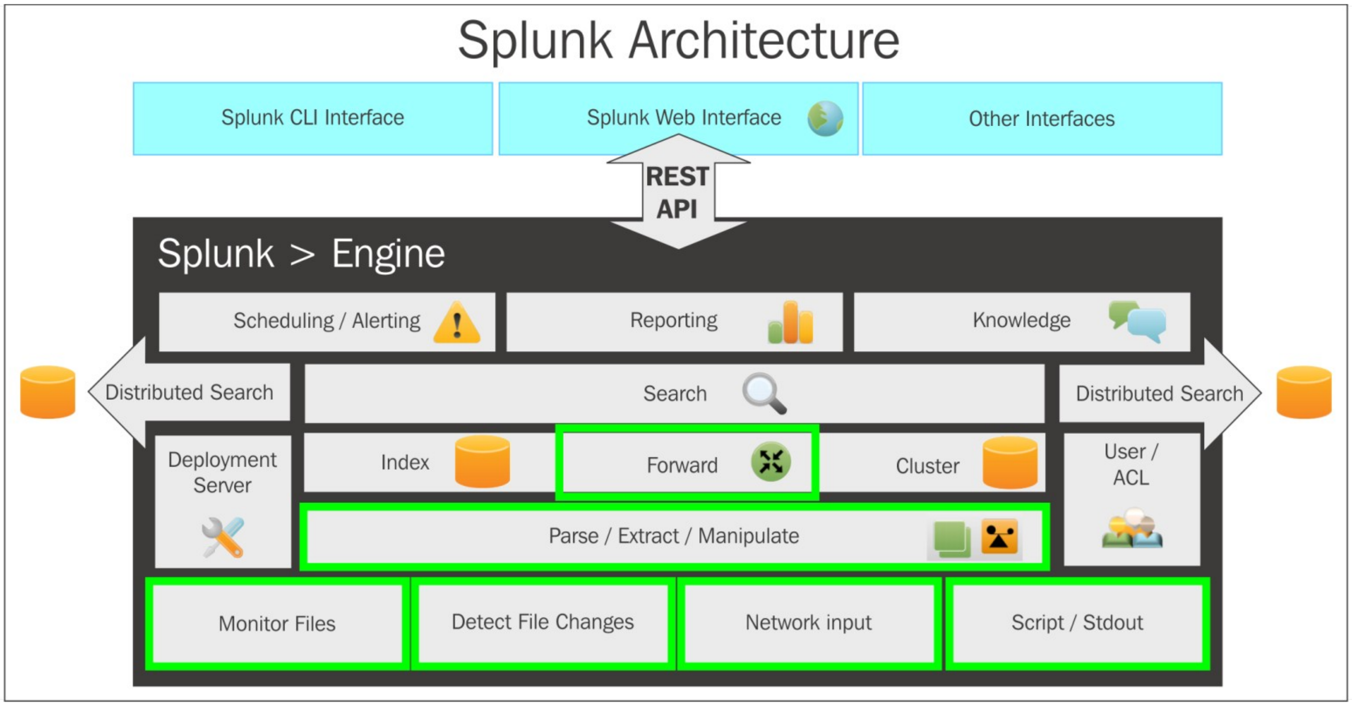
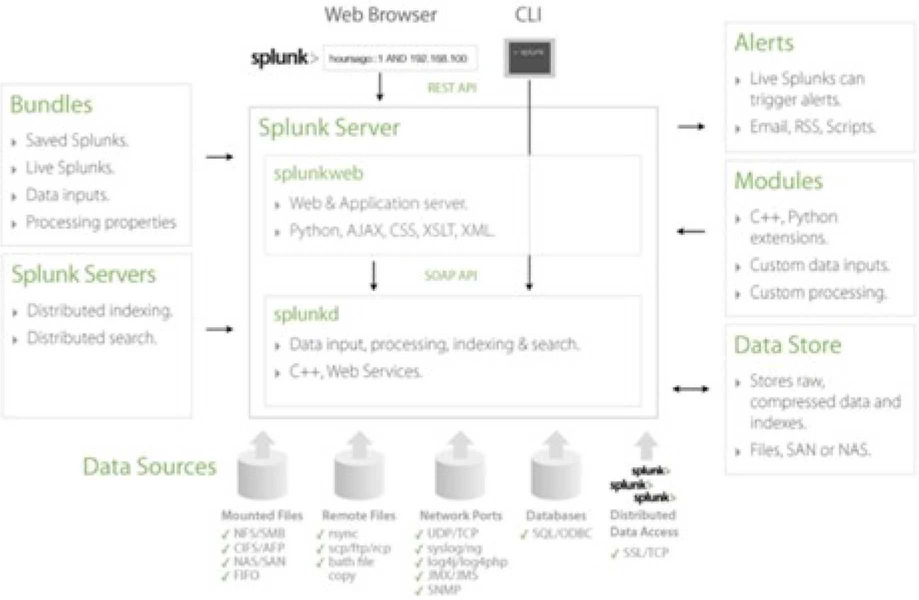
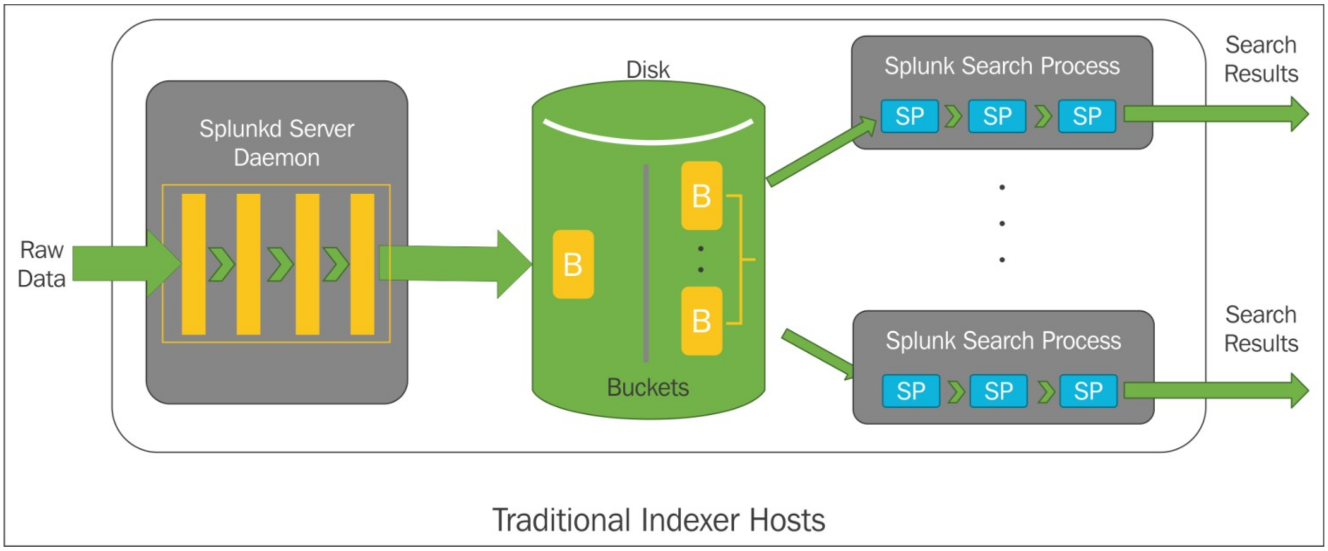
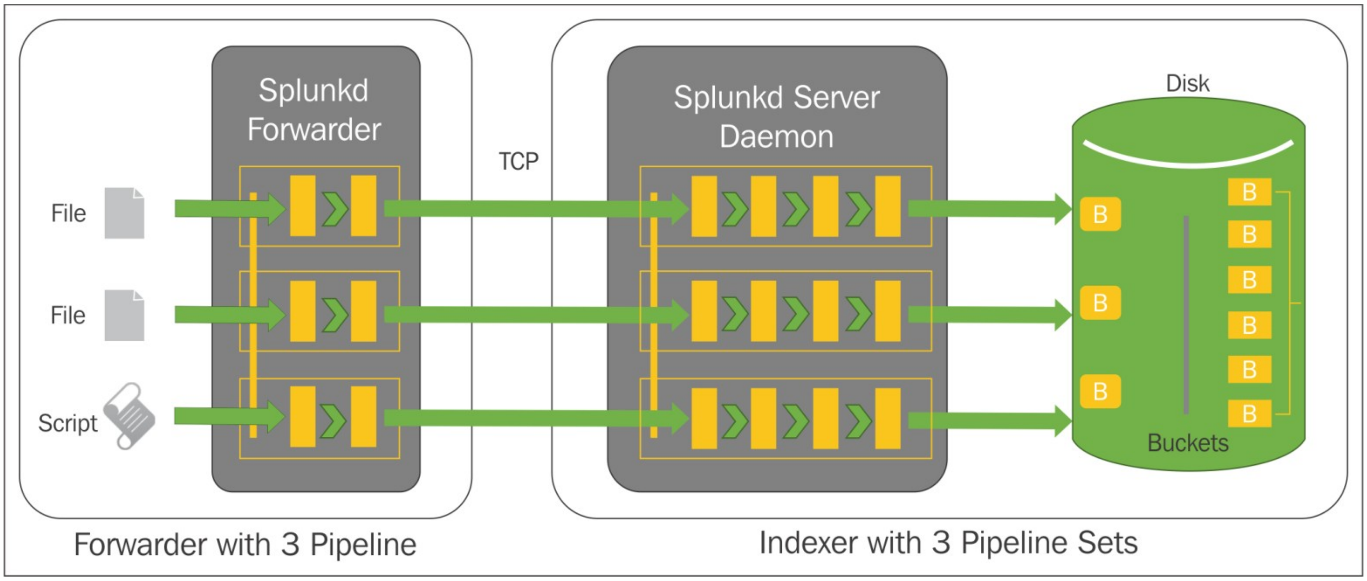
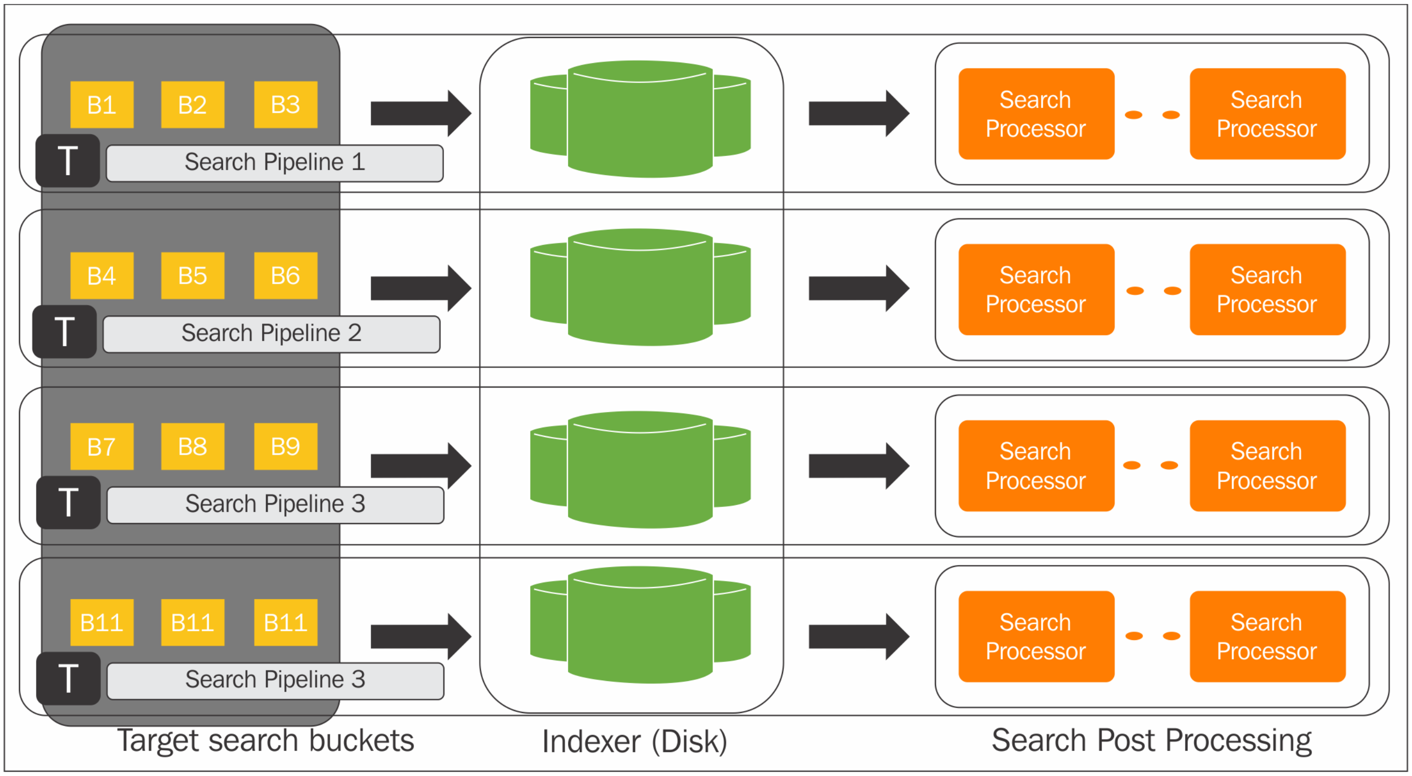
Chapter 1: What's new in Splunk 6.3?

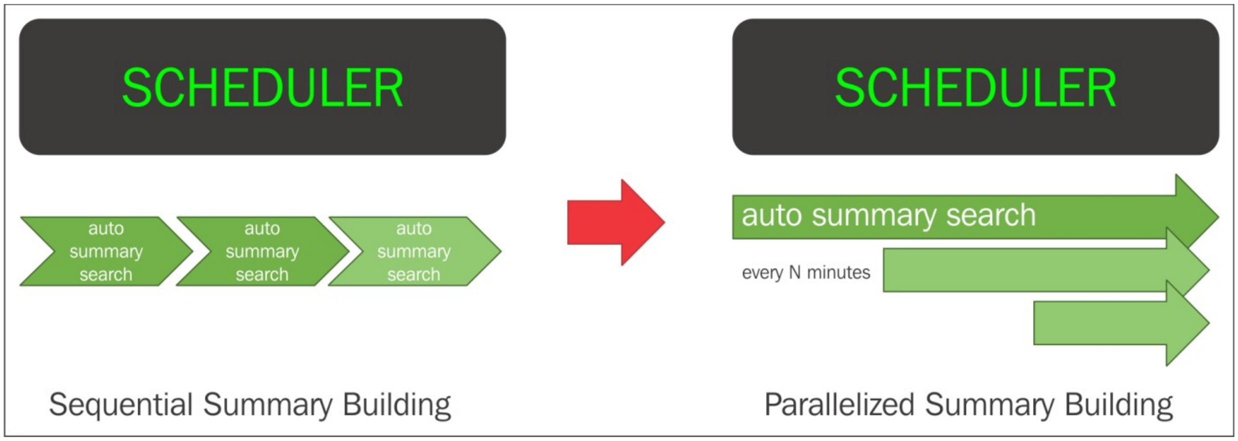


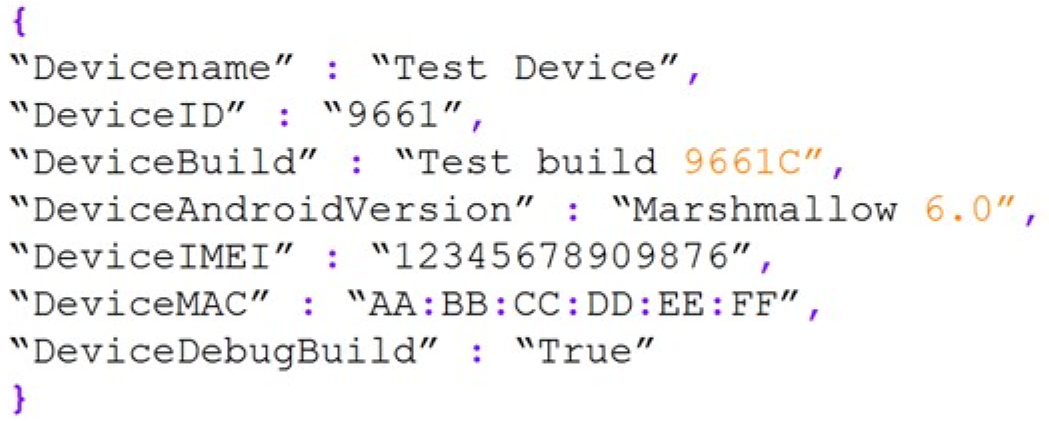



Raw Data
Splunkd Server Daemon
Disk
B
B
B
Buckets
Splunk Search Process
SP
SP
SP
Search Results
Splunk Search Process
SP
SP
SP
Search Results
Traditional Indexer Hosts

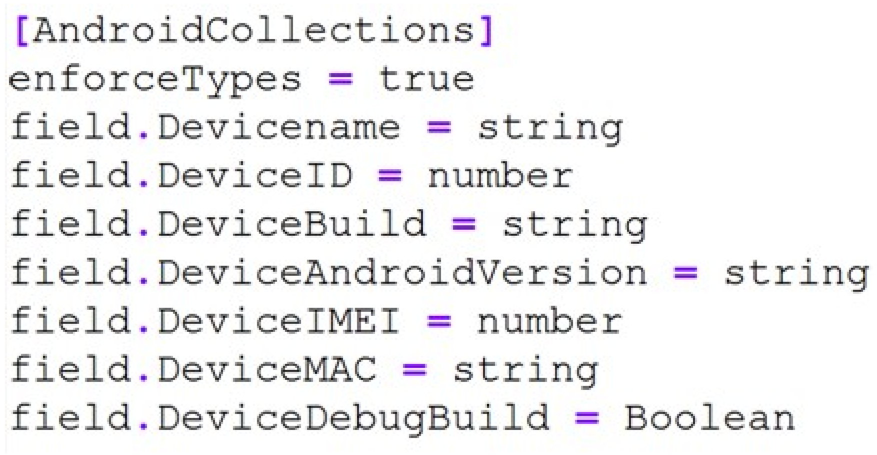

File
File
Script
Splunkd Forwarder
TCP
Splunkd Server Daemon
Disk
B
B
B
B
B
B
B
B
B
Buckets
Forwarder with 3 Pipeline
Indexer with 3 Pipeline Sets



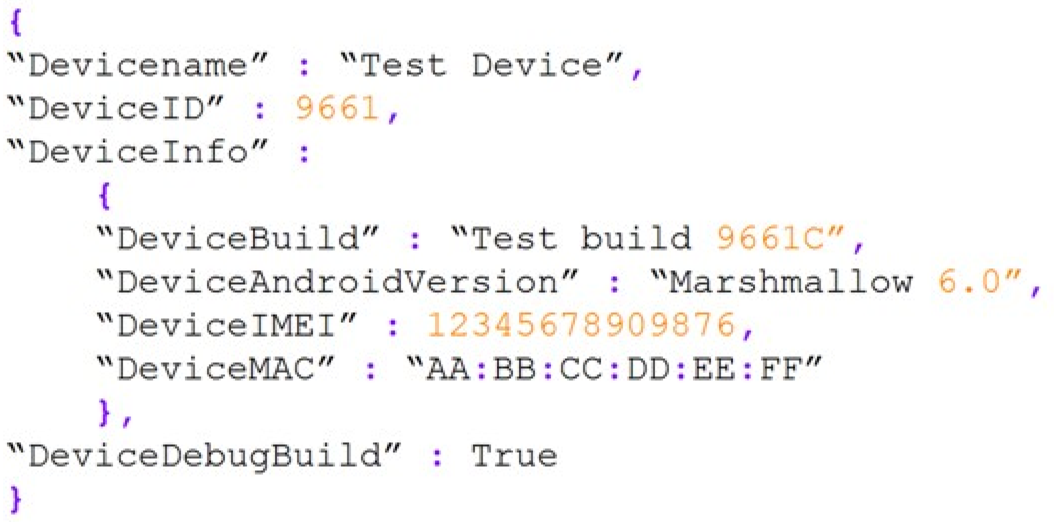




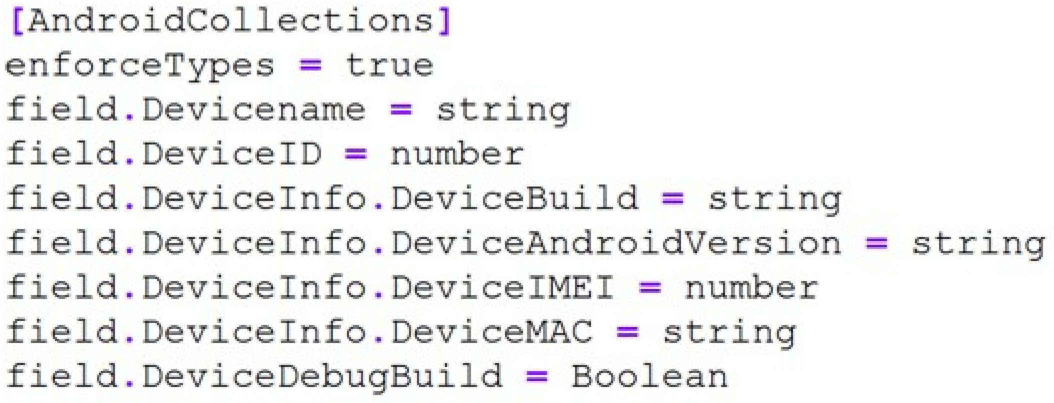
```
{
"Devicename" : "Test Device",
"DeviceID" : "9661",
"DeviceBuild" : "Test build 9661C",
"DeviceAndroidVersion" : "Marshmallow 6.0",
"DeviceIMEI" : "12345678909876",
"DeviceMAC" : "AA:BB:CC:DD:EE:FF",
"DeviceDebugBuild" : "True"
}
```



```
[AndroidCollections]
enforceTypes = true
field.Devicename = string
field.DeviceID = number
field.DeviceBuild = string
field.DeviceAndroidVersion = string
field.DeviceIMEI = number
field.DeviceMAC = string
field.DeviceDebugBuild = Boolean
```

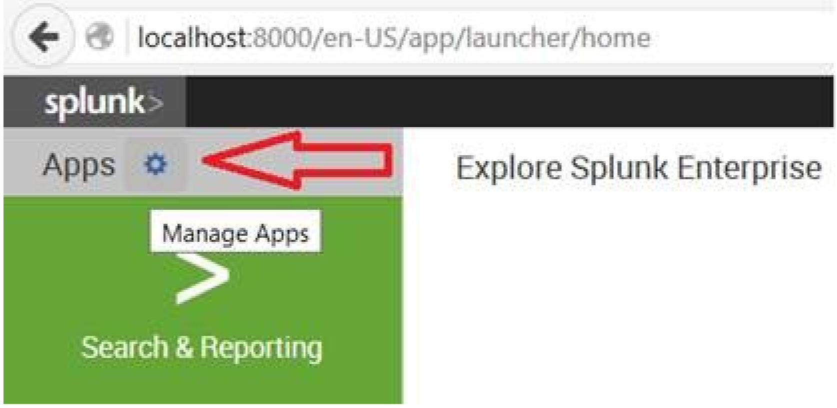


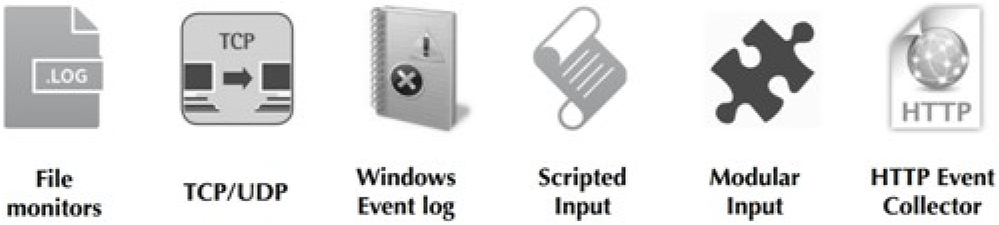
```
{
“Devicename” : “Test Device”,
“DeviceID” : 9661,
“DeviceInfo” :
    {
    “DeviceBuild” : “Test build 9661C”,
    “DeviceAndroidVersion” : “Marshmallow 6.0”,
    “DeviceIMEI” : 12345678909876,
    “DeviceMAC” : “AA:BB:CC:DD:EE:FF”
    },
“DeviceDebugBuild” : True
}
```

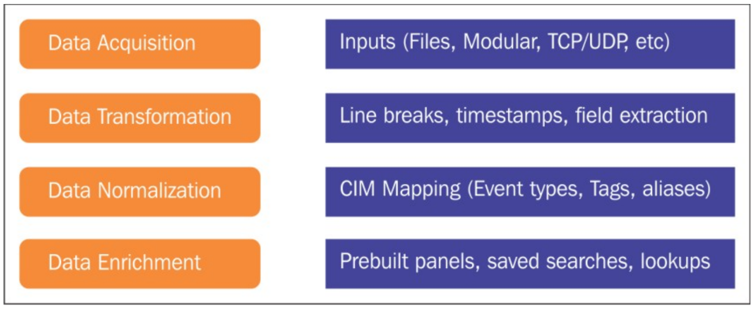


```
[AndroidCollections]
enforceTypes = true
field.Devicename = string
field.DeviceID = number
field.DeviceInfo.DeviceBuild = string
field.DeviceInfo.DeviceAndroidVersion = string
field.DeviceInfo.DeviceIMEI = number
field.DeviceInfo.DeviceMAC = string
field.DeviceDebugBuild = Boolean
```

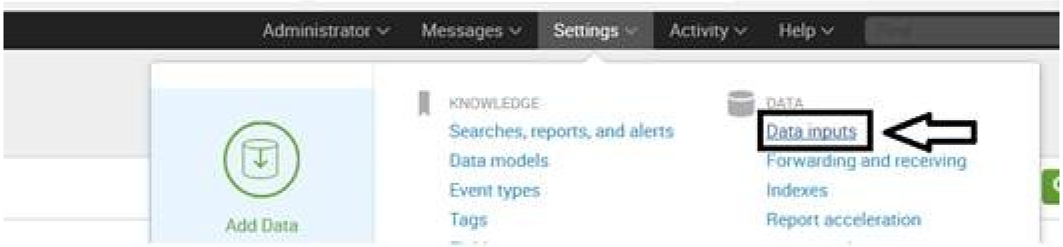
Chapter 2: Developing application on Splunk


localhost:8000/en-US/app/launcher/home
splunk>
Apps
Manage Apps
Search & Reporting
Explore Splunk Enterprise

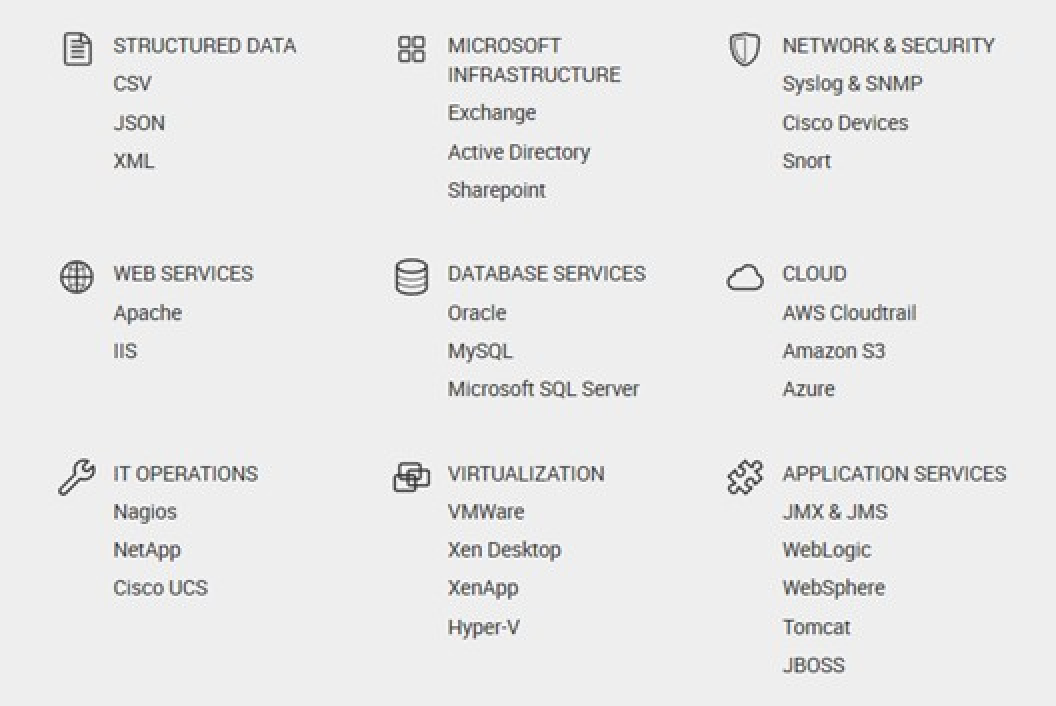




Data Acquisition	Inputs (Files, Modular, TCP/UDP, etc)
Data Transformation	Line breaks, timestamps, field extraction
Data Normalization	CIM Mapping (Event types, Tags, aliases)
Data Enrichment	Prebuilt panels, saved searches, lookups



Chapter 3: On-boarding data in Splunk



STRUCTURED DATA
CSV
JSON
XML

MICROSOFT INFRASTRUCTURE
Exchange
Active Directory
Sharepoint

NETWORK & SECURITY
Syslog & SNMP
Cisco Devices
Snort

WEB SERVICES
Apache
IIS

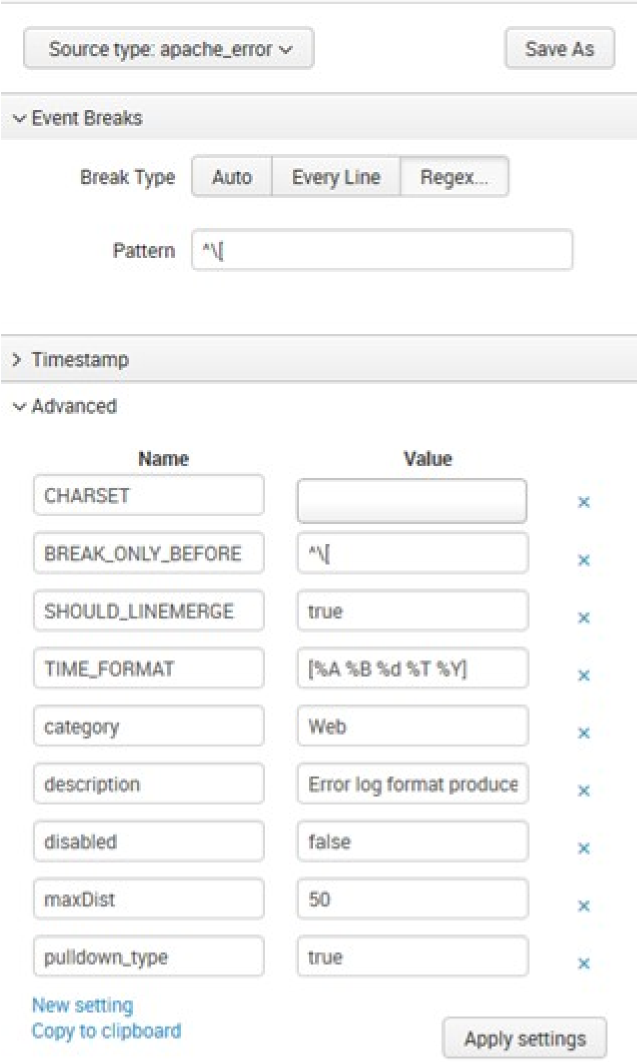
DATABASE SERVICES
Oracle
MySQL
Microsoft SQL Server

CLOUD
AWS Cloudtrail
Amazon S3
Azure

IT OPERATIONS
Nagios
NetApp
Cisco UCS

VIRTUALIZATION
VMWare
Xen Desktop
XenApp
Hyper-V

APPLICATION SERVICES
JMX & JMS
WebLogic
WebSphere
Tomcat
JBOSS



Source type: apache_error ⌄ Save As

⌄ Event Breaks

Break Type: Auto | Every Line | [✓ Regex...]

Pattern: ^\[

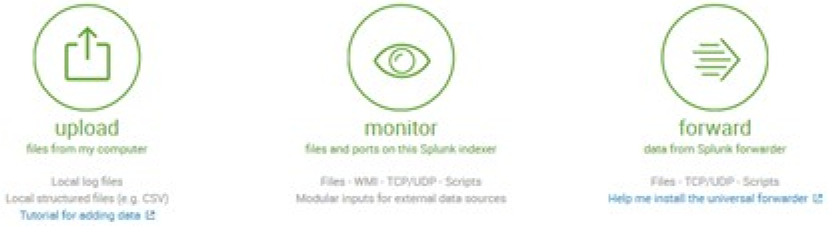
> Timestamp

⌄ Advanced

Name	Value
CHARSET	
BREAK_ONLY_BEFORE	^\[
SHOULD_LINEMERGE	true
TIME_FORMAT	[%A %B %d %T %Y]
category	Web
description	Error log format produce
disabled	false
maxDist	50
pulldown_type	true

New setting
Copy to clipboard

Apply settings



upload
files from my computer

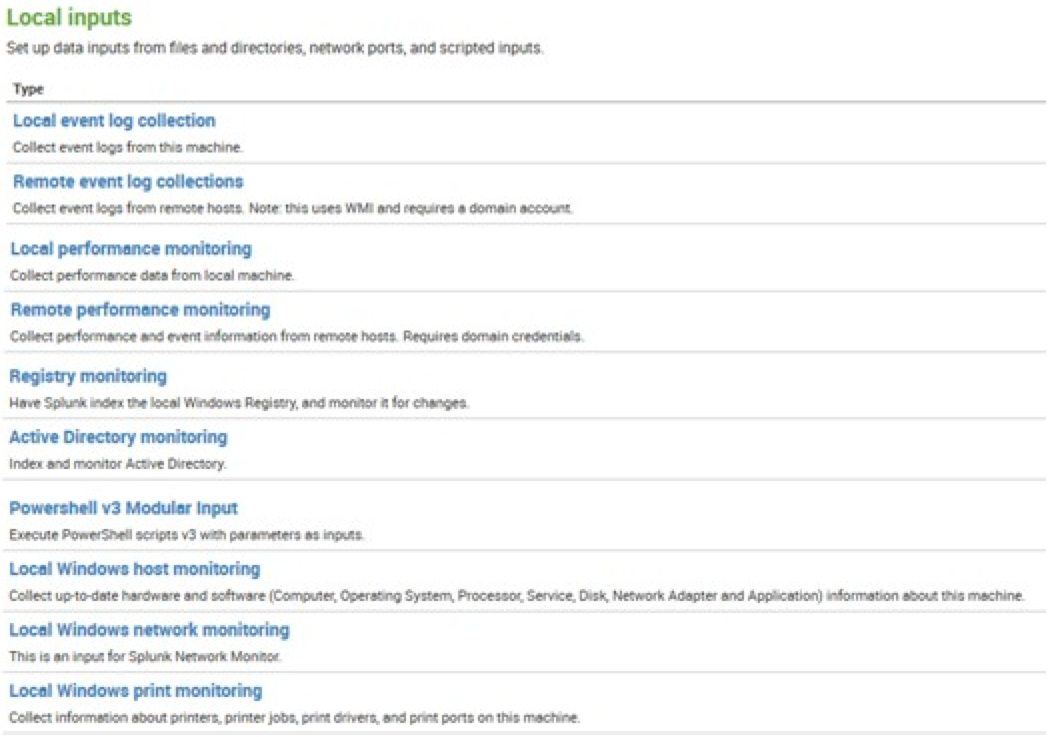
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

monitor
files and ports on this Splunk indexer

Files · WMI · TCP/UDP · Scripts
Modular inputs for external data sources

forward
data from Splunk forwarder

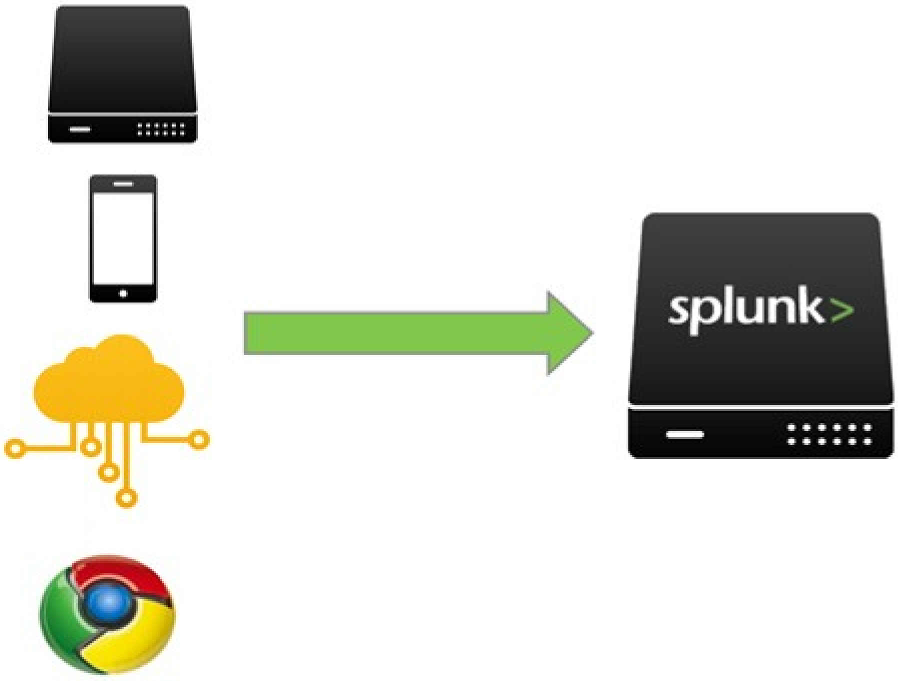
Files · TCP/UDP · Scripts
Help me install the universal forwarder

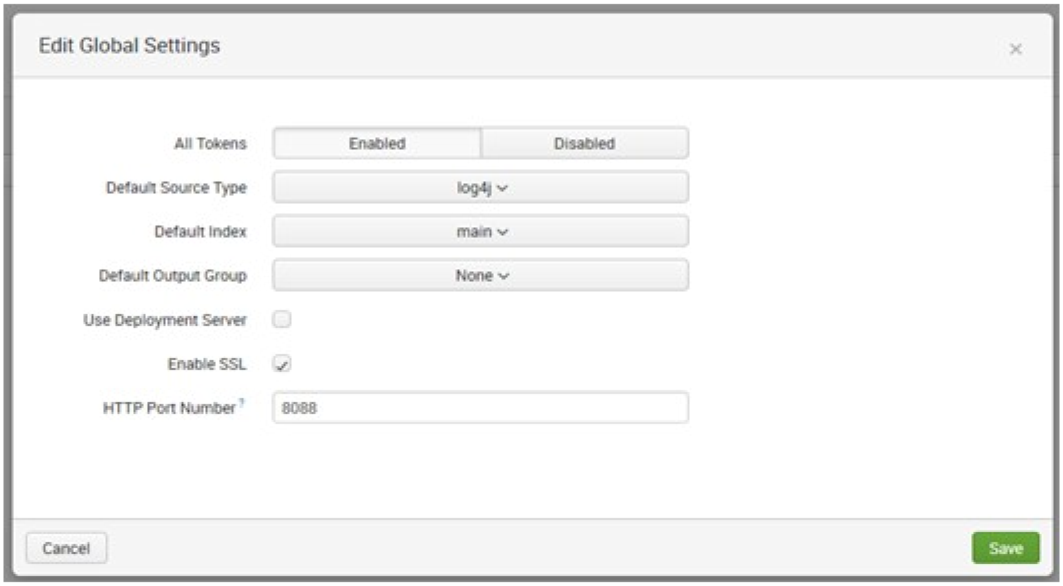


Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs.

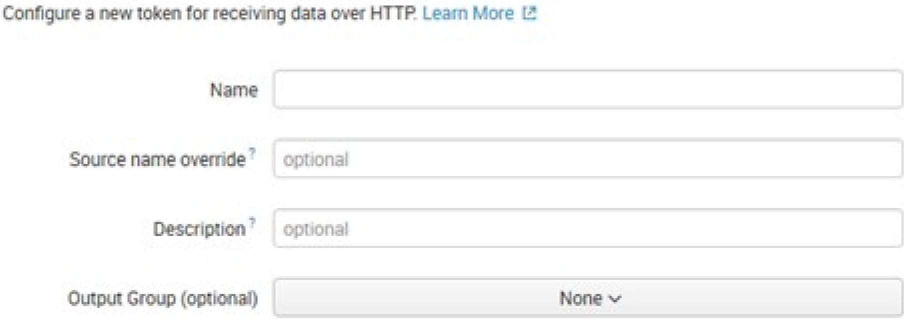
Type
Local event log collection Collect event logs from this machine.
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.
Local performance monitoring Collect performance data from local machine.
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.
Registry monitoring Have Splunk index the local Windows Registry, and monitor it for changes.
Active Directory monitoring Index and monitor Active Directory.
Powershell v3 Modular Input Execute PowerShell scripts v3 with parameters as inputs.
Local Windows host monitoring Collect up-to-date hardware and software (Computer, Operating System, Processor, Service, Disk, Network Adapter and Application) information about this machine.
Local Windows network monitoring This is an input for Splunk Network Monitor.
Local Windows print monitoring Collect information about printers, printer jobs, print drivers, and print ports on this machine.





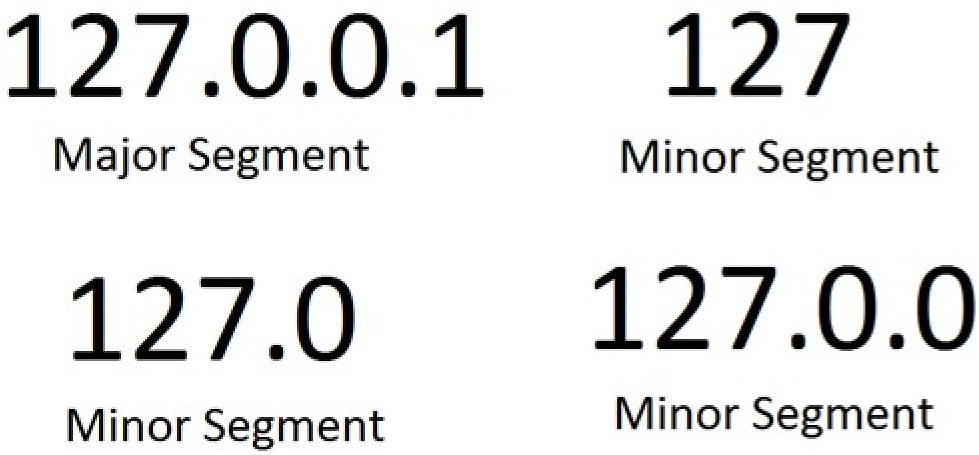
Edit Global Settings

All Tokens	Enabled / Disabled
Default Source Type	log4j
Default Index	main
Default Output Group	None
Use Deployment Server	□
Enable SSL	☑
HTTP Port Number	8088



Configure a new token for receiving data over HTTP. Learn More

Name	
Source name override	optional
Description	optional
Output Group (optional)	None



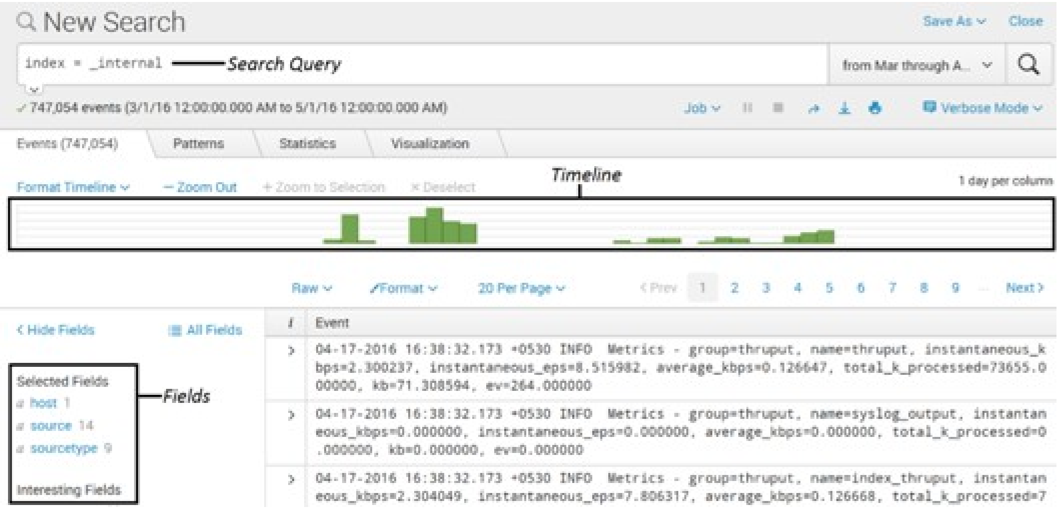
127.0.0.1
Major Segment

127
Minor Segment

127.0
Minor Segment

127.0.0
Minor Segment

Chapter 4: Data Analytics

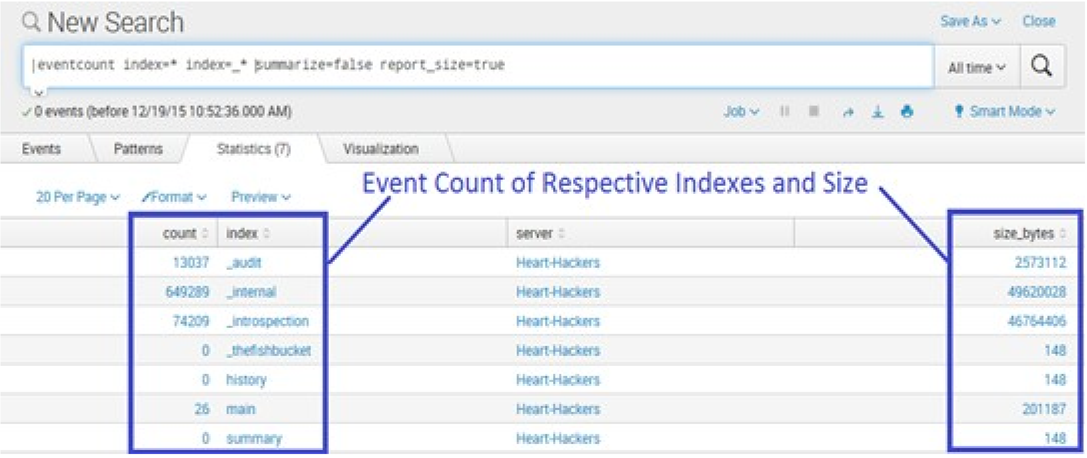


```
index = _internal
```

from Mar through A...

