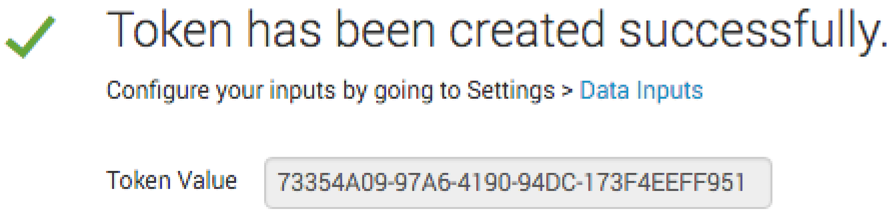


New Search

```
index=main sourcetype=inventory:scanner
```

✓3 events (5/10/16 5:00:00.000 AM to 5/11/16 5:14:17.000 AM) No Event Sampling

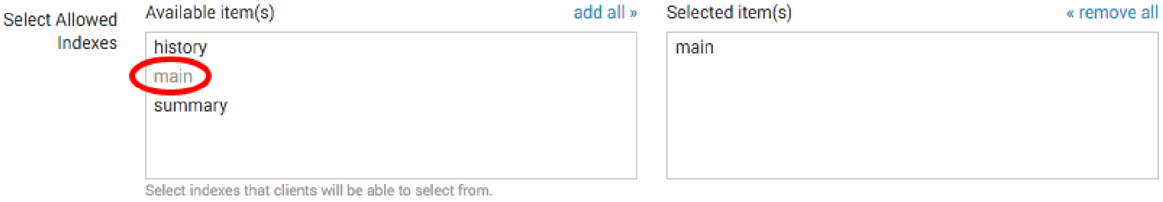
```
> 5/11/16 5:13:59.000 AM
{ [-]
   count: 200
   itemId: 1000015
}
host = localhost:8088   source = inventory:scanner   sourcetype = inventory:scanner

> 5/11/16 5:13:56.000 AM
{ [-]
   count: 200
   itemId: 1000015
}
host = localhost:8088   source = inventory:scanner   sourcetype = inventory:scanner
```



Token has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Token Value 73354A09-97A6-4190-94DC-173F4EEFF951

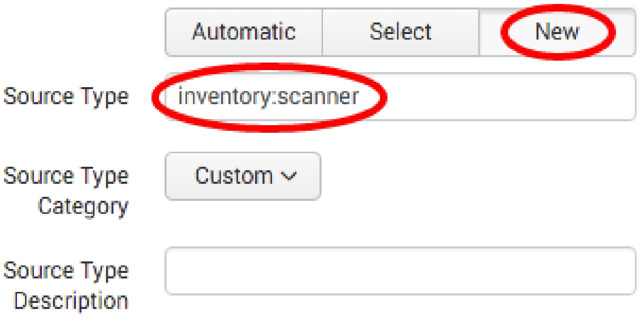


Select Allowed Indexes

Available item(s) — history, main, summary

Selected item(s) — main

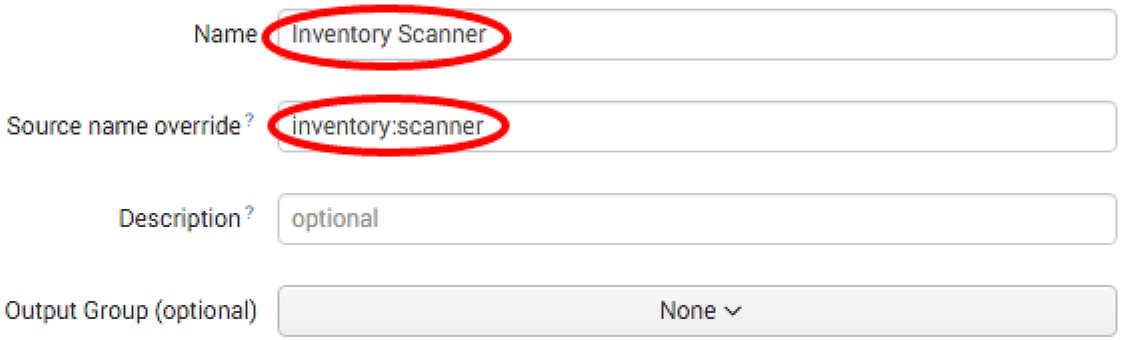
Select indexes that clients will be able to select from.



Source Type: inventory:scanner

Source Type Category: Custom

Source Type Description:

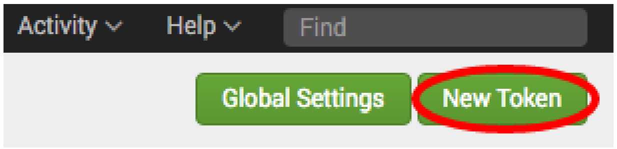


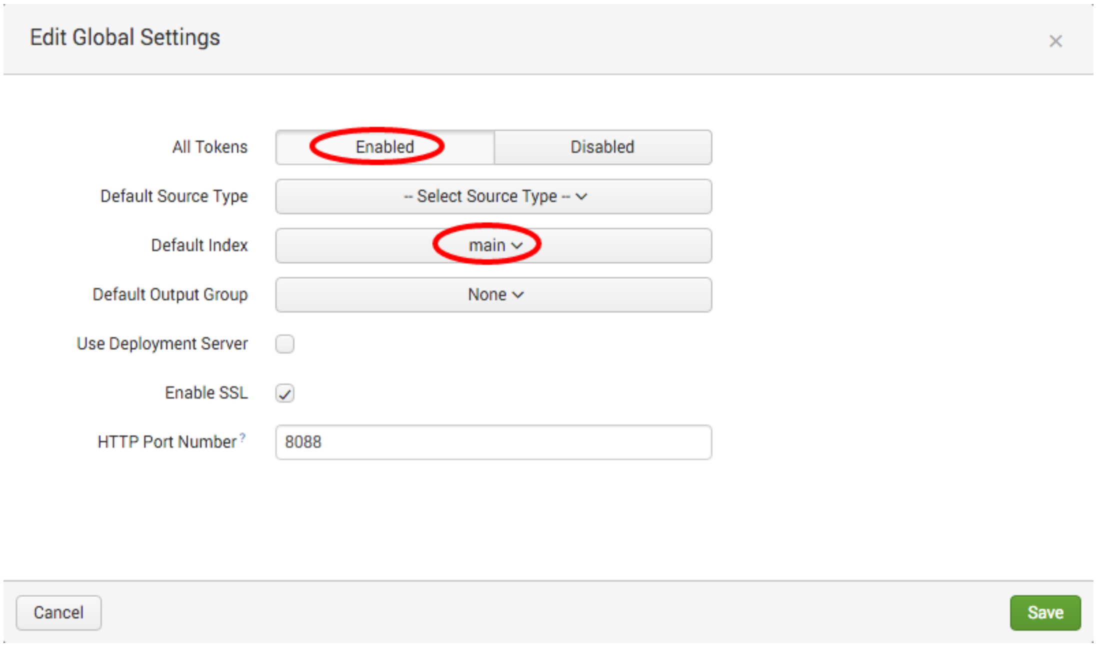
Name: Inventory Scanner

Source name override ?: inventory:scanner

Description ?: optional

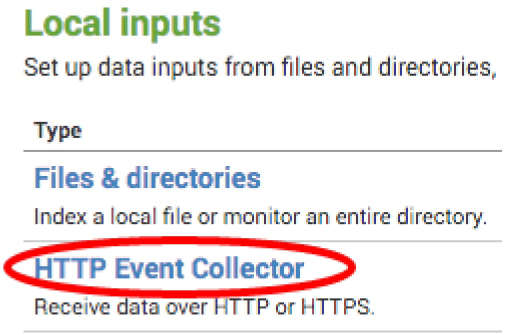
Output Group (optional): None





Edit Global Settings

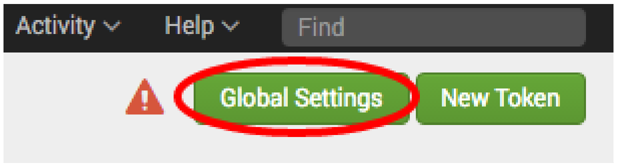
All Tokens	[✓ Enabled] Disabled
Default Source Type	-- Select Source Type --
Default Index	main
Default Output Group	None
Use Deployment Server	□
Enable SSL	☑
HTTP Port Number ?	8088