✓ 747,054 events (3/1/16 12:00:00.000 AM to 5/1/16 12:00:00.000 AM)

```
04-17-2016 16:38:32.173 +0530 INFO  Metrics - group=thruput, name=thruput, instantaneous_k
bps=2.300237, instantaneous_eps=8.515982, average_kbps=0.126647, total_k_processed=73655.0
00000, kb=71.308594, ev=264.000000

04-17-2016 16:38:32.173 +0530 INFO  Metrics - group=thruput, name=syslog_output, instantan
eous_kbps=0.000000, instantaneous_eps=0.000000, average_kbps=0.000000, total_k_processed=0
.000000, kb=0.000000, ev=0.000000

04-17-2016 16:38:32.173 +0530 INFO  Metrics - group=thruput, name=index_thruput, instantan
eous_kbps=2.304049, instantaneous_eps=7.806317, average_kbps=0.126668, total_k_processed=7
```

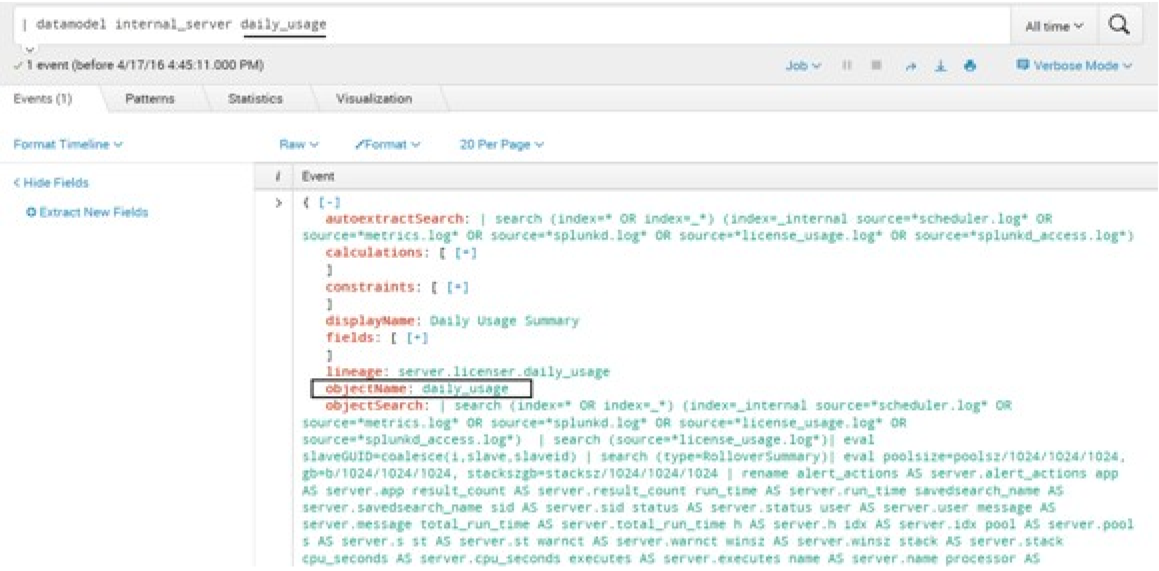


```
|eventcount index=* index=_* summarize=false report_size=true
```

All time

✓ 0 events (before 12/19/15 10:52:36.000 AM)

count	index	server	size_bytes
13037	_audit	Heart-Hackers	2573112
649289	_internal	Heart-Hackers	49620028
74209	_introspection	Heart-Hackers	46764406
0	_thefishbucket	Heart-Hackers	148
0	history	Heart-Hackers	148
26	main	Heart-Hackers	201187
0	summary	Heart-Hackers	148

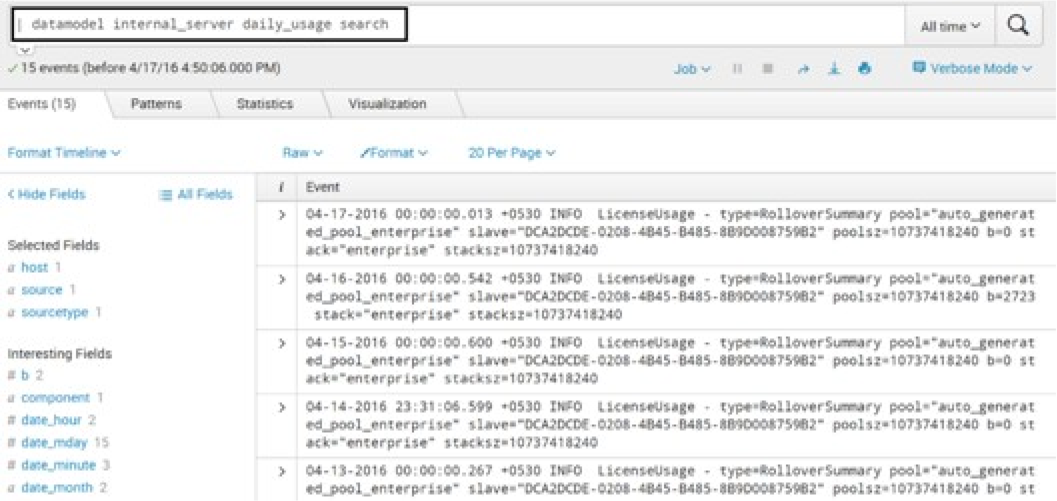


```
| datamodel internal_server daily_usage
```

All time

✓ 1 event (before 4/17/16 4:45:11.000 PM)

```
{ [-]
   autoextractSearch: | search (index=* OR index=_*) (index=_internal source=*scheduler.log* OR
source=*metrics.log* OR source=*splunkd.log* OR source=*license_usage.log* OR source=*splunkd_access.log*)
   calculations: [ [+]
   ]
   constraints: [ [+]
   ]
   displayName: Daily Usage Summary
   fields: [ [+]
   ]
   lineage: server.licenser.daily_usage
   objectName: daily_usage
   objectSearch: | search (index=* OR index=_*) (index=_internal source=*scheduler.log* OR
source=*metrics.log* OR source=*splunkd.log* OR source=*license_usage.log* OR
source=*splunkd_access.log*)  | search (source=*license_usage.log*)| eval
slaveGUID=coalesce(i,slave,slaveid) | search (type=RolloverSummary)| eval poolsize=poolsz/1024/1024/1024,
gb=b/1024/1024/1024, stackszgb=stacksz/1024/1024/1024 | rename alert_actions AS server.alert_actions app
AS server.app result_count AS server.result_count run_time AS server.run_time savedsearch_name AS
server.savedsearch_name sid AS server.sid status AS server.status user AS server.user message AS
server.message total_run_time AS server.total_run_time h AS server.h idx AS server.idx pool AS server.pool
s AS server.s st AS server.st warnct AS server.warnct winsz AS server.winsz stack AS server.stack
cpu_seconds AS server.cpu_seconds executes AS server.executes name AS server.name processor AS
```



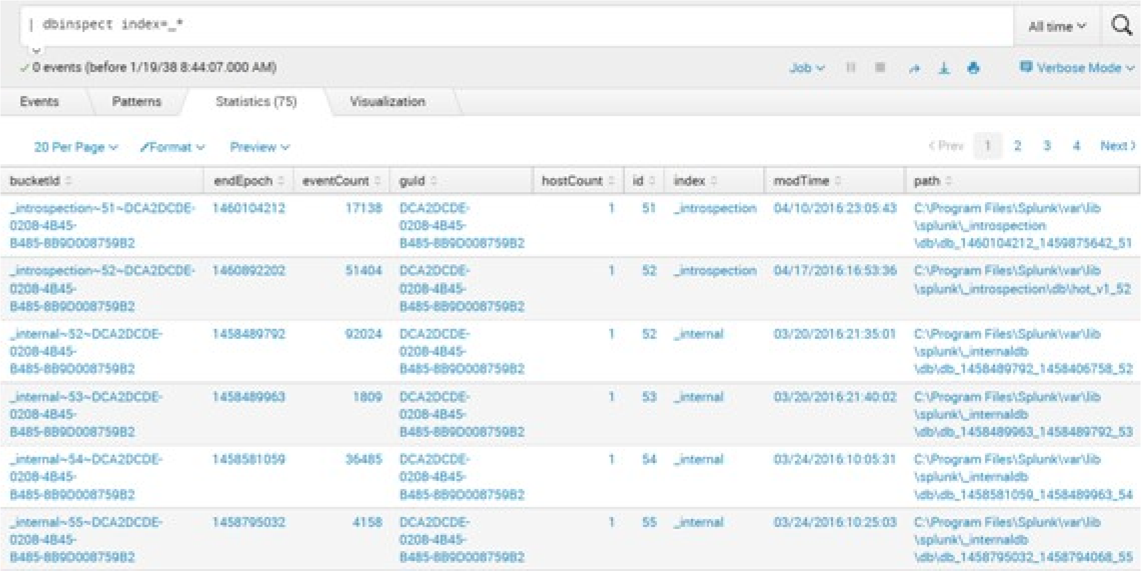
```
| datamodel internal_server daily_usage search
```

✓ 15 events (before 4/17/16 4:50:06.000 PM)

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

Interesting Fields
- # b 2
- a component 1
- # date_hour 2
- # date_mday 15
- # date_minute 3
- a date_month 2

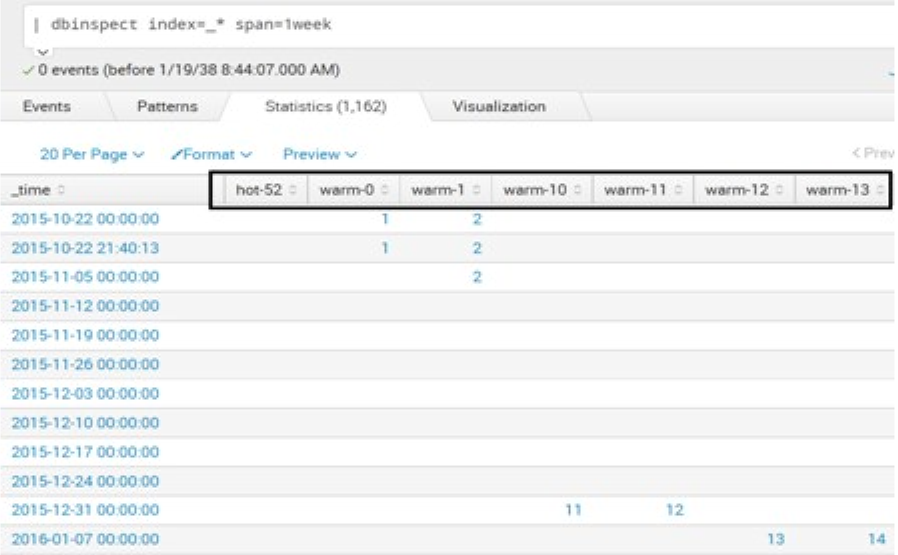
```
i  Event
>  04-17-2016 00:00:00.013 +0530 INFO  LicenseUsage - type=RolloverSummary pool="auto_generat
   ed_pool_enterprise" slave="DCA2DCDE-0208-4B45-B485-8B9D008759B2" poolsz=10737418240 b=0 st
   ack="enterprise" stacksz=10737418240
>  04-16-2016 00:00:00.542 +0530 INFO  LicenseUsage - type=RolloverSummary pool="auto_generat
   ed_pool_enterprise" slave="DCA2DCDE-0208-4B45-B485-8B9D008759B2" poolsz=10737418240 b=2723
    stack="enterprise" stacksz=10737418240
>  04-15-2016 00:00:00.600 +0530 INFO  LicenseUsage - type=RolloverSummary pool="auto_generat
   ed_pool_enterprise" slave="DCA2DCDE-0208-4B45-B485-8B9D008759B2" poolsz=10737418240 b=0 st
   ack="enterprise" stacksz=10737418240
>  04-14-2016 23:31:06.599 +0530 INFO  LicenseUsage - type=RolloverSummary pool="auto_generat
   ed_pool_enterprise" slave="DCA2DCDE-0208-4B45-B485-8B9D008759B2" poolsz=10737418240 b=0 st
   ack="enterprise" stacksz=10737418240
>  04-13-2016 00:00:00.267 +0530 INFO  LicenseUsage - type=RolloverSummary pool="auto_generat
   ed_pool_enterprise" slave="DCA2DCDE-0208-4B45-B485-8B9D008759B2" poolsz=10737418240 b=0 st
```



```
| dbinspect index=_*
```

✓ 0 events (before 1/19/38 8:44:07.000 AM)

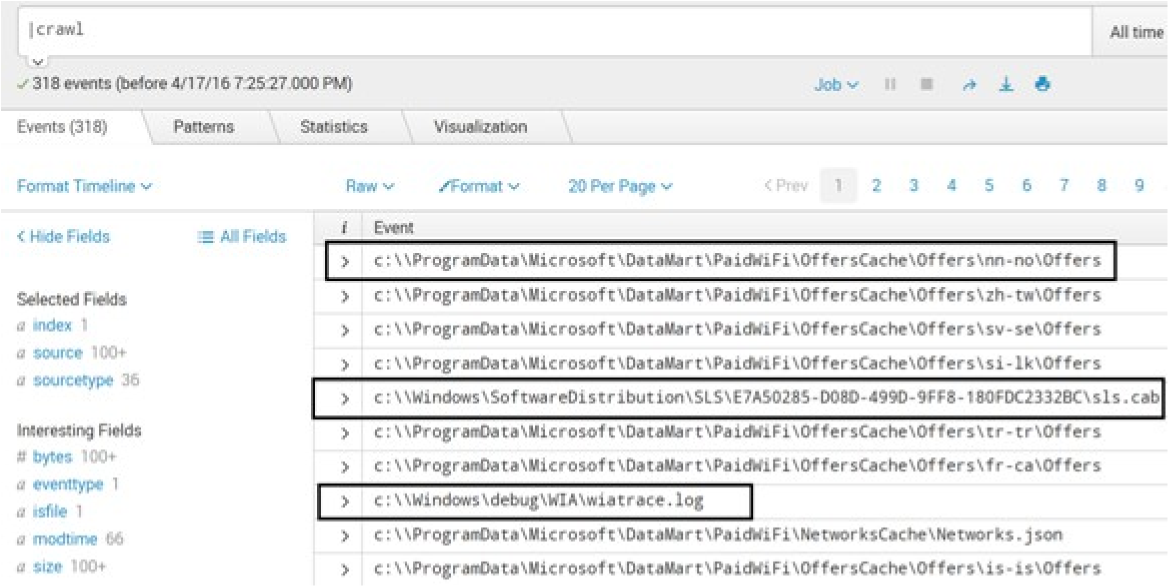
bucketId	endEpoch	eventCount	guId	hostCount	id	index	modTime	path
_introspection~51~DCA2DCDE-0208-4B45-B485-8B9D008759B2	1460104212	17138	DCA2DCDE-0208-4B45-B485-8B9D008759B2	1	51	_introspection	04/10/2016 23:05:43	C:\Program Files\Splunk\var\lib\splunk_introspection\db\db_1460104212_1459875642_51
_introspection~52~DCA2DCDE-0208-4B45-B485-8B9D008759B2	1460892202	51404	DCA2DCDE-0208-4B45-B485-8B9D008759B2	1	52	_introspection	04/17/2016 16:53:36	C:\Program Files\Splunk\var\lib\splunk_introspection\db\hot_v1_52
_internal~52~DCA2DCDE-0208-4B45-B485-8B9D008759B2	1458489792	92024	DCA2DCDE-0208-4B45-B485-8B9D008759B2	1	52	_internal	03/20/2016 21:35:01	C:\Program Files\Splunk\var\lib\splunk_internaldb\db\db_1458489792_1458406758_52
_internal~53~DCA2DCDE-0208-4B45-B485-8B9D008759B2	1458489963	1809	DCA2DCDE-0208-4B45-B485-8B9D008759B2	1	53	_internal	03/20/2016 21:40:02	C:\Program Files\Splunk\var\lib\splunk_internaldb\db\db_1458489963_1458489792_53
_internal~54~DCA2DCDE-0208-4B45-B485-8B9D008759B2	1458581059	36485	DCA2DCDE-0208-4B45-B485-8B9D008759B2	1	54	_internal	03/24/2016 10:05:31	C:\Program Files\Splunk\var\lib\splunk_internaldb\db\db_1458581059_1458489963_54
_internal~55~DCA2DCDE-0208-4B45-B485-8B9D008759B2	1458795032	4158	DCA2DCDE-0208-4B45-B485-8B9D008759B2	1	55	_internal	03/24/2016 10:25:03	C:\Program Files\Splunk\var\lib\splunk_internaldb\db\db_1458795032_1458794068_55



```
| dbinspect index=_* span=1week
```

✓ 0 events (before 1/19/38 8:44:07.000 AM)

_time	hot-52	warm-0	warm-1	warm-10	warm-11	warm-12	warm-13
2015-10-22 00:00:00		1	2				
2015-10-22 21:40:13		1	2				
2015-11-05 00:00:00			2				
2015-11-12 00:00:00							
2015-11-19 00:00:00							
2015-11-26 00:00:00							
2015-12-03 00:00:00							
2015-12-10 00:00:00							
2015-12-17 00:00:00							
2015-12-24 00:00:00							
2015-12-31 00:00:00				11	12		
2016-01-07 00:00:00						13	14



```
|crawl
```

✓ 318 events (before 4/17/16 7:25:27.000 PM)

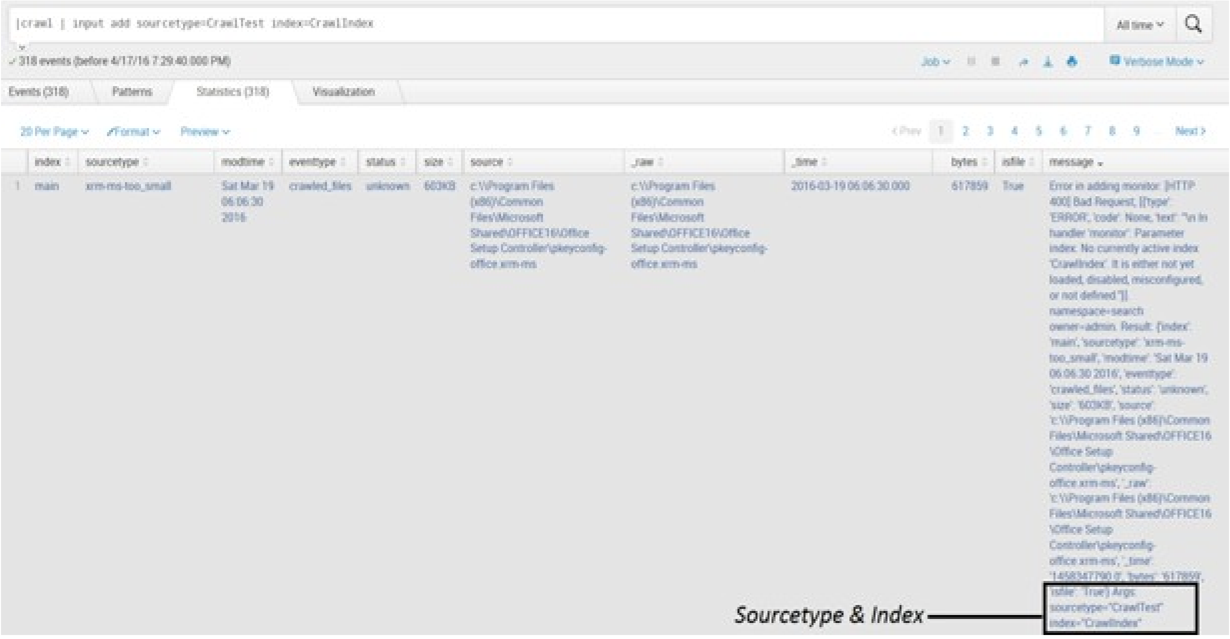
Selected Fields

- a index 1
- a source 100+
- a sourcetype 36

Interesting Fields

- # bytes 100+
- a eventtype 1
- a isfile 1
- a modtime 66
- a size 100+

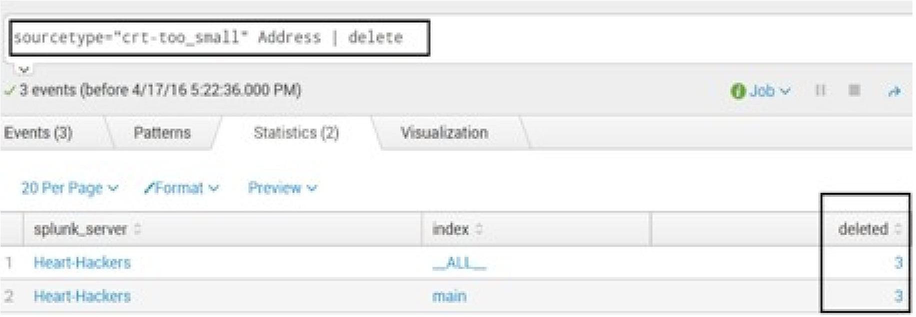
```
i  Event
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\OffersCache\Offers\nn-no\Offers
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\OffersCache\Offers\zh-tw\Offers
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\OffersCache\Offers\sv-se\Offers
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\OffersCache\Offers\si-lk\Offers
>  c:\\Windows\SoftwareDistribution\SLS\E7A50285-D08D-499D-9FF8-180FDC2332BC\sls.cab
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\OffersCache\Offers\tr-tr\Offers
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\OffersCache\Offers\fr-ca\Offers
>  c:\\Windows\debug\WIA\wiatrace.log
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\NetworksCache\Networks.json
>  c:\\ProgramData\Microsoft\DataMart\PaidWiFi\OffersCache\Offers\is-is\Offers
```



```
|crawl | input add sourcetype=CrawlTest index=CrawlIndex
```

✓ 318 events (before 4/17/16 7:29:40.000 PM)

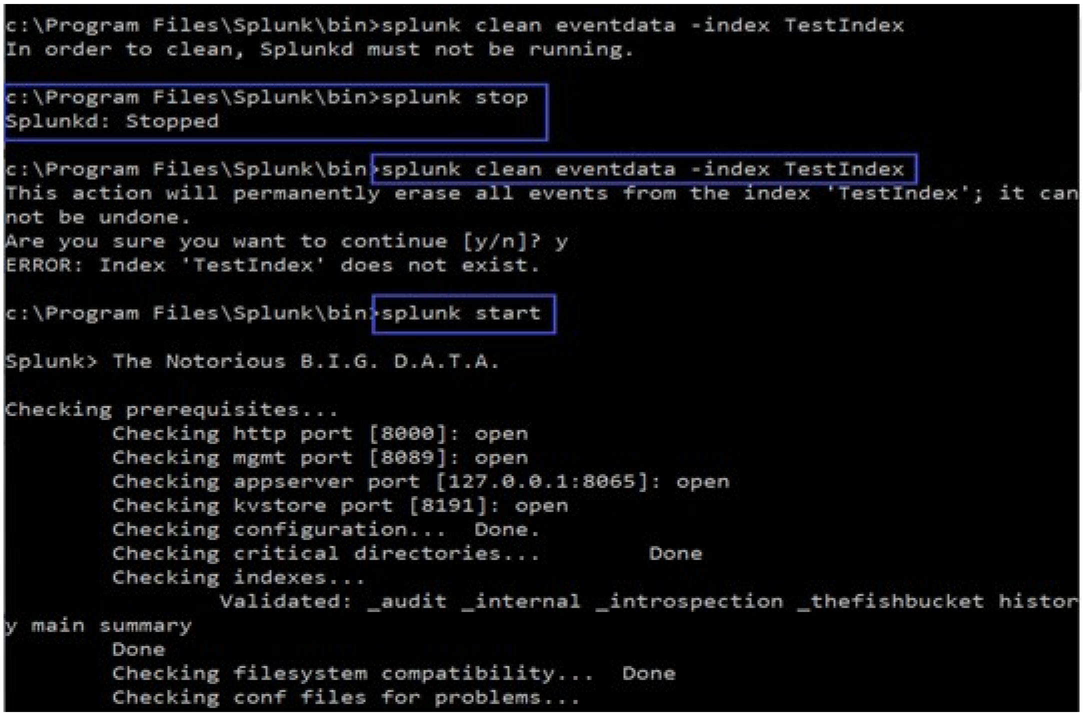
	index	sourcetype	modtime	eventtype	status	size	source	_raw	_time	bytes	isfile	message
1	main	xrm-ms-too_small	Sat Mar 19 06:06:30 2016	crawled_files	unknown	603KB	c:\\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms	c:\\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms	2016-03-19 06:06:30.000	617859	True	Error in adding monitor: [HTTP 400] Bad Request; [{'type': 'ERROR', 'code': None, 'text': "\n In handler 'monitor': Parameter index: No currently active index 'CrawlIndex'. It is either not yet loaded, disabled, misconfigured, or not defined."}]. namespace=search owner=admin. Result: {'index': 'main', 'sourcetype': 'xrm-ms-too_small', 'modtime': 'Sat Mar 19 06:06:30 2016', 'eventtype': 'crawled_files', 'status': 'unknown', 'size': '603KB', 'source': 'c:\\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms', '_raw': 'c:\\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms', '_time': '1458347790.0', 'bytes': '617859', 'isfile': 'True'} Args: sourcetype="CrawlTest" index="CrawlIndex"



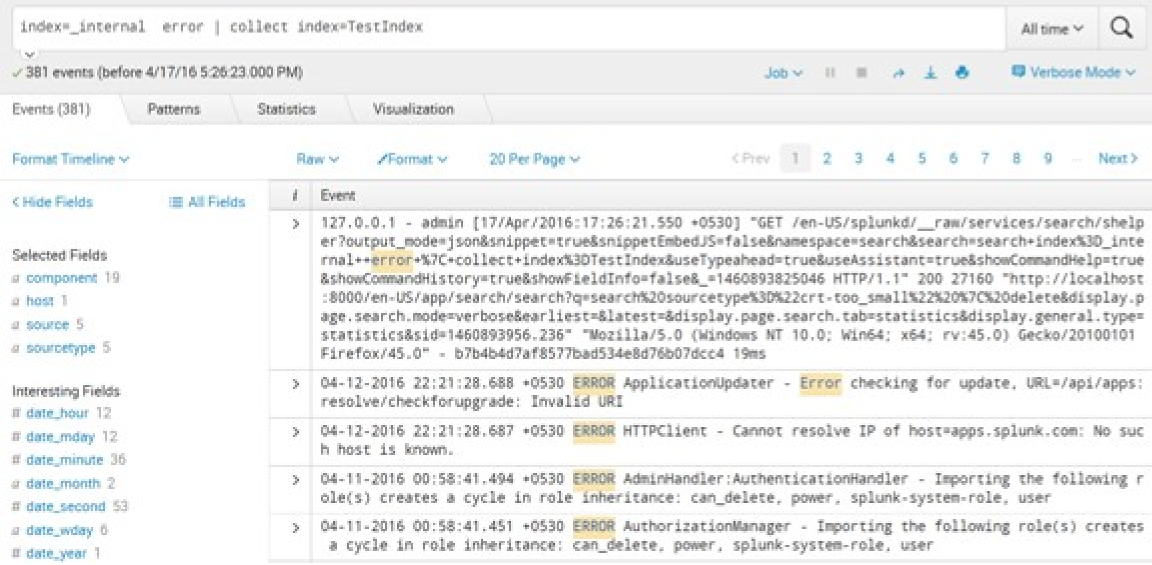
```
sourcetype="crt-too_small" Address | delete
```

✓ 3 events (before 4/17/16 5:22:36.000 PM)

	splunk_server	index	deleted
1	Heart-Hackers	__ALL__	3
2	Heart-Hackers	main	3



```
c:\Program Files\Splunk\bin>splunk clean eventdata -index TestIndex
In order to clean, Splunkd must not be running.

c:\Program Files\Splunk\bin>splunk stop
Splunkd: Stopped

c:\Program Files\Splunk\bin>splunk clean eventdata -index TestIndex
This action will permanently erase all events from the index 'TestIndex'; it can
not be undone.
Are you sure you want to continue [y/n]? y
ERROR: Index 'TestIndex' does not exist.

c:\Program Files\Splunk\bin>splunk start

Splunk> The Notorious B.I.G. D.A.T.A.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration...  Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _internal _introspection _thefishbucket histor
y main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
```



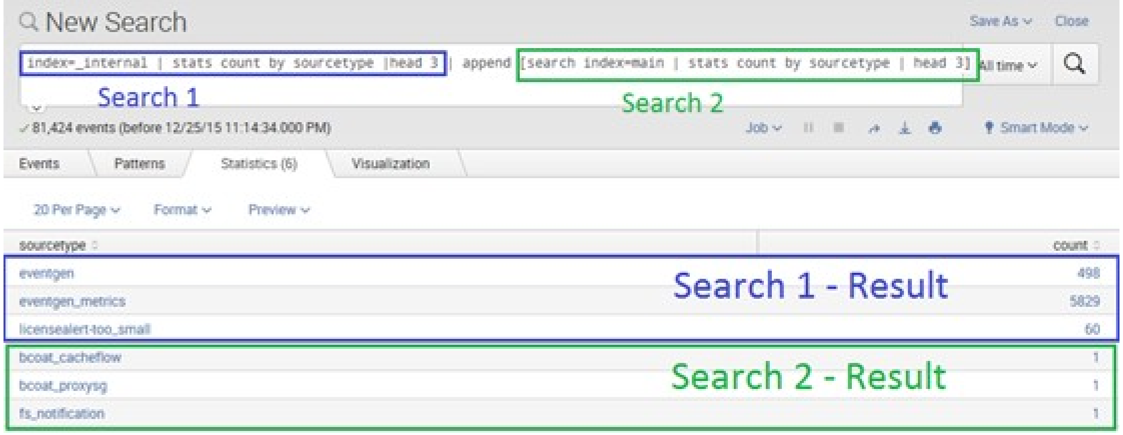
```
index=_internal  error | collect index=TestIndex
```

✓381 events (before 4/17/16 5:26:23.000 PM)

Selected Fields
- component 19
- host 1
- source 5
- sourcetype 5

Interesting Fields
- date_hour 12
- date_mday 12
- date_minute 36
- date_month 2
- date_second 53
- date_wday 6
- date_year 1

```
i  Event
>  127.0.0.1 - admin [17/Apr/2016:17:26:21.550 +0530] "GET /en-US/splunkd/__raw/services/search/shelp
   er?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search+index%3D_inte
   rnal++error+%7C+collect+index%3DTestIndex&useTypeahead=true&useAssistant=true&showCommandHelp=true
   &showCommandHistory=true&showFieldInfo=false&_=1460893825046 HTTP/1.1" 200 27160 "http://localhost
   :8000/en-US/app/search/search?q=search%20sourcetype%3D%22crt-too_small%22%20%7C%20delete&display.p
   age.search.mode=verbose&earliest=&latest=&display.page.search.tab=statistics&display.general.type=
   statistics&sid=1460893956.236" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0) Gecko/20100101
   Firefox/45.0" - b7b4b4d7af8577bad534e8d76b07dcc4 19ms
>  04-12-2016 22:21:28.688 +0530 ERROR ApplicationUpdater - Error checking for update, URL=/api/apps:
   resolve/checkforupgrade: Invalid URI
>  04-12-2016 22:21:28.687 +0530 ERROR HTTPClient - Cannot resolve IP of host=apps.splunk.com: No suc
   h host is known.
>  04-11-2016 00:58:41.494 +0530 ERROR AdminHandler:AuthenticationHandler - Importing the following r
   ole(s) creates a cycle in role inheritance: can_delete, power, splunk-system-role, user
>  04-11-2016 00:58:41.451 +0530 ERROR AuthorizationManager - Importing the following role(s) creates
    a cycle in role inheritance: can_delete, power, splunk-system-role, user
```



```
index=_internal | stats count by sourcetype |head 3| append [search index=main | stats count by sourcetype | head 3]
```

Search 1

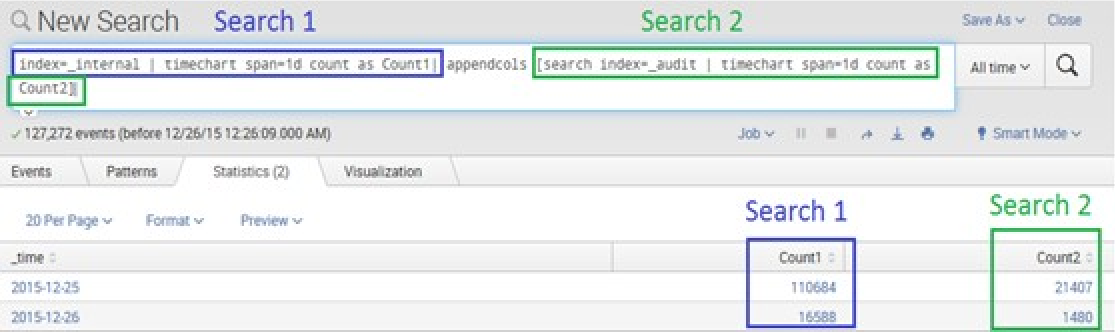
Search 2

✓81,424 events (before 12/25/15 11:14:34.000 PM)

sourcetype	count
eventgen	498
eventgen_metrics	5829
licensealert-too_small	60
bcoat_cacheflow	1
bcoat_proxysg	1
fs_notification	1

Search 1 - Result

Search 2 - Result



Search 1

Search 2

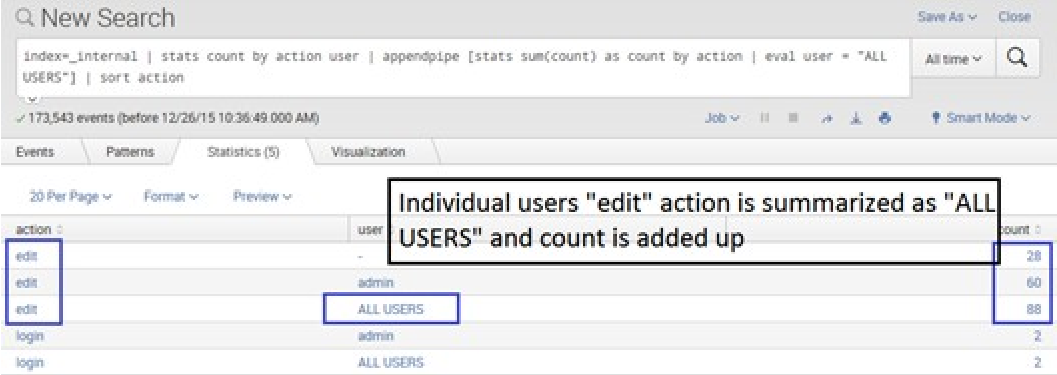
```
index=_internal | timechart span=1d count as Count1| appendcols [search index=_audit | timechart span=1d count as
Count2]
```

✓127,272 events (before 12/26/15 12:26:09.000 AM)

Search 1

Search 2

_time	Count1	Count2
2015-12-25	110684	21407
2015-12-26	16588	1480

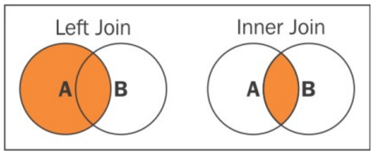


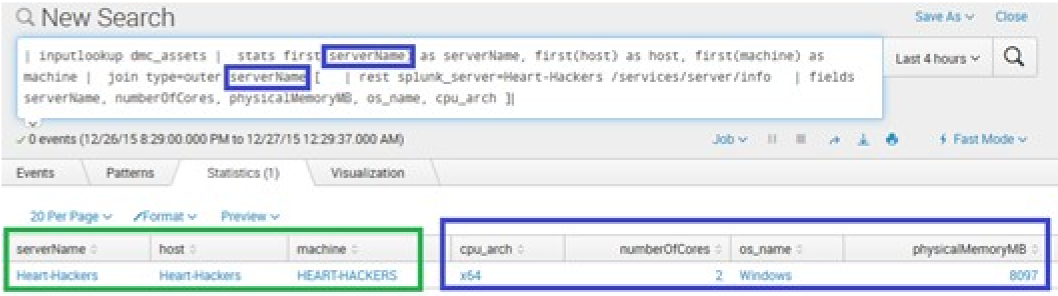
```
index=_internal | stats count by action user | appendpipe [stats sum(count) as count by action | eval user = "ALL
USERS"] | sort action
```

✓173,543 events (before 12/26/15 10:36:49.000 AM)

action	user	count
edit	-	28
edit	admin	60
edit	ALL USERS	88
login	admin	2
login	ALL USERS	2

Individual users "edit" action is summarized as "ALL USERS" and count is added up

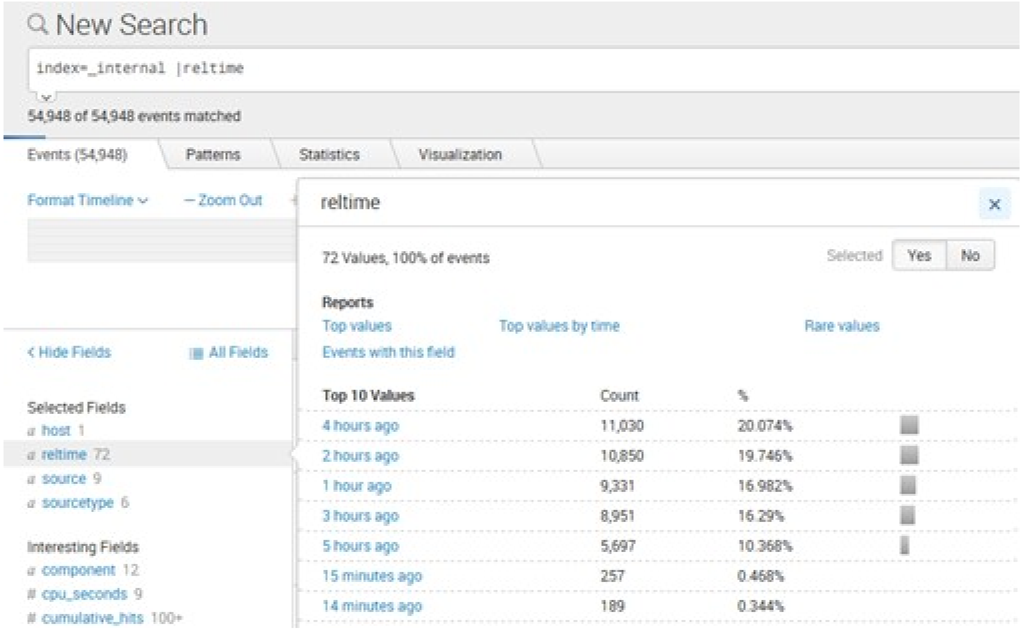




```
| inputlookup dmc_assets |  stats first(serverName) as serverName, first(host) as host, first(machine) as
machine |  join type=outer serverName [   | rest splunk_server=Heart-Hackers /services/server/info   | fields
serverName, numberOfCores, physicalMemoryMB, os_name, cpu_arch ]]
```

✓0 events (12/26/15 8:29:00.000 PM to 12/27/15 12:29:37.000 AM)

serverName	host	machine	cpu_arch	numberOfCores	os_name	physicalMemoryMB
Heart-Hackers	Heart-Hackers	HEART-HACKERS	x64	2	Windows	8097



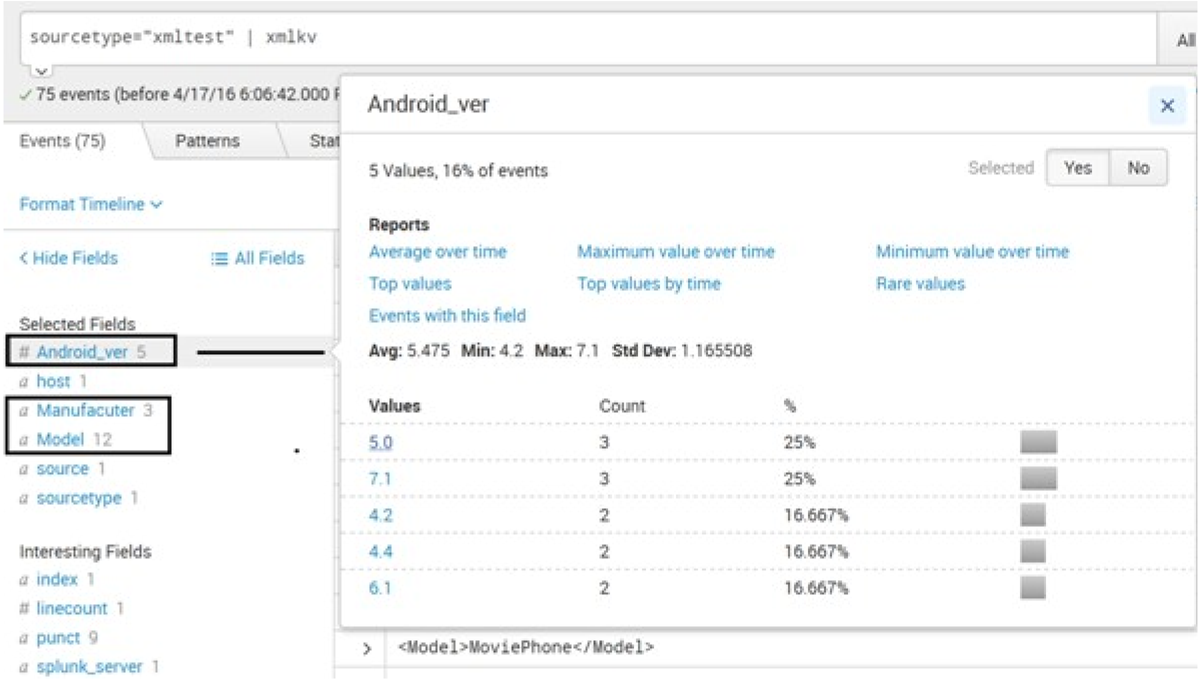
```
index=_internal |reltime
```

54,948 of 54,948 events matched

reltime

72 Values, 100% of events

Top 10 Values	Count	%
4 hours ago	11,030	20.074%
2 hours ago	10,850	19.746%
1 hour ago	9,331	16.982%
3 hours ago	8,951	16.29%
5 hours ago	5,697	10.368%
15 minutes ago	257	0.468%
14 minutes ago	189	0.344%



```
sourcetype="xmltest" | xmlkv
```

✓ 75 events (before 4/17/16 6:06:42.000 F

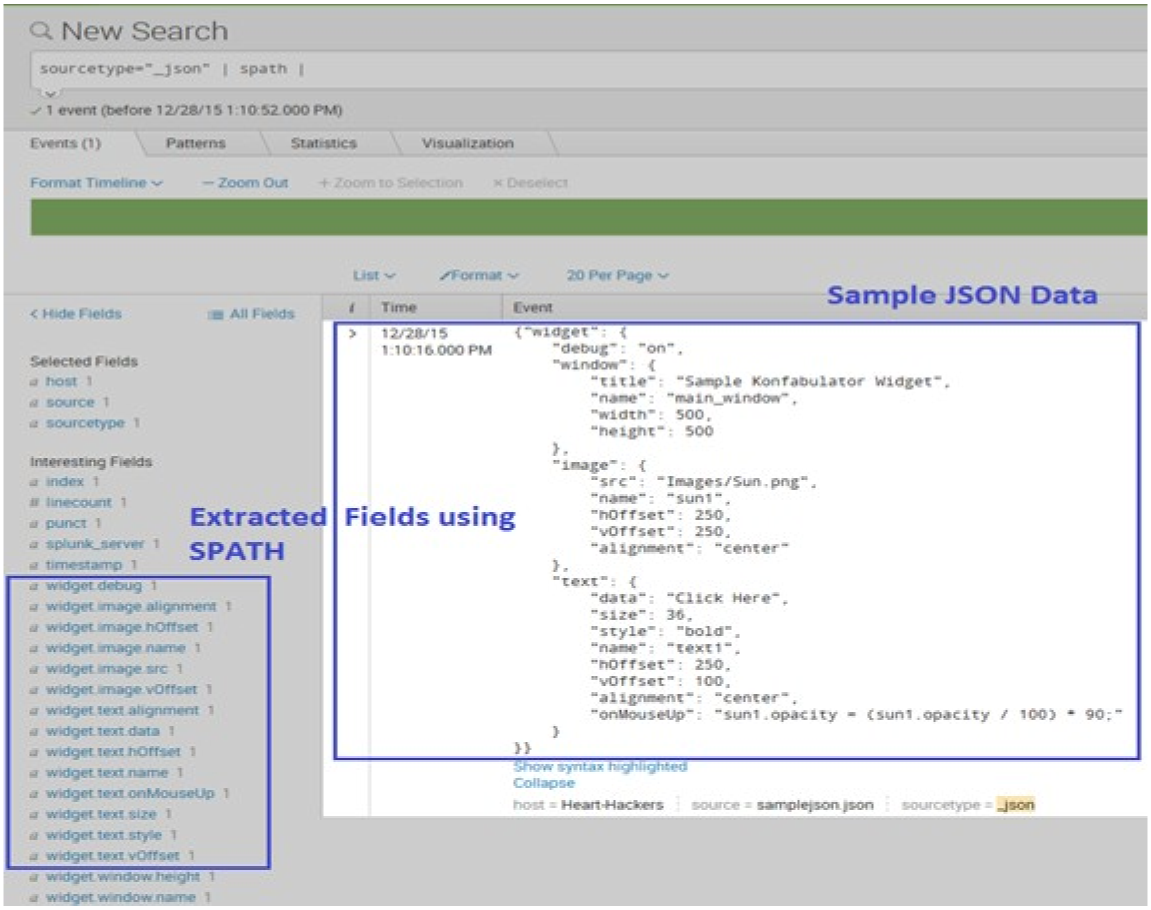
Android_ver

5 Values, 16% of events

Avg: 5.475 **Min:** 4.2 **Max:** 7.1 **Std Dev:** 1.165508

Values	Count	%
5.0	3	25%
7.1	3	25%
4.2	2	16.667%
4.4	2	16.667%
6.1	2	16.667%

```
<Model>MoviePhone</Model>
```



```
sourcetype="_json" | spath |
```