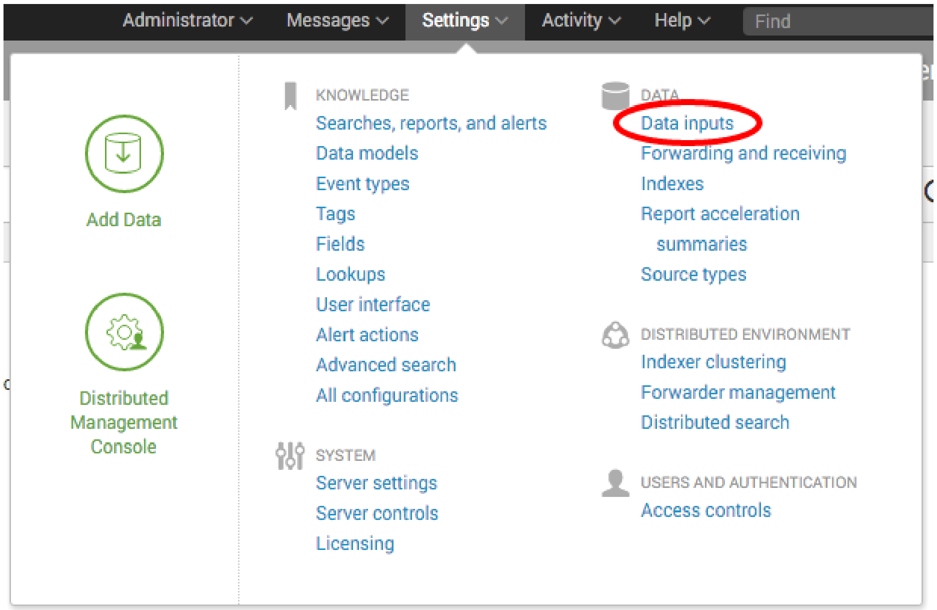


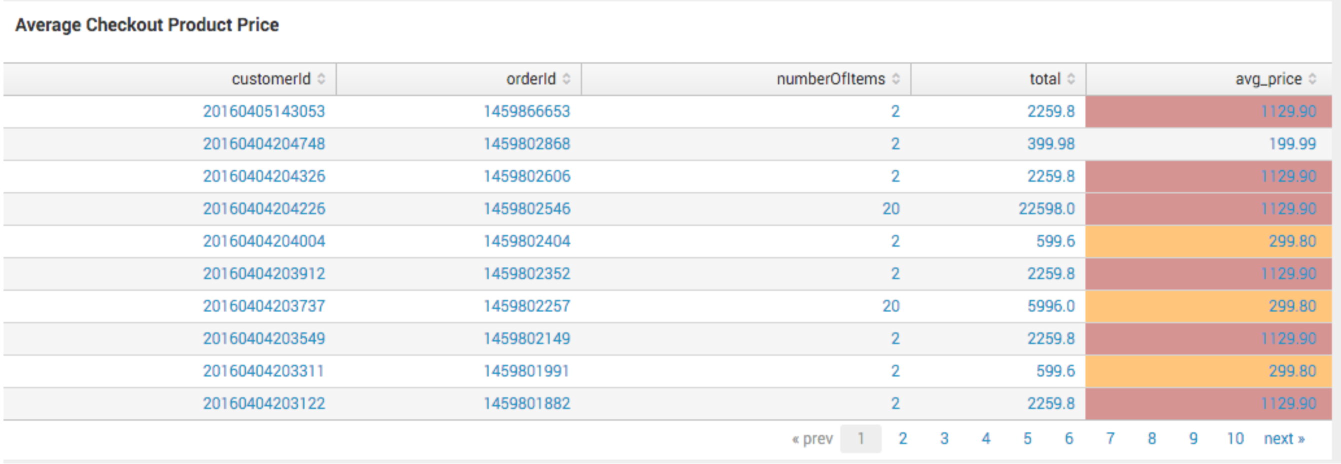
Local inputs

Set up data inputs from files and directories,

Type
Files & directories Index a local file or monitor an entire directory.
HTTP Event Collector Receive data over HTTP or HTTPS.

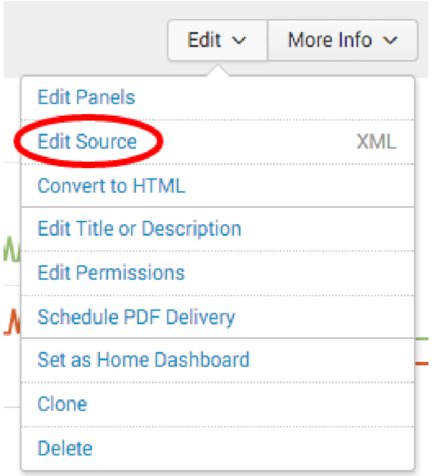


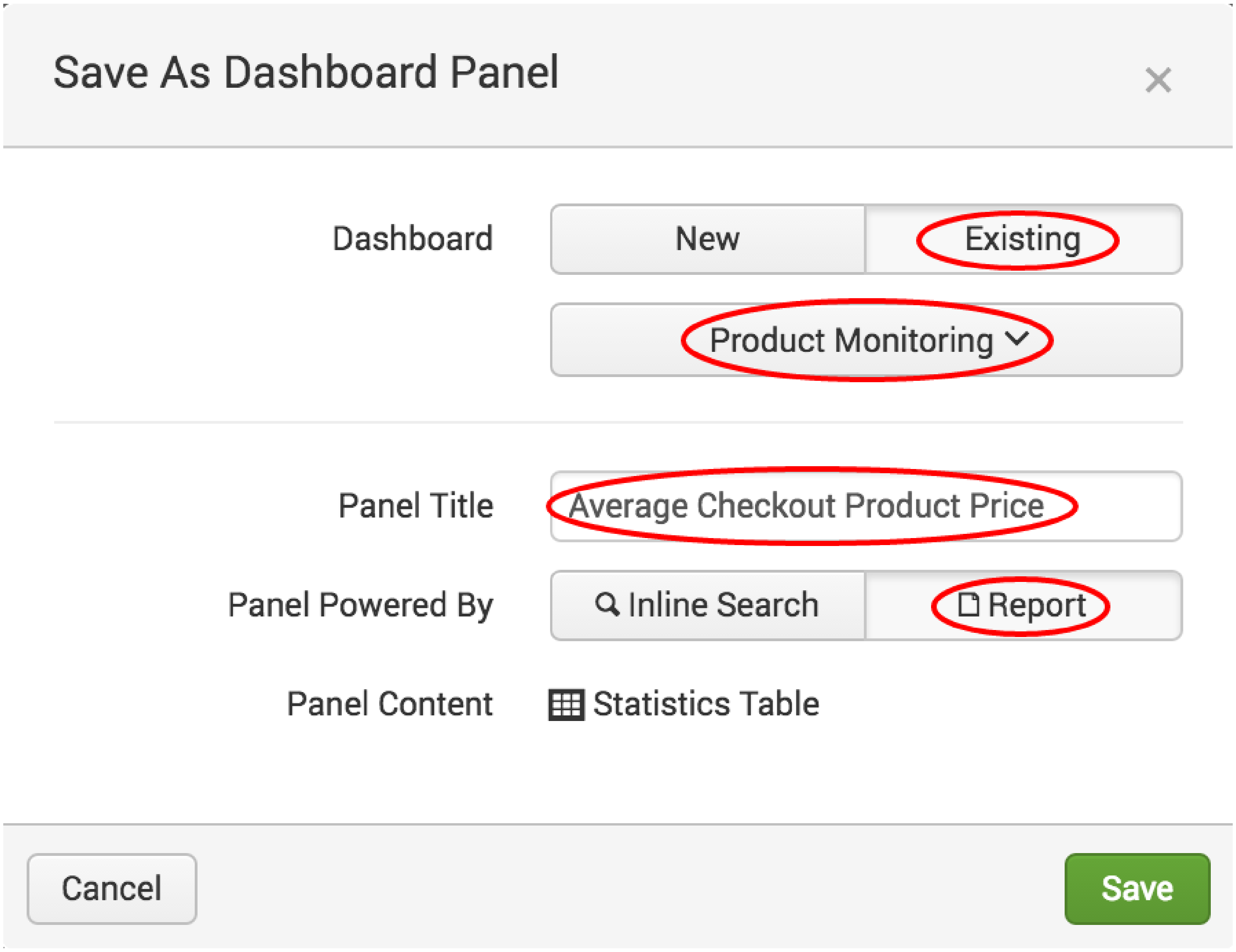




Average Checkout Product Price

customerId	orderId	numberOfItems	total	avg_price
20160405143053	1459866653	2	2259.8	1129.90
20160404204748	1459802868	2	399.98	199.99
20160404204326	1459802606	2	2259.8	1129.90
20160404204226	1459802546	20	22598.0	1129.90
20160404204004	1459802404	2	599.6	299.80
20160404203912	1459802352	2	2259.8	1129.90
20160404203737	1459802257	20	5996.0	299.80
20160404203549	1459802149	2	2259.8	1129.90
20160404203311	1459801991	2	599.6	299.80
20160404203122	1459801882	2	2259.8	1129.90





Save As Dashboard Panel

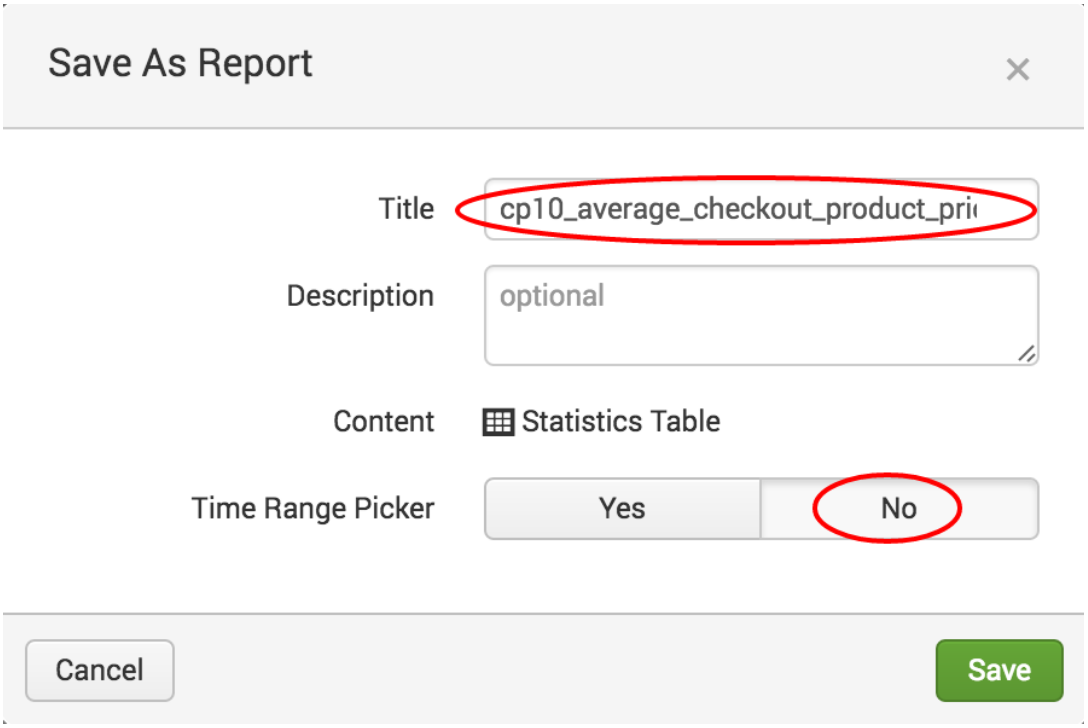
Dashboard: New [✓ Existing]

[✓ Product Monitoring]

Panel Title: [✓ Average Checkout Product Price]

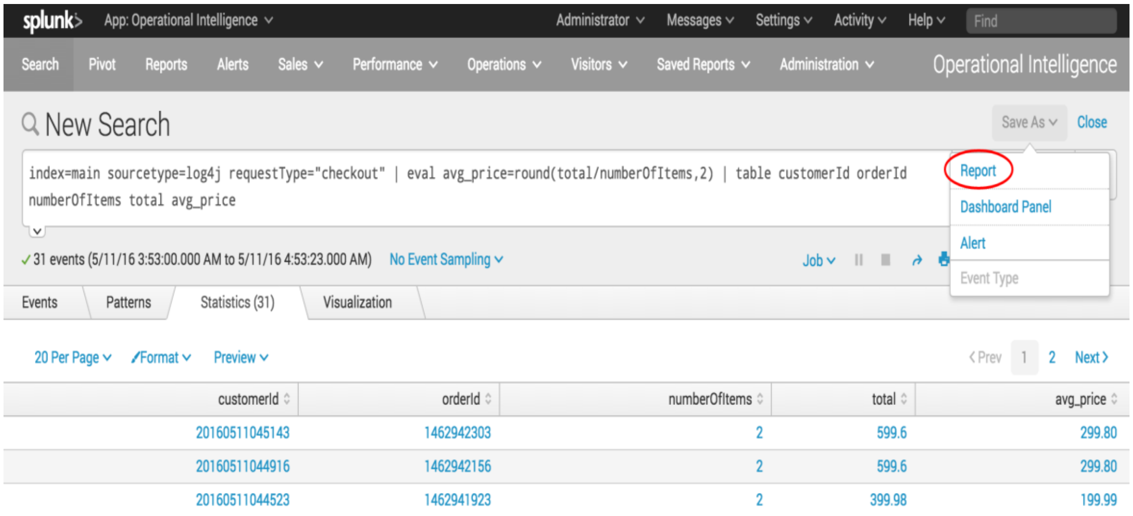
Panel Powered By: Inline Search [✓ Report]

Panel Content: ▦ Statistics Table



Save As Report

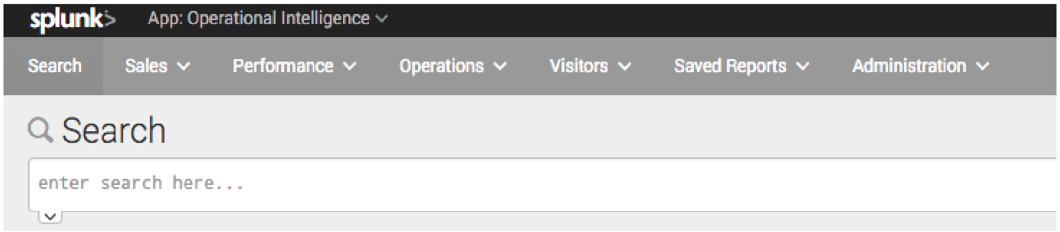
Title	cp10_average_checkout_product_pri
Description	optional
Content	▦ Statistics Table
Time Range Picker	Yes [✓ No]