✓ 1 event (before 12/28/15 1:10:52.000 PM)

Sample JSON Data

Extracted Fields using SPATH

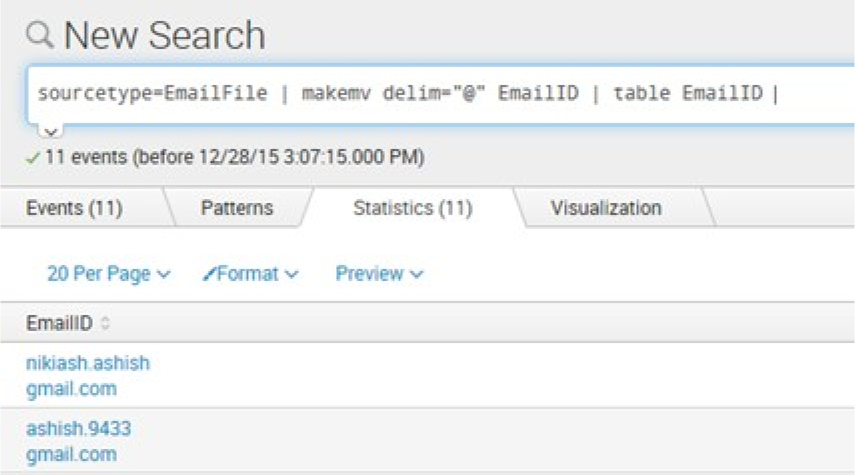
Selected Fields
host 1
source 1
sourcetype 1

Interesting Fields
index 1
linecount 1
punct 1
splunk_server 1
timestamp 1
widget.debug 1
widget.image.alignment 1
widget.image.hOffset 1
widget.image.name 1
widget.image.src 1
widget.image.vOffset 1
widget.text.alignment 1
widget.text.data 1
widget.text.hOffset 1
widget.text.name 1
widget.text.onMouseUp 1
widget.text.size 1
widget.text.style 1
widget.text.vOffset 1
widget.window.height 1
widget.window.name 1

i	Time	Event
>	12/28/15 1:10:16.000 PM	

```
{"widget": {
    "debug": "on",
    "window": {
        "title": "Sample Konfabulator Widget",
        "name": "main_window",
        "width": 500,
        "height": 500
    },
    "image": {
        "src": "Images/Sun.png",
        "name": "sun1",
        "hOffset": 250,
        "vOffset": 250,
        "alignment": "center"
    },
    "text": {
        "data": "Click Here",
        "size": 36,
        "style": "bold",
        "name": "text1",
        "hOffset": 250,
        "vOffset": 100,
        "alignment": "center",
        "onMouseUp": "sun1.opacity = (sun1.opacity / 100) * 90;"
    }
}}
```

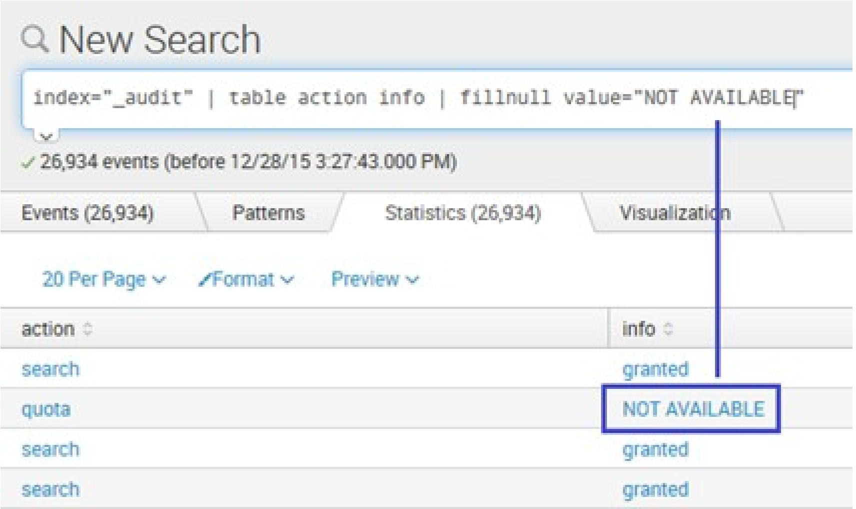
host = Heart-Hackers | source = samplejson.json | sourcetype = _json



```
sourcetype=EmailFile | makemv delim="@" EmailID | table EmailID |
```

✓ 11 events (before 12/28/15 3:07:15.000 PM)

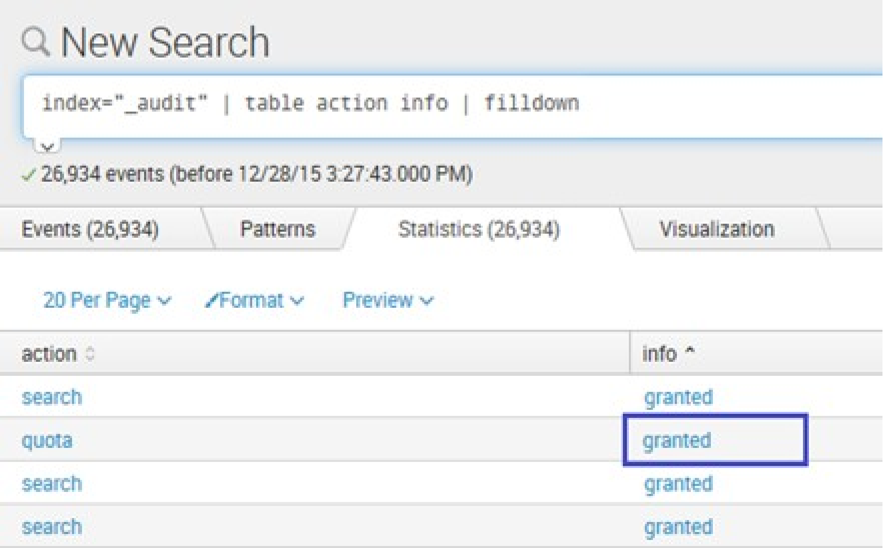
EmailID
nikiash.ashish gmail.com
ashish.9433 gmail.com



```
index="_audit" | table action info | fillnull value="NOT AVAILABLE"
```

✓ 26,934 events (before 12/28/15 3:27:43.000 PM)

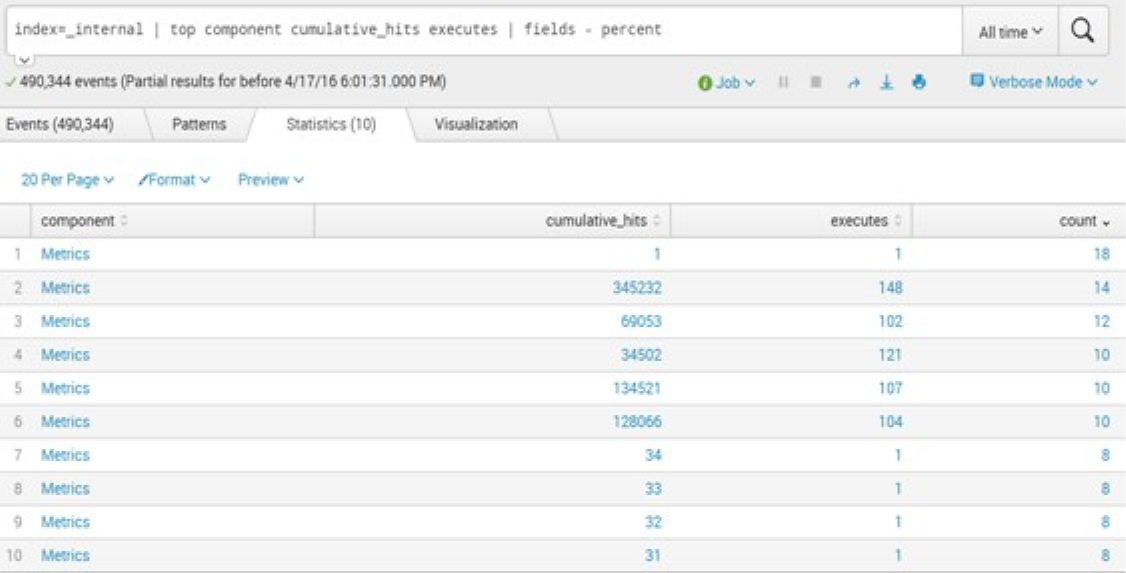
action	info
search	granted
quota	NOT AVAILABLE
search	granted
search	granted



```
index="_audit" | table action info | filldown
```

✓ 26,934 events (before 12/28/15 3:27:43.000 PM)

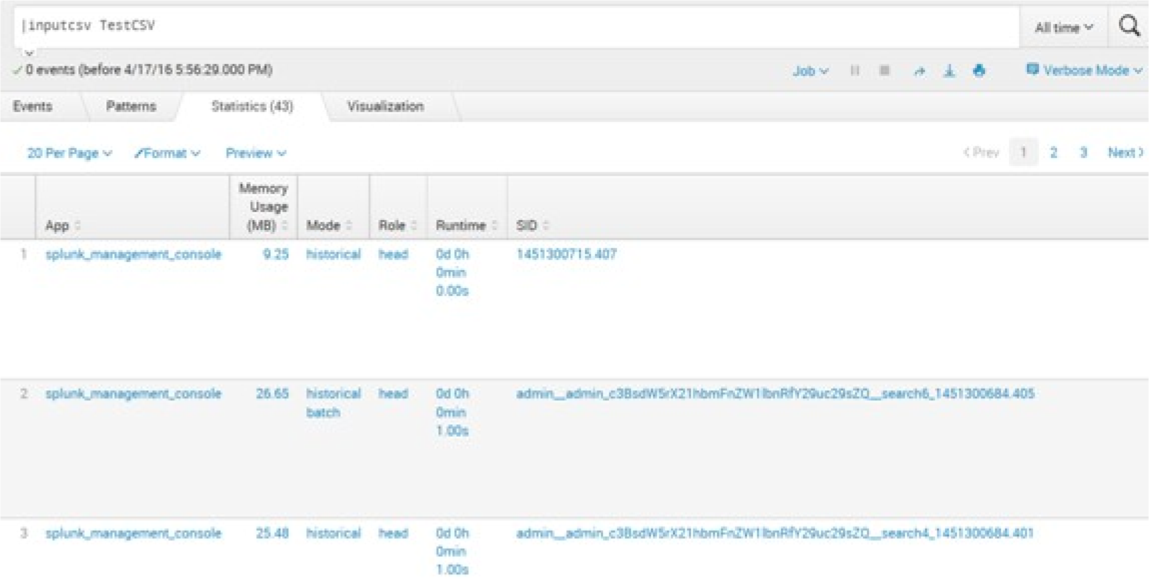
action	info
search	granted
quota	granted
search	granted
search	granted



```
index=_internal | top component cumulative_hits executes | fields - percent
```

✓ 490,344 events (Partial results for before 4/17/16 6:01:31.000 PM)

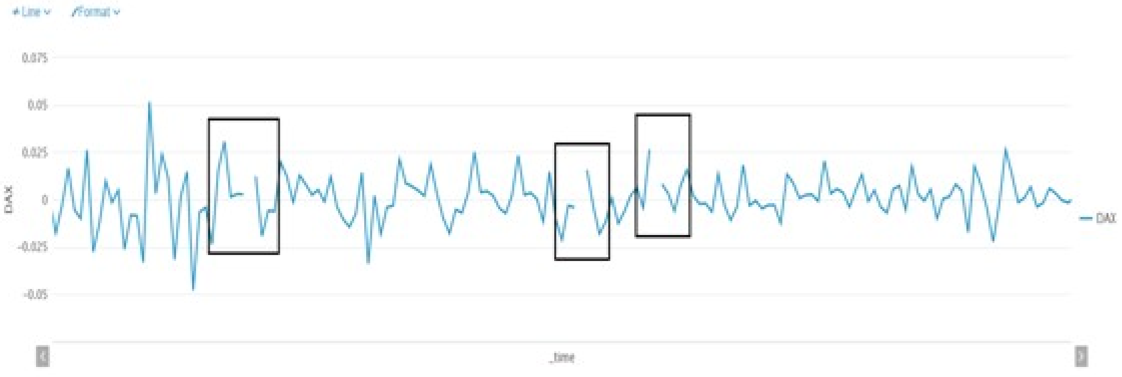
	component	cumulative_hits	executes	count
1	Metrics	1	1	18
2	Metrics	345232	148	14
3	Metrics	69053	102	12
4	Metrics	34502	121	10
5	Metrics	134521	107	10
6	Metrics	128066	104	10
7	Metrics	34	1	8
8	Metrics	33	1	8
9	Metrics	32	1	8
10	Metrics	31	1	8

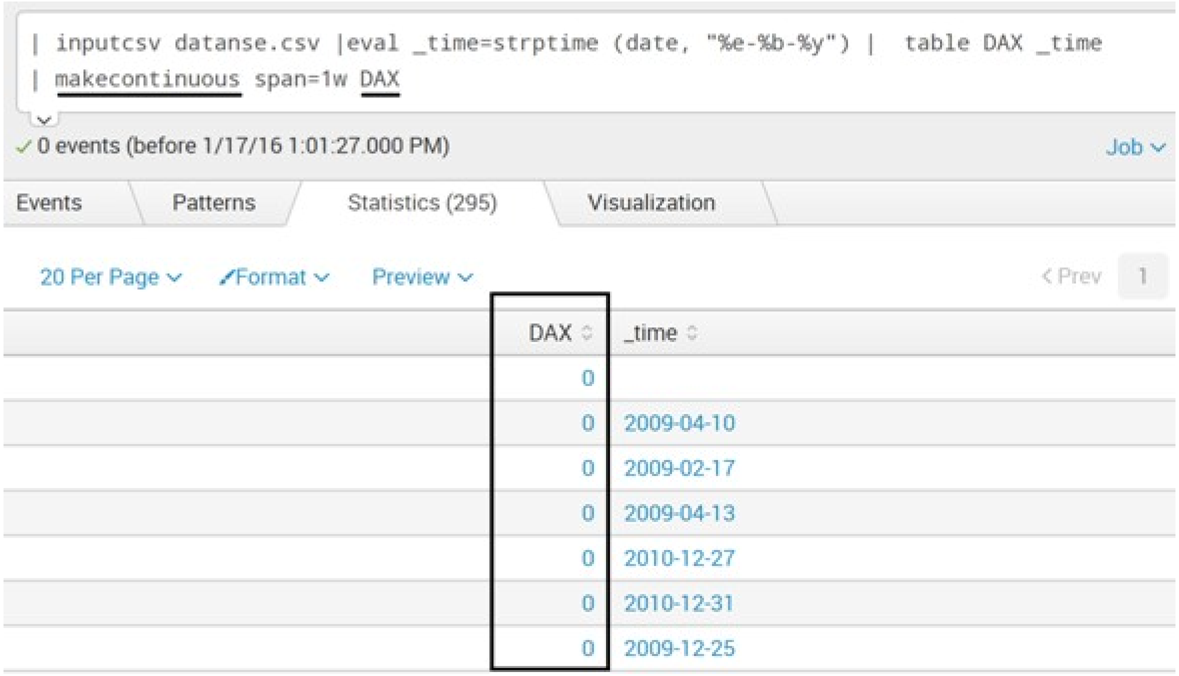


```
|inputcsv TestCSV
```

	App	Memory Usage (MB)	Mode	Role	Runtime	SID
1	splunk_management_console	9.25	historical	head	0d 0h 0min 0.00s	1451300715.407
2	splunk_management_console	26.65	historical batch	head	0d 0h 0min 1.00s	admin__admin_c3BsdW5rX21hbmFnZW1lbnRfY29uc29sZQ__search6_1451300684.405
3	splunk_management_console	25.48	historical	head	0d 0h 0min 1.00s	admin__admin_c3BsdW5rX21hbmFnZW1lbnRfY29uc29sZQ__search4_1451300684.401

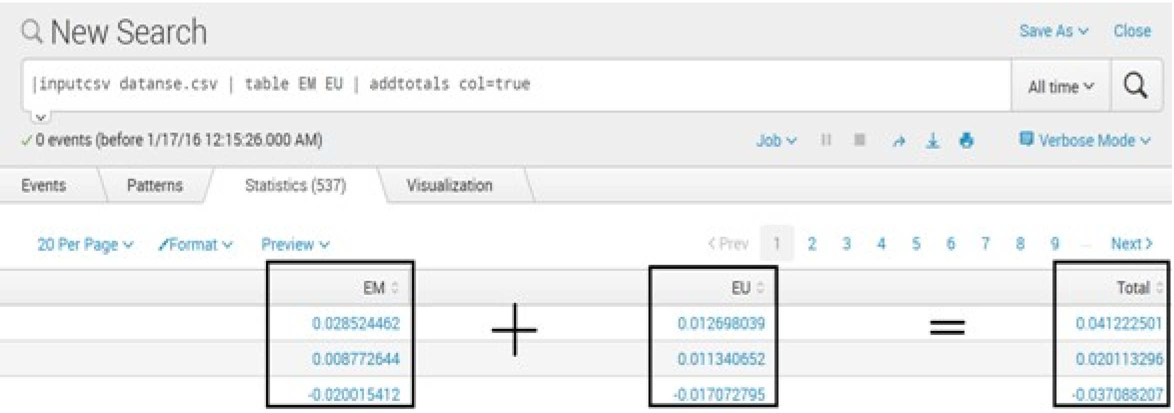
Chapter 5: Advanced Data Analytics




```
| inputcsv datanse.csv |eval _time=strptime (date, "%e-%b-%y") |  table DAX _time
| makecontinuous span=1w DAX
```

✓ 0 events (before 1/17/16 1:01:27.000 PM)

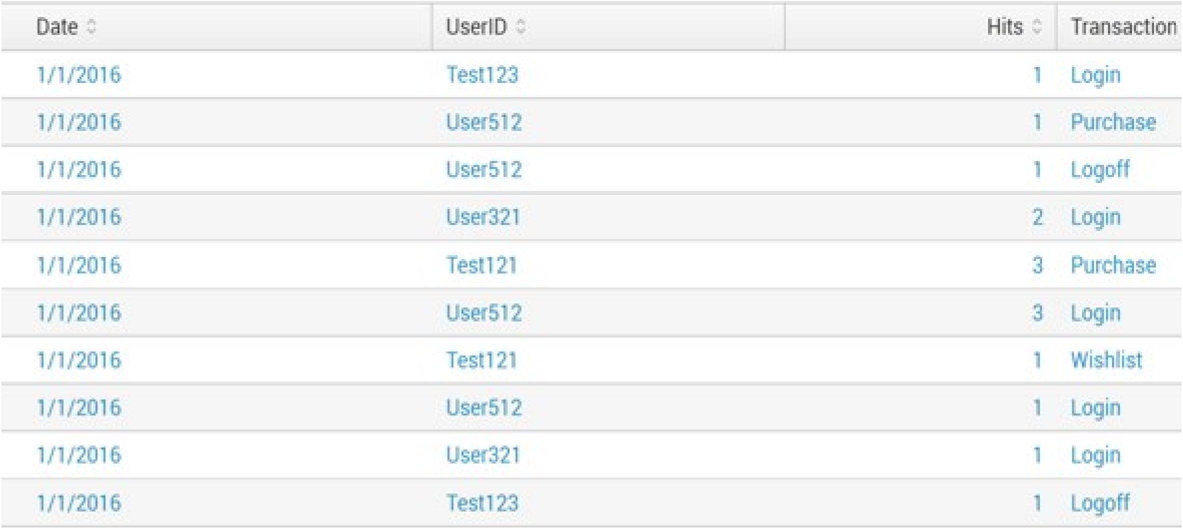
DAX	_time
0	
0	2009-04-10
0	2009-02-17
0	2009-04-13
0	2010-12-27
0	2010-12-31
0	2009-12-25



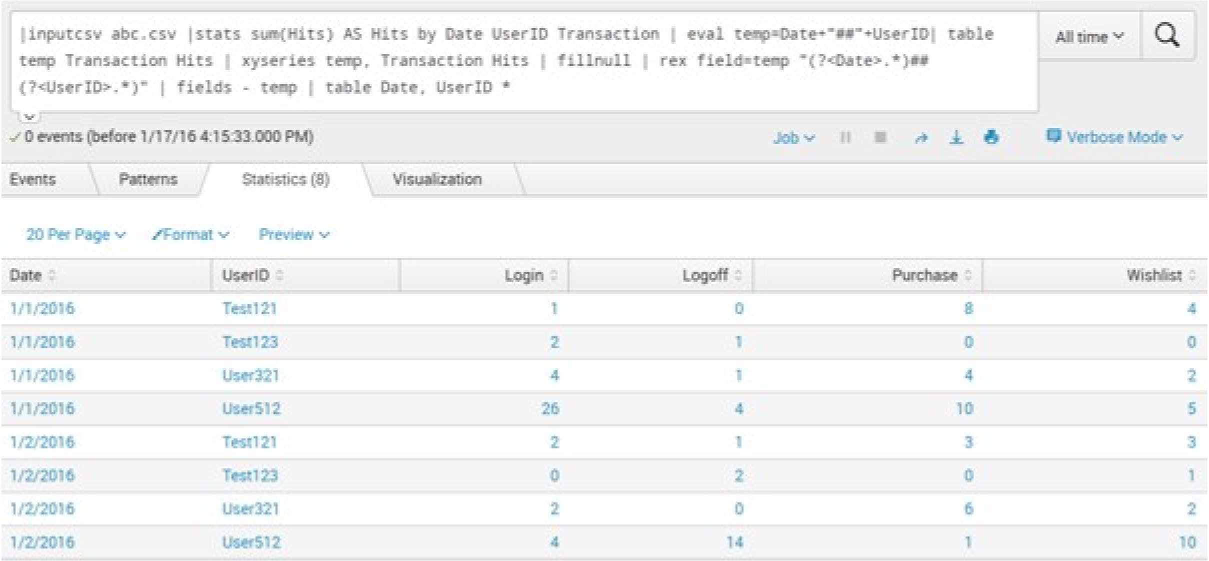
```
|inputcsv datanse.csv | table EM EU | addtotals col=true
```

✓ 0 events (before 1/17/16 12:15:26.000 AM)

EM	EU	Total
0.028524462	0.012698039	0.041222501
0.008772644	0.011340652	0.020113296
-0.020015412	-0.017072795	-0.037088207



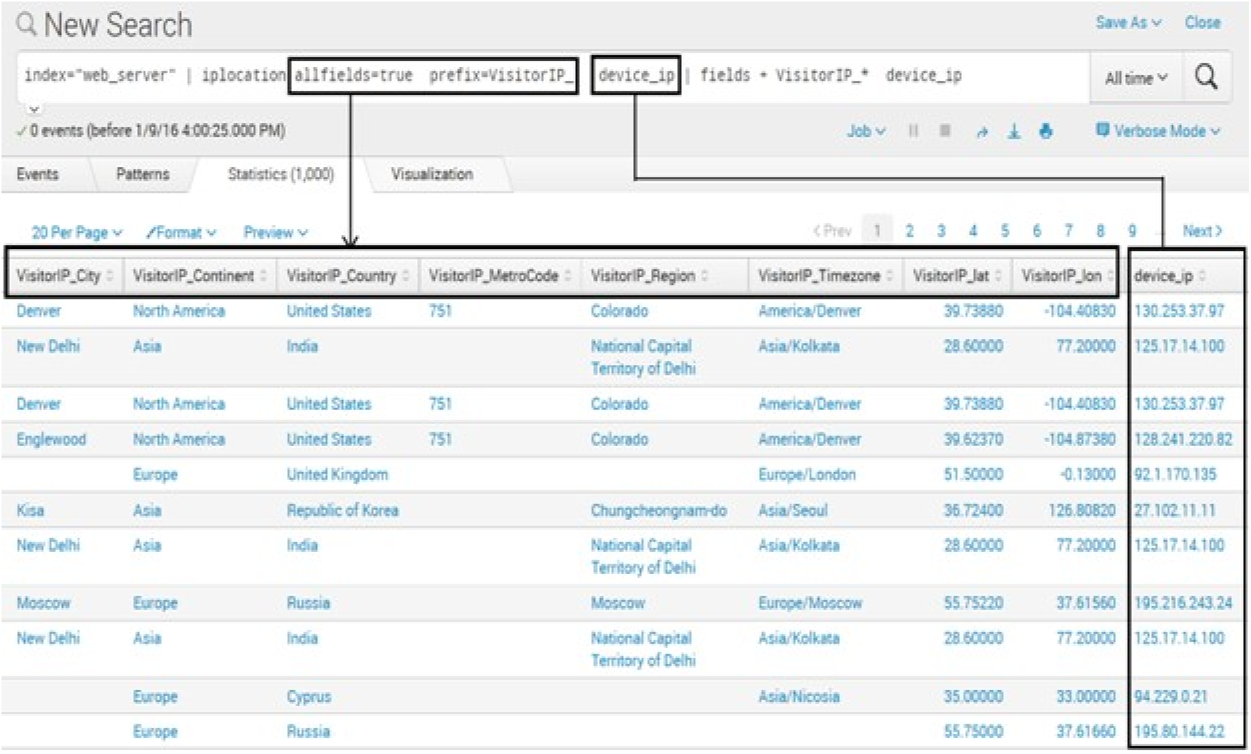
Date	UserID	Hits	Transaction
1/1/2016	Test123	1	Login
1/1/2016	User512	1	Purchase
1/1/2016	User512	1	Logoff
1/1/2016	User321	2	Login
1/1/2016	Test121	3	Purchase
1/1/2016	User512	3	Login
1/1/2016	Test121	1	Wishlist
1/1/2016	User512	1	Login
1/1/2016	User321	1	Login
1/1/2016	Test123	1	Logoff



```
|inputcsv abc.csv |stats sum(Hits) AS Hits by Date UserID Transaction | eval temp=Date+"##"+UserID| table
temp Transaction Hits | xyseries temp, Transaction Hits | fillnull | rex field=temp "(?<Date>.*)##
(?<UserID>.*)" | fields - temp | table Date, UserID *
```

✓ 0 events (before 1/17/16 4:15:33.000 PM)

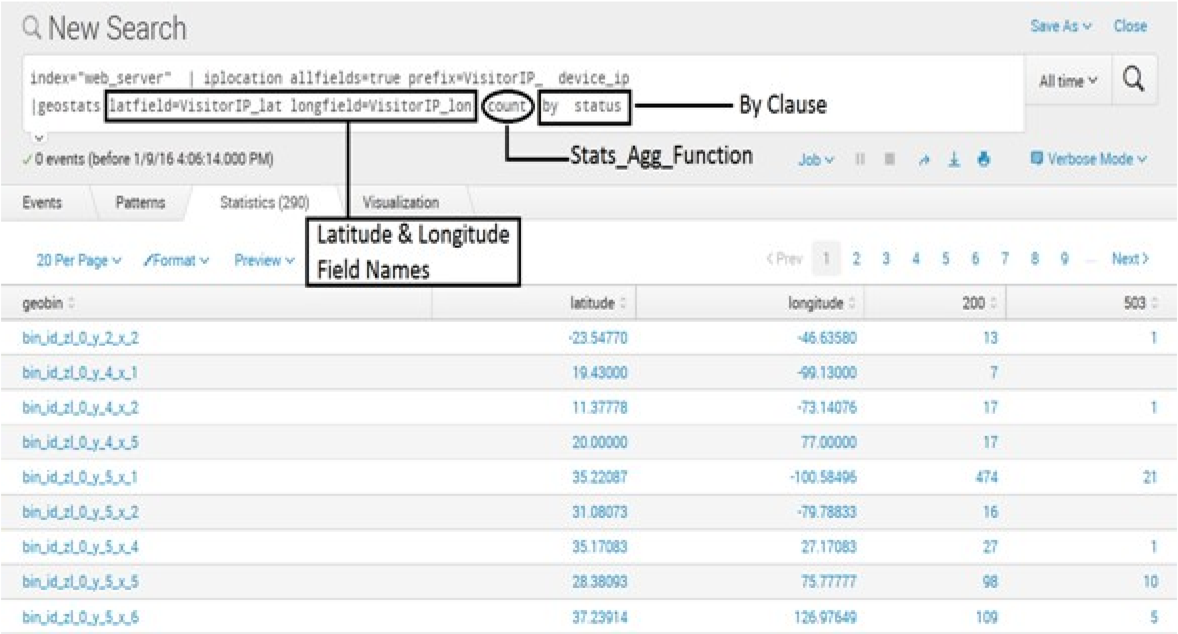
Date	UserID	Login	Logoff	Purchase	Wishlist
1/1/2016	Test121	1	0	8	4
1/1/2016	Test123	2	1	0	0
1/1/2016	User321	4	1	4	2
1/1/2016	User512	26	4	10	5
1/2/2016	Test121	2	1	3	3
1/2/2016	Test123	0	2	0	1
1/2/2016	User321	2	0	6	2
1/2/2016	User512	4	14	1	10



```
index="web_server" | iplocation allfields=true  prefix=VisitorIP_  device_ip | fields + VisitorIP_*  device_ip
```

✓ 0 events (before 1/9/16 4:00:25.000 PM)

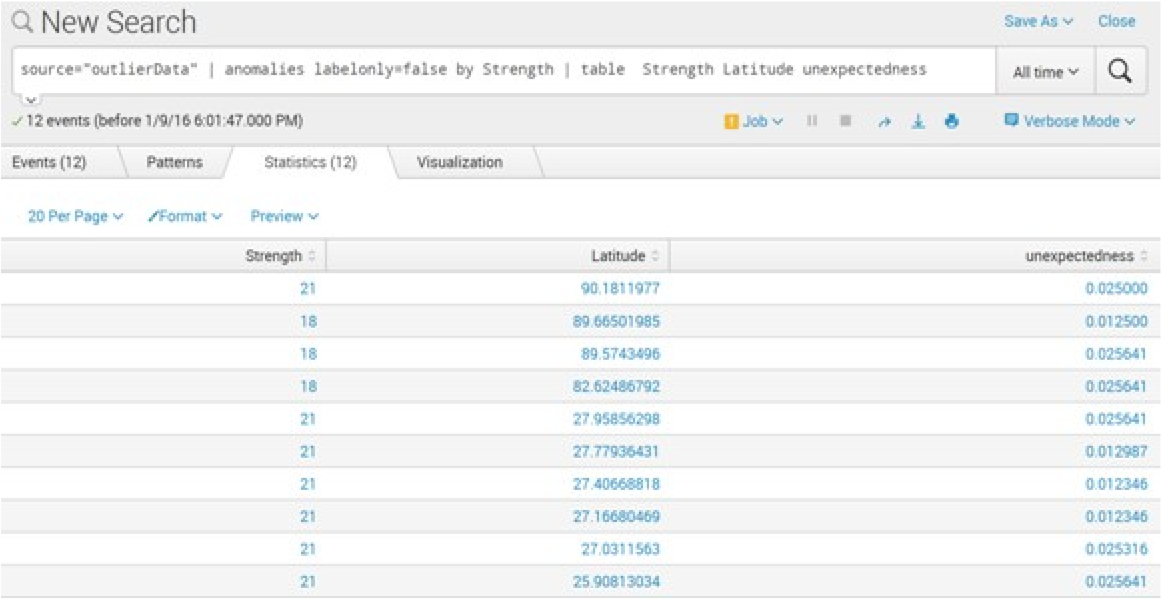
VisitorIP_City	VisitorIP_Continent	VisitorIP_Country	VisitorIP_MetroCode	VisitorIP_Region	VisitorIP_Timezone	VisitorIP_lat	VisitorIP_lon	device_ip
Denver	North America	United States	751	Colorado	America/Denver	39.73880	-104.40830	130.253.37.97
New Delhi	Asia	India		National Capital Territory of Delhi	Asia/Kolkata	28.60000	77.20000	125.17.14.100
Denver	North America	United States	751	Colorado	America/Denver	39.73880	-104.40830	130.253.37.97
Englewood	North America	United States	751	Colorado	America/Denver	39.62370	-104.87380	128.241.220.82
	Europe	United Kingdom			Europe/London	51.50000	-0.13000	92.1.170.135
Kisa	Asia	Republic of Korea		Chungcheongnam-do	Asia/Seoul	36.72400	126.80820	27.102.11.11
New Delhi	Asia	India		National Capital Territory of Delhi	Asia/Kolkata	28.60000	77.20000	125.17.14.100
Moscow	Europe	Russia		Moscow	Europe/Moscow	55.75220	37.61560	195.216.243.24
New Delhi	Asia	India		National Capital Territory of Delhi	Asia/Kolkata	28.60000	77.20000	125.17.14.100
	Europe	Cyprus			Asia/Nicosia	35.00000	33.00000	94.229.0.21
	Europe	Russia				55.75000	37.61660	195.80.144.22



```
index="web_server"  | iplocation allfields=true prefix=VisitorIP_  device_ip
|geostats latfield=VisitorIP_lat longfield=VisitorIP_lon count by  status
```

✓ 0 events (before 1/9/16 4:06:14.000 PM)

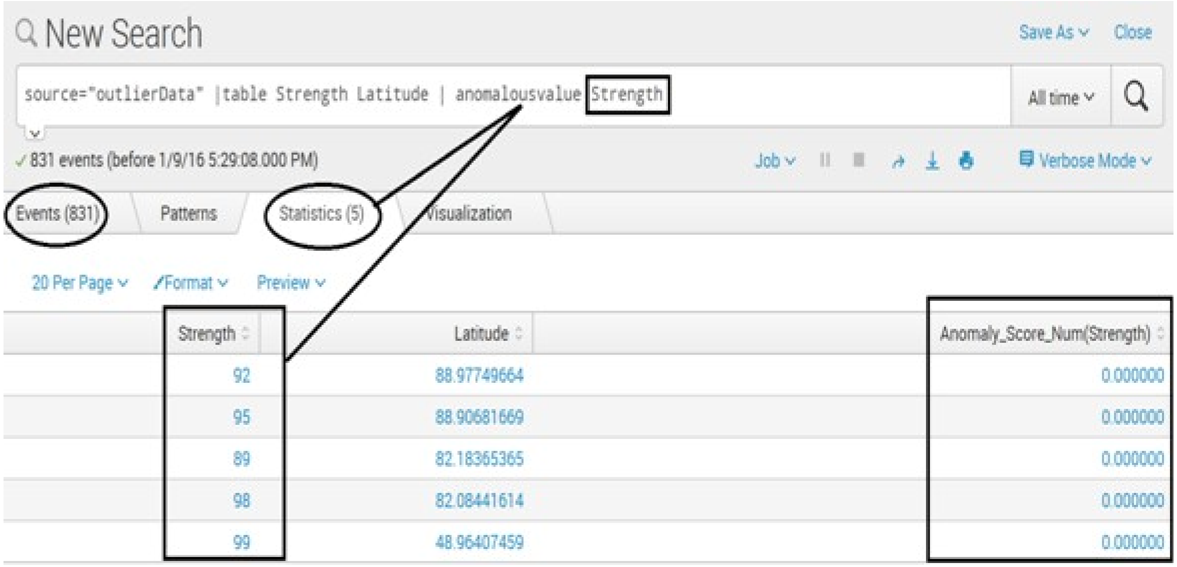
geobin	latitude	longitude	200	503
bin_id_zl_0_y_2_x_2	-23.54770	-46.63580	13	1
bin_id_zl_0_y_4_x_1	19.43000	-99.13000	7	
bin_id_zl_0_y_4_x_2	11.37778	-73.14076	17	1
bin_id_zl_0_y_4_x_5	20.00000	77.00000	17	
bin_id_zl_0_y_5_x_1	35.22087	-100.58496	474	21
bin_id_zl_0_y_5_x_2	31.08073	-79.78833	16	
bin_id_zl_0_y_5_x_4	35.17083	27.17083	27	1
bin_id_zl_0_y_5_x_5	28.38093	75.77777	98	10
bin_id_zl_0_y_5_x_6	37.23914	126.97649	109	5



```
source="outlierData" | anomalies labelonly=false by Strength | table  Strength Latitude unexpectedness
```

✓ 12 events (before 1/9/16 6:01:47.000 PM)

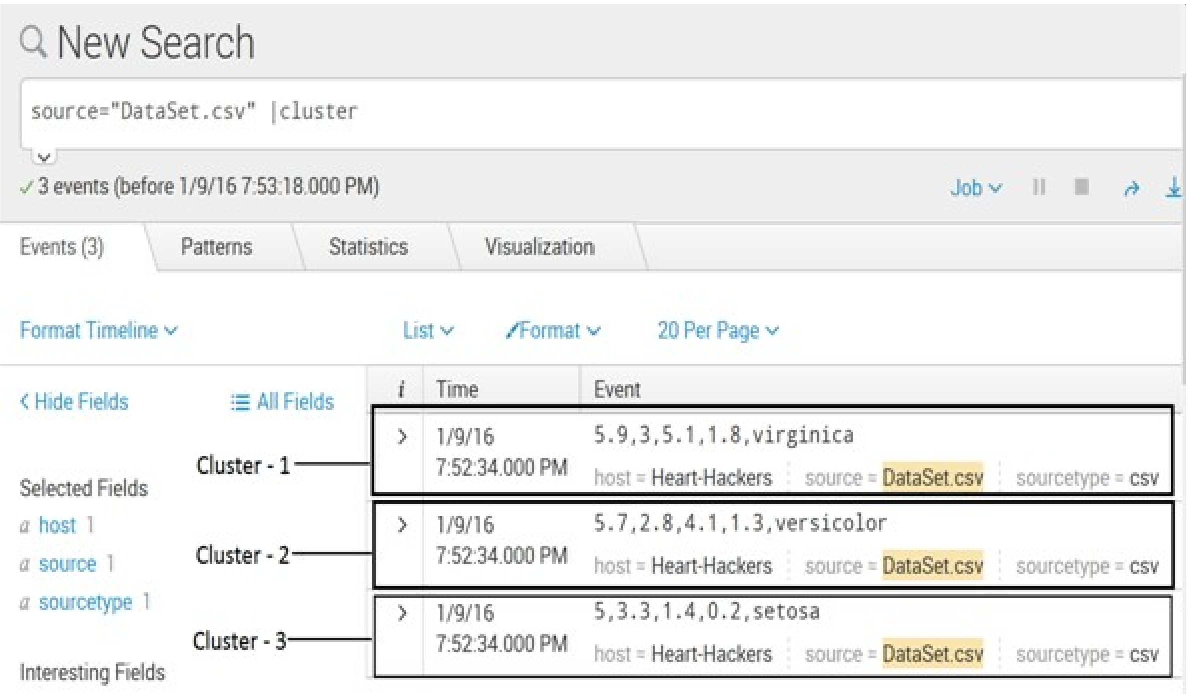
Strength	Latitude	unexpectedness
21	90.1811977	0.025000
18	89.66501985	0.012500
18	89.5743496	0.025641
18	82.62486792	0.025641
21	27.95856298	0.025641
21	27.77936431	0.012987
21	27.40668818	0.012346
21	27.16680469	0.012346
21	27.0311563	0.025316
21	25.90813034	0.025641



```
source="outlierData" |table Strength Latitude | anomalousvalue Strength
```

✓ 831 events (before 1/9/16 5:29:08.000 PM)

Strength	Latitude	Anomaly_Score_Num(Strength)
92	88.97749664	0.000000
95	88.90681669	0.000000
89	82.18365365	0.000000
98	82.08441614	0.000000
99	48.96407459	0.000000

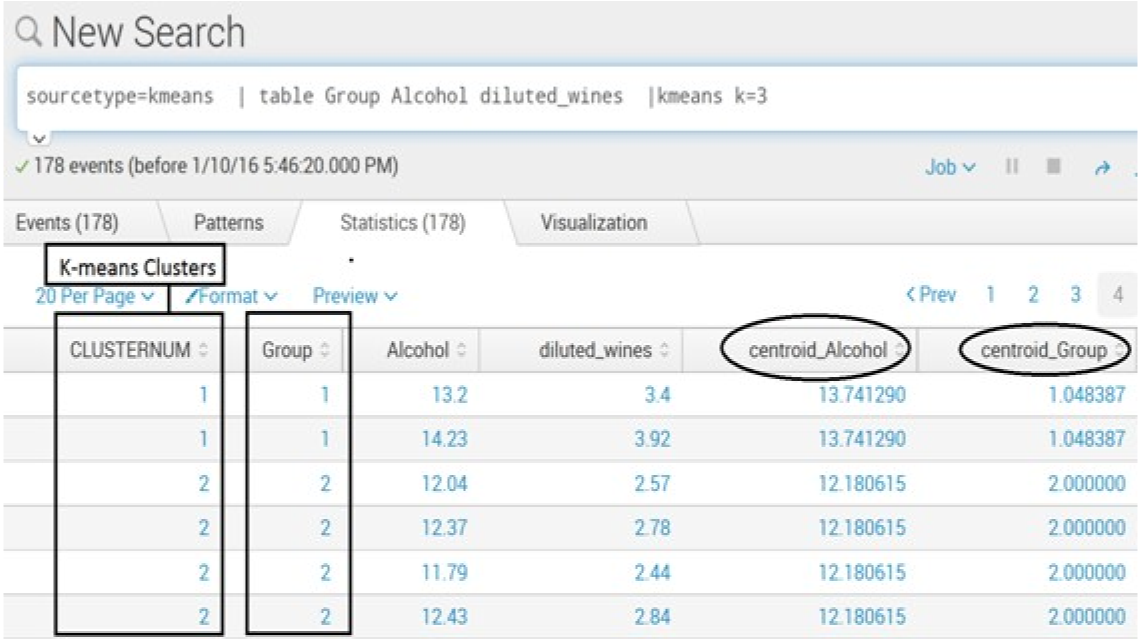


New Search

```
source="DataSet.csv" |cluster
```

✓ 3 events (before 1/9/16 7:53:18.000 PM)

i	Time	Event
>	1/9/16 7:52:34.000 PM	5.9,3,5.1,1.8,virginica host = Heart-Hackers source = DataSet.csv sourcetype = csv
>	1/9/16 7:52:34.000 PM	5.7,2.8,4.1,1.3,versicolor host = Heart-Hackers source = DataSet.csv sourcetype = csv
>	1/9/16 7:52:34.000 PM	5,3.3,1.4,0.2,setosa host = Heart-Hackers source = DataSet.csv sourcetype = csv

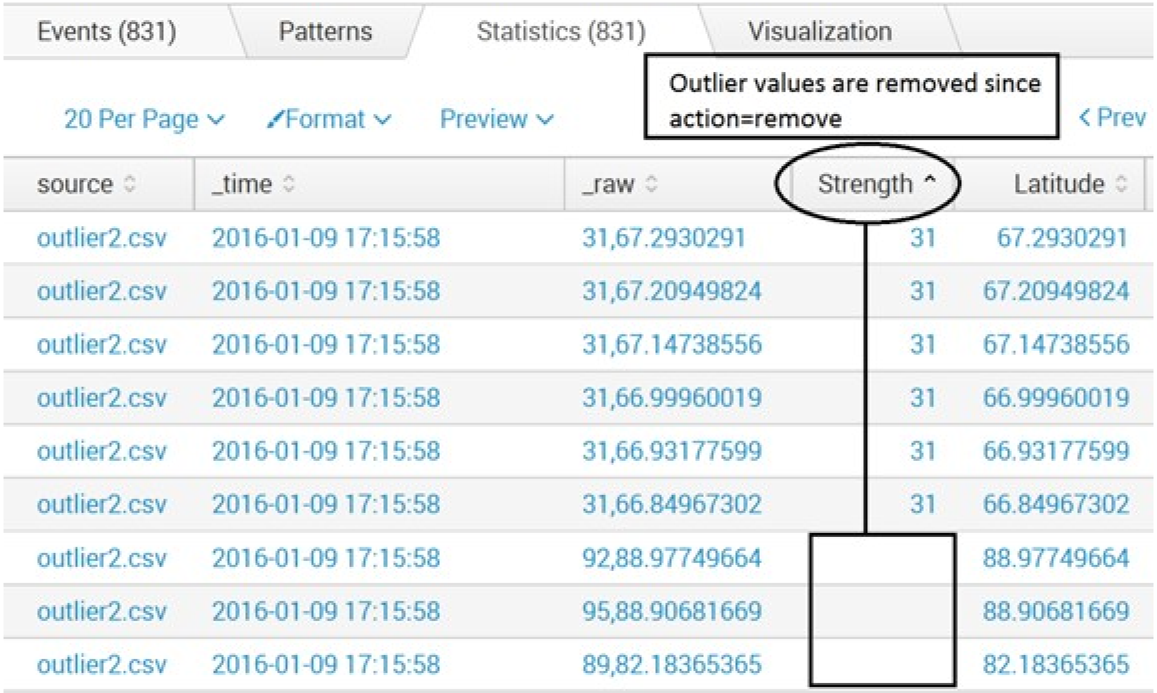


New Search

```
sourcetype=kmeans  | table Group Alcohol diluted_wines  |kmeans k=3
```