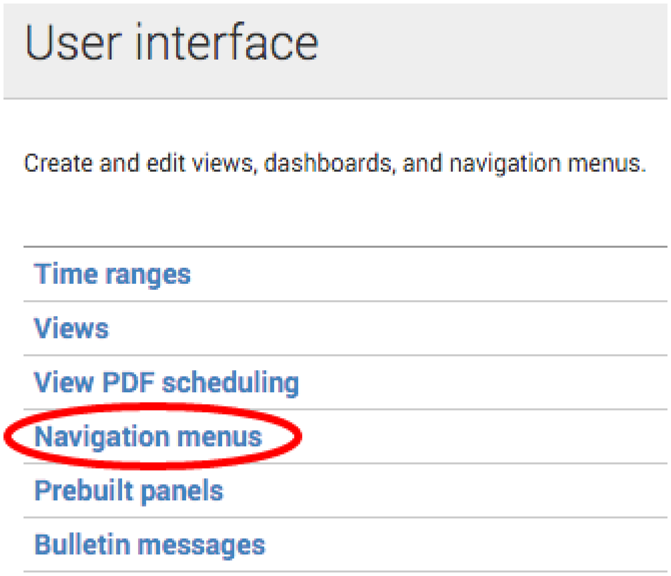


```
index=main sourcetype=log4j requestType="checkout" | eval avg_price=round(total/numberOfItems,2) | table customerId orderId
numberOfItems total avg_price
```

✓31 events (5/11/16 3:53:00.000 AM to 5/11/16 4:53:23.000 AM) No Event Sampling

customerId	orderId	numberOfItems	total	avg_price
20160511045143	1462942303	2	599.6	299.80
20160511044916	1462942156	2	599.6	299.80
20160511044523	1462941923	2	399.98	199.99

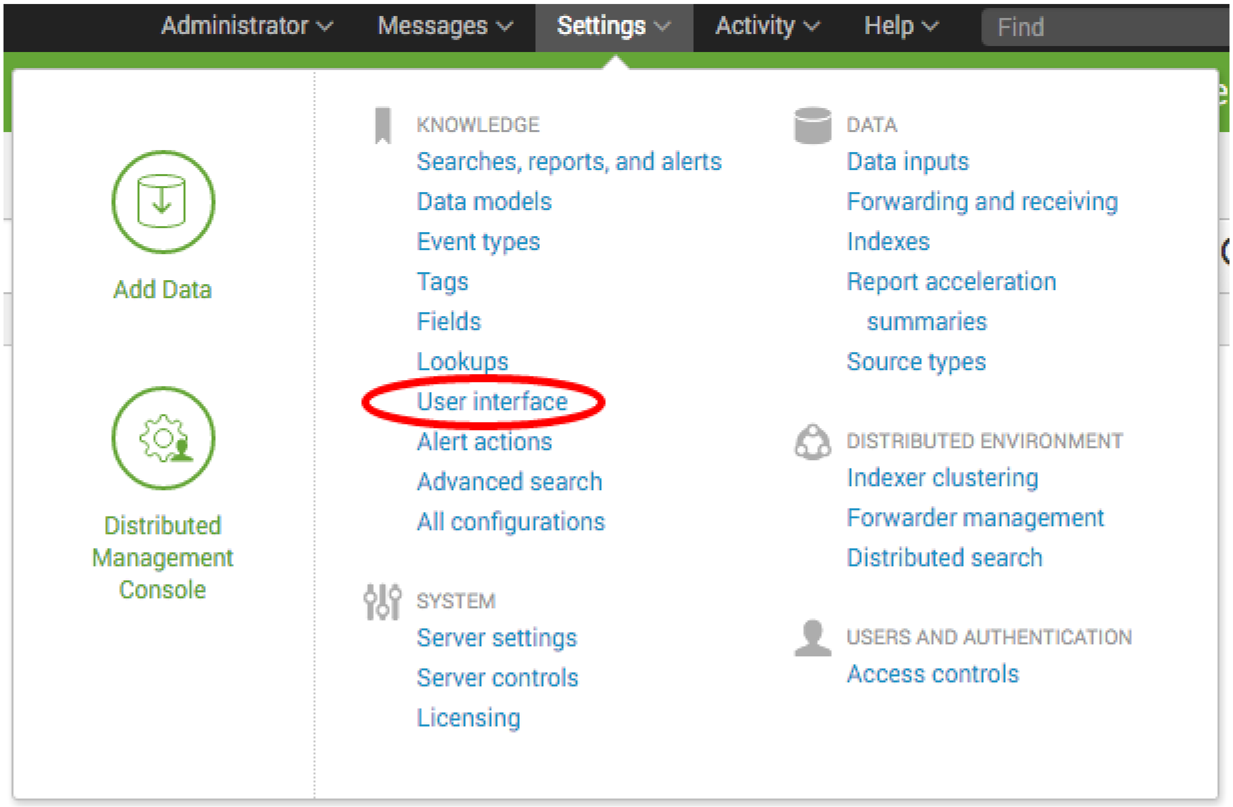




User interface

Create and edit views, dashboards, and navigation menus.

- Time ranges
- Views
- View PDF scheduling
- Navigation menus
- Prebuilt panels
- Bulletin messages



Administrator Messages Settings Activity Help Find

Add Data

Distributed Management Console

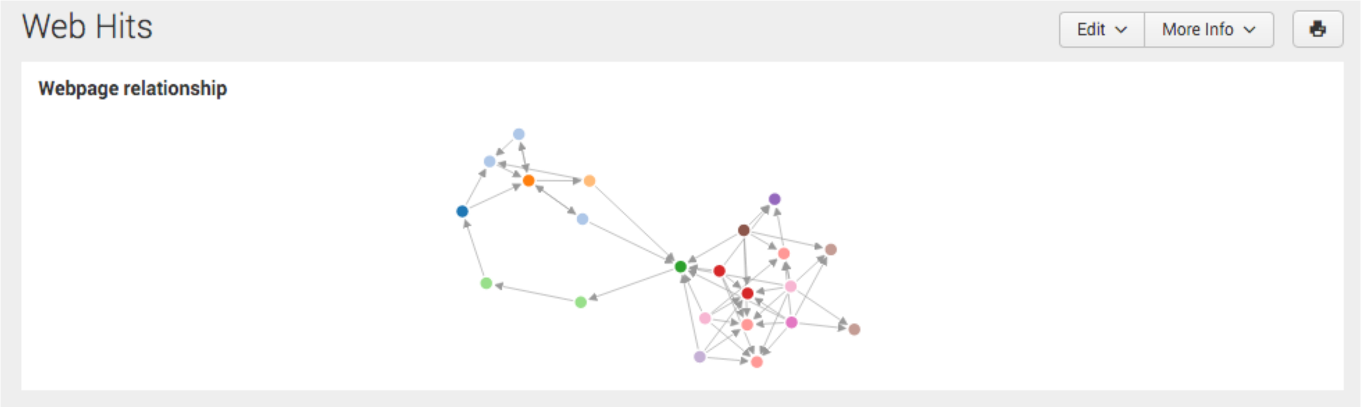
KNOWLEDGE
- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

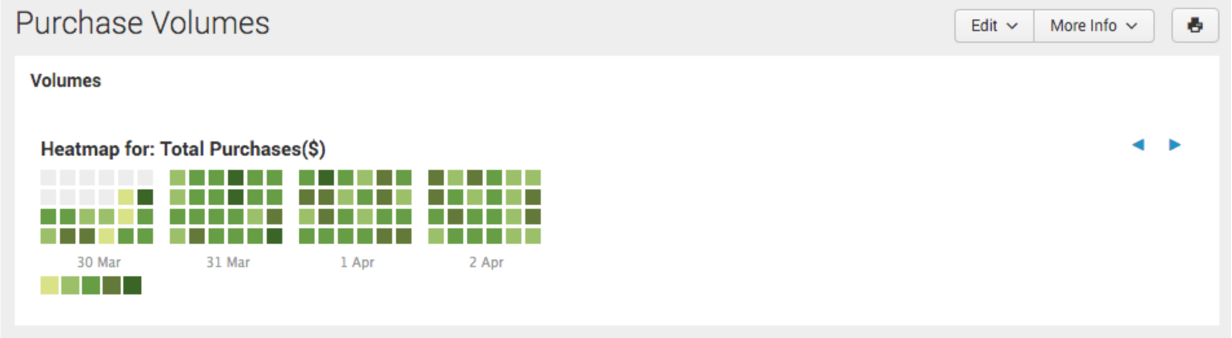
SYSTEM
- Server settings
- Server controls
- Licensing

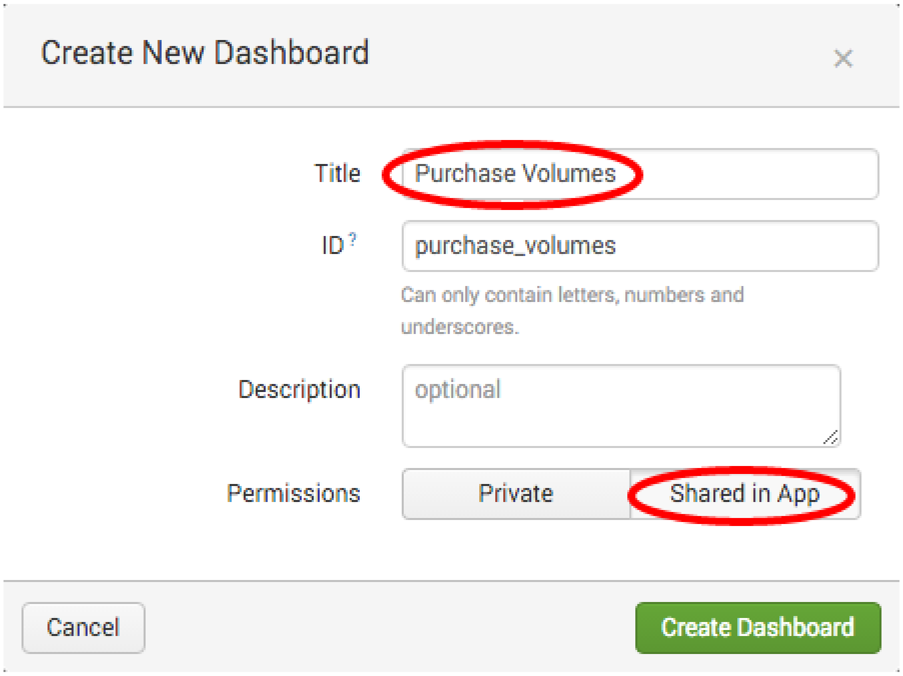
DATA
- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Source types

DISTRIBUTED ENVIRONMENT
- Indexer clustering
- Forwarder management
- Distributed search