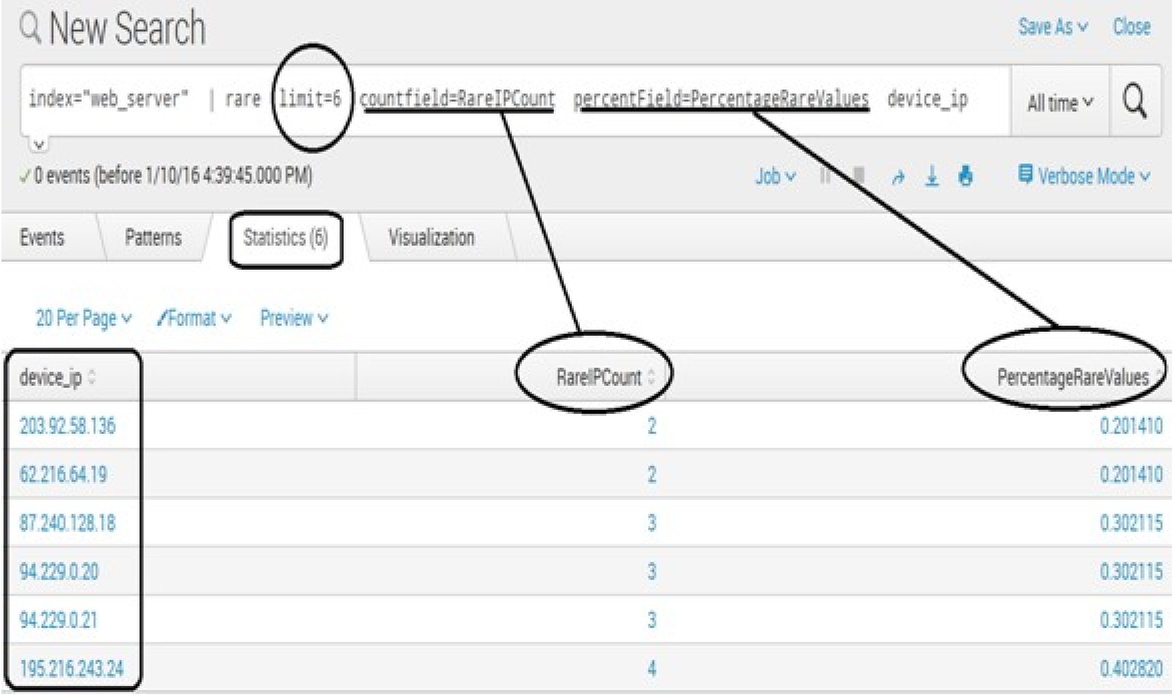
✓ 178 events (before 1/10/16 5:46:20.000 PM)

CLUSTERNUM	Group	Alcohol	diluted_wines	centroid_Alcohol	centroid_Group
1	1	13.2	3.4	13.741290	1.048387
1	1	14.23	3.92	13.741290	1.048387
2	2	12.04	2.57	12.180615	2.000000
2	2	12.37	2.78	12.180615	2.000000
2	2	11.79	2.44	12.180615	2.000000
2	2	12.43	2.84	12.180615	2.000000



Outlier values are removed since action=remove

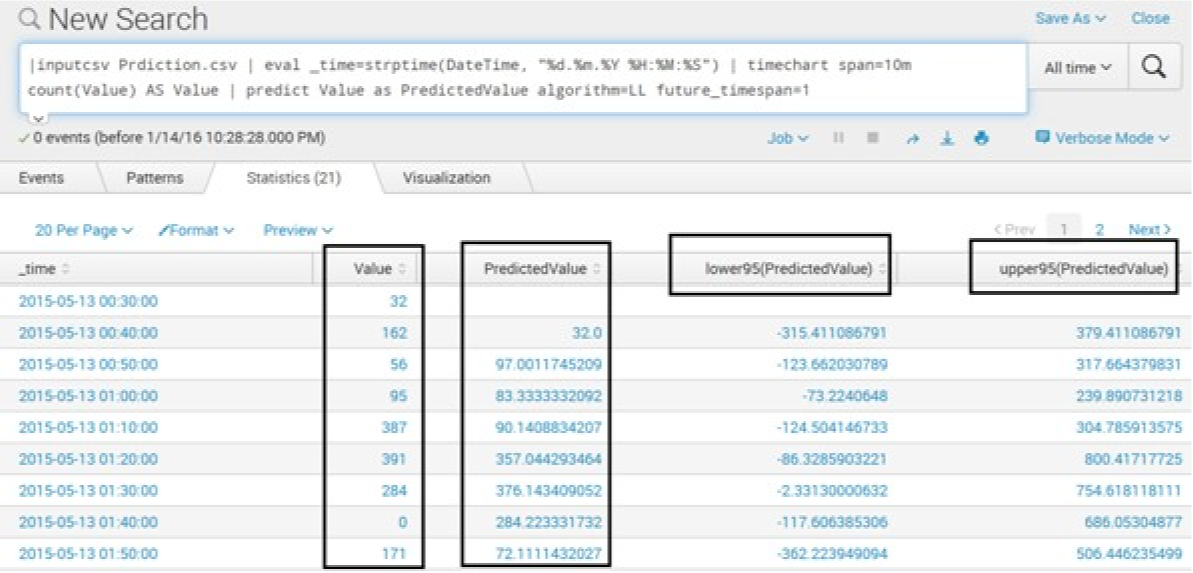
source	_time	_raw	Strength	Latitude
outlier2.csv	2016-01-09 17:15:58	31,67.2930291	31	67.2930291
outlier2.csv	2016-01-09 17:15:58	31,67.20949824	31	67.20949824
outlier2.csv	2016-01-09 17:15:58	31,67.14738556	31	67.14738556
outlier2.csv	2016-01-09 17:15:58	31,66.99960019	31	66.99960019
outlier2.csv	2016-01-09 17:15:58	31,66.93177599	31	66.93177599
outlier2.csv	2016-01-09 17:15:58	31,66.84967302	31	66.84967302
outlier2.csv	2016-01-09 17:15:58	92,88.97749664		88.97749664
outlier2.csv	2016-01-09 17:15:58	95,88.90681669		88.90681669
outlier2.csv	2016-01-09 17:15:58	89,82.18365365		82.18365365



```
index="web_server"  | rare limit=6 countfield=RareIPCount  percentField=PercentageRareValues  device_ip
```

✓0 events (before 1/10/16 4:39:45.000 PM)

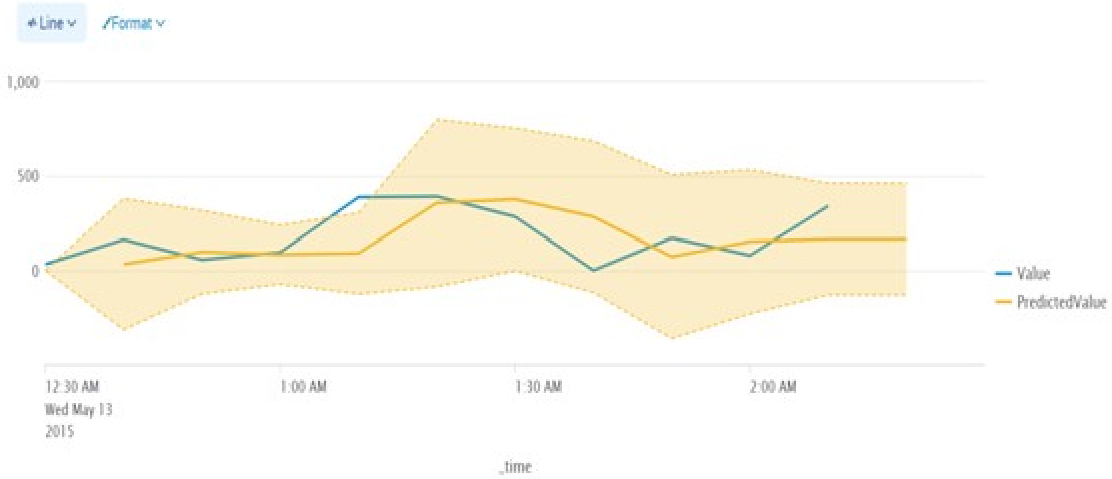
device_ip	RareIPCount	PercentageRareValues
203.92.58.136	2	0.201410
62.216.64.19	2	0.201410
87.240.128.18	3	0.302115
94.229.0.20	3	0.302115
94.229.0.21	3	0.302115
195.216.243.24	4	0.402820

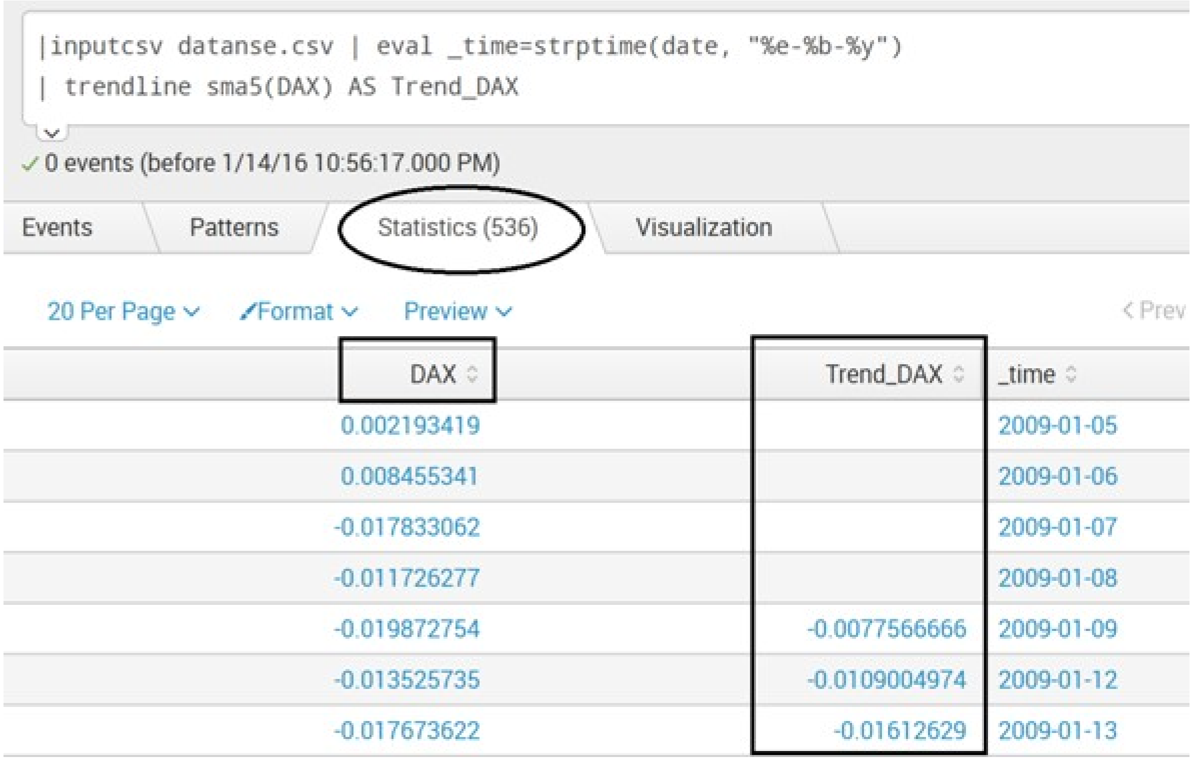


```
|inputcsv Prdiction.csv | eval _time=strptime(DateTime, "%d.%m.%Y %H:%M:%S") | timechart span=10m
count(Value) AS Value | predict Value as PredictedValue algorithm=LL future_timespan=1
```

✓ 0 events (before 1/14/16 10:28:28.000 PM)

_time	Value	PredictedValue	lower95(PredictedValue)	upper95(PredictedValue)
2015-05-13 00:30:00	32			
2015-05-13 00:40:00	162	32.0	-315.411086791	379.411086791
2015-05-13 00:50:00	56	97.0011745209	-123.662030789	317.664379831
2015-05-13 01:00:00	95	83.3333332092	-73.2240648	239.890731218
2015-05-13 01:10:00	387	90.1408834207	-124.504146733	304.785913575
2015-05-13 01:20:00	391	357.044293464	-86.3285903221	800.41717725
2015-05-13 01:30:00	284	376.143409052	-2.33130000632	754.618118111
2015-05-13 01:40:00	0	284.223331732	-117.606385306	686.05304877
2015-05-13 01:50:00	171	72.1111432027	-362.223949094	506.446235499

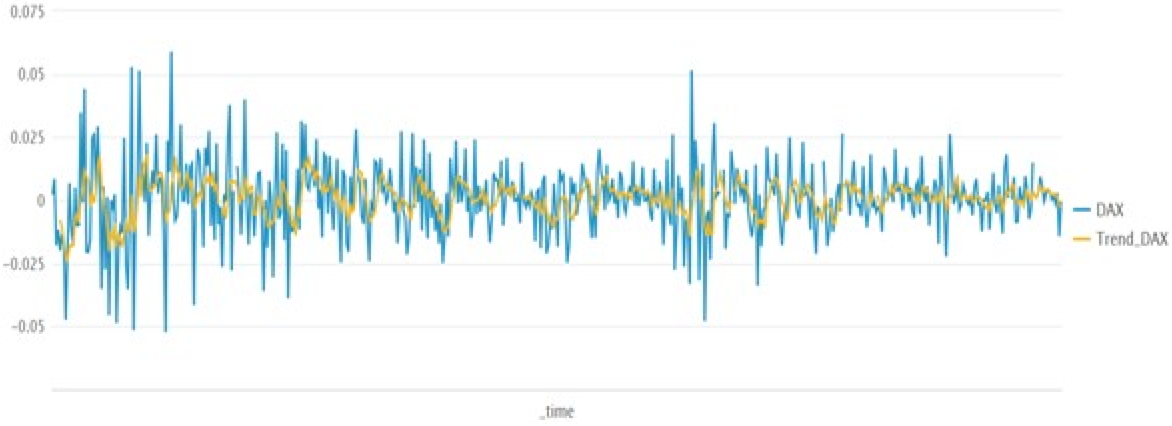


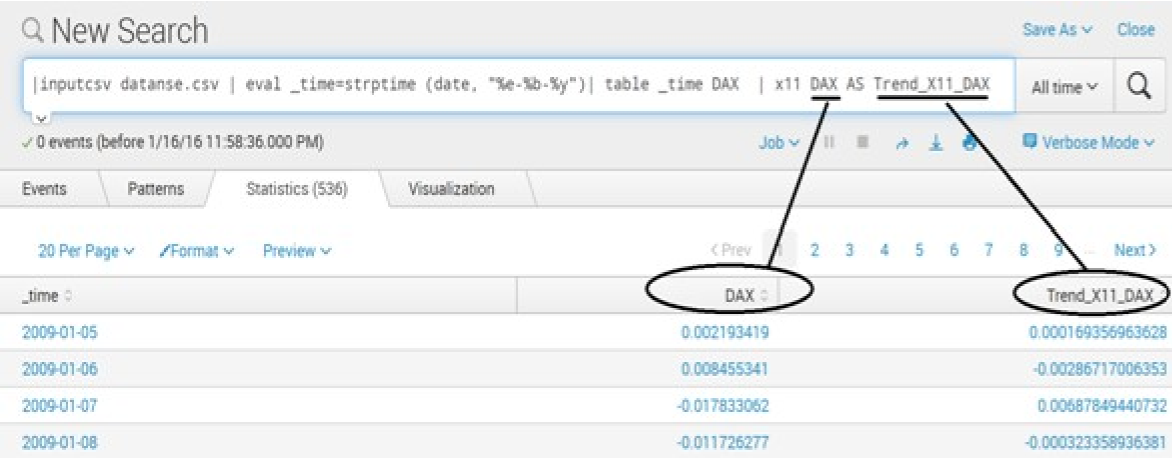


```
|inputcsv datanse.csv | eval _time=strptime(date, "%e-%b-%y")
| trendline sma5(DAX) AS Trend_DAX
```

✓ 0 events (before 1/14/16 10:56:17.000 PM)

DAX	Trend_DAX	_time
0.002193419		2009-01-05
0.008455341		2009-01-06
-0.017833062		2009-01-07
-0.011726277		2009-01-08
-0.019872754	-0.0077566666	2009-01-09
-0.013525735	-0.0109004974	2009-01-12
-0.017673622	-0.01612629	2009-01-13

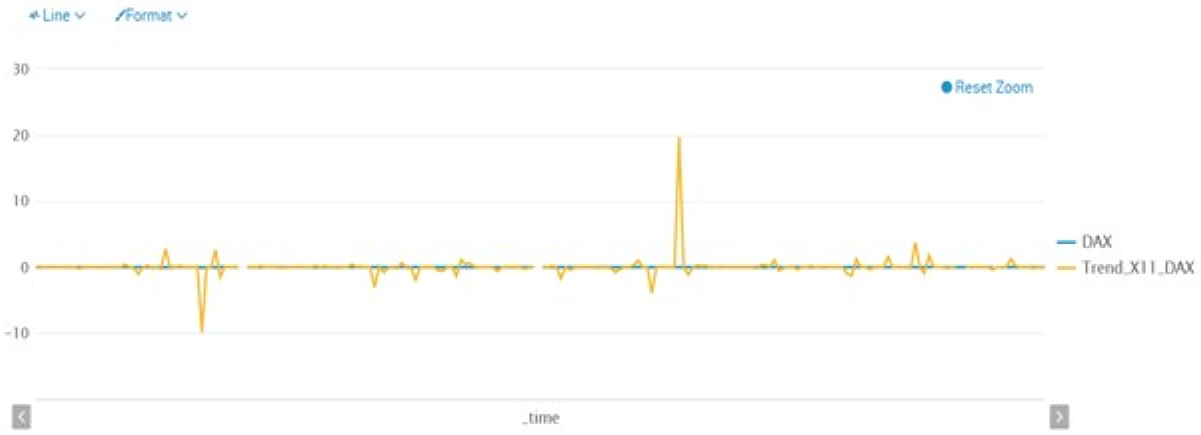


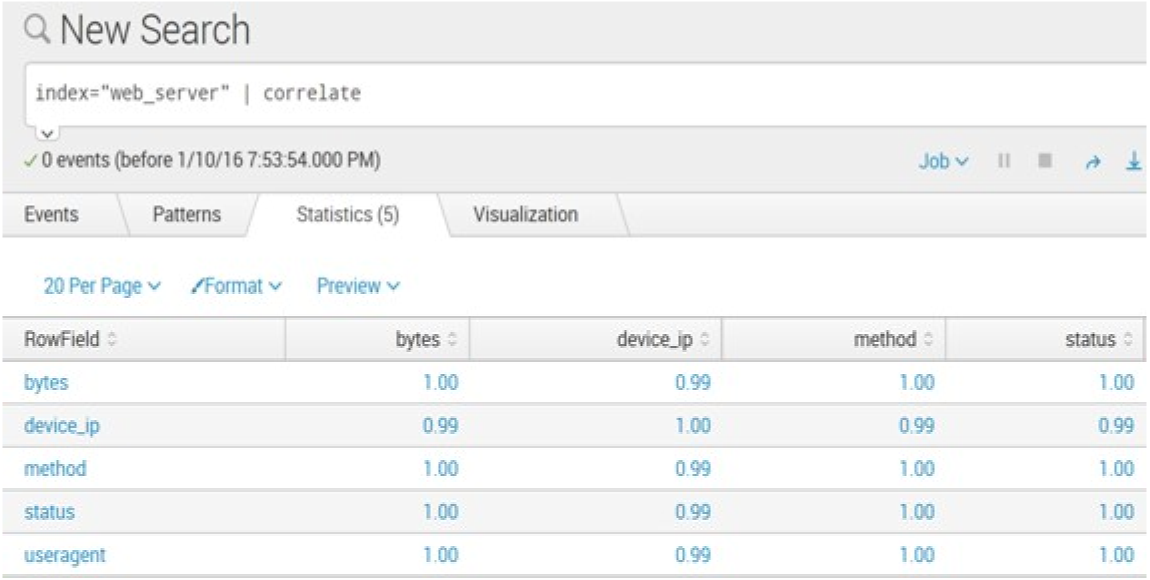


```
|inputcsv datanse.csv | eval _time=strptime (date, "%e-%b-%y")| table _time DAX  | x11 DAX AS Trend_X11_DAX
```

✓ 0 events (before 1/16/16 11:58:36.000 PM)

_time	DAX	Trend_X11_DAX
2009-01-05	0.002193419	0.000169356963628
2009-01-06	0.008455341	-0.00286717006353
2009-01-07	-0.017833062	0.00687849440732
2009-01-08	-0.011726277	-0.000323358936381

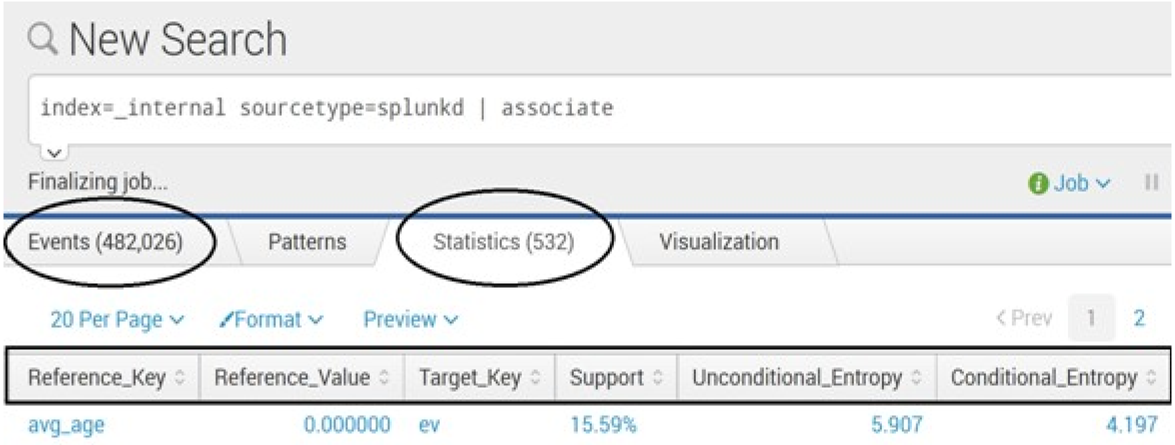




```
index="web_server" | correlate
```

✓ 0 events (before 1/10/16 7:53:54.000 PM)

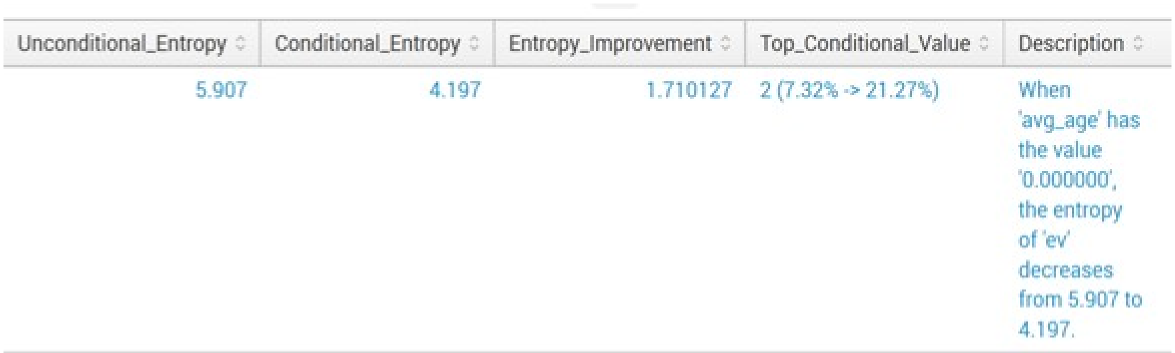
RowField	bytes	device_ip	method	status
bytes	1.00	0.99	1.00	1.00
device_ip	0.99	1.00	0.99	0.99
method	1.00	0.99	1.00	1.00
status	1.00	0.99	1.00	1.00
useragent	1.00	0.99	1.00	1.00



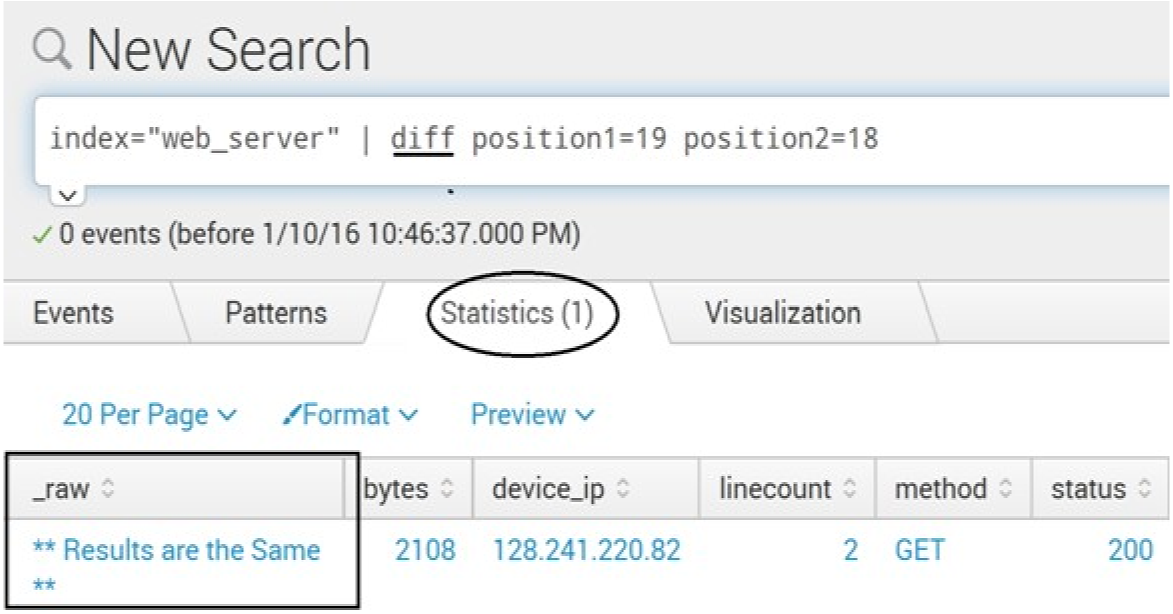
```
index=_internal sourcetype=splunkd | associate
```

Finalizing job...

Reference_Key	Reference_Value	Target_Key	Support	Unconditional_Entropy	Conditional_Entropy
avg_age	0.000000	ev	15.59%	5.907	4.197



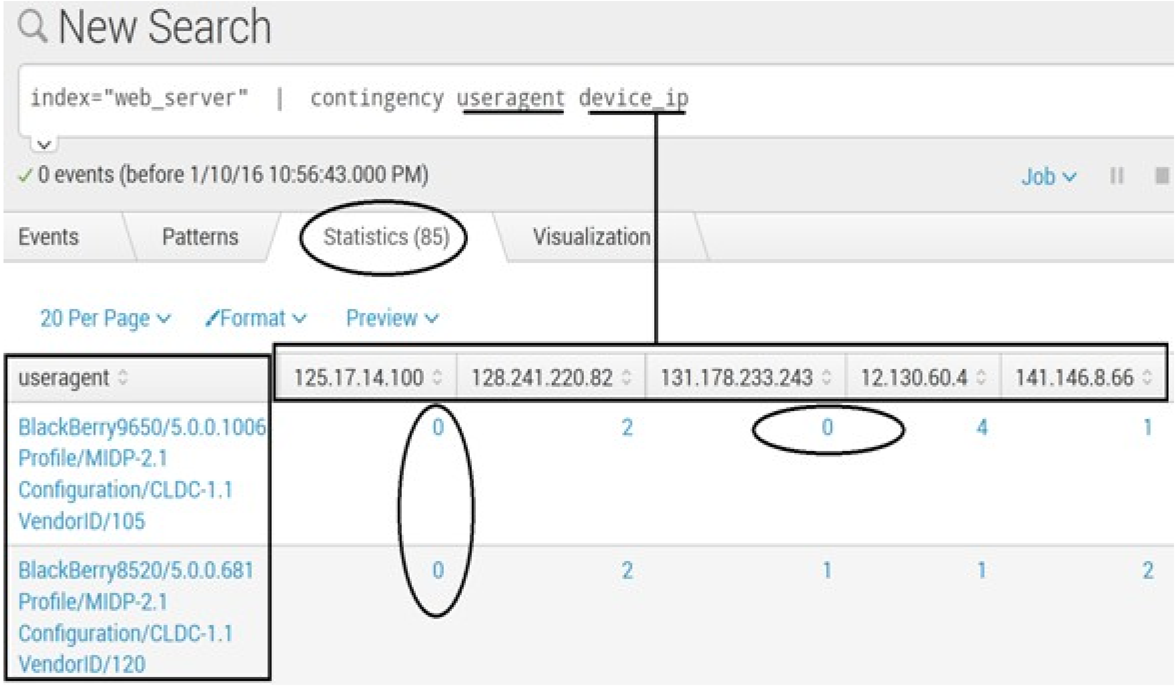
Unconditional_Entropy	Conditional_Entropy	Entropy_Improvement	Top_Conditional_Value	Description
5.907	4.197	1.710127	2 (7.32% -> 21.27%)	When 'avg_age' has the value '0.000000', the entropy of 'ev' decreases from 5.907 to 4.197.



```
index="web_server" | diff position1=19 position2=18
```

✓ 0 events (before 1/10/16 10:46:37.000 PM)

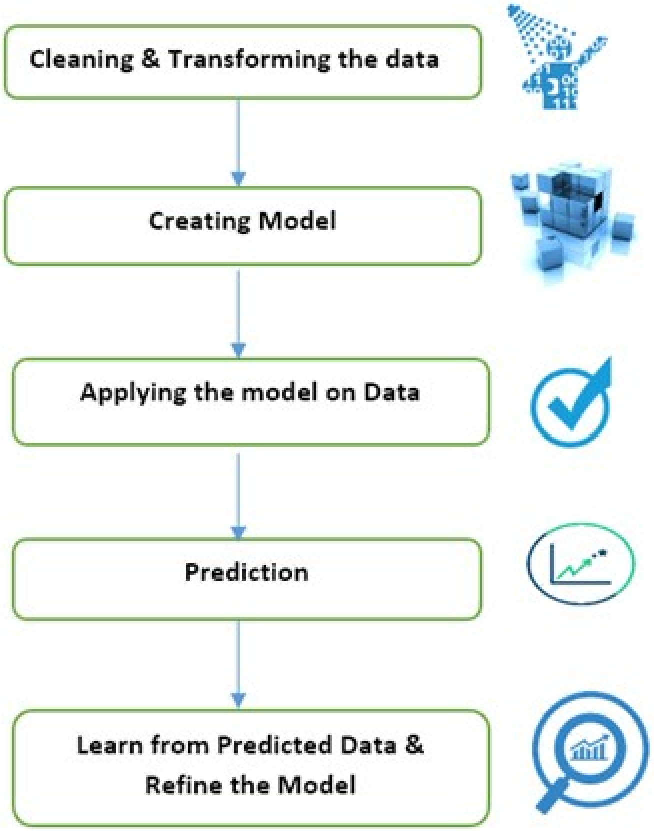
_raw	bytes	device_ip	linecount	method	status
** Results are the Same **	2108	128.241.220.82	2	GET	200

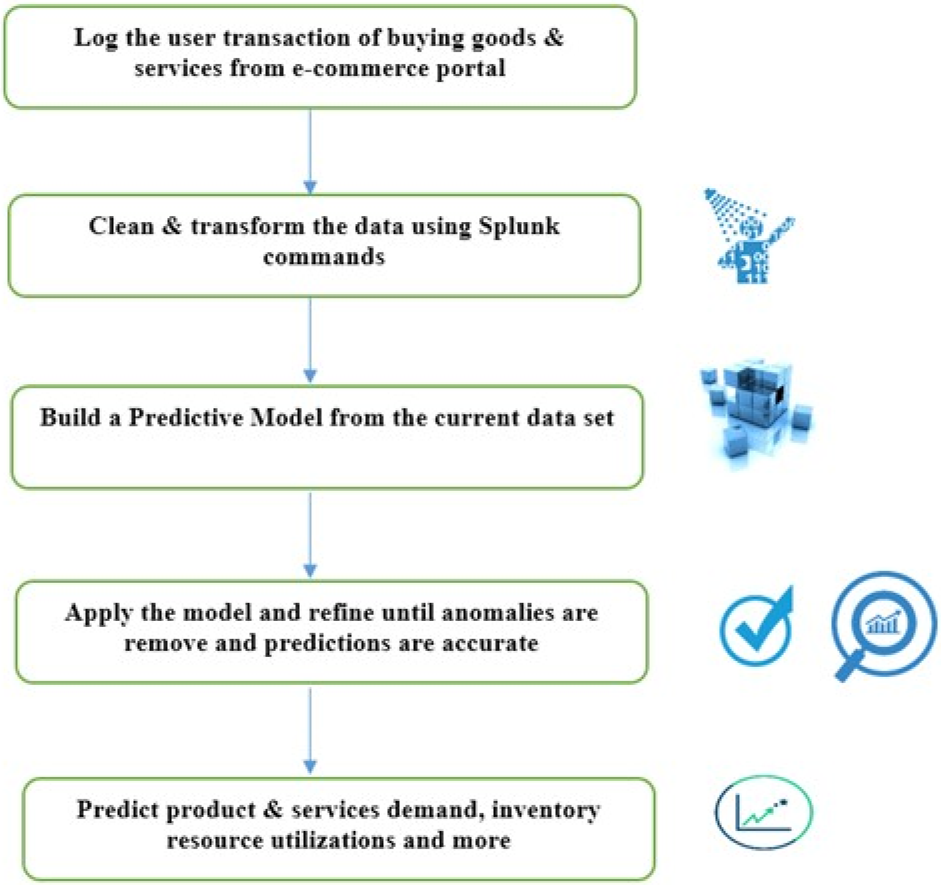


```
index="web_server"  |  contingency useragent device_ip
```

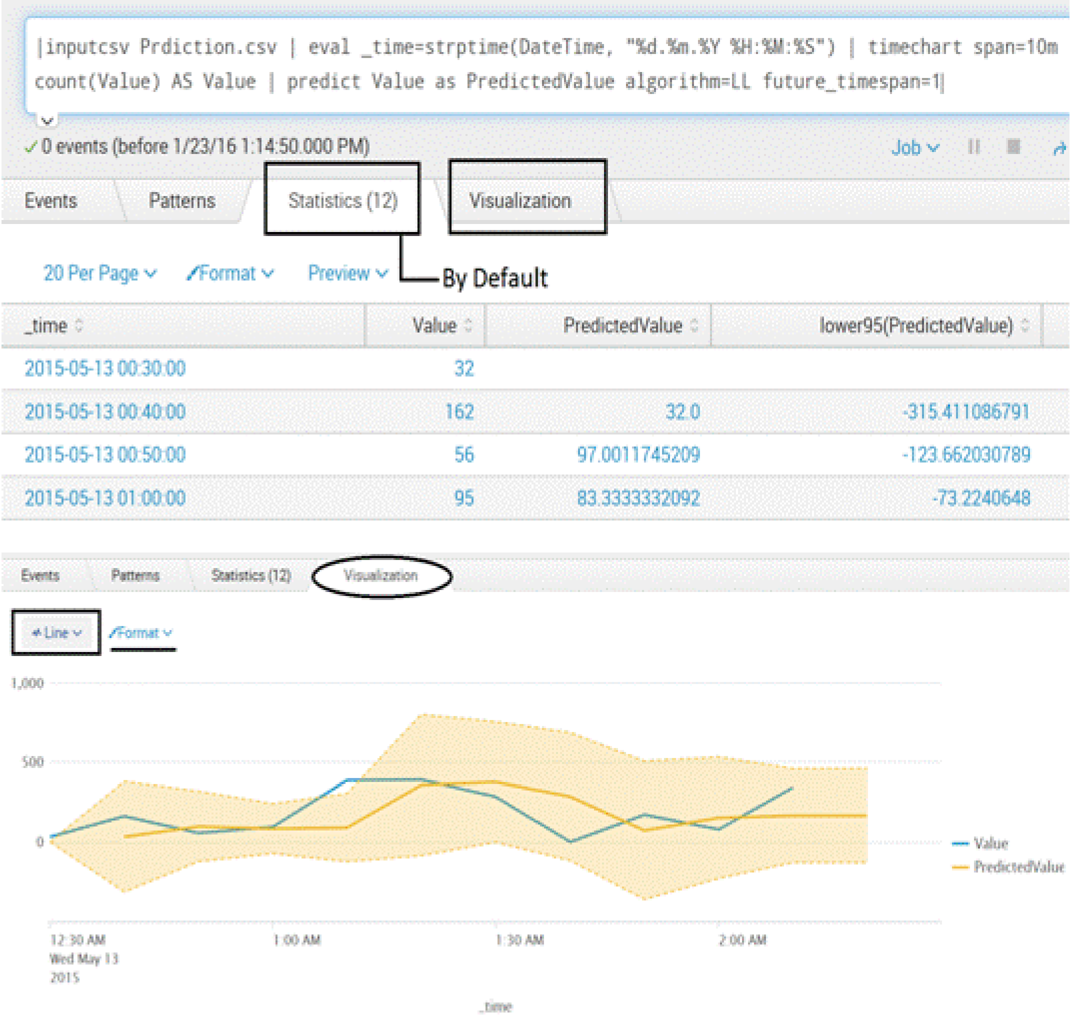
✓ 0 events (before 1/10/16 10:56:43.000 PM)

useragent	125.17.14.100	128.241.220.82	131.178.233.243	12.130.60.4	141.146.8.66
BlackBerry9650/5.0.0.1006 Profile/MIDP-2.1 Configuration/CLDC-1.1 VendorID/105	0	2	0	4	1
BlackBerry8520/5.0.0.681 Profile/MIDP-2.1 Configuration/CLDC-1.1 VendorID/120	0	2	1	1	2


Cleaning & Transforming the data
Creating Model
Applying the model on Data
Prediction
Learn from Predicted Data &
Refine the Model


Log the user transaction of buying goods & services from e-commerce portal
Clean & transform the data using Splunk commands
Build a Predictive Model from the current data set
Apply the model and refine until anomalies are remove and predictions are accurate
Predict product & services demand, inventory resource utilizations and more

Chapter 6: Visualization

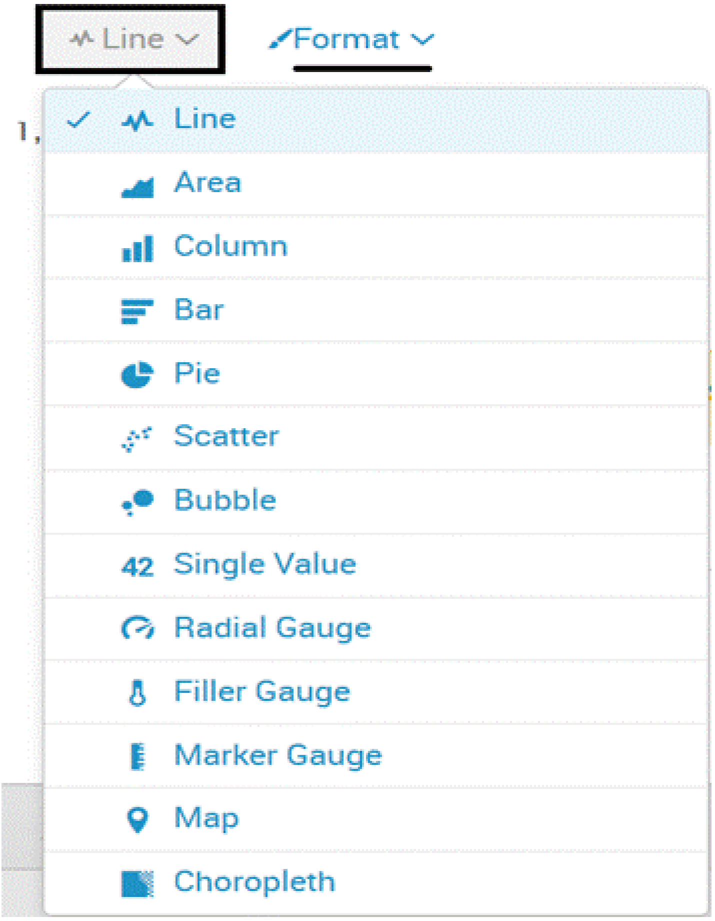


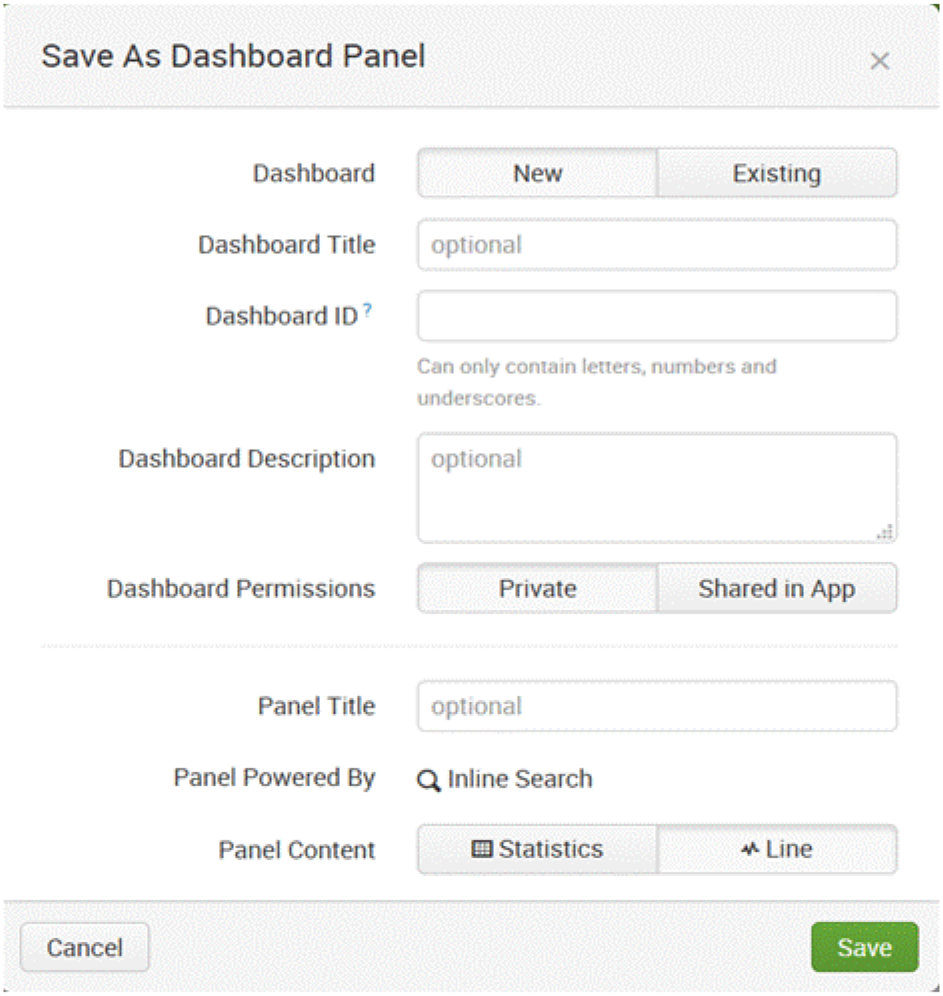
```
|inputcsv Prdiction.csv | eval _time=strptime(DateTime, "%d.%m.%Y %H:%M:%S") | timechart span=10m
count(Value) AS Value | predict Value as PredictedValue algorithm=LL future_timespan=1
```

✓ 0 events (before 1/23/16 1:14:50.000 PM)

By Default

_time	Value	PredictedValue	lower95(PredictedValue)
2015-05-13 00:30:00	32		
2015-05-13 00:40:00	162	32.0	-315.411086791
2015-05-13 00:50:00	56	97.0011745209	-123.662030789
2015-05-13 01:00:00	95	83.3333332092	-73.2240648


Line
Format
✓ Line
Area
Column
Bar
Pie
Scatter
Bubble
42 Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Map
Choropleth



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: optional

Dashboard ID ?

Can only contain letters, numbers and underscores.