USERS AND AUTHENTICATION
- Access controls







Create New Dashboard

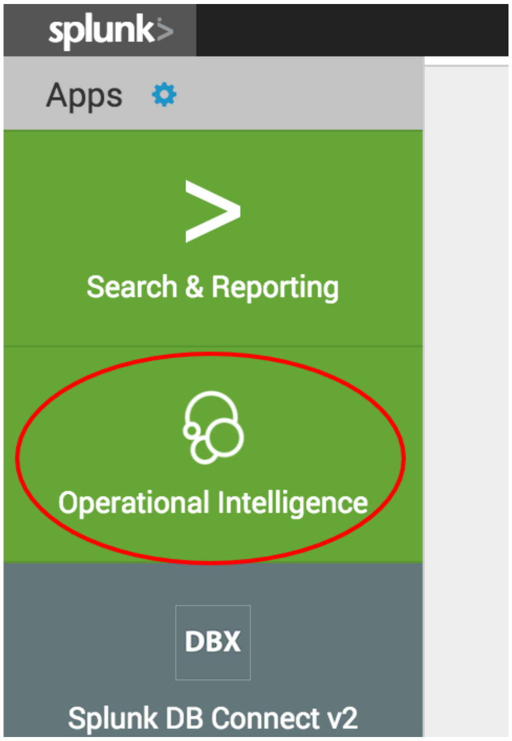
Title: Purchase Volumes

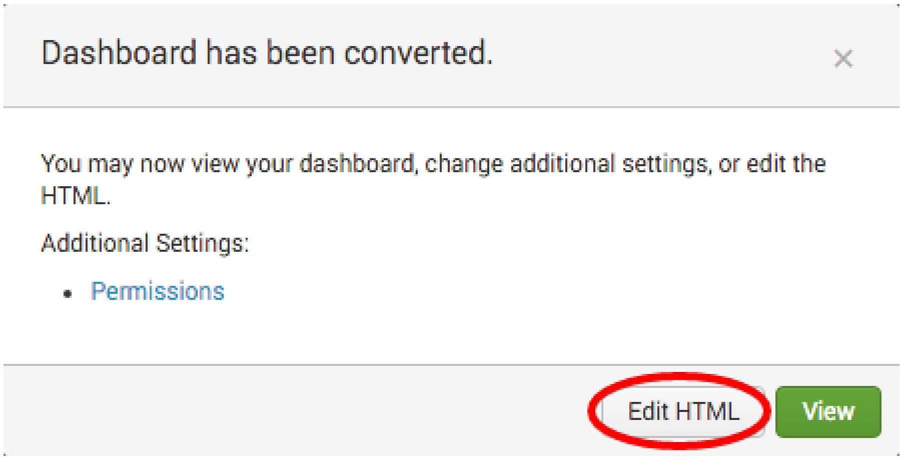
ID: purchase_volumes

Can only contain letters, numbers and underscores.

Description: optional

Permissions: Private [✓ Shared in App]



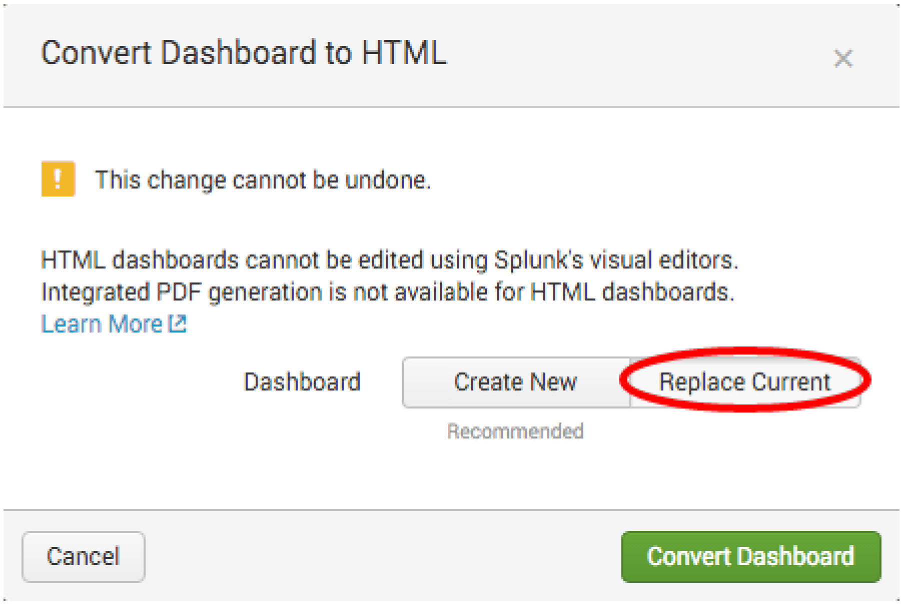


Dashboard has been converted.

You may now view your dashboard, change additional settings, or edit the HTML.

Additional Settings:

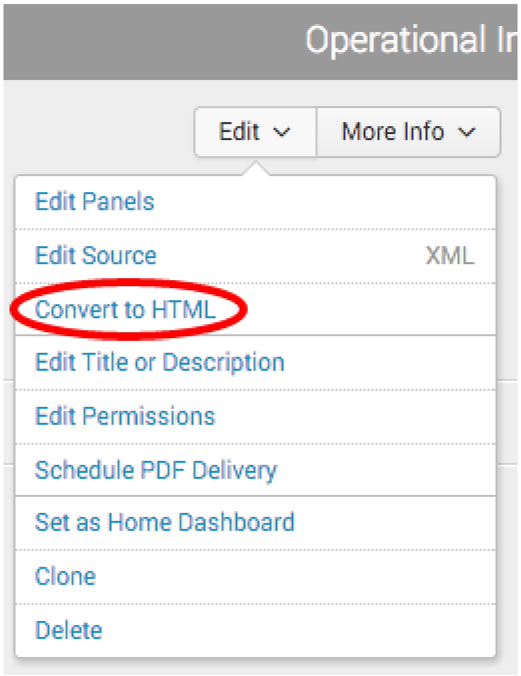
- Permissions

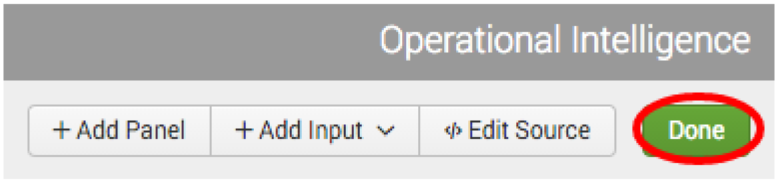

Convert Dashboard to HTML

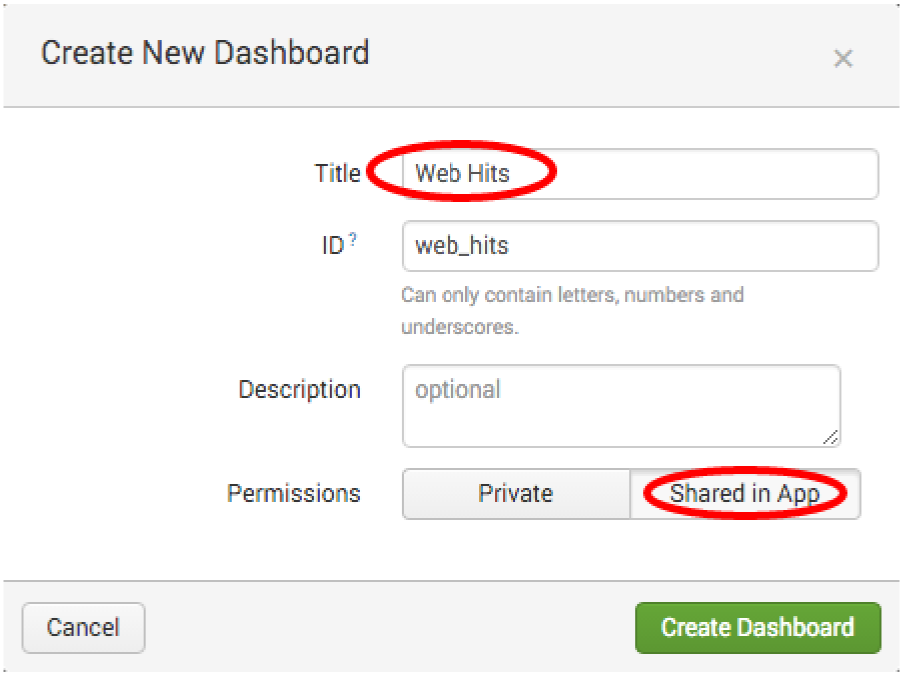
This change cannot be undone.

HTML dashboards cannot be edited using Splunk's visual editors.
Integrated PDF generation is not available for HTML dashboards.

Dashboard: [✓ Replace Current]







Create New Dashboard

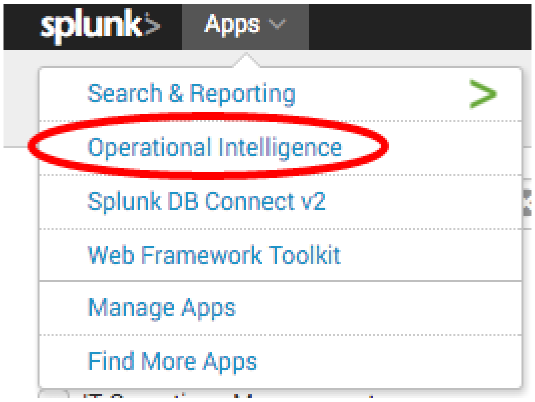
Title: Web Hits

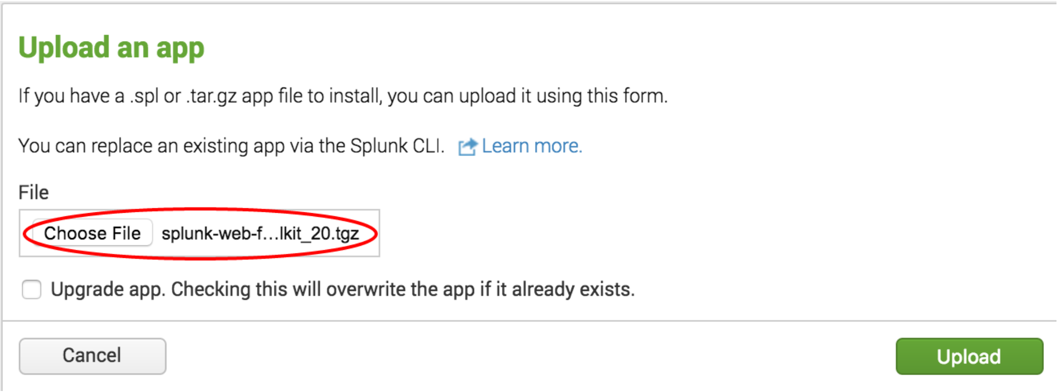
ID: web_hits

Can only contain letters, numbers and underscores.

Description: optional

Permissions: Private [✓ Shared in App]





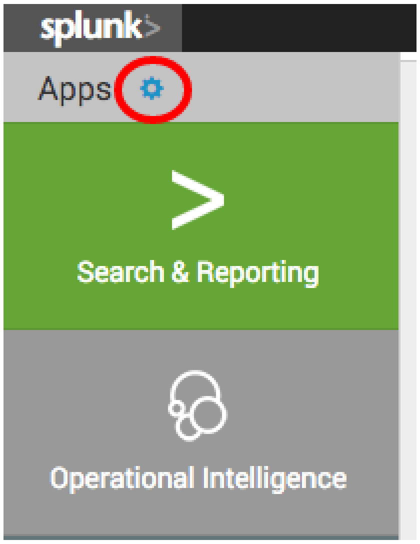
Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File: Choose File splunk-web-f...lkit_20.tgz

□ Upgrade app. Checking this will overwrite the app if it already exists.


splunk>
Apps
Search & Reporting
Operational Intelligence