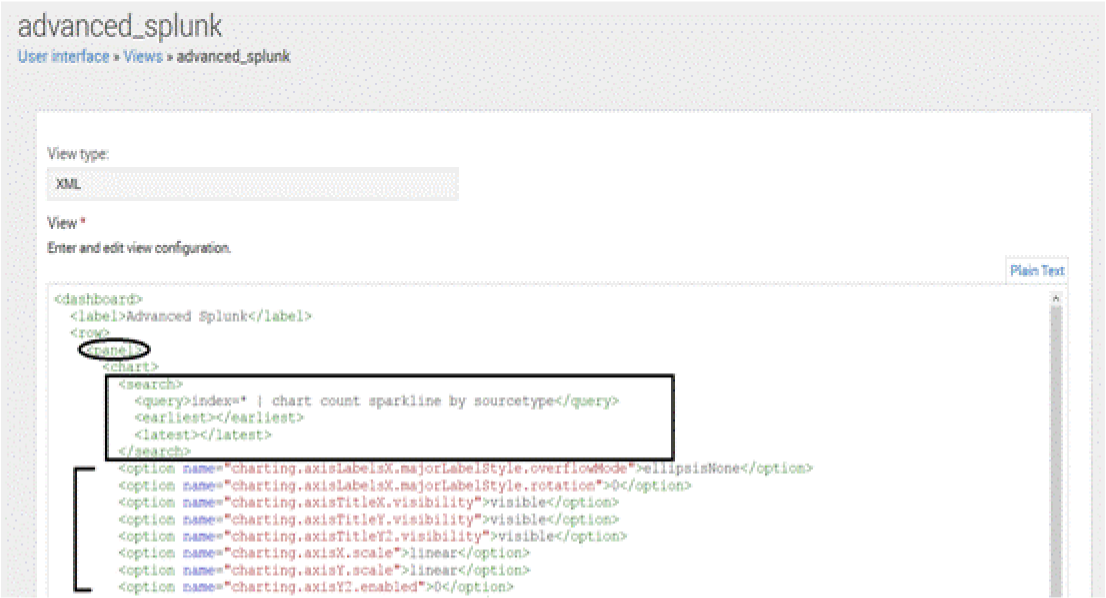
Dashboard Description: optional

Dashboard Permissions: Private | Shared in App

Panel Title: optional

Panel Powered By: Inline Search

Panel Content: Statistics | Line



advanced_splunk

User interface » Views » advanced_splunk

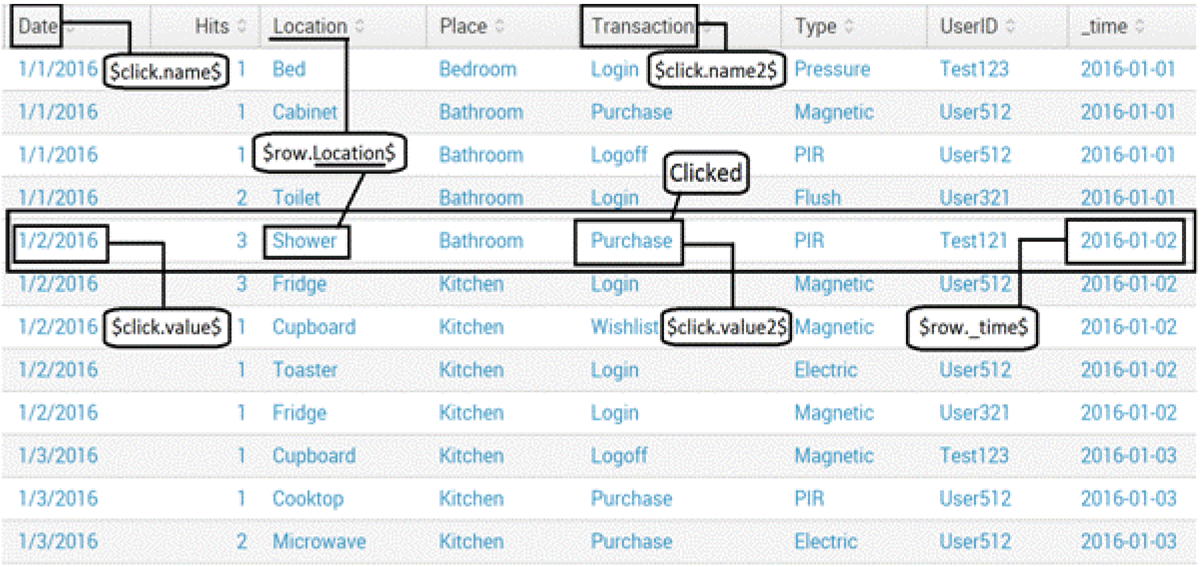
View type:

XML

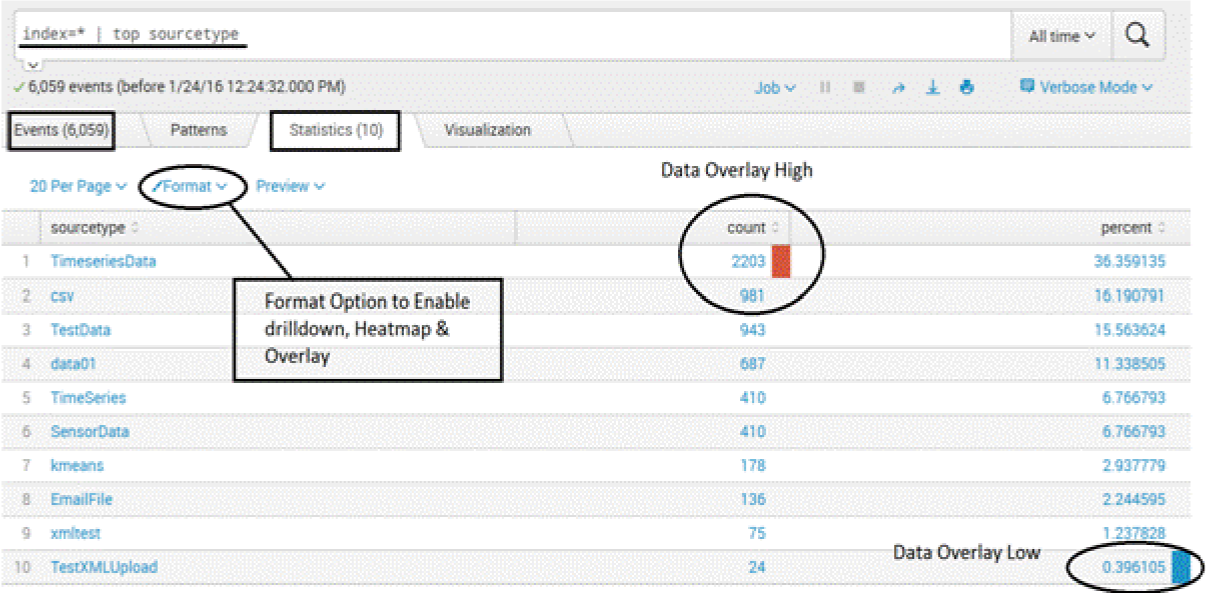
View *

Enter and edit view configuration.

```
<dashboard>
  <label>Advanced Splunk</label>
  <row>
   <panel>
    <chart>
     <search>
      <query>index=* | chart count sparkline by sourcetype</query>
      <earliest></earliest>
      <latest></latest>
     </search>
     <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>
     <option name="charting.axisY.scale">linear</option>
     <option name="charting.axisY2.enabled">0</option>
```



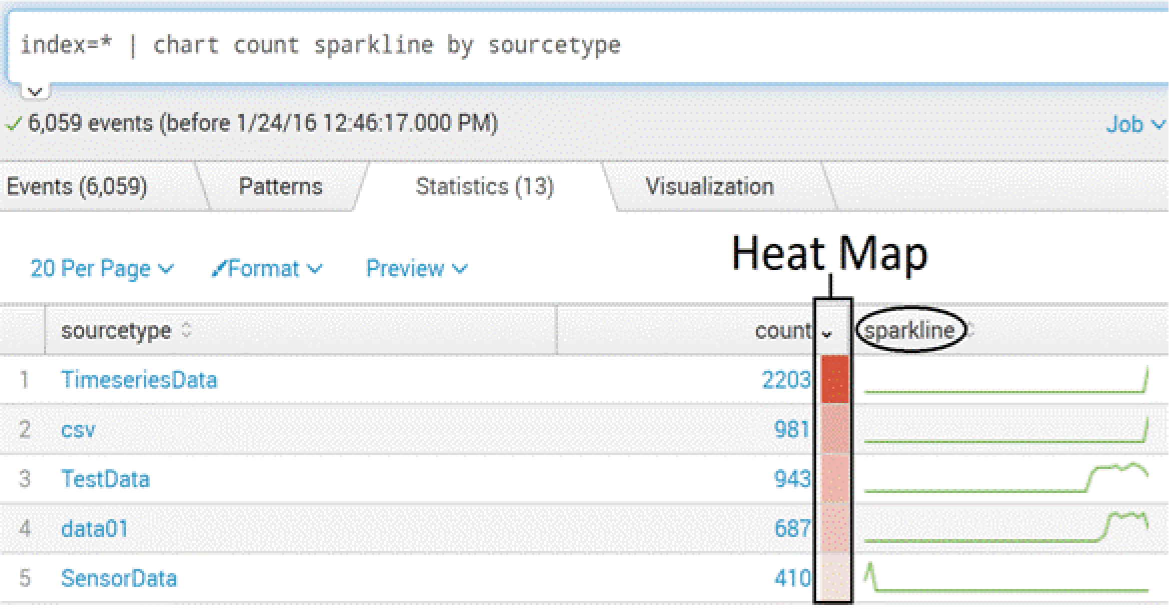
Date	Hits	Location	Place	Transaction	Type	UserID	_time
1/1/2016	1	Bed	Bedroom	Login	Pressure	Test123	2016-01-01
1/1/2016	1	Cabinet	Bathroom	Purchase	Magnetic	User512	2016-01-01
1/1/2016	1	Sink	Bathroom	Logoff	PIR	User512	2016-01-01
1/1/2016	2	Toilet	Bathroom	Login	Flush	User321	2016-01-01
1/2/2016	3	Shower	Bathroom	Purchase	PIR	Test121	2016-01-02
1/2/2016	3	Fridge	Kitchen	Login	Magnetic	User512	2016-01-02
1/2/2016	1	Cupboard	Kitchen	Wishlist	Magnetic	User512	2016-01-02
1/2/2016	1	Toaster	Kitchen	Login	Electric	User512	2016-01-02
1/2/2016	1	Fridge	Kitchen	Login	Magnetic	User321	2016-01-02
1/3/2016	1	Cupboard	Kitchen	Logoff	Magnetic	Test123	2016-01-03
1/3/2016	1	Cooktop	Kitchen	Purchase	PIR	User512	2016-01-03
1/3/2016	2	Microwave	Kitchen	Purchase	Electric	User512	2016-01-03



```
index=* | top sourcetype
```

✓ 6,059 events (before 1/24/16 12:24:32.000 PM)

	sourcetype	count	percent
1	TimeseriesData	2203	36.359135
2	csv	981	16.190791
3	TestData	943	15.563624
4	data01	687	11.338505
5	TimeSeries	410	6.766793
6	SensorData	410	6.766793
7	kmeans	178	2.937779
8	EmailFile	136	2.244595
9	xmltest	75	1.237828
10	TestXMLUpload	24	0.396105



```
index=* | chart count sparkline by sourcetype
```

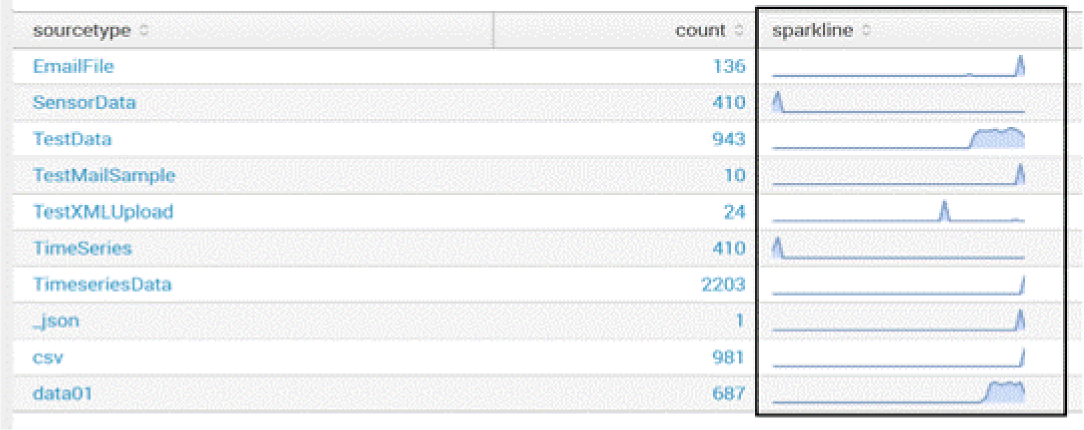
✓ 6,059 events (before 1/24/16 12:46:17.000 PM)

	sourcetype	count	sparkline
1	TimeseriesData	2203	
2	csv	981	
3	TestData	943	
4	data01	687	
5	SensorData	410	

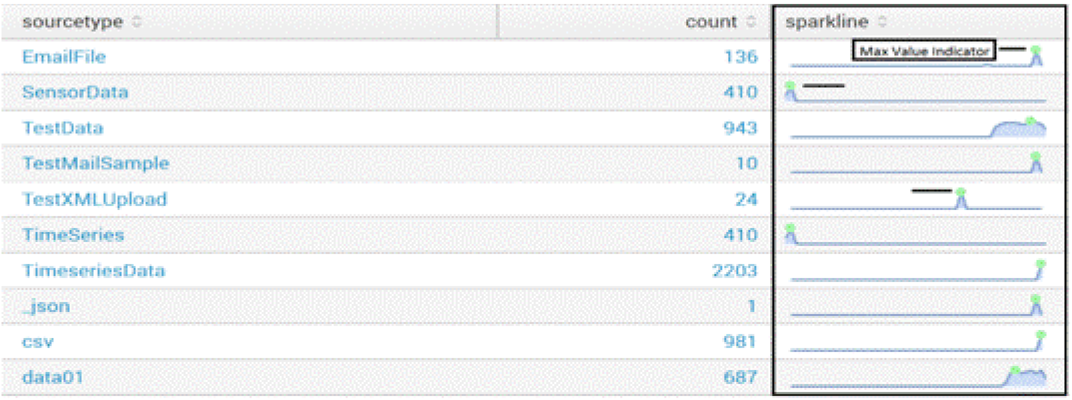
```
<dashboard>
  <label>Advanced Splunk</label>
  <row>
    <panel>
      <title>Sparkline</title>
      <table>

        <search>
          <query>index=* | chart count sparkline by sourcetype</query>
        </search>

      <!-- CODE TO FILL & CHANGE COLOUR OF SPARKLINE -->

      <format type="sparkline" field="sparkline">
        <option name="lineColor">#5379af</option>
        <option name="fillColor">#CCDDFF</option>
      </format>

      </table>
    </panel>
  </row>
</dashboard>
```

Identify the correct Panel to make changes

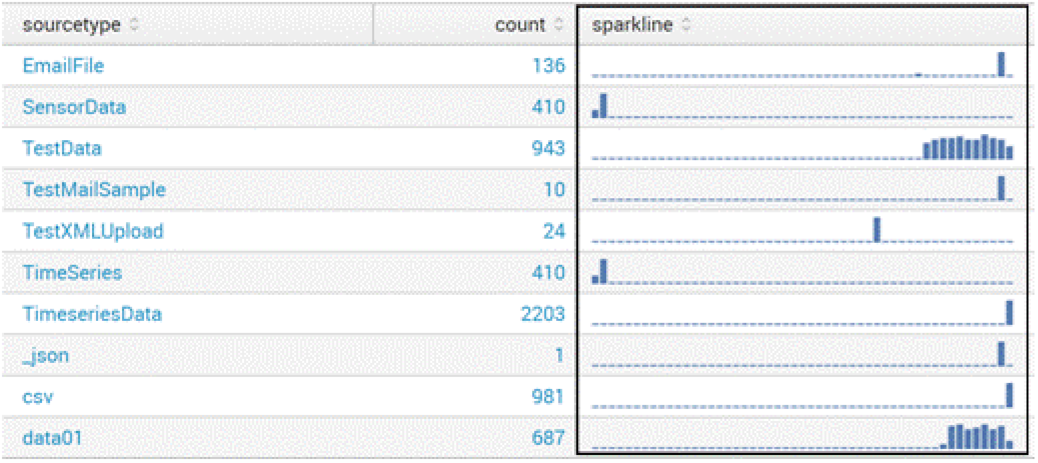
Format Code



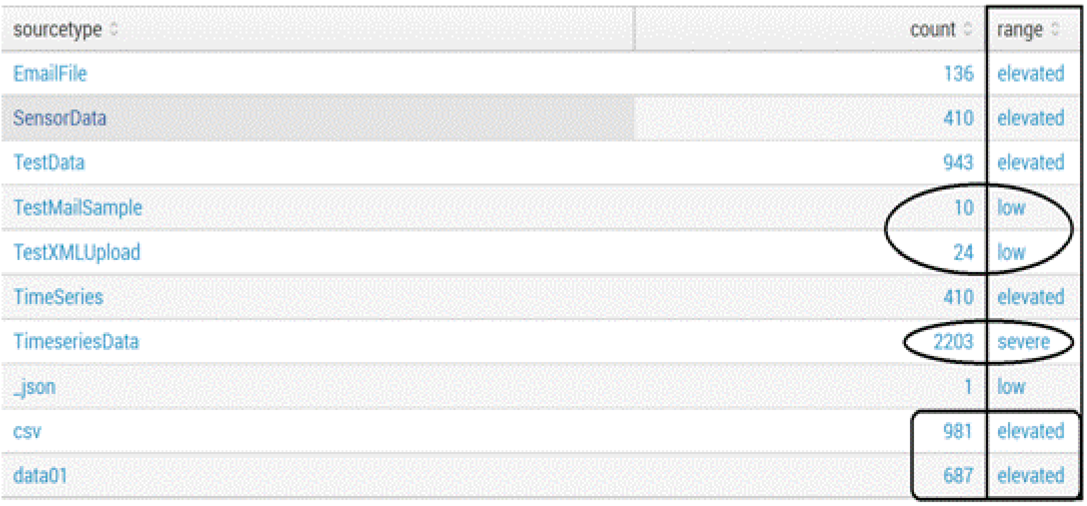
sourcetype	count	sparkline
EmailFile	136	
SensorData	410	
TestData	943	
TestMailSample	10	
TestXMLUpload	24	
TimeSeries	410	
TimeseriesData	2203	
_json	1	
csv	981	
data01	687	



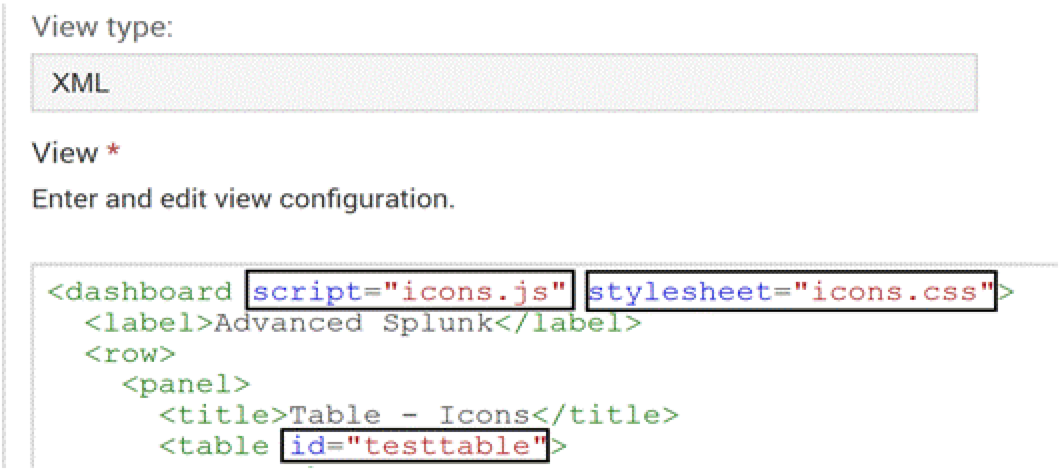
sourcetype	count	sparkline
EmailFile	136	
SensorData	410	
TestData	943	
TestMailSample	10	
TestXMLUpload	24	
TimeSeries	410	
TimeseriesData	2203	
_json	1	
csv	981	
data01	687	



sourcetype	count	sparkline
EmailFile	136	
SensorData	410	
TestData	943	
TestMailSample	10	
TestXMLUpload	24	
TimeSeries	410	
TimeseriesData	2203	
_json	1	
csv	981	
data01	687	



sourcetype	count	range
EmailFile	136	elevated
SensorData	410	elevated
TestData	943	elevated
TestMailSample	10	low
TestXMLUpload	24	low
TimeSeries	410	elevated
TimeseriesData	2203	severe
_json	1	low
csv	981	elevated
data01	687	elevated



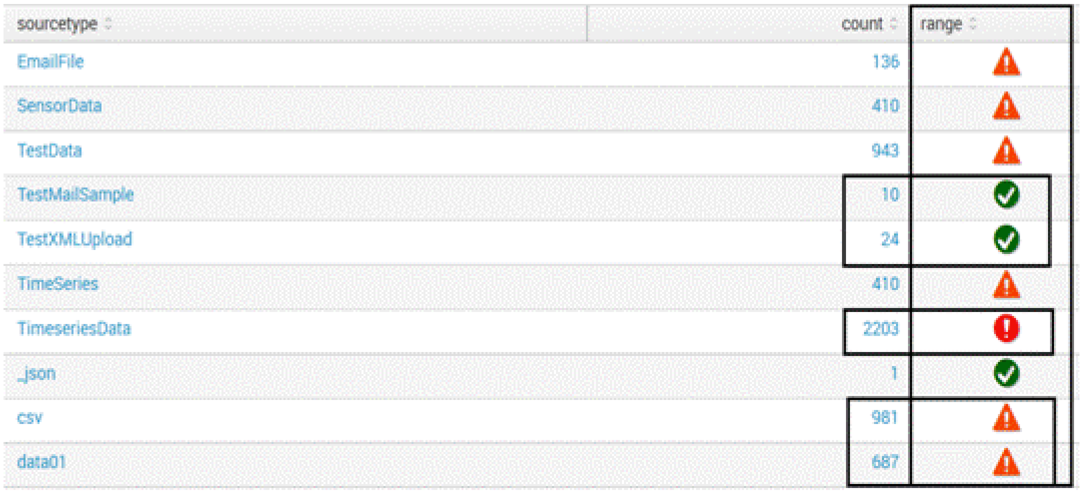
View type:

XML

View *

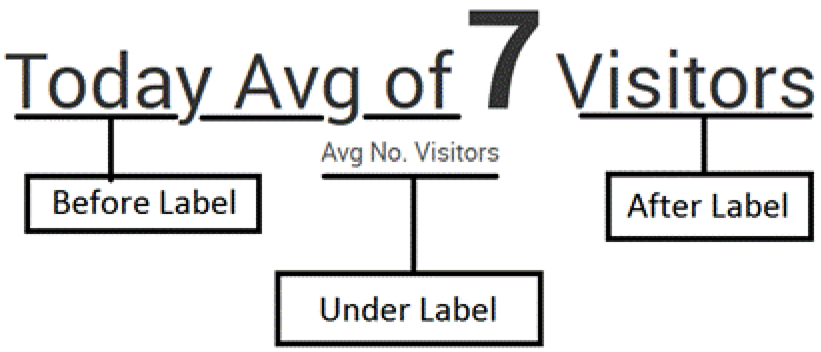
Enter and edit view configuration.

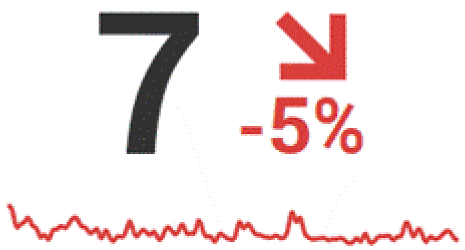
```
<dashboard script="icons.js" stylesheet="icons.css">
  <label>Advanced Splunk</label>
  <row>
    <panel>
      <title>Table - Icons</title>
      <table id="testtable">
```

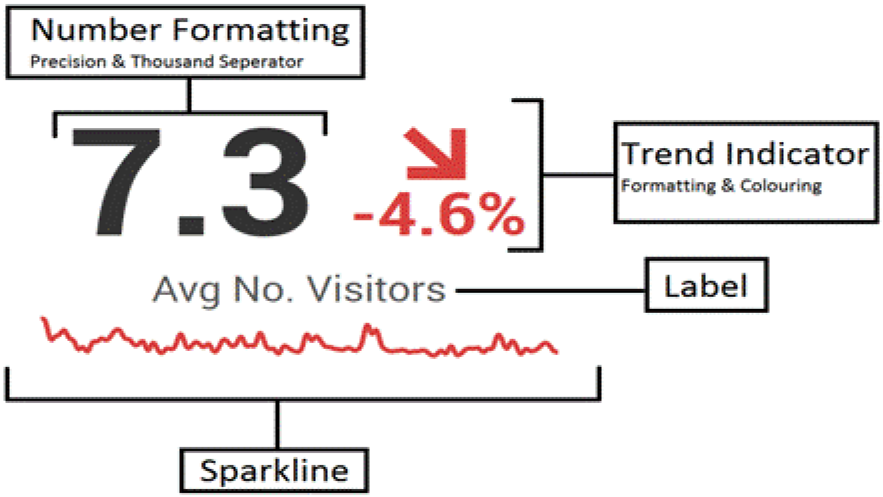


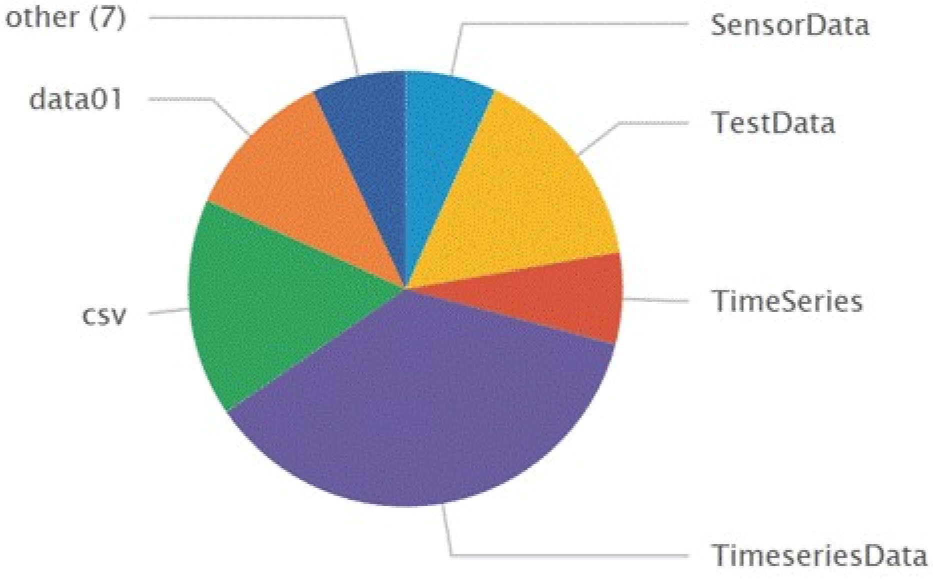
sourcetype	count	range
EmailFile	136	⚠
SensorData	410	⚠
TestData	943	⚠
TestMailSample	10	✓
TestXMLUpload	24	✓
TimeSeries	410	⚠
TimeseriesData	2203	!
_json	1	✓
csv	981	⚠
data01	687	⚠

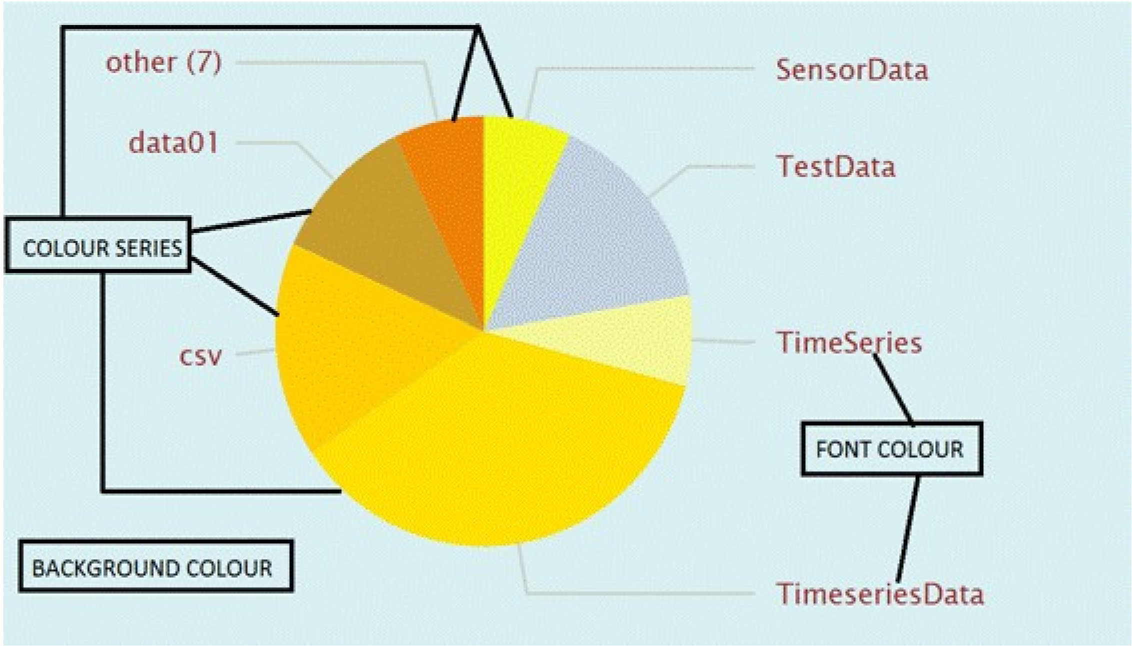
7



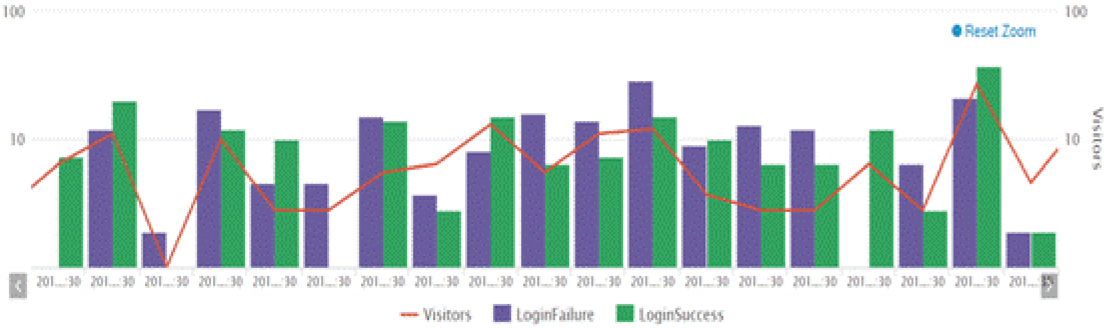

7
-5%


Number Formatting
Precision & Thousand Seperator
7.3
-4.6%
Trend Indicator
Formatting & Colouring
Avg No. Visitors
Label
Sparkline

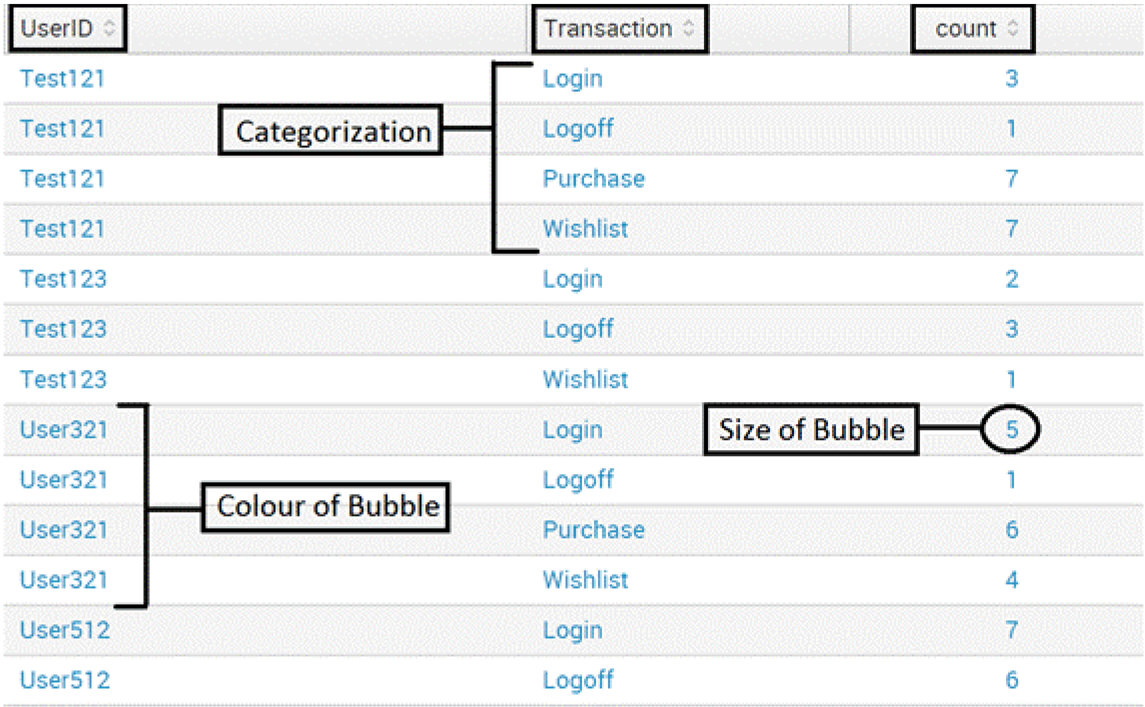

other (7)
data01
csv
SensorData
TestData
TimeSeries
TimeseriesData



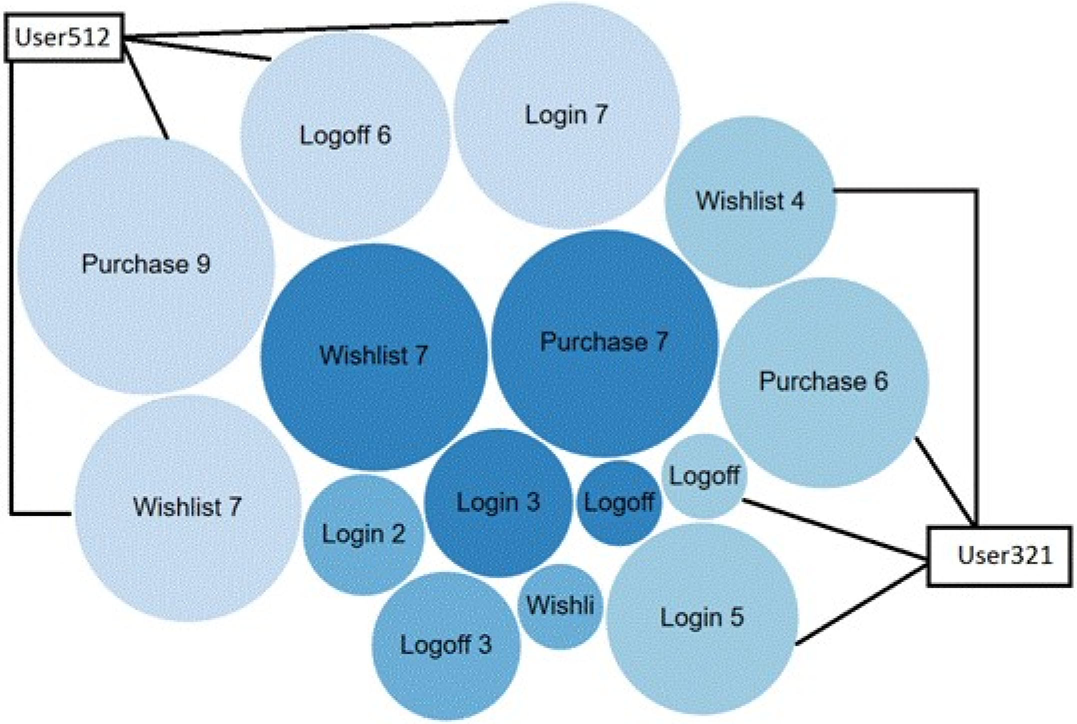
other (7)
SensorData
data01
TestData
COLOUR SERIES
TimeSeries
csv
FONT COLOUR
BACKGROUND COLOUR
TimeseriesData

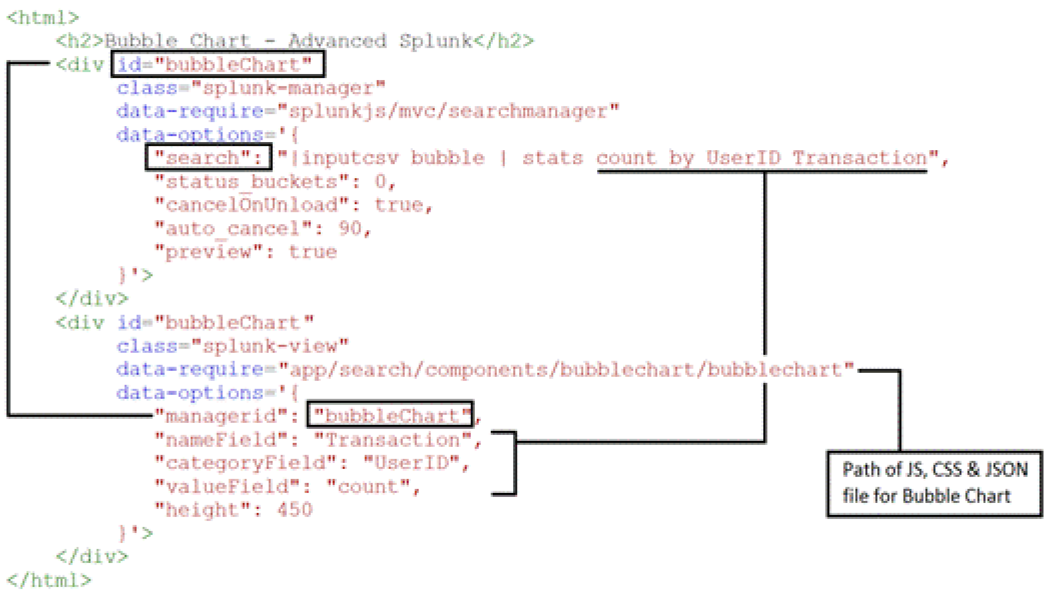


100
10
100
10
Reset Zoom
Visitors
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...:30
201...
Visitors
LoginFailure
LoginSuccess

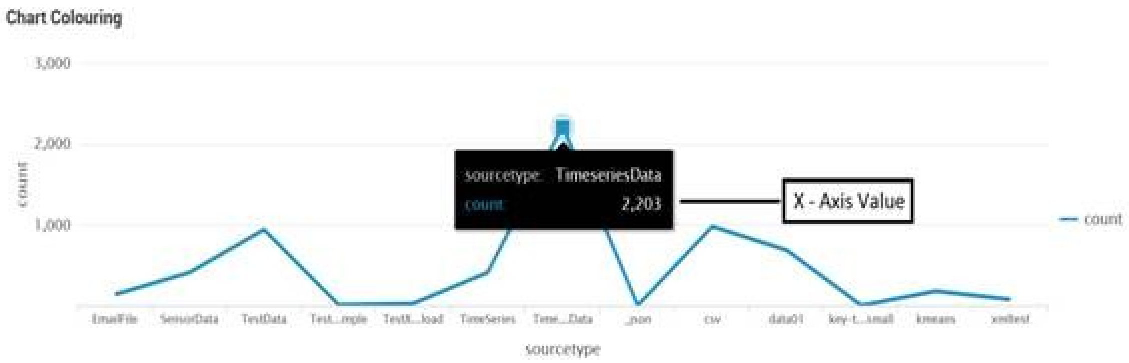


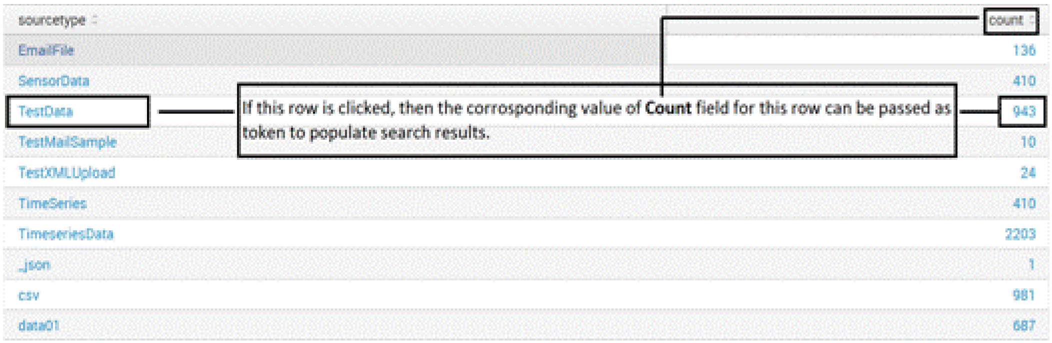
UserID	Transaction	count
Test121	Login	3
Test121	Logoff	1
Test121	Purchase	7
Test121	Wishlist	7
Test123	Login	2
Test123	Logoff	3
Test123	Wishlist	1
User321	Login	5
User321	Logoff	1
User321	Purchase	6
User321	Wishlist	4
User512	Login	7
User512	Logoff	6





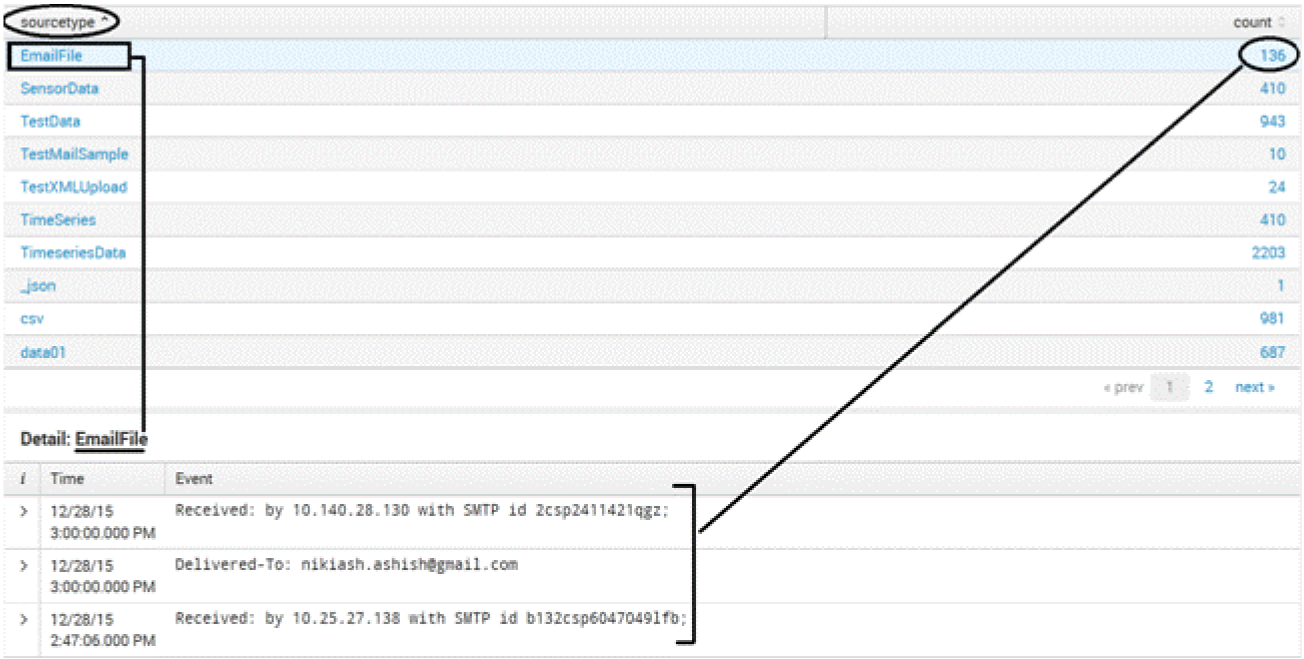
```
<html>
    <h2>Bubble Chart - Advanced Splunk</h2>
    <div id="bubbleChart"
         class="splunk-manager"
         data-require="splunkjs/mvc/searchmanager"
         data-options='{
            "search": "|inputcsv bubble | stats count by UserID Transaction",
            "status_buckets": 0,
            "cancelOnUnload": true,
            "auto_cancel": 90,
            "preview": true
         }'>
    </div>
    <div id="bubbleChart"
         class="splunk-view"
         data-require="app/search/components/bubblechart/bubblechart"
         data-options='{
            "managerid": "bubbleChart",
            "nameField": "Transaction",
            "categoryField": "UserID",
            "valueField": "count",
            "height": 450
         }'>
    </div>
</html>
```





sourcetype	count
EmailFile	136
SensorData	410
TestData	943
TestMailSample	10
TestXMLUpload	24
TimeSeries	410
TimeseriesData	2203
_json	1
csv	981
data01	687

If this row is clicked, then the corrosponding value of **Count** field for this row can be passed as token to populate search results.

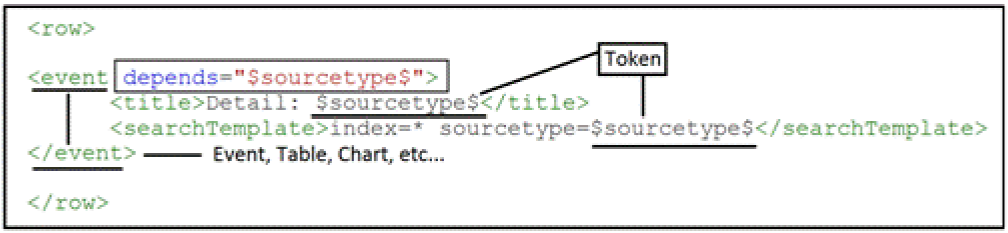


sourcetype ^	count
EmailFile	136
SensorData	410
TestData	943
TestMailSample	10
TestXMLUpload	24
TimeSeries	410
TimeseriesData	2203
_json	1
csv	981
data01	687

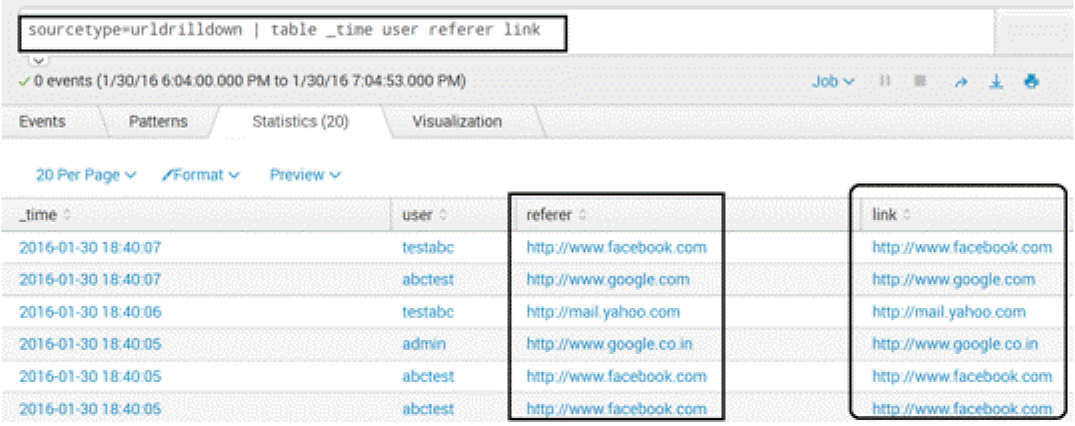
« prev 1 2 next »

Detail: EmailFile

i	Time	Event
>	12/28/15 3:00:00.000 PM	Received: by 10.140.28.130 with SMTP id 2csp2411421qgz;
>	12/28/15 3:00:00.000 PM	Delivered-To: nikiash.ashish@gmail.com
>	12/28/15 2:47:06.000 PM	Received: by 10.25.27.138 with SMTP id b132csp6047049lfb;



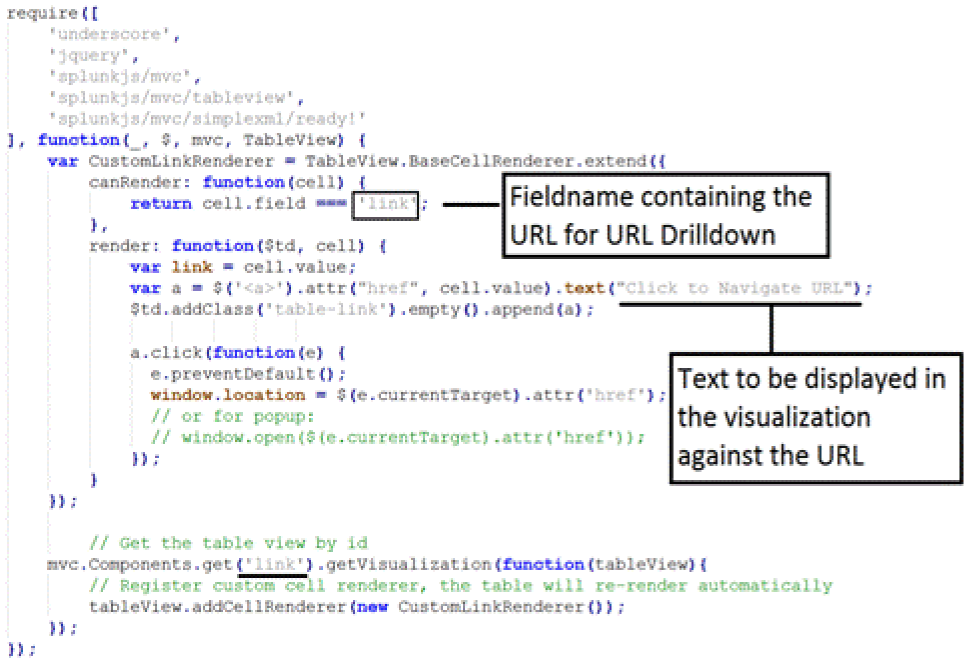
```
<row>

<event depends="$sourcetype$">
    <title>Detail: $sourcetype$</title>
    <searchTemplate>index=* sourcetype=$sourcetype$</searchTemplate>
</event>

</row>
```



```
sourcetype=urldrilldown | table _time user referer link
```

✓ 0 events (1/30/16 6:04:00.000 PM to 1/30/16 7:04:53.000 PM)

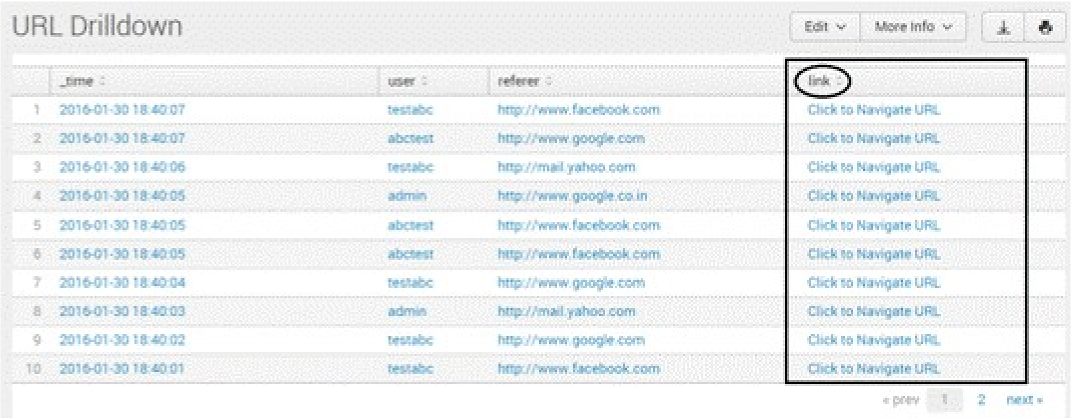
_time	user	referer	link
2016-01-30 18:40:07	testabc	http://www.facebook.com	http://www.facebook.com
2016-01-30 18:40:07	abctest	http://www.google.com	http://www.google.com
2016-01-30 18:40:06	testabc	http://mail.yahoo.com	http://mail.yahoo.com
2016-01-30 18:40:05	admin	http://www.google.co.in	http://www.google.co.in
2016-01-30 18:40:05	abctest	http://www.facebook.com	http://www.facebook.com
2016-01-30 18:40:05	abctest	http://www.facebook.com	http://www.facebook.com



```
require([
    'underscore',
    'jquery',
    'splunkjs/mvc',
    'splunkjs/mvc/tableview',
    'splunkjs/mvc/simplexml/ready!'
], function(_, $, mvc, TableView) {
    var CustomLinkRenderer = TableView.BaseCellRenderer.extend({
        canRender: function(cell) {
            return cell.field === 'link';
        },
        render: function($td, cell) {
            var link = cell.value;
            var a = $('<a>').attr("href", cell.value).text("Click to Navigate URL");
            $td.addClass('table-link').empty().append(a);

            a.click(function(e) {
              e.preventDefault();
              window.location = $(e.currentTarget).attr('href');
              // or for popup:
              // window.open($(e.currentTarget).attr('href'));
            });
        }
    });

        // Get the table view by id
    mvc.Components.get('link').getVisualization(function(tableView){
        // Register custom cell renderer, the table will re-render automatically
        tableView.addCellRenderer(new CustomLinkRenderer());
    });
});
```

Fieldname containing the URL for URL Drilldown

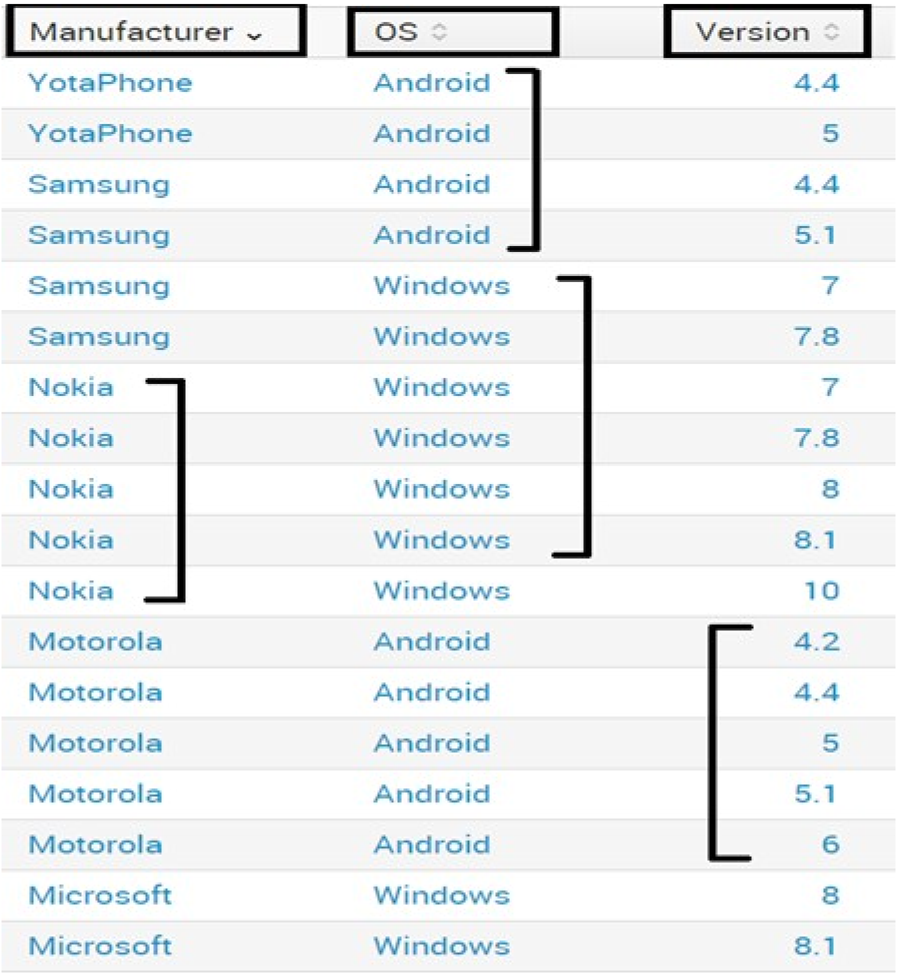
Text to be displayed in the visualization against the URL



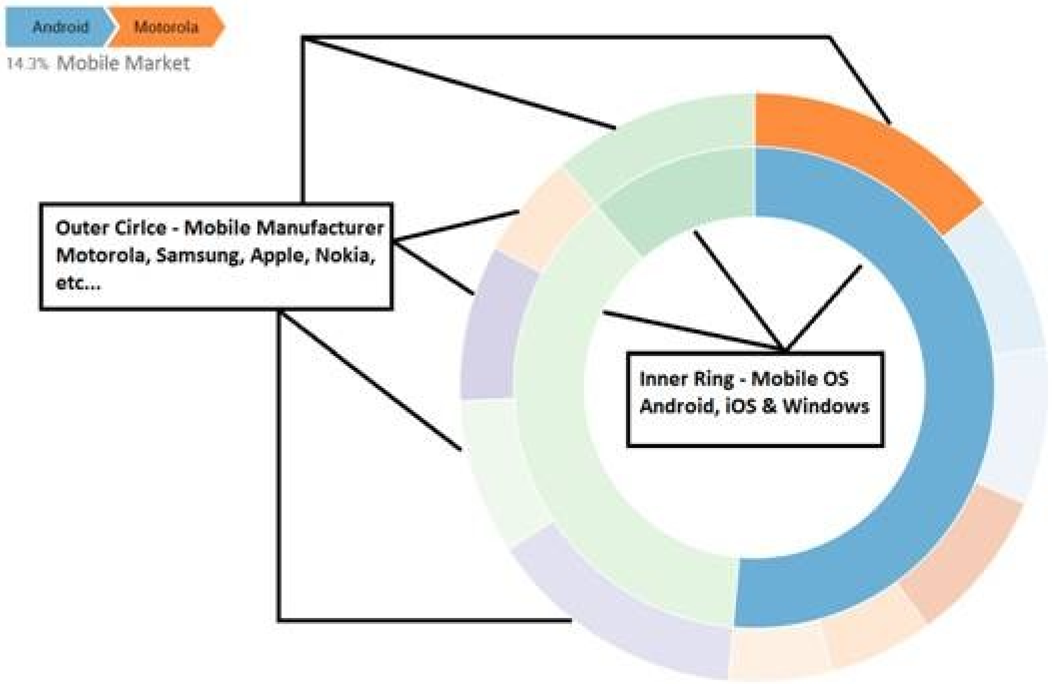
URL Drilldown

	_time	user	referer	link
1	2016-01-30 18:40:07	testabc	http://www.facebook.com	Click to Navigate URL
2	2016-01-30 18:40:07	abctest	http://www.google.com	Click to Navigate URL
3	2016-01-30 18:40:06	testabc	http://mail.yahoo.com	Click to Navigate URL
4	2016-01-30 18:40:05	admin	http://www.google.co.in	Click to Navigate URL
5	2016-01-30 18:40:05	abctest	http://www.facebook.com	Click to Navigate URL
6	2016-01-30 18:40:05	abctest	http://www.facebook.com	Click to Navigate URL
7	2016-01-30 18:40:04	testabc	http://www.google.com	Click to Navigate URL
8	2016-01-30 18:40:03	admin	http://mail.yahoo.com	Click to Navigate URL
9	2016-01-30 18:40:02	testabc	http://www.google.com	Click to Navigate URL
10	2016-01-30 18:40:01	testabc	http://www.facebook.com	Click to Navigate URL

Chapter 7: Advanced Visualization

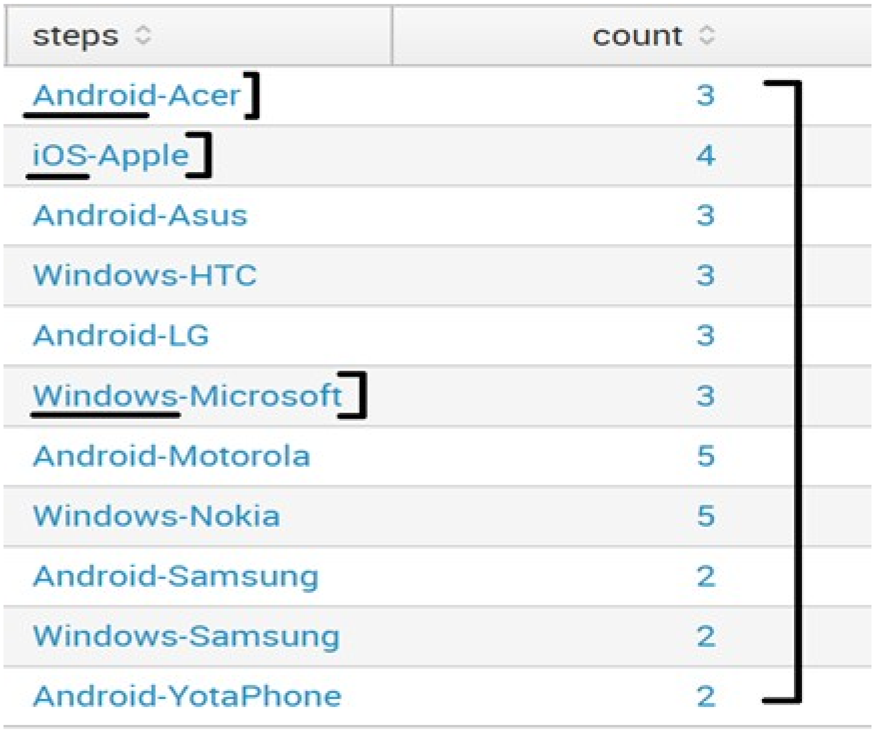


Manufacturer ⌄	OS ⇕	Version ⇕
YotaPhone	Android	4.4
YotaPhone	Android	5
Samsung	Android	4.4
Samsung	Android	5.1
Samsung	Windows	7
Samsung	Windows	7.8
Nokia	Windows	7
Nokia	Windows	7.8
Nokia	Windows	8
Nokia	Windows	8.1
Nokia	Windows	10
Motorola	Android	4.2
Motorola	Android	4.4
Motorola	Android	5
Motorola	Android	5.1
Motorola	Android	6
Microsoft	Windows	8
Microsoft	Windows	8.1

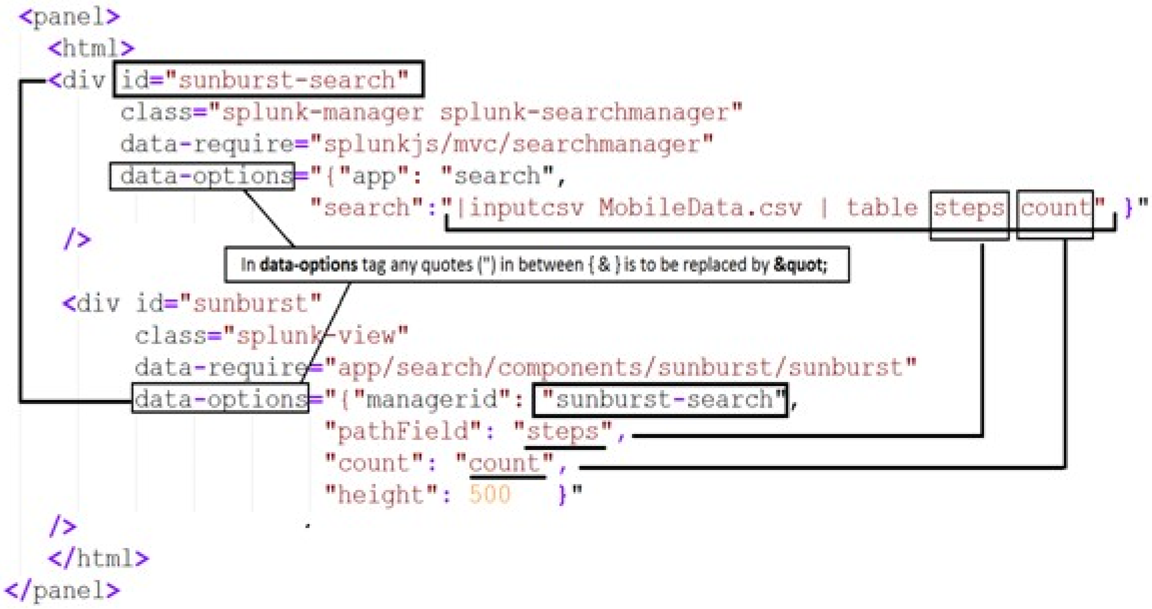


Outer Cirlce - Mobile Manufacturer Motorola, Samsung, Apple, Nokia, etc...

Inner Ring - Mobile OS Android, iOS & Windows

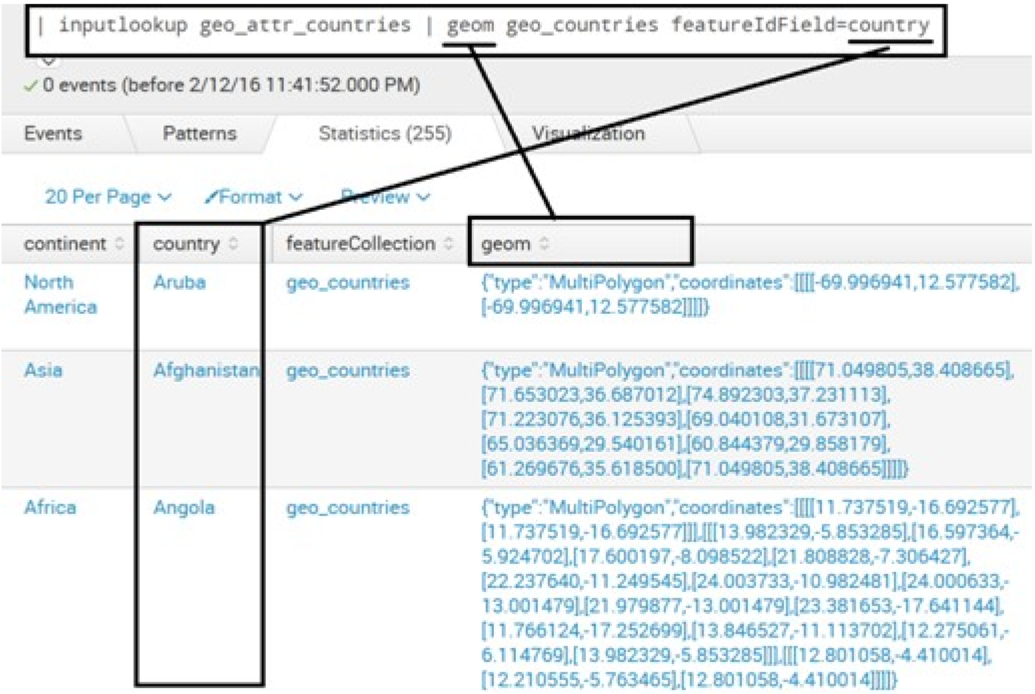


steps	count
Android-Acer	3
iOS-Apple	4
Android-Asus	3
Windows-HTC	3
Android-LG	3
Windows-Microsoft	3
Android-Motorola	5
Windows-Nokia	5
Android-Samsung	2
Windows-Samsung	2
Android-YotaPhone	2



```
<panel>
  <html>
  <div id="sunburst-search"
       class="splunk-manager splunk-searchmanager"
       data-require="splunkjs/mvc/searchmanager"
       data-options="{"app": "search",
                      "search":"|inputcsv MobileData.csv | table steps count" }"
   />

   <div id="sunburst"
        class="splunk-view"
        data-require="app/search/components/sunburst/sunburst"
        data-options="{"managerid": "sunburst-search",
                       "pathField": "steps",
                       "count": "count",
                       "height": 500   }"
   />
  </html>
</panel>
```

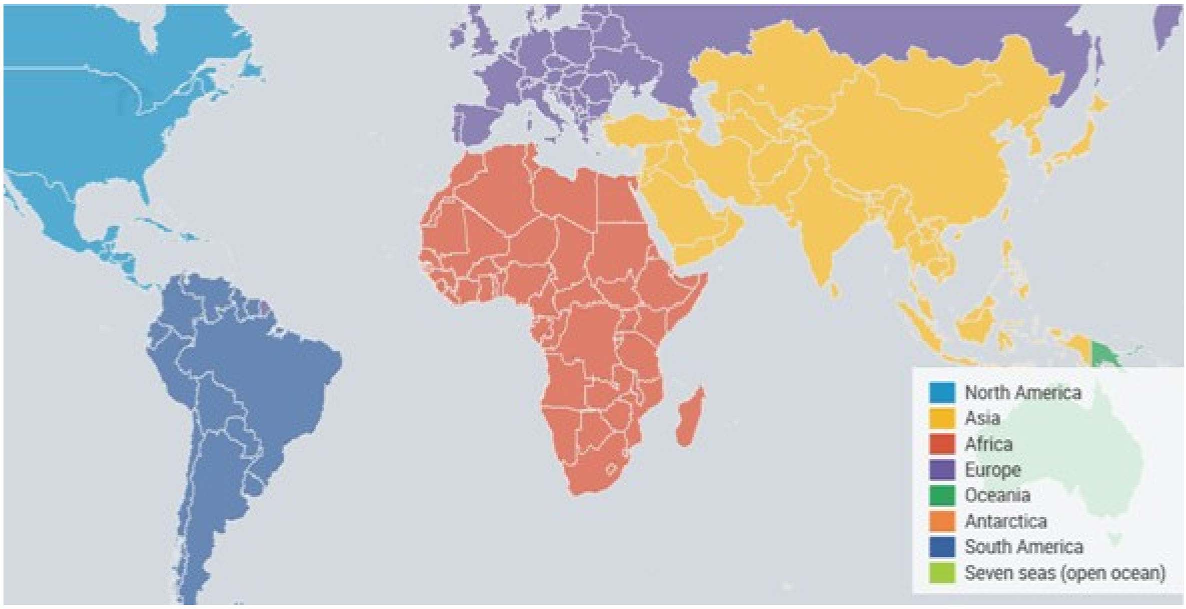
In **data-options** tag any quotes (") in between { & } is to be replaced by **&quot;**

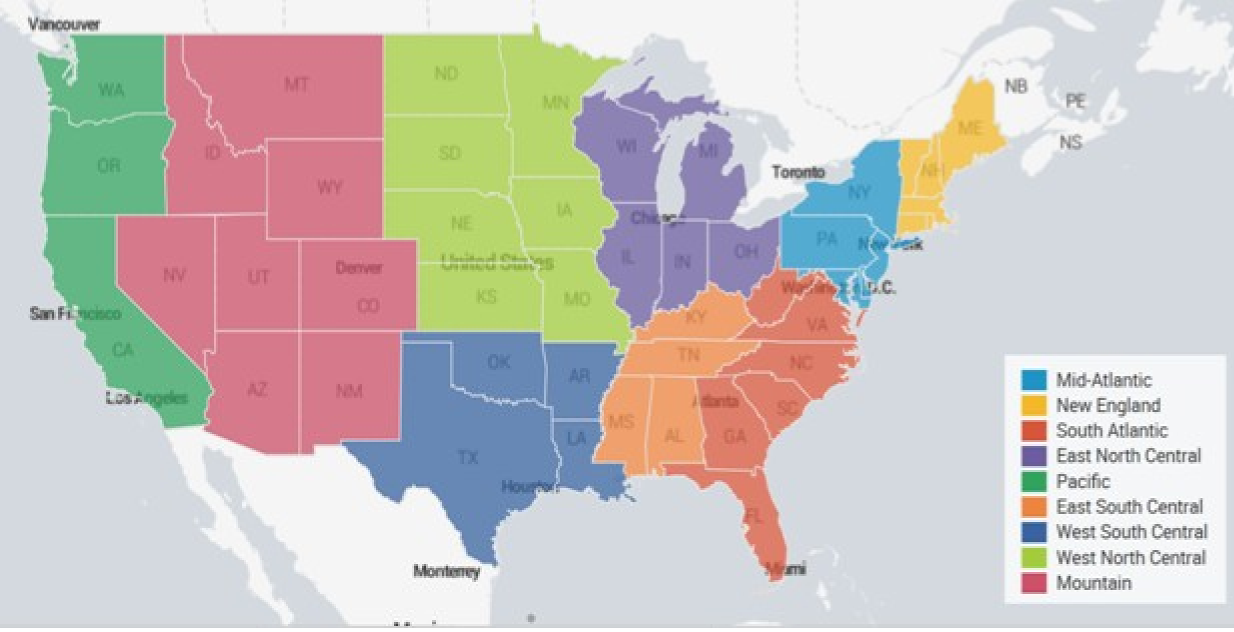


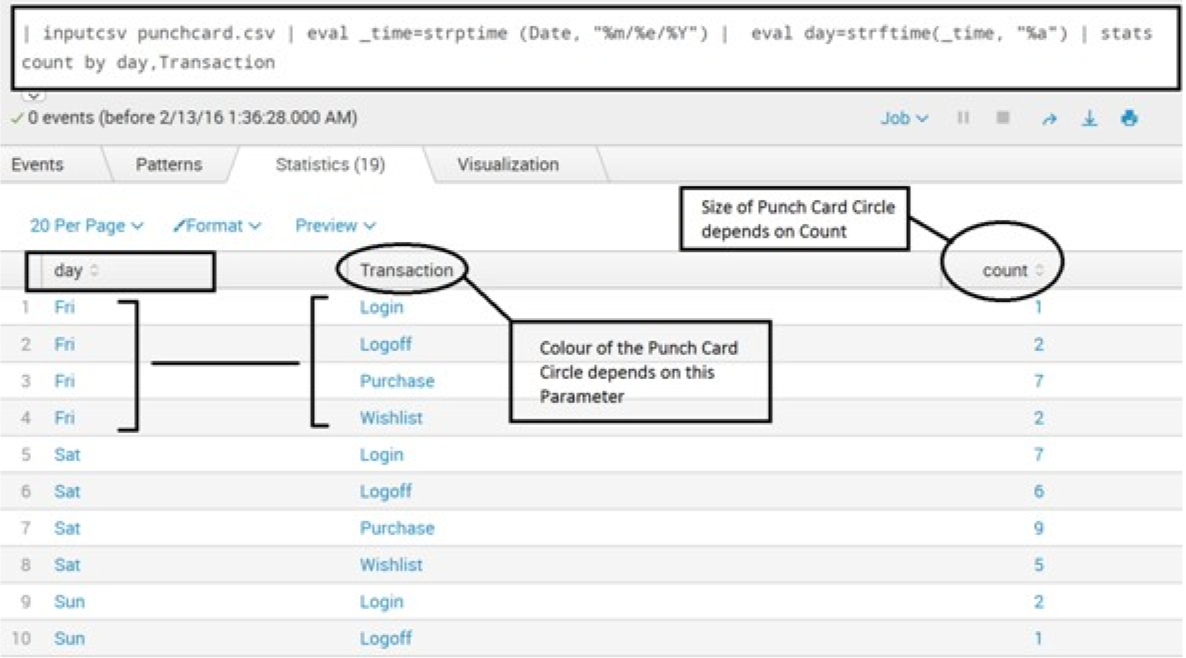
```
| inputlookup geo_attr_countries | geom geo_countries featureIdField=country
```

✓ 0 events (before 2/12/16 11:41:52.000 PM)

continent	country	featureCollection	geom
North America	Aruba	geo_countries	{"type":"MultiPolygon","coordinates":[[[[-69.996941,12.577582],[-69.996941,12.577582]]]]}
Asia	Afghanistan	geo_countries	{"type":"MultiPolygon","coordinates":[[[[71.049805,38.408665],[71.653023,36.687012],[74.892303,37.231113],[71.223076,36.125393],[69.040108,31.673107],[65.036369,29.540161],[60.844379,29.858179],[61.269676,35.618500],[71.049805,38.408665]]]]}
Africa	Angola	geo_countries	{"type":"MultiPolygon","coordinates":[[[[11.737519,-16.692577],[11.737519,-16.692577]]],[[[13.982329,-5.853285],[16.597364,-5.924702],[17.600197,-8.098522],[21.808828,-7.306427],[22.237640,-11.249545],[24.003733,-10.982481],[24.000633,-13.001479],[21.979877,-13.001479],[23.381653,-17.641144],[11.766124,-17.252699],[13.846527,-11.113702],[12.275061,-6.114769],[13.982329,-5.853285]]],[[[12.801058,-4.410014],[12.210555,-5.763465],[12.801058,-4.410014]]]]}


North America
Asia
Africa
Europe
Oceania
Antarctica
South America
Seven seas (open ocean)


Vancouver
WA
MT
ND
MN
NB
PE
NS
ME
WI
MI
ID
SD
OR
Toronto
NH
WY
NY
NE
IA
Chicago
PA
New York
United States
IL
IN
OH
NV
UT
Denver
Washington D.C.
San Francisco
CO
KS
MO
KY
VA
CA
TN
NC
OK
AR
Los Angeles
AZ
NM
MS
AL
Atlanta
SC
GA
LA
TX
Houston
FL
Monterrey
Miami
Mid-Atlantic
New England
South Atlantic
East North Central
Pacific
East South Central
West South Central
West North Central
Mountain



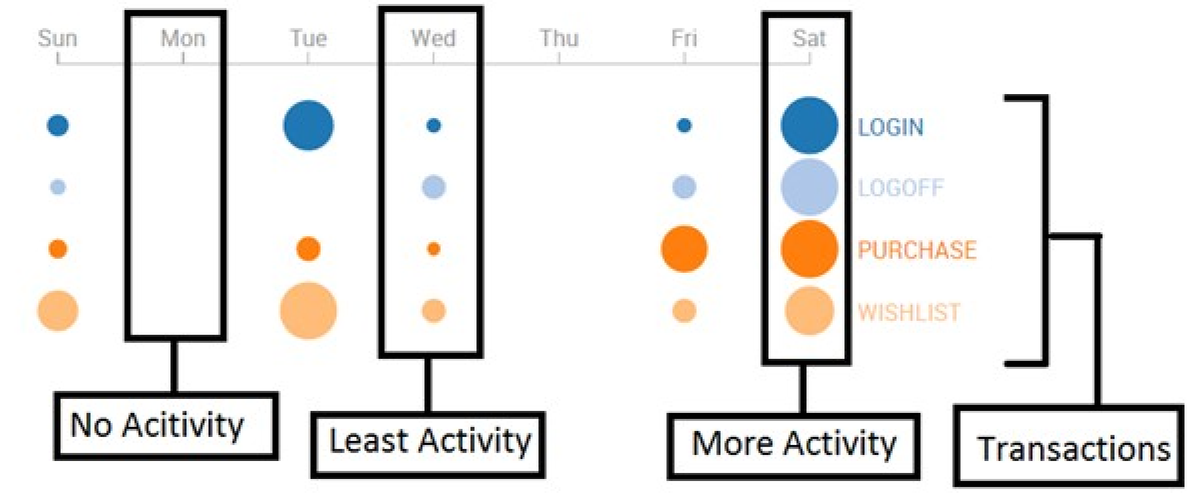
```
| inputcsv punchcard.csv | eval _time=strptime (Date, "%m/%e/%Y") |  eval day=strftime(_time, "%a") | stats count by day,Transaction
```

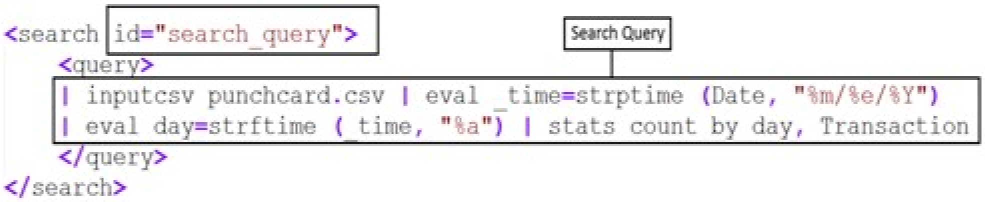
✓ 0 events (before 2/13/16 1:36:28.000 AM)

Size of Punch Card Circle depends on Count

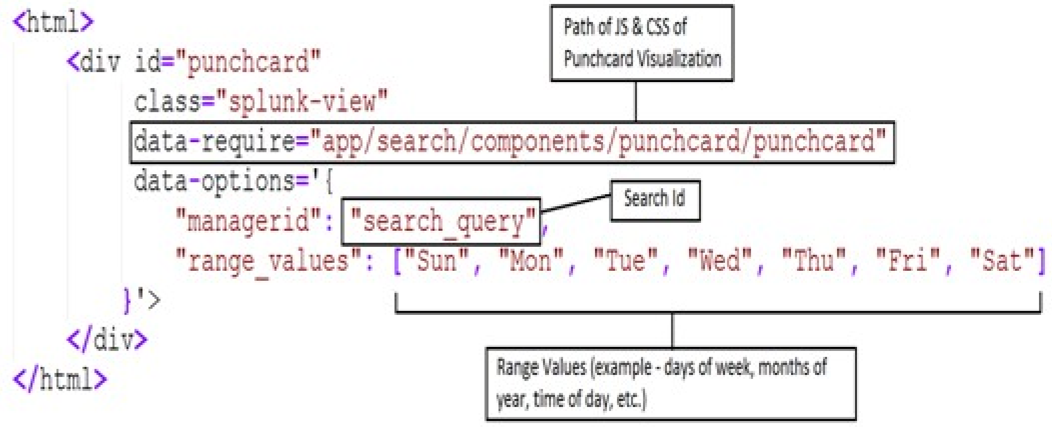
Colour of the Punch Card Circle depends on this Parameter

	day	Transaction	count
1	Fri	Login	1
2	Fri	Logoff	2
3	Fri	Purchase	7
4	Fri	Wishlist	2
5	Sat	Login	7
6	Sat	Logoff	6
7	Sat	Purchase	9
8	Sat	Wishlist	5
9	Sun	Login	2
10	Sun	Logoff	1





```
<search id="search_query">
    <query>
    | inputcsv punchcard.csv | eval _time=strptime (Date, "%m/%e/%Y")
    | eval day=strftime (_time, "%a") | stats count by day, Transaction
    </query>
</search>
```

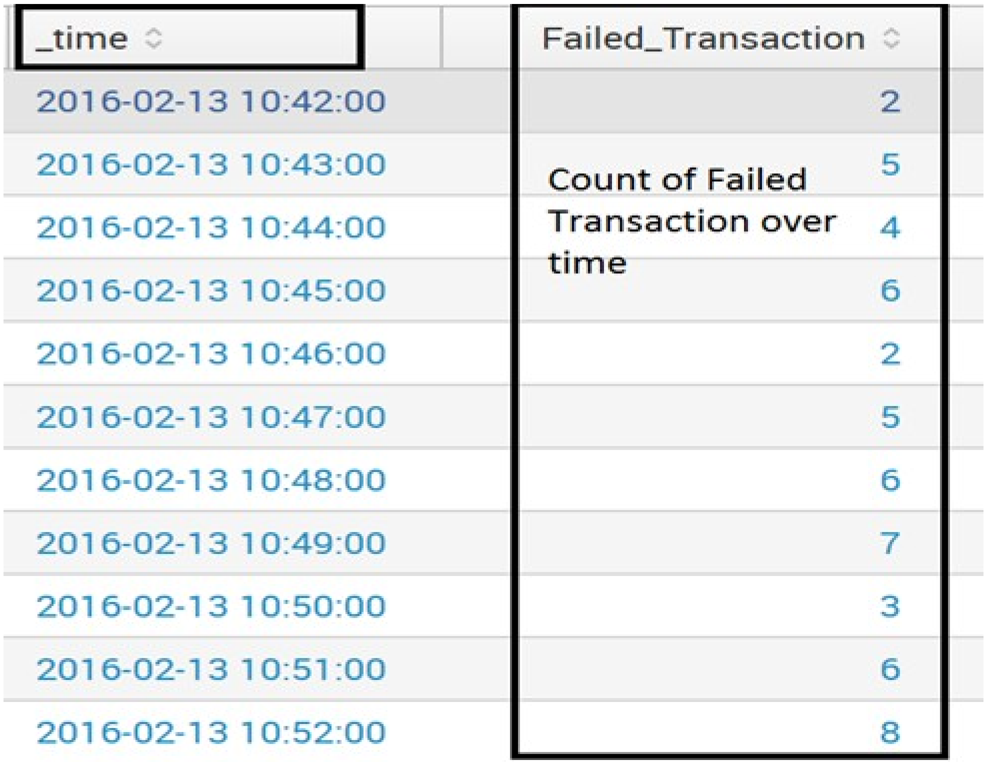


```
<html>
    <div id="punchcard"
         class="splunk-view"
         data-require="app/search/components/punchcard/punchcard"
         data-options='{
            "managerid": "search_query",
            "range_values": ["Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"]
        }'>
    </div>
</html>
```

Path of JS & CSS of Punchcard Visualization

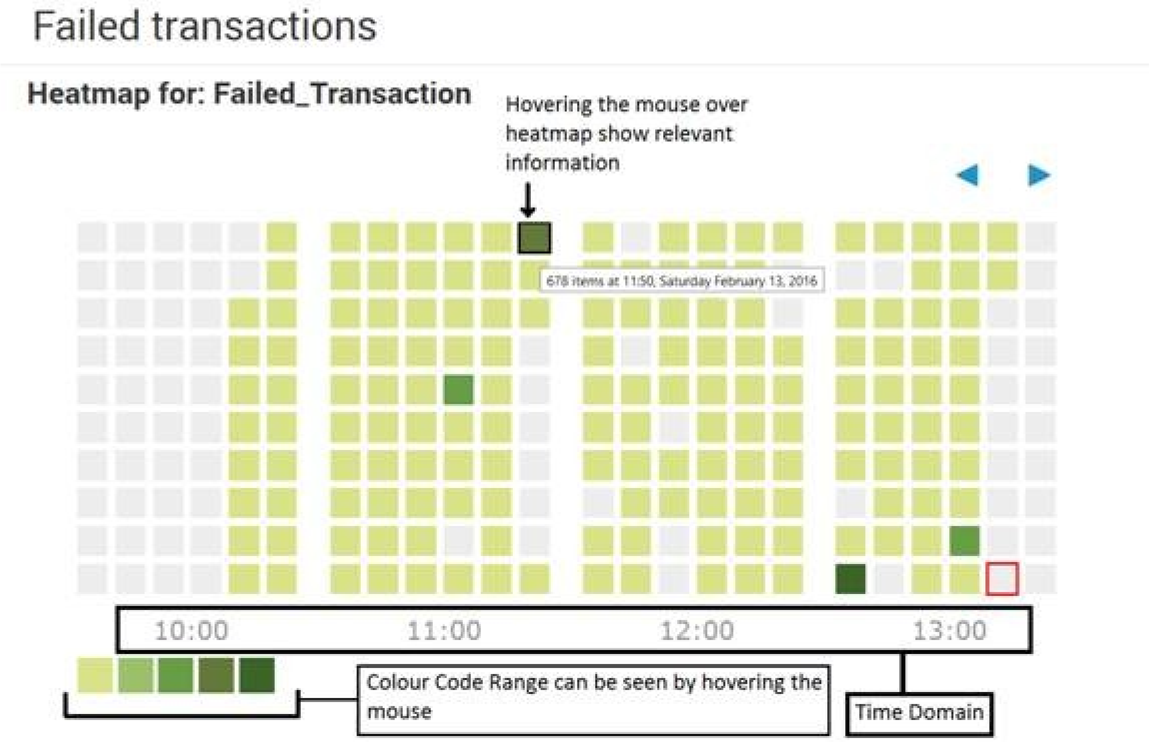
Search Id

Range Values (example - days of week, months of year, time of day, etc.)



_time	Failed_Transaction
2016-02-13 10:42:00	2
2016-02-13 10:43:00	5
2016-02-13 10:44:00	4
2016-02-13 10:45:00	6
2016-02-13 10:46:00	2
2016-02-13 10:47:00	5
2016-02-13 10:48:00	6
2016-02-13 10:49:00	7
2016-02-13 10:50:00	3
2016-02-13 10:51:00	6
2016-02-13 10:52:00	8

Count of Failed Transaction over time



Failed transactions

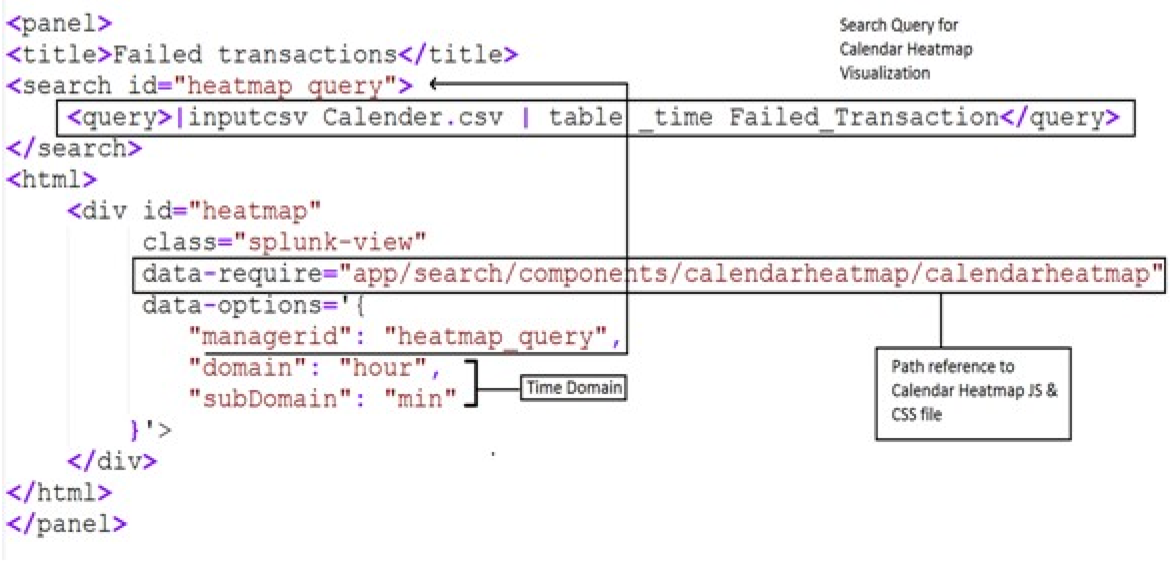
Heatmap for: Failed_Transaction

Hovering the mouse over heatmap show relevant information

678 items at 11:50, Saturday February 13, 2016

Colour Code Range can be seen by hovering the mouse

Time Domain

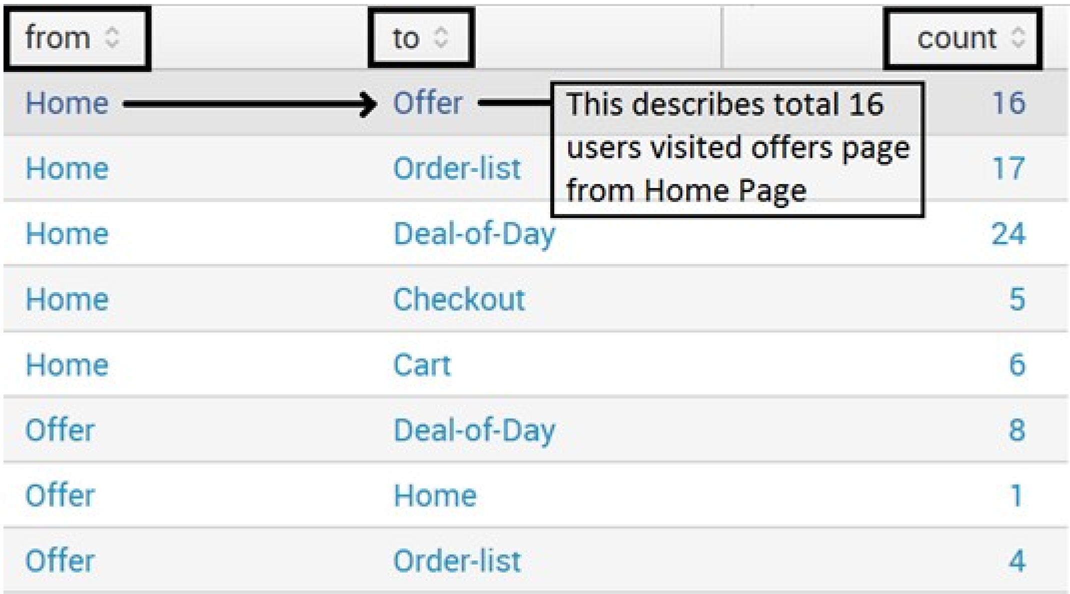


```
<panel>
<title>Failed transactions</title>
<search id="heatmap_query">
    <query>|inputcsv Calender.csv | table _time Failed_Transaction</query>
</search>
<html>
    <div id="heatmap"
         class="splunk-view"
         data-require="app/search/components/calendarheatmap/calendarheatmap"
         data-options='{
            "managerid": "heatmap_query",
            "domain": "hour",
            "subDomain": "min"
        }'>
    </div>
</html>
</panel>
```

Search Query for Calendar Heatmap Visualization

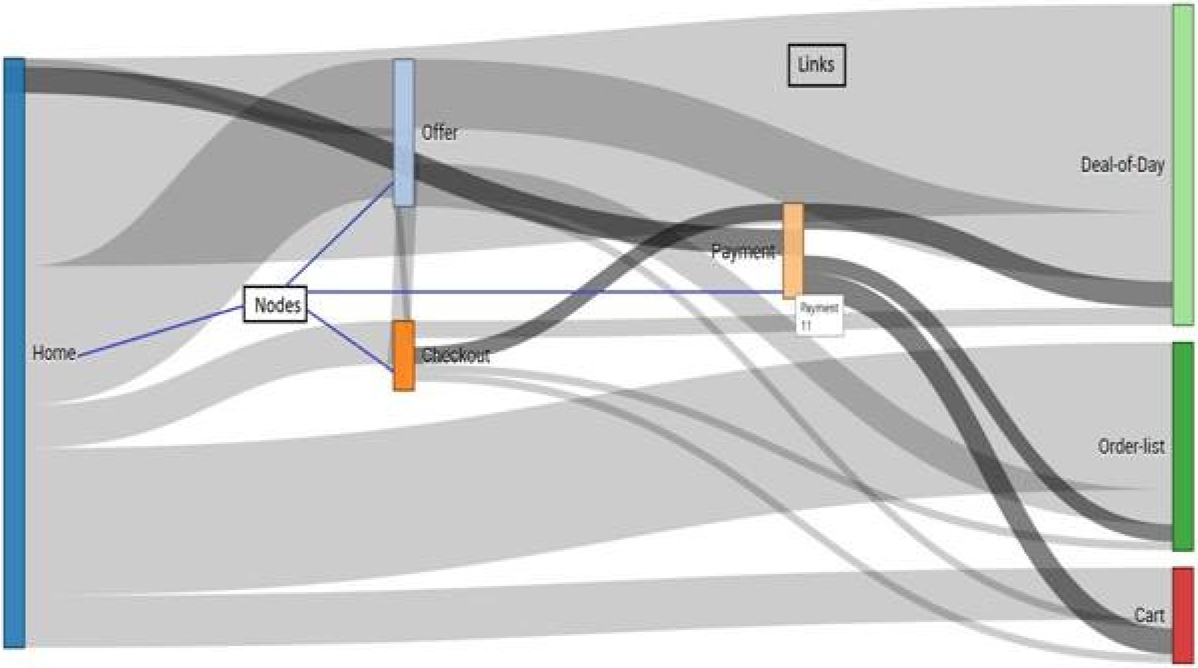
Time Domain

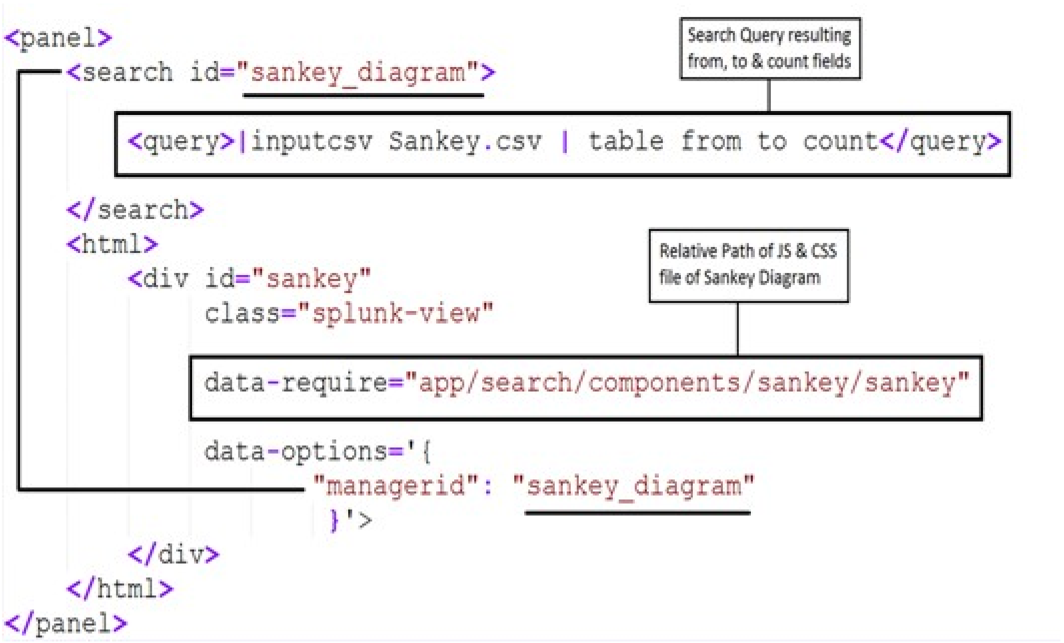
Path reference to Calendar Heatmap JS & CSS file



from	to	count
Home	Offer	16
Home	Order-list	17
Home	Deal-of-Day	24
Home	Checkout	5
Home	Cart	6
Offer	Deal-of-Day	8
Offer	Home	1
Offer	Order-list	4

This describes total 16 users visited offers page from Home Page

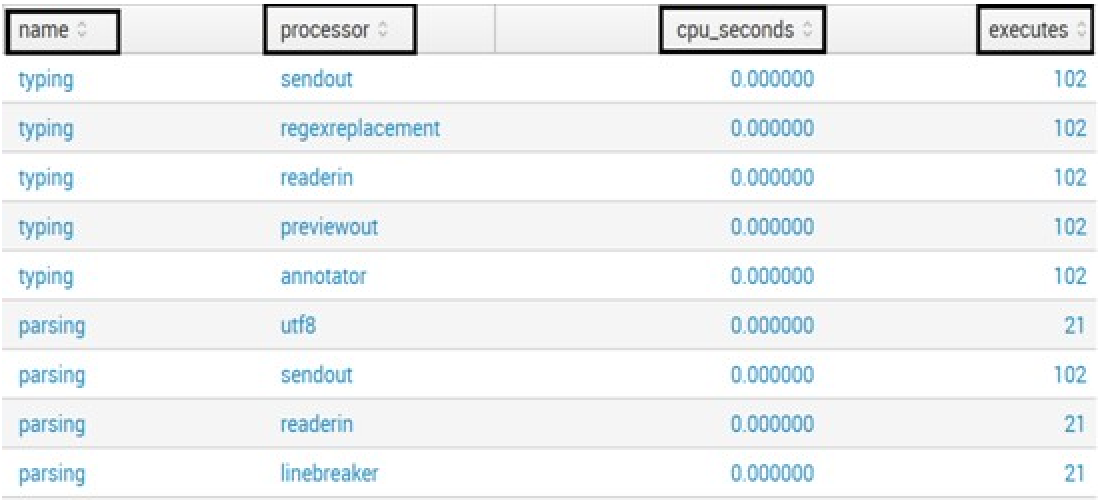




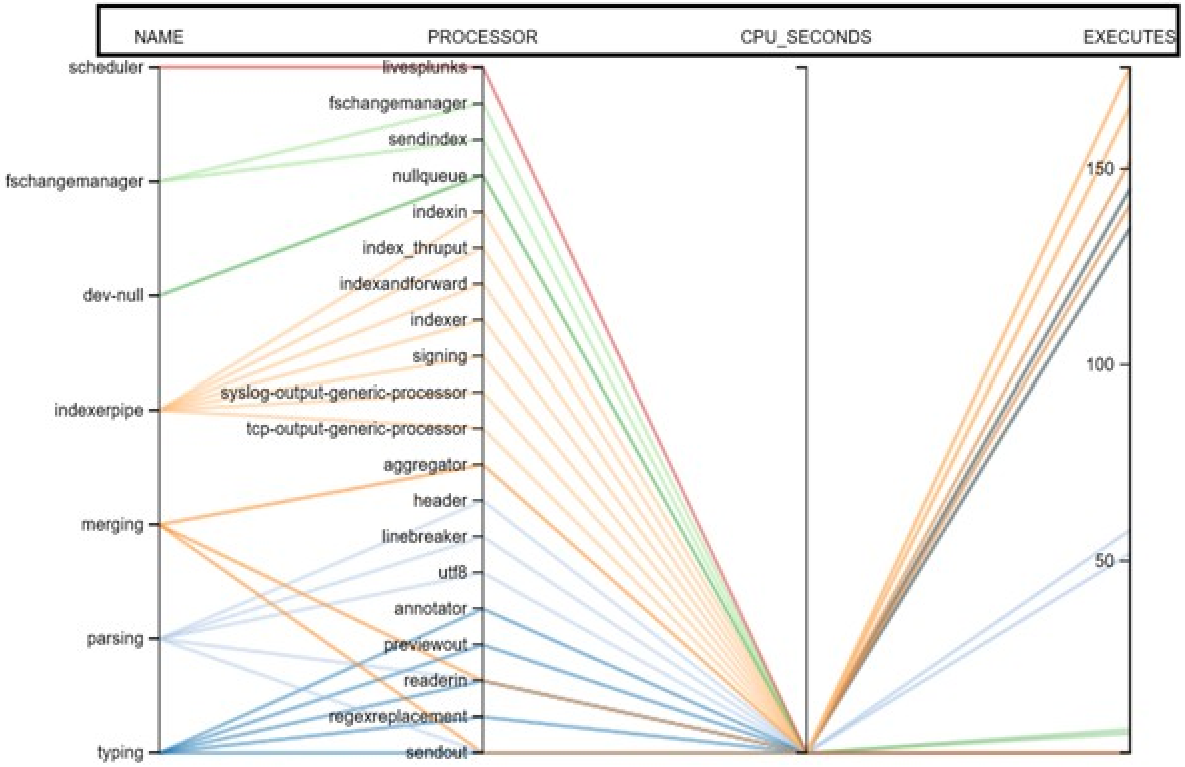
Search Query resulting from, to & count fields

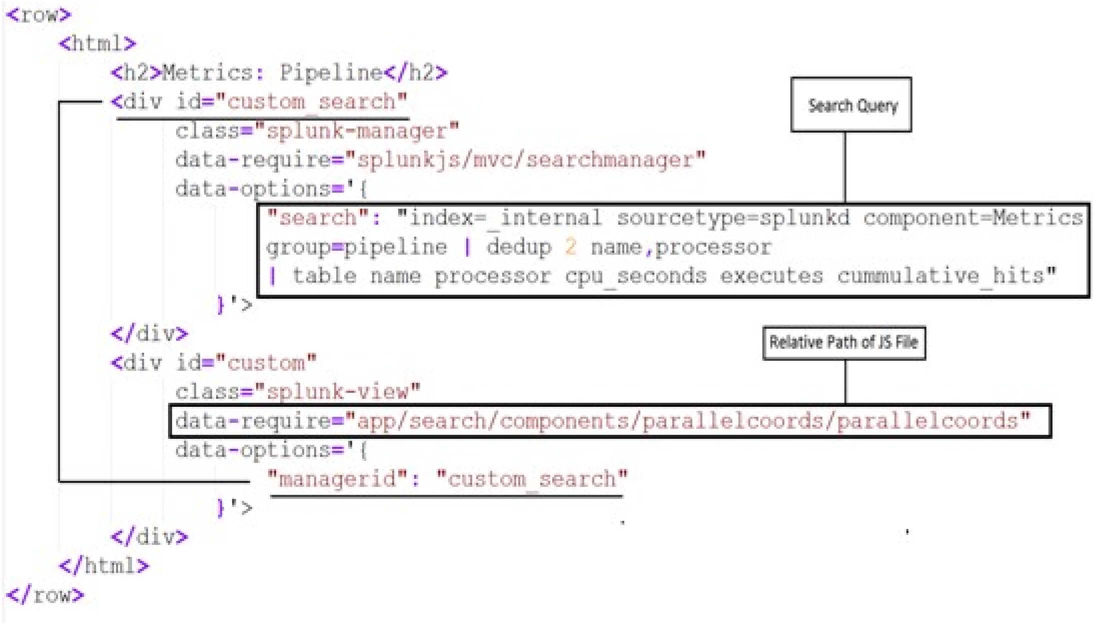
Relative Path of JS & CSS file of Sankey Diagram

```
<panel>
    <search id="sankey_diagram">

        <query>|inputcsv Sankey.csv | table from to count</query>

    </search>
    <html>
        <div id="sankey"
             class="splunk-view"

             data-require="app/search/components/sankey/sankey"

             data-options='{
                 "managerid": "sankey_diagram"
                  }'>
        </div>
    </html>
</panel>
```

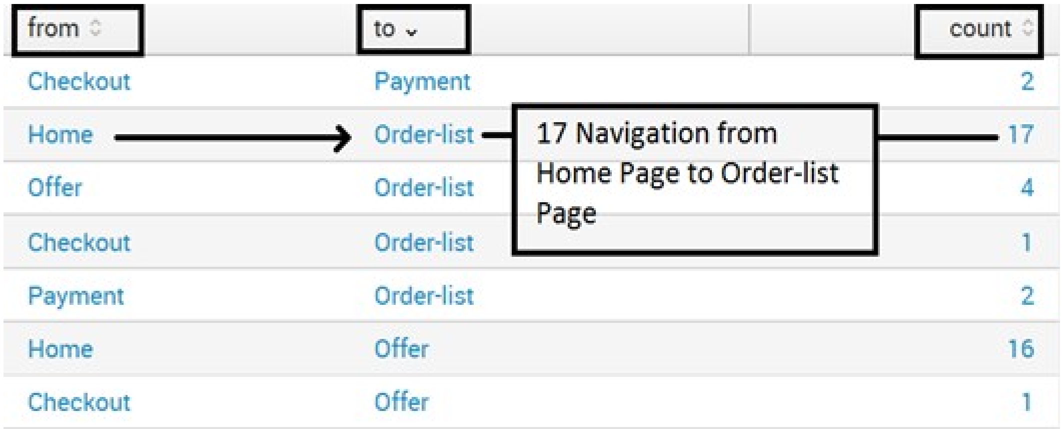


name	processor	cpu_seconds	executes
typing	sendout	0.000000	102
typing	regexreplacement	0.000000	102
typing	readerin	0.000000	102
typing	previewout	0.000000	102
typing	annotator	0.000000	102
parsing	utf8	0.000000	21
parsing	sendout	0.000000	102
parsing	readerin	0.000000	21
parsing	linebreaker	0.000000	21



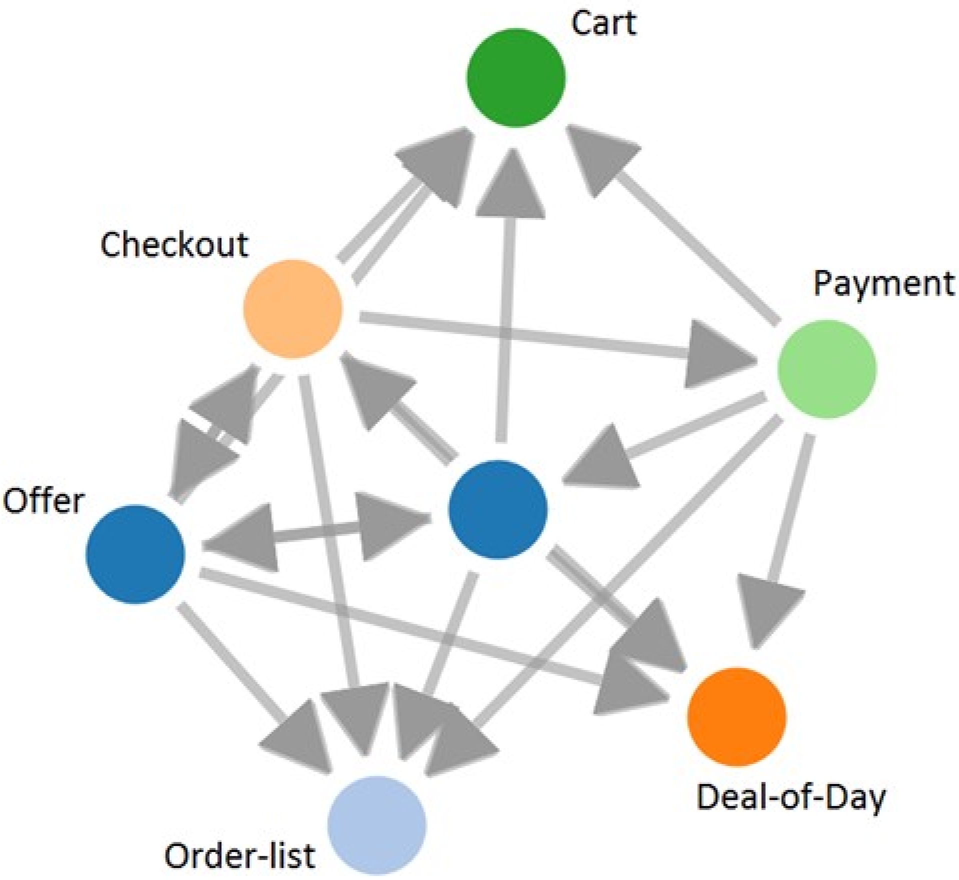


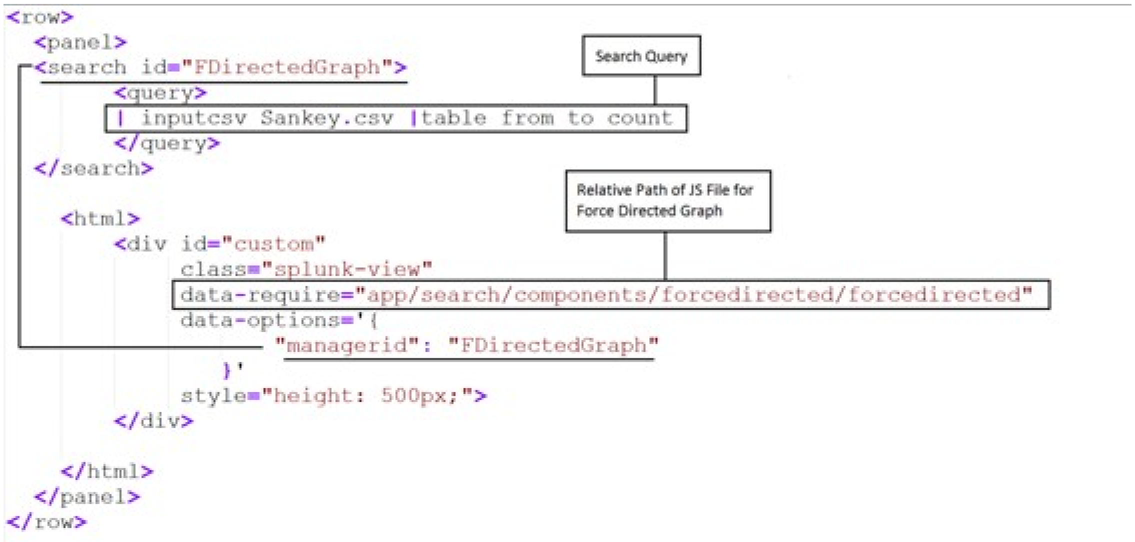
```
<row>
    <html>
        <h2>Metrics: Pipeline</h2>
        <div id="custom_search"
            class="splunk-manager"
            data-require="splunkjs/mvc/searchmanager"
            data-options='{
                "search": "index=_internal sourcetype=splunkd component=Metrics
                group=pipeline | dedup 2 name,processor
                | table name processor cpu_seconds executes cummulative_hits"
            }'>
        </div>
        <div id="custom"
            class="splunk-view"
            data-require="app/search/components/parallelcoords/parallelcoords"
            data-options='{
                "managerid": "custom_search"
            }'>
        </div>
    </html>
</row>
```



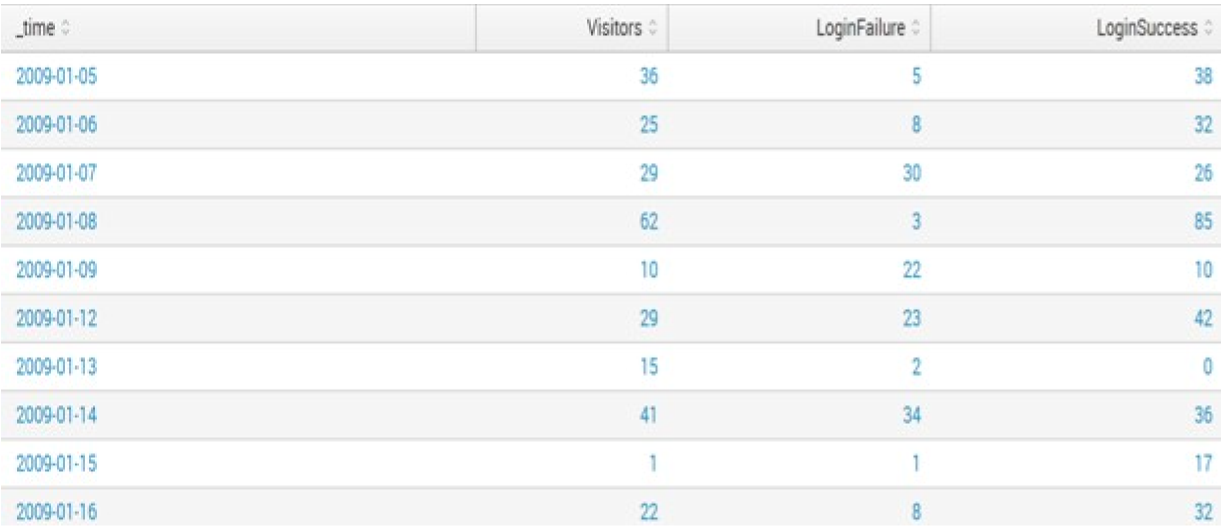
from	to	count
Checkout	Payment	2
Home	Order-list	17
Offer	Order-list	4
Checkout	Order-list	1
Payment	Order-list	2
Home	Offer	16
Checkout	Offer	1

17 Navigation from Home Page to Order-list Page

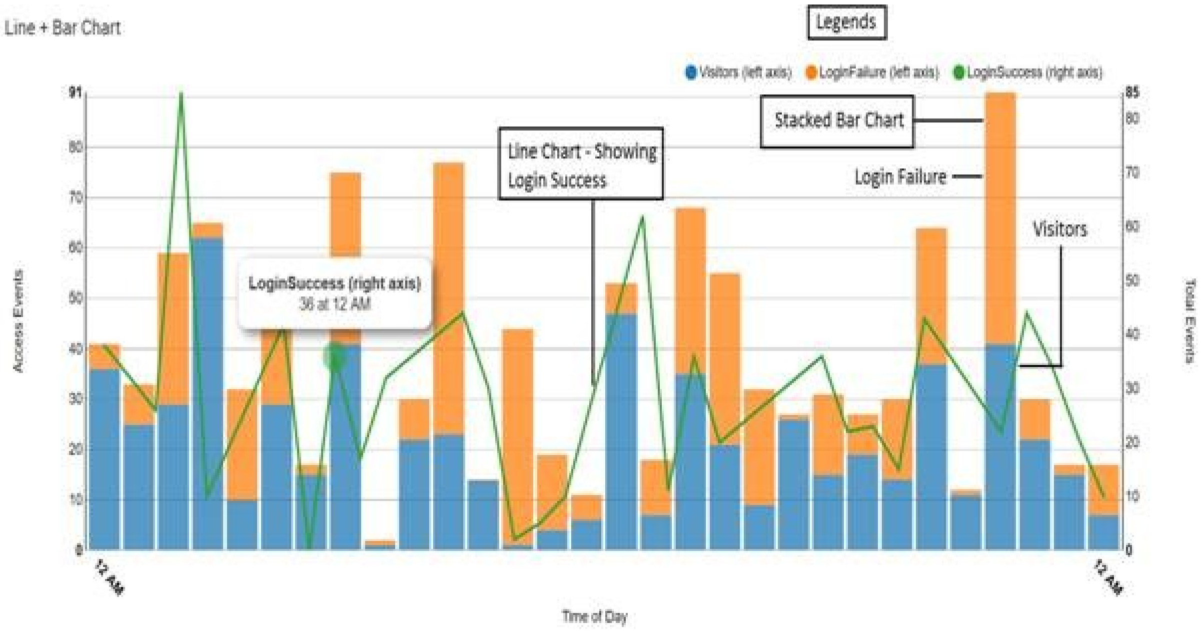


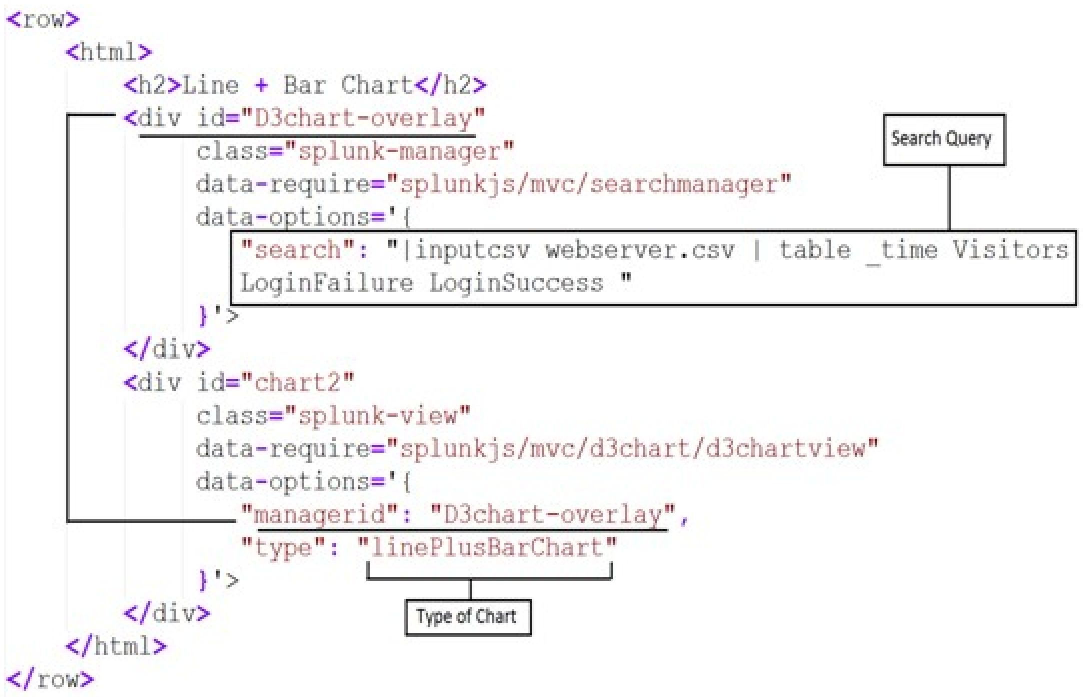


```
<row>
  <panel>
  <search id="FDirectedGraph">
        <query>
        | inputcsv Sankey.csv |table from to count
        </query>
  </search>

    <html>
        <div id="custom"
             class="splunk-view"
             data-require="app/search/components/forcedirected/forcedirected"
             data-options='{
                    "managerid": "FDirectedGraph"
                }'
             style="height: 500px;">
        </div>

    </html>
  </panel>
</row>
```

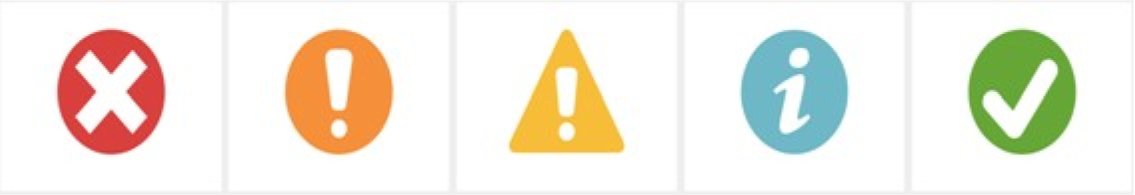


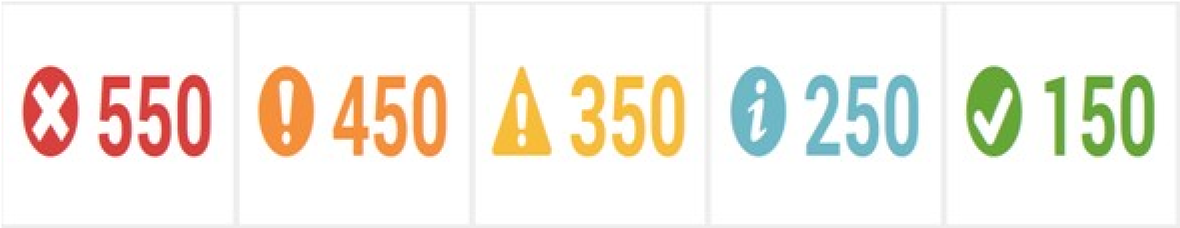
_time	Visitors	LoginFailure	LoginSuccess
2009-01-05	36	5	38
2009-01-06	25	8	32
2009-01-07	29	30	26
2009-01-08	62	3	85
2009-01-09	10	22	10
2009-01-12	29	23	42
2009-01-13	15	2	0
2009-01-14	41	34	36
2009-01-15	1	1	17
2009-01-16	22	8	32

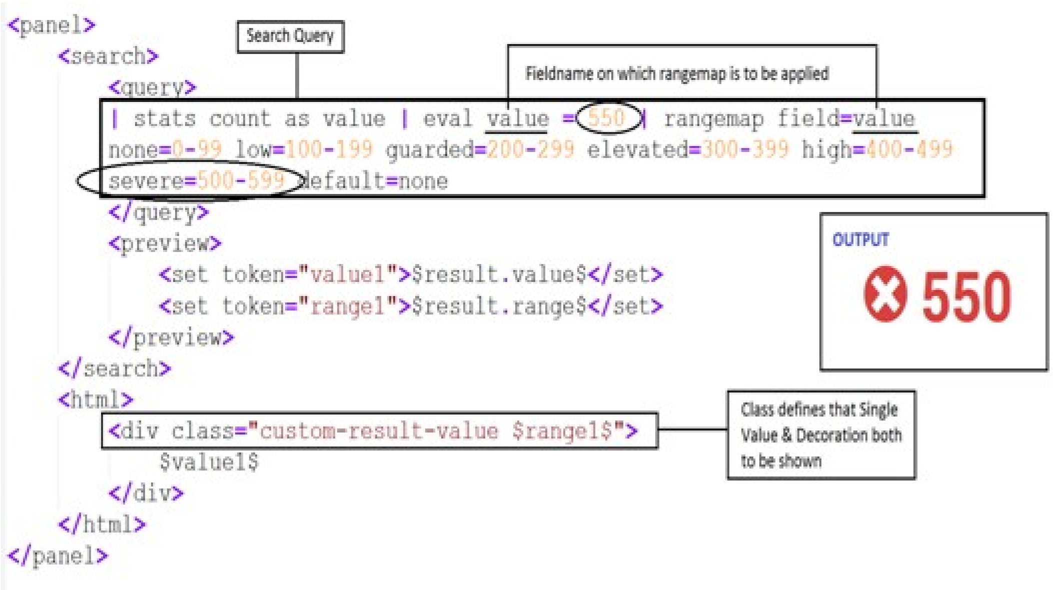




```
<row>
    <html>
        <h2>Line + Bar Chart</h2>
        <div id="D3chart-overlay"
             class="splunk-manager"
             data-require="splunkjs/mvc/searchmanager"
             data-options='{
                "search": "|inputcsv webserver.csv | table _time Visitors
                LoginFailure LoginSuccess "
             }'>
        </div>
        <div id="chart2"
             class="splunk-view"
             data-require="splunkjs/mvc/d3chart/d3chartview"
             data-options='{
                "managerid": "D3chart-overlay",
                "type": "linePlusBarChart"
             }'>
        </div>
    </html>
</row>
```







```
<panel>
    <search>
        <query>
        | stats count as value | eval value = 550 | rangemap field=value
        none=0-99 low=100-199 guarded=200-299 elevated=300-399 high=400-499
        severe=500-599 default=none
        </query>
        <preview>
            <set token="value1">$result.value$</set>
            <set token="range1">$result.range$</set>
        </preview>
    </search>
    <html>
        <div class="custom-result-value $range1$">
            $value1$
        </div>
    </html>
</panel>
```

Search Query

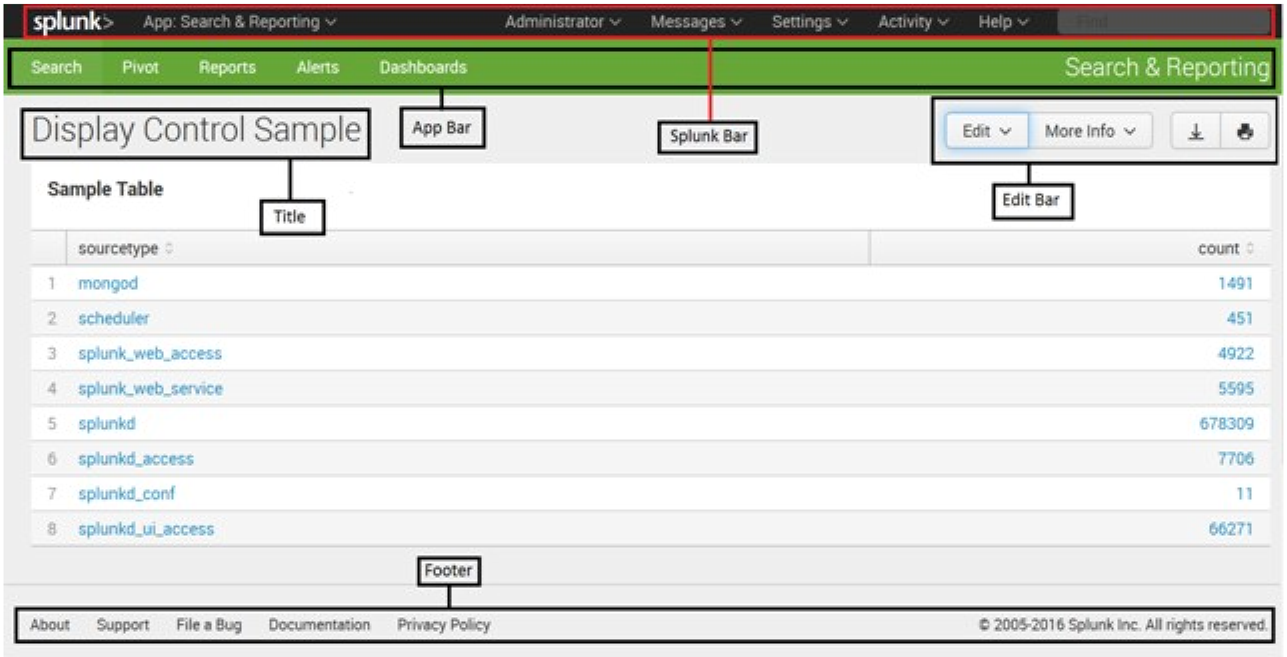
Fieldname on which rangemap is to be applied

OUTPUT

550

Class defines that Single Value & Decoration both to be shown

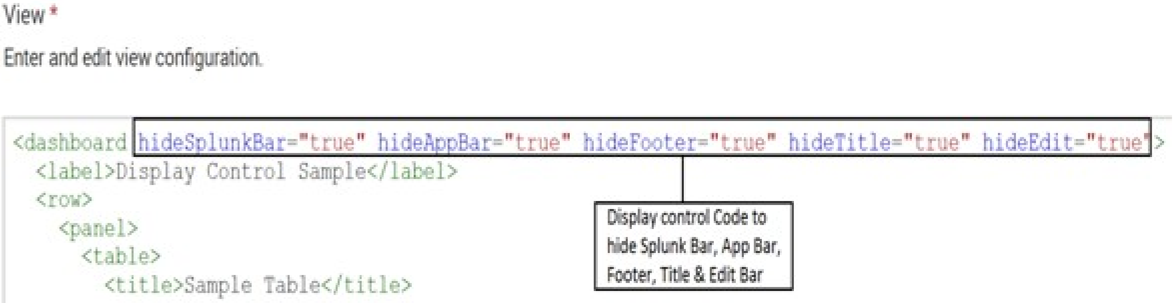
Chapter 8: Dashboard Customization



Display Control Sample

Sample Table

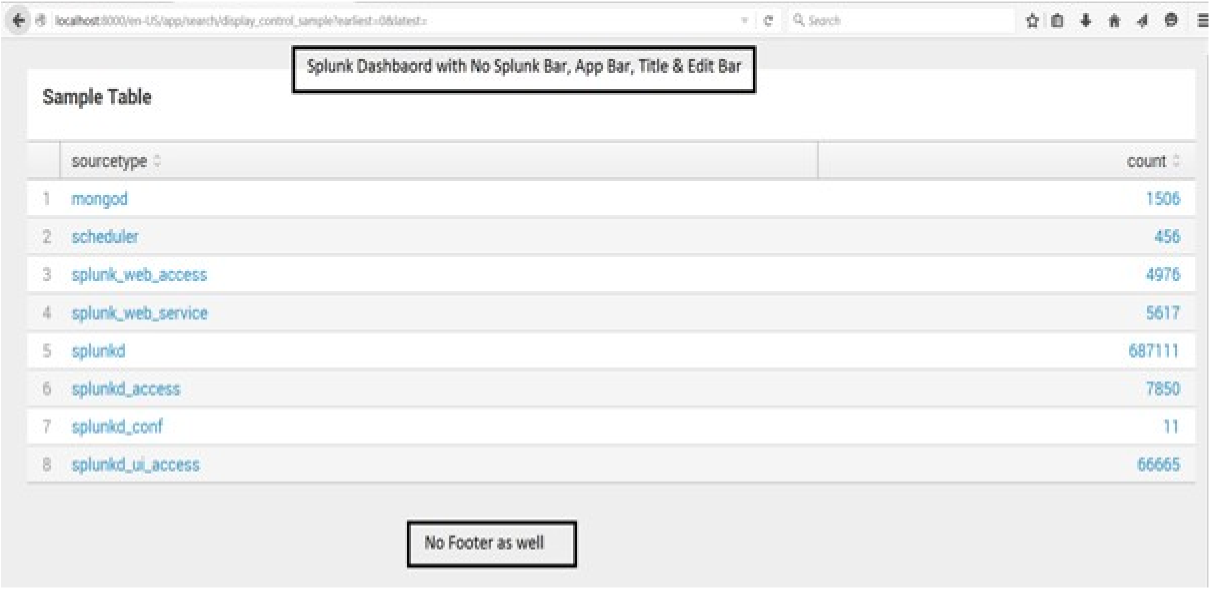
	sourcetype	count
1	mongod	1491
2	scheduler	451
3	splunk_web_access	4922
4	splunk_web_service	5595
5	splunkd	678309
6	splunkd_access	7706
7	splunkd_conf	11
8	splunkd_ui_access	66271


Display control Code to hide Splunk Bar, App Bar, Footer, Title & Edit Bar

View *

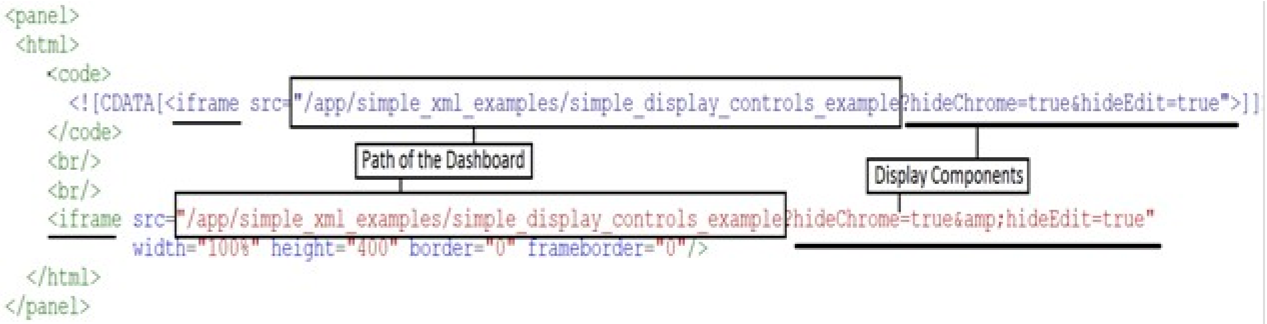
Enter and edit view configuration.

```
<dashboard hideSplunkBar="true" hideAppBar="true" hideFooter="true" hideTitle="true" hideEdit="true">
  <label>Display Control Sample</label>
  <row>
    <panel>
      <table>
        <title>Sample Table</title>
```

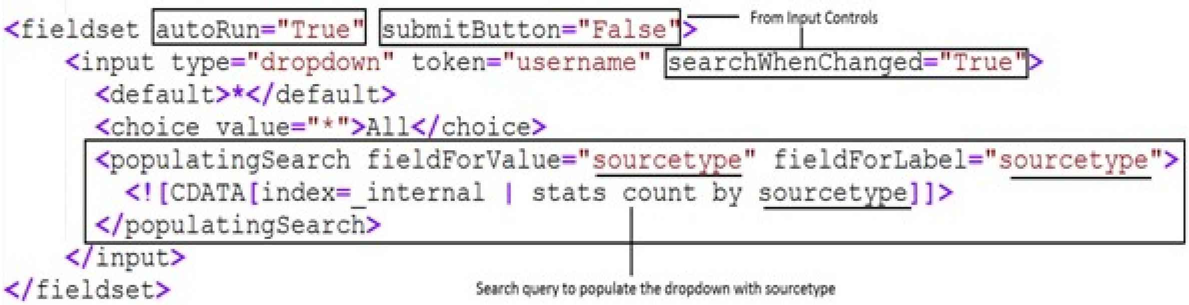

localhost:8000/en-US/app/search/display_control_sample?earliest=0&latest=
Search
Splunk Dashbaord with No Splunk Bar, App Bar, Title & Edit Bar
No Footer as well

Sample Table

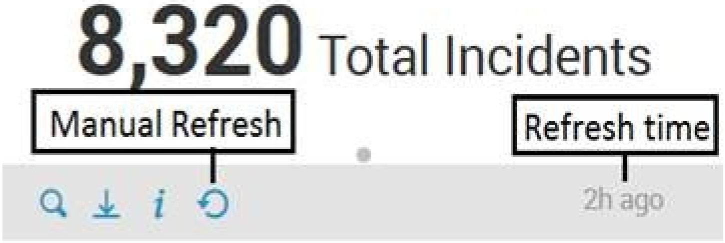
	sourcetype	count
1	mongod	1506
2	scheduler	456
3	splunk_web_access	4976
4	splunk_web_service	5617
5	splunkd	687111
6	splunkd_access	7850
7	splunkd_conf	11
8	splunkd_ui_access	66665

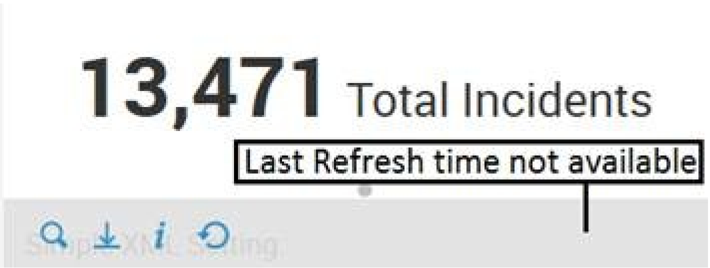


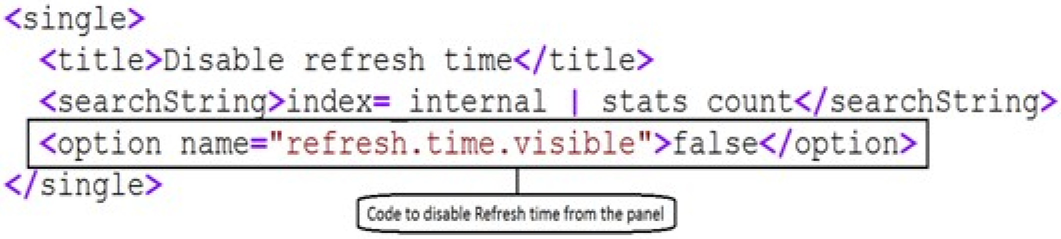
```
<panel>
 <html>
   <code>
     <![CDATA[<iframe src="/app/simple_xml_examples/simple_display_controls_example?hideChrome=true&hideEdit=true">]]
   </code>
   <br/>
   <br/>
   <iframe src="/app/simple_xml_examples/simple_display_controls_example?hideChrome=true&amp;hideEdit=true"
        width="100%" height="400" border="0" frameborder="0"/>
  </html>
</panel>
```



```
<fieldset autoRun="True" submitButton="False">
    <input type="dropdown" token="username" searchWhenChanged="True">
      <default>*</default>
      <choice value="*">All</choice>
      <populatingSearch fieldForValue="sourcetype" fieldForLabel="sourcetype">
        <![CDATA[index=_internal | stats count by sourcetype]]>
      </populatingSearch>
    </input>
</fieldset>
```

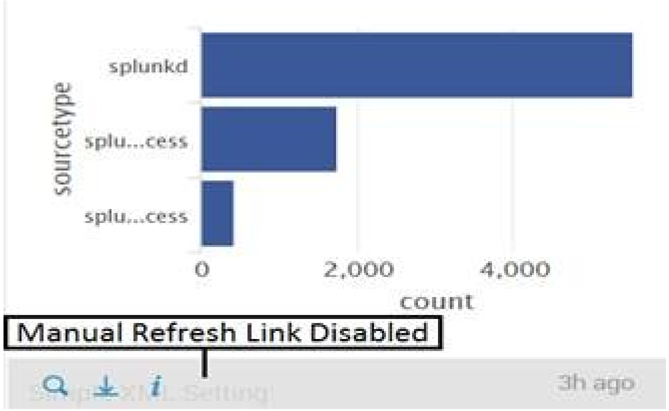


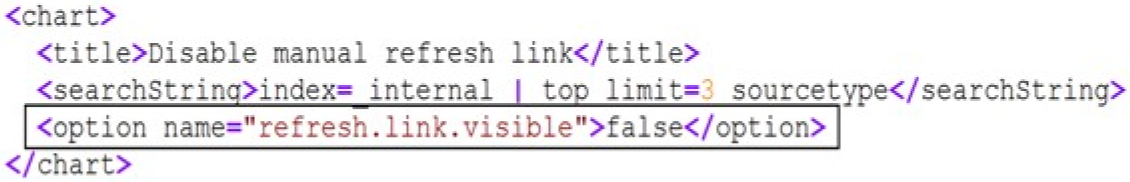




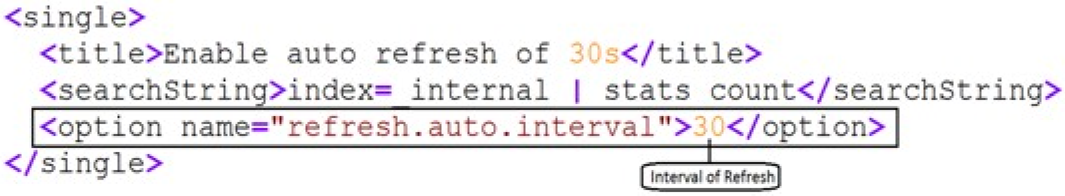
```
<single>
  <title>Disable refresh time</title>
  <searchString>index=_internal | stats count</searchString>
  <option name="refresh.time.visible">false</option>
</single>
```

Code to disable Refresh time from the panel



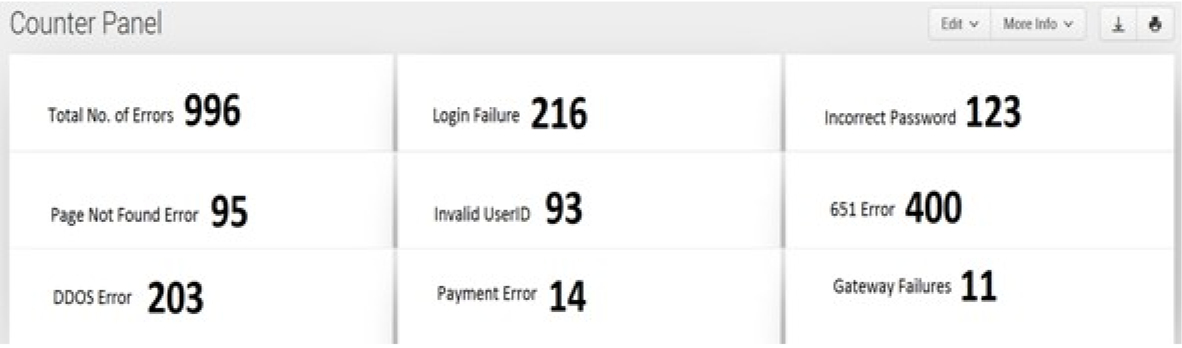


```
<chart>
  <title>Disable manual refresh link</title>
  <searchString>index=_internal | top limit=3 sourcetype</searchString>
  <option name="refresh.link.visible">false</option>
</chart>
```



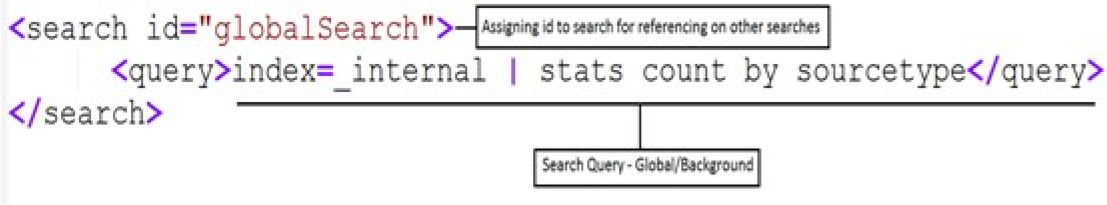
```
<single>
  <title>Enable auto refresh of 30s</title>
  <searchString>index=_internal | stats count</searchString>
  <option name="refresh.auto.interval">30</option>
</single>
```

Interval of Refresh



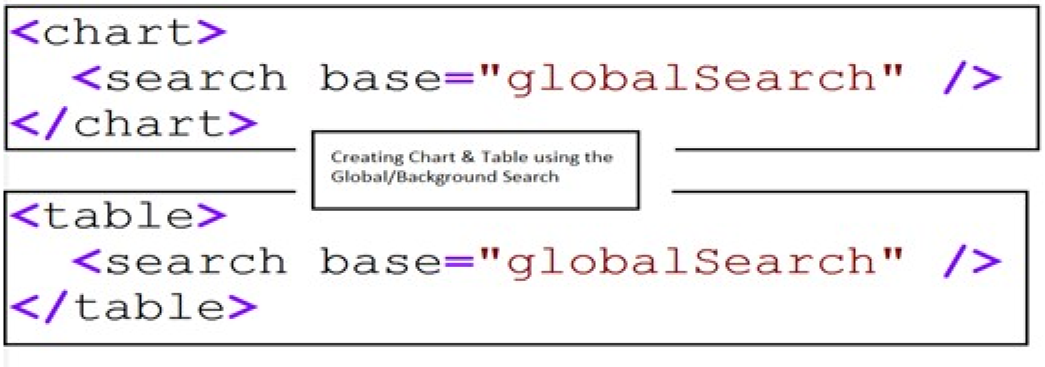
Counter Panel

Total No. of Errors 996	Login Failure 216	Incorrect Password 123
Page Not Found Error 95	Invalid UserID 93	651 Error 400
DDOS Error 203	Payment Error 14	Gateway Failures 11

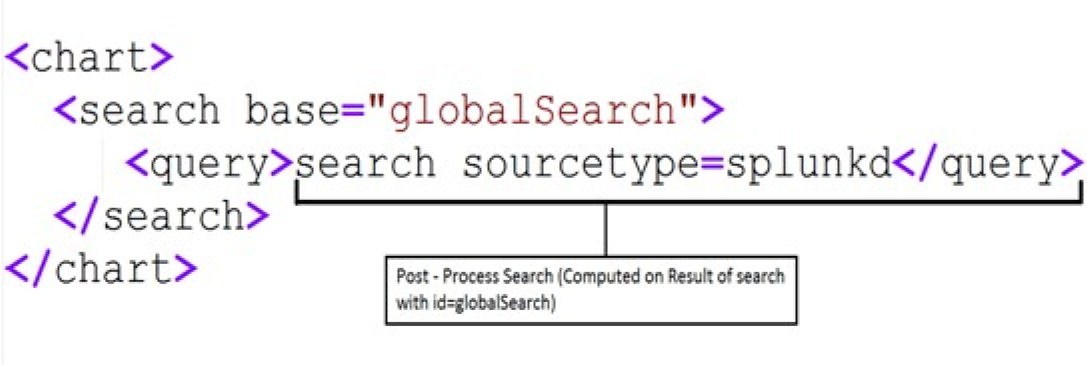


```
<search id="globalSearch">
    <query>index=_internal | stats count by sourcetype</query>
</search>
```

Assigning id to search for referencing on other searches
Search Query - Global/Background

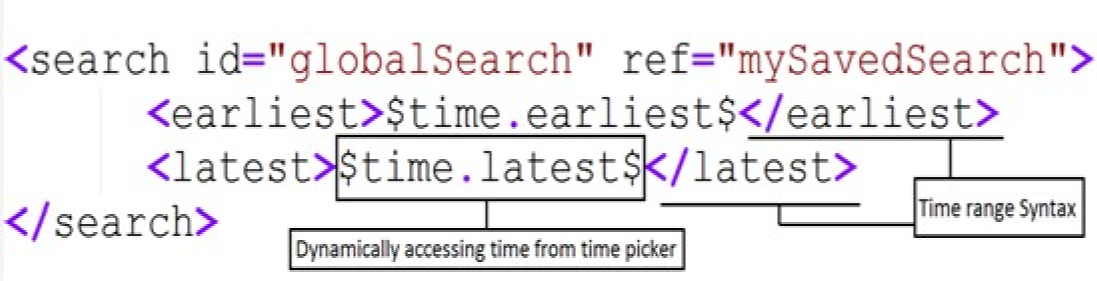


```
<chart>
  <search base="globalSearch" />
</chart>
<table>
  <search base="globalSearch" />
</table>
```

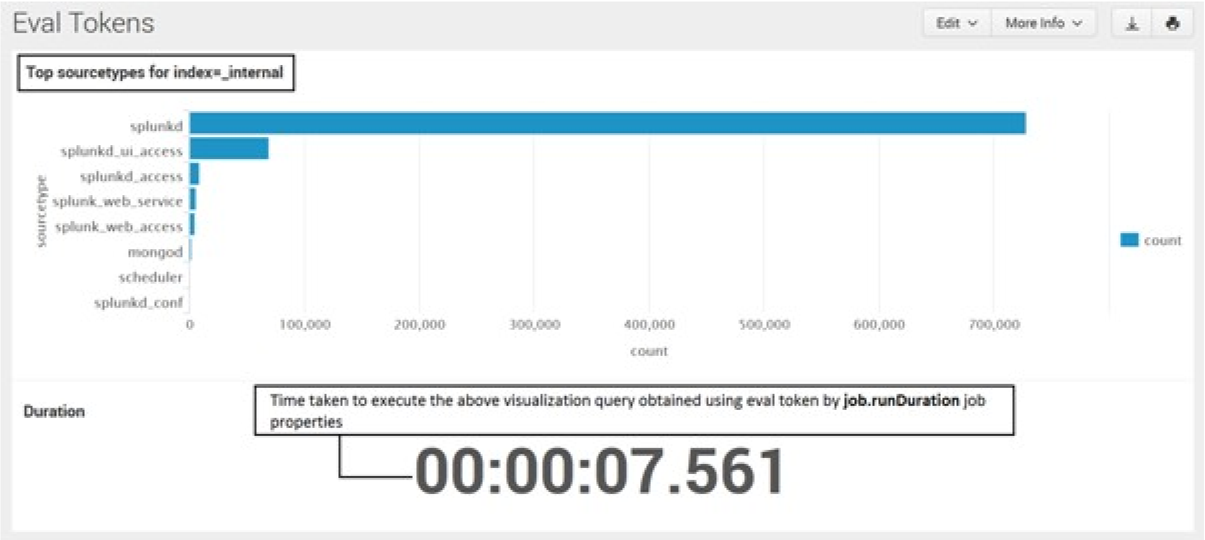


```
<chart>
  <search base="globalSearch">
    <query>search sourcetype=splunkd</query>
  </search>
</chart>
```

Post - Process Search (Computed on Result of search with id=globalSearch)



```
<search id="globalSearch" ref="mySavedSearch">
      <earliest>$time.earliest$</earliest>
      <latest>$time.latest$</latest>
</search>
```



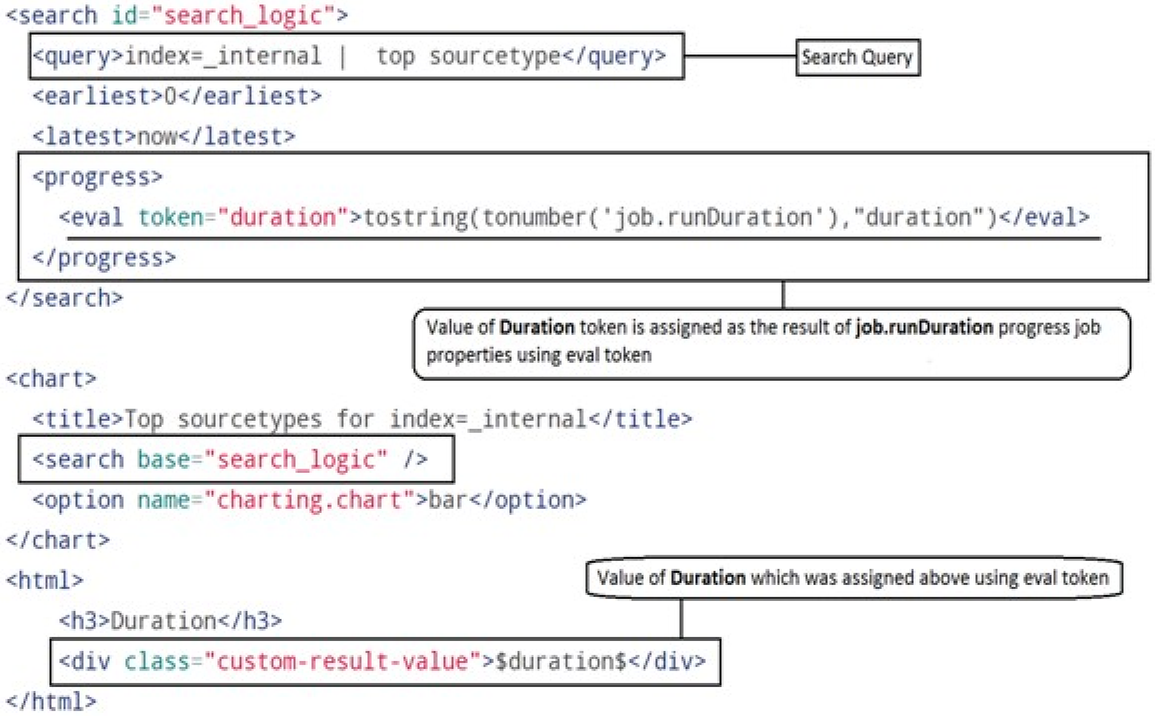
Eval Tokens

Top sourcetypes for index=_internal

Duration

Time taken to execute the above visualization query obtained using eval token by **job.runDuration** job properties

00:00:07.561

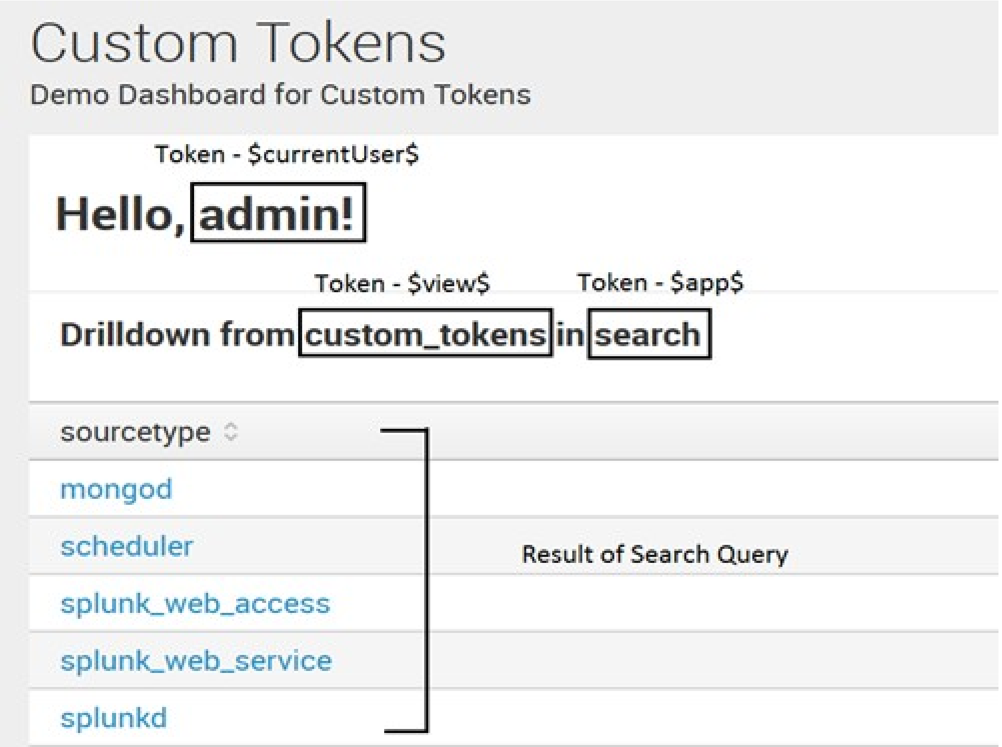


```
<search id="search_logic">
  <query>index=_internal |  top sourcetype</query>
  <earliest>0</earliest>
  <latest>now</latest>
  <progress>
    <eval token="duration">tostring(tonumber('job.runDuration'),"duration")</eval>
  </progress>
</search>

<chart>
  <title>Top sourcetypes for index=_internal</title>
  <search base="search_logic" />
  <option name="charting.chart">bar</option>
</chart>
<html>
    <h3>Duration</h3>
    <div class="custom-result-value">$duration$</div>
</html>
```

Search Query

Value of **Duration** token is assigned as the result of **job.runDuration** progress job properties using eval token

Value of **Duration** which was assigned above using eval token



Custom Tokens

Demo Dashboard for Custom Tokens

Token - $currentUser$

Hello, admin!

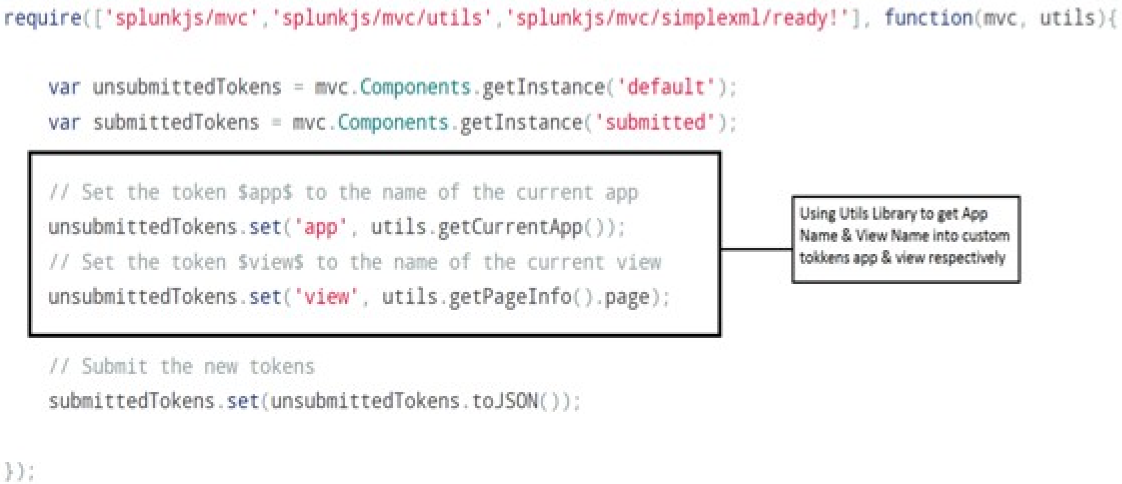
Token - $view$

Token - app

Drilldown from custom_tokens in search

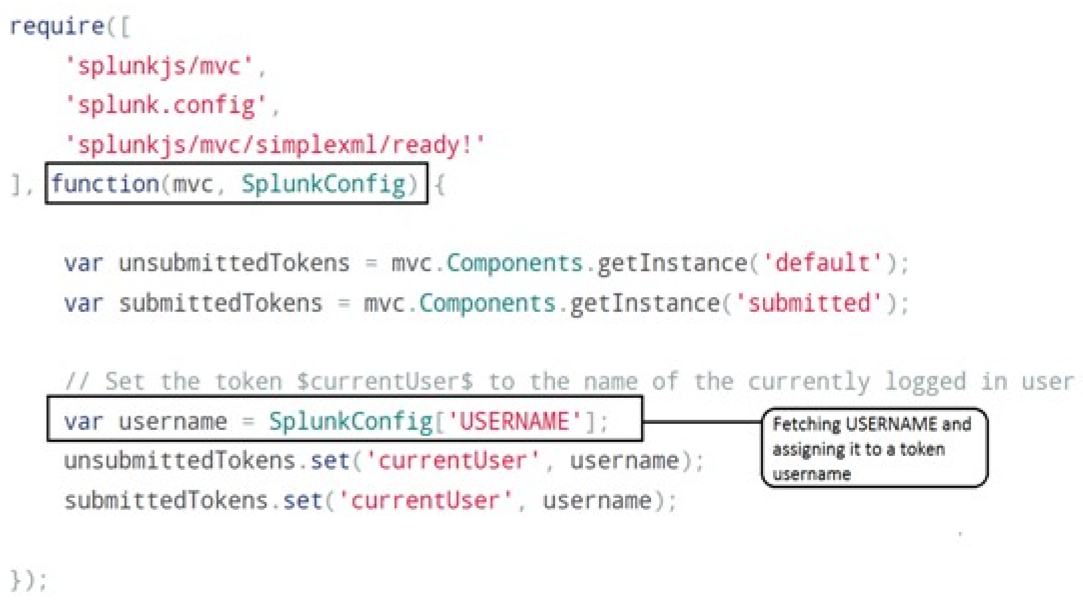
sourcetype
mongod
scheduler
splunk_web_access
splunk_web_service
splunkd

Result of Search Query



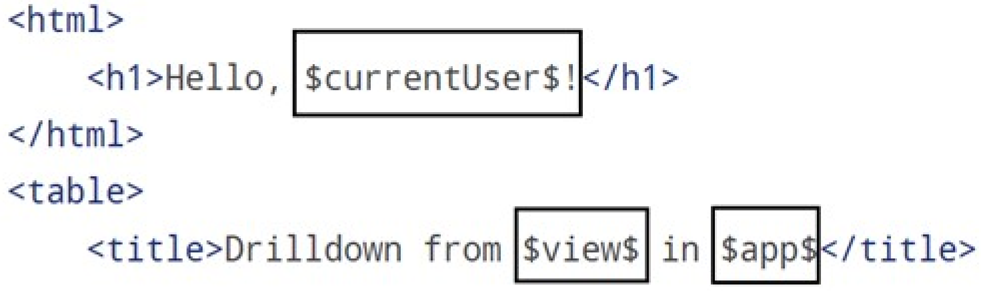
```
require(['splunkjs/mvc','splunkjs/mvc/utils','splunkjs/mvc/simplexml/ready!'], function(mvc, utils){

    var unsubmittedTokens = mvc.Components.getInstance('default');
    var submittedTokens = mvc.Components.getInstance('submitted');

    // Set the token $app$ to the name of the current app
    unsubmittedTokens.set('app', utils.getCurrentApp());
    // Set the token $view$ to the name of the current view
    unsubmittedTokens.set('view', utils.getPageInfo().page);

    // Submit the new tokens
    submittedTokens.set(unsubmittedTokens.toJSON());

});
```

Using Utils Library to get App Name & View Name into custom tokkens app & view respectively

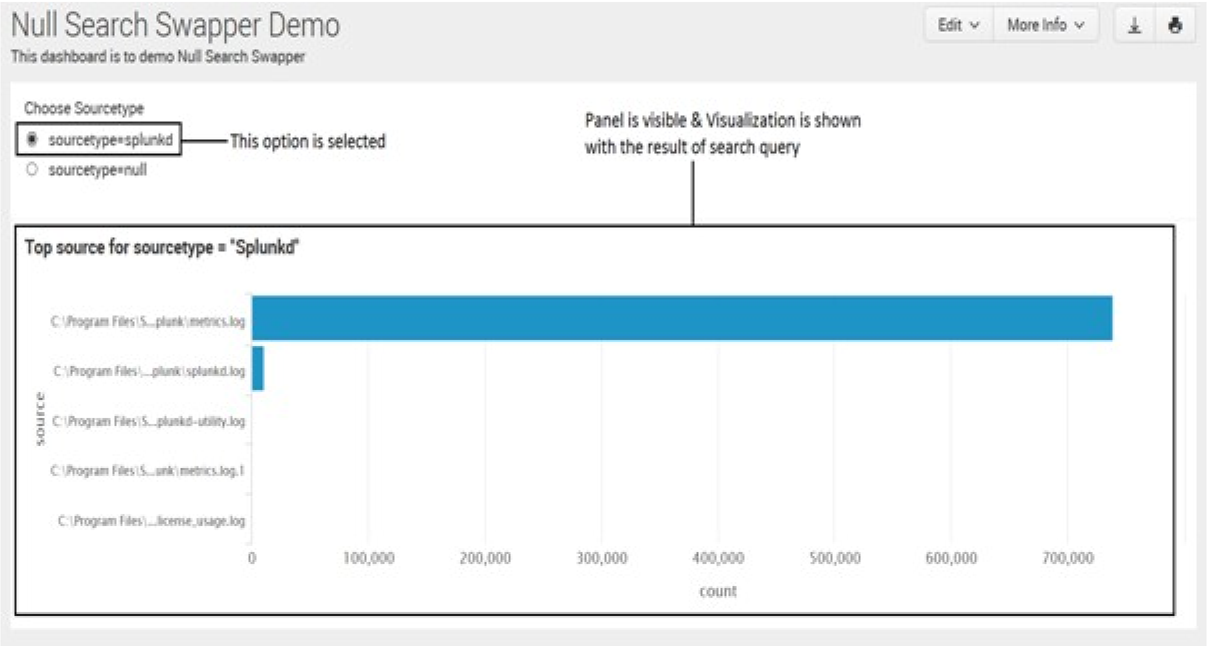


```
require([
    'splunkjs/mvc',
    'splunk.config',
    'splunkjs/mvc/simplexml/ready!'
], function(mvc, SplunkConfig) {

    var unsubmittedTokens = mvc.Components.getInstance('default');
    var submittedTokens = mvc.Components.getInstance('submitted');

    // Set the token $currentUser$ to the name of the currently logged in user
    var username = SplunkConfig['USERNAME'];
    unsubmittedTokens.set('currentUser', username);
    submittedTokens.set('currentUser', username);

});
```

Fetching USERNAME and assigning it to a token username



```
<html>
    <h1>Hello, $currentUser$!</h1>
</html>
<table>
    <title>Drilldown from $view$ in $app$</title>
```



Null Search Swapper Demo

This dashboard is to demo Null Search Swapper

Choose Sourcetype

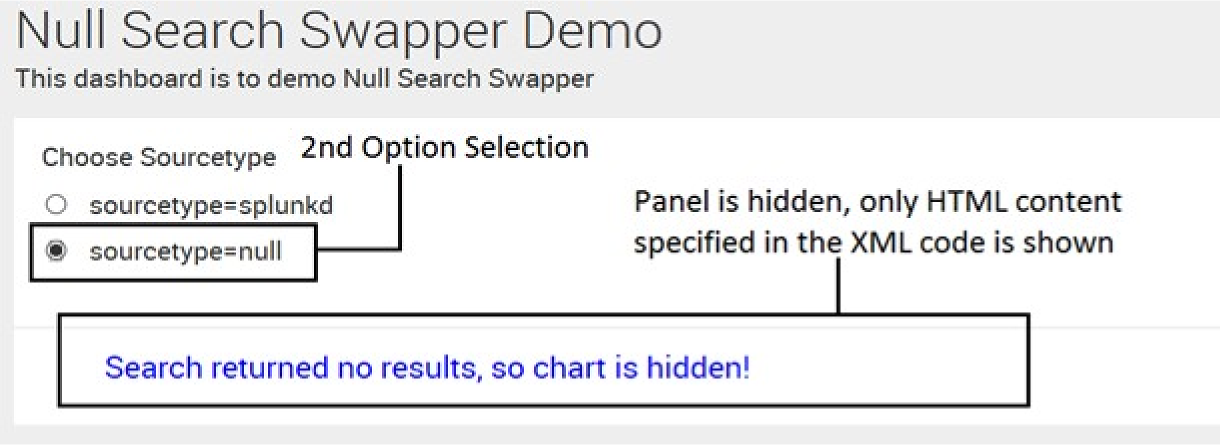
● sourcetype=splunkd

○ sourcetype=null

This option is selected

Panel is visible & Visualization is shown with the result of search query

Edit
More Info
Top source for sourcetype = "Splunkd"
source
C:\Program Files\S...plunk\metrics.log
C:\Program Files\...plunk\splunkd.log
C:\Program Files\S...plunkd-utility.log
C:\Program Files\S...unk\metrics.log.1
C:\Program Files\...license_usage.log
0
100,000
200,000
300,000
400,000
500,000
600,000
700,000
count



Null Search Swapper Demo

This dashboard is to demo Null Search Swapper

Choose Sourcetype

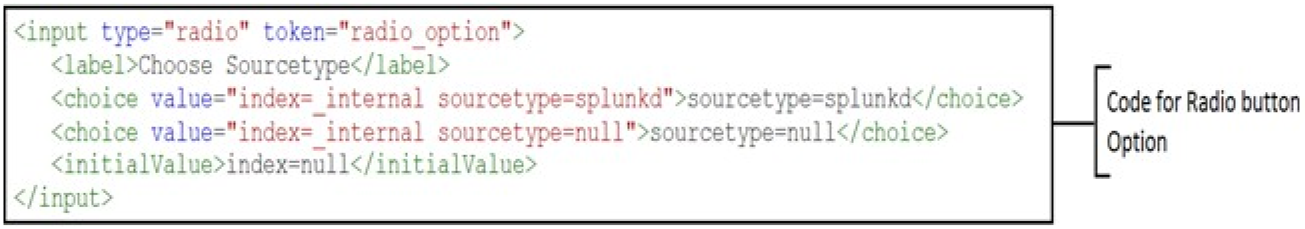
○ sourcetype=splunkd

● sourcetype=null

Search returned no results, so chart is hidden!

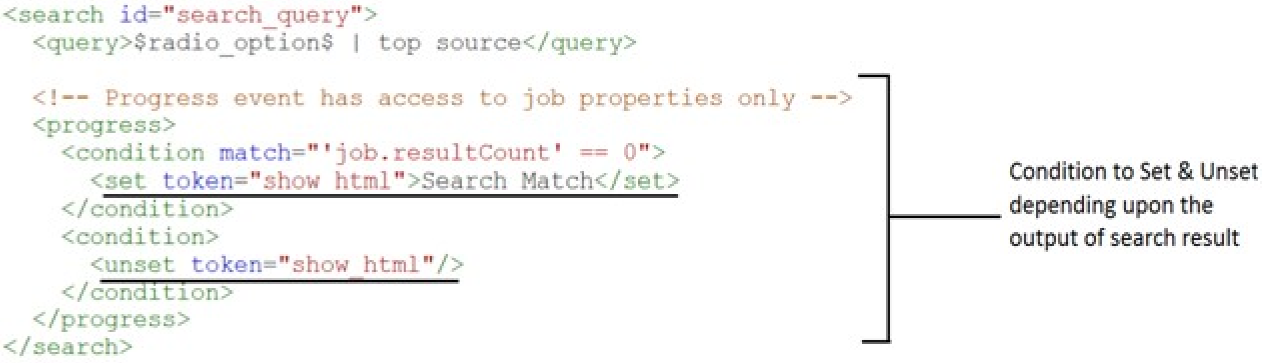
2nd Option Selection

Panel is hidden, only HTML content specified in the XML code is shown



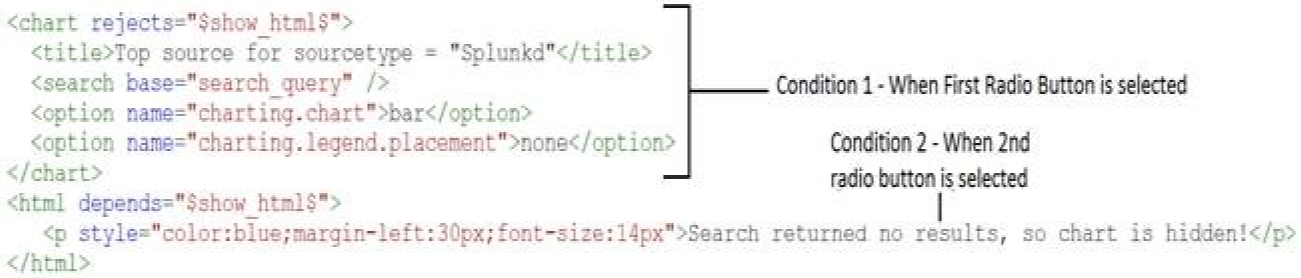
```
<input type="radio" token="radio_option">
   <label>Choose Sourcetype</label>
   <choice value="index=_internal sourcetype=splunkd">sourcetype=splunkd</choice>
   <choice value="index=_internal sourcetype=null">sourcetype=null</choice>
   <initialValue>index=null</initialValue>
</input>
```

Code for Radio button Option



```
<search id="search_query">
  <query>$radio_option$ | top source</query>

  <!-- Progress event has access to job properties only -->
  <progress>
    <condition match="'job.resultCount' == 0">
      <set token="show_html">Search Match</set>
    </condition>
    <condition>
      <unset token="show_html"/>
    </condition>
  </progress>
</search>
```

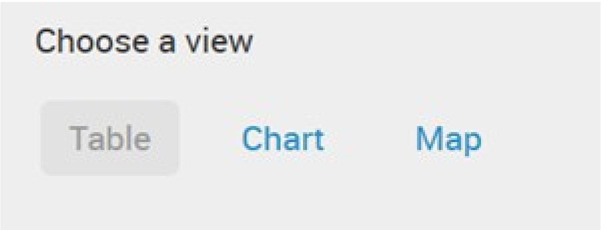
Condition to Set & Unset depending upon the output of search result



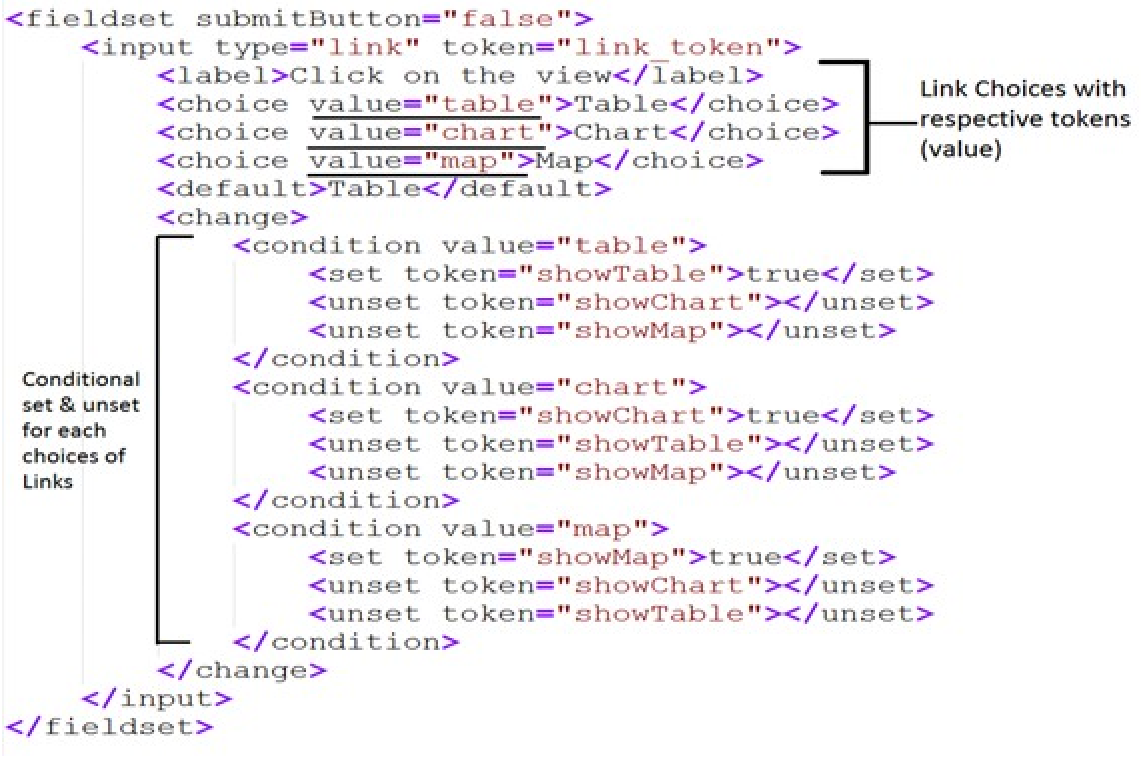
```
<chart rejects="$show_html$">
  <title>Top source for sourcetype = "Splunkd"</title>
  <search base="search_query" />
  <option name="charting.chart">bar</option>
  <option name="charting.legend.placement">none</option>
</chart>
<html depends="$show_html$">
   <p style="color:blue;margin-left:30px;font-size:14px">Search returned no results, so chart is hidden!</p>
</html>
```

Condition 1 - When First Radio Button is selected

Condition 2 - When 2nd radio button is selected



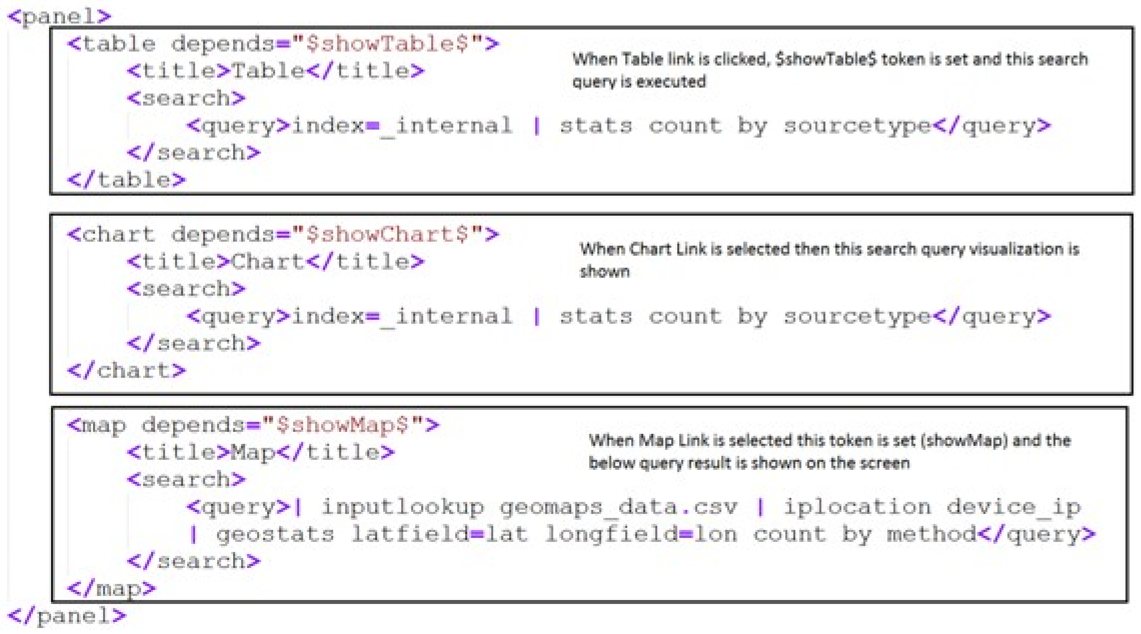
Choose a view



```
<fieldset submitButton="false">
    <input type="link" token="link_token">
        <label>Click on the view</label>
        <choice value="table">Table</choice>
        <choice value="chart">Chart</choice>
        <choice value="map">Map</choice>
        <default>Table</default>
        <change>
            <condition value="table">
                <set token="showTable">true</set>
                <unset token="showChart"></unset>
                <unset token="showMap"></unset>
            </condition>
            <condition value="chart">
                <set token="showChart">true</set>
                <unset token="showTable"></unset>
                <unset token="showMap"></unset>
            </condition>
            <condition value="map">
                <set token="showMap">true</set>
                <unset token="showChart"></unset>
                <unset token="showTable"></unset>
            </condition>
        </change>
    </input>
</fieldset>
```

Link Choices with respective tokens (value)

Conditional set & unset for each choices of Links

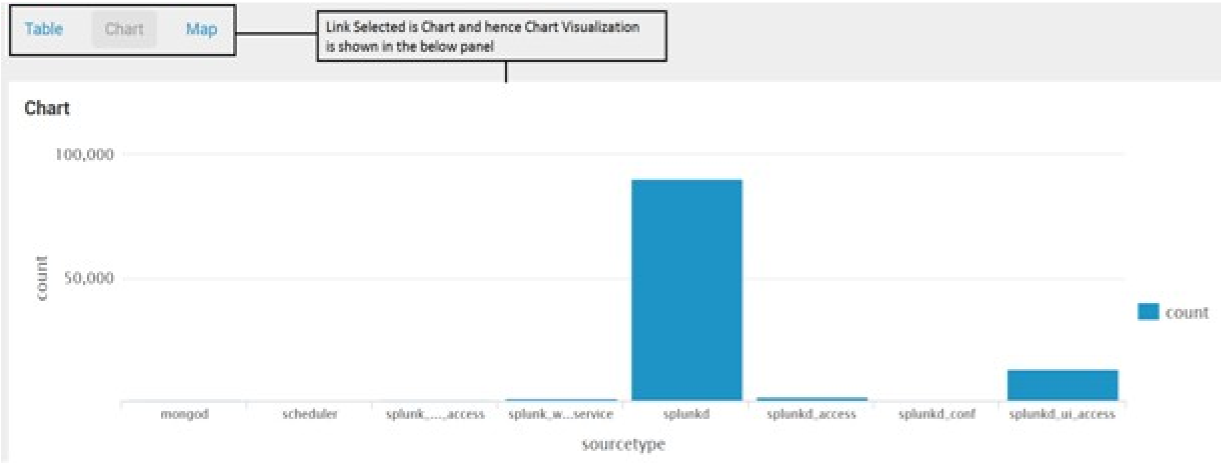


```
<panel>
    <table depends="$showTable$">
        <title>Table</title>
        <search>
            <query>index=_internal | stats count by sourcetype</query>
        </search>
    </table>

    <chart depends="$showChart$">
        <title>Chart</title>
        <search>
            <query>index=_internal | stats count by sourcetype</query>
        </search>
    </chart>

    <map depends="$showMap$">
        <title>Map</title>
        <search>
            <query>| inputlookup geomaps_data.csv | iplocation device_ip
            | geostats latfield=lat longfield=lon count by method</query>
        </search>
    </map>
</panel>
```

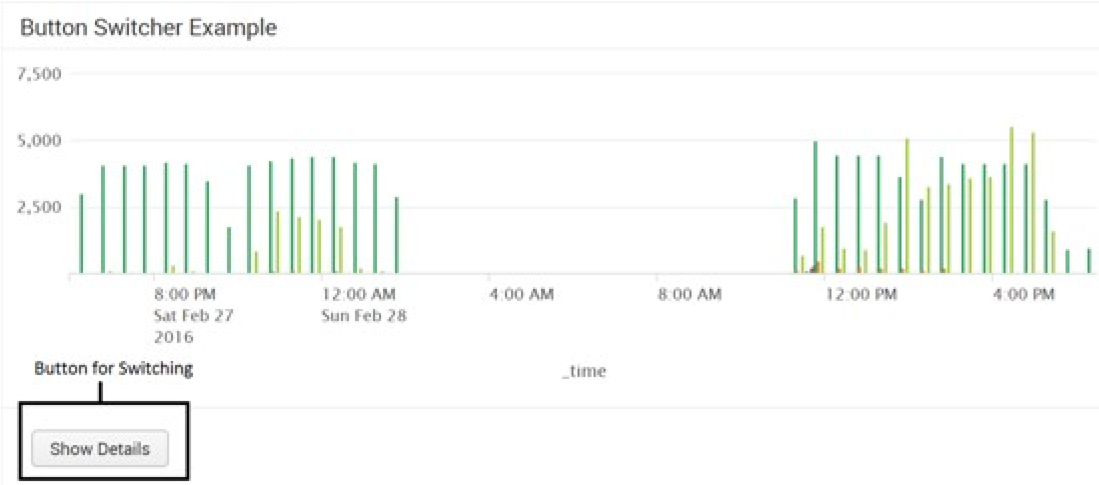
When Table link is clicked, $showTable$ token is set and this search query is executed

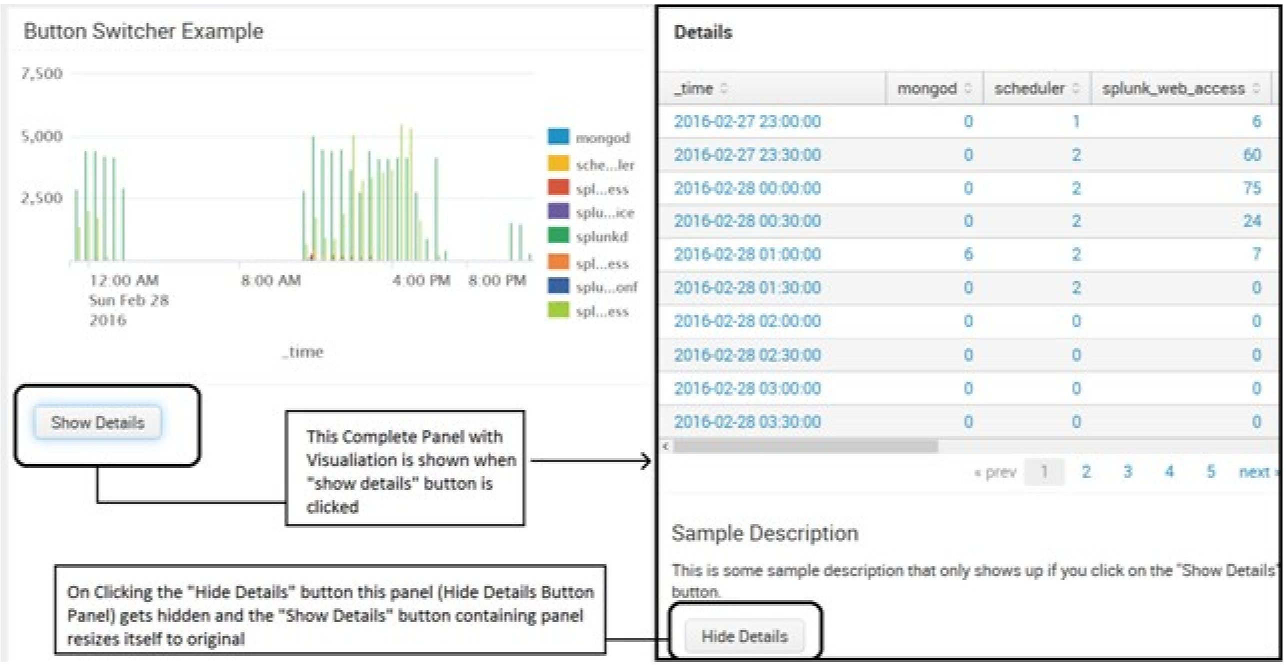
When Chart Link is selected then this search query visualization is shown

When Map Link is selected this token is set (showMap) and the below query result is shown on the screen



Link Selected is Chart and hence Chart Visualization is shown in the below panel





Details

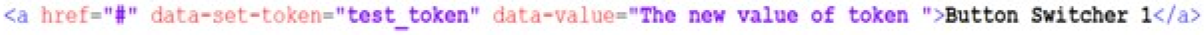
_time	mongod	scheduler	splunk_web_access
2016-02-27 23:00:00	0	1	6
2016-02-27 23:30:00	0	2	60
2016-02-28 00:00:00	0	2	75
2016-02-28 00:30:00	0	2	24
2016-02-28 01:00:00	6	2	7
2016-02-28 01:30:00	0	2	0
2016-02-28 02:00:00	0	0	0
2016-02-28 02:30:00	0	0	0
2016-02-28 03:00:00	0	0	0
2016-02-28 03:30:00	0	0	0

Sample Description

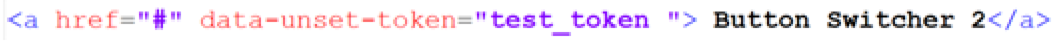
This is some sample description that only shows up if you click on the "Show Details" button.

This Complete Panel with Visualiation is shown when "show details" button is clicked

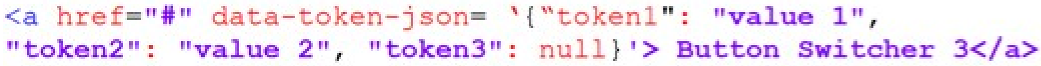
On Clicking the "Hide Details" button this panel (Hide Details Button Panel) gets hidden and the "Show Details" button containing panel resizes itself to original



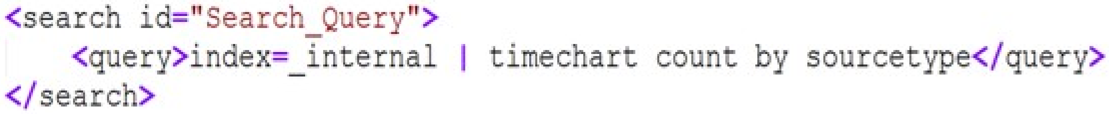
```
<a href="#" data-set-token="test_token" data-value="The new value of token ">Button Switcher 1</a>
```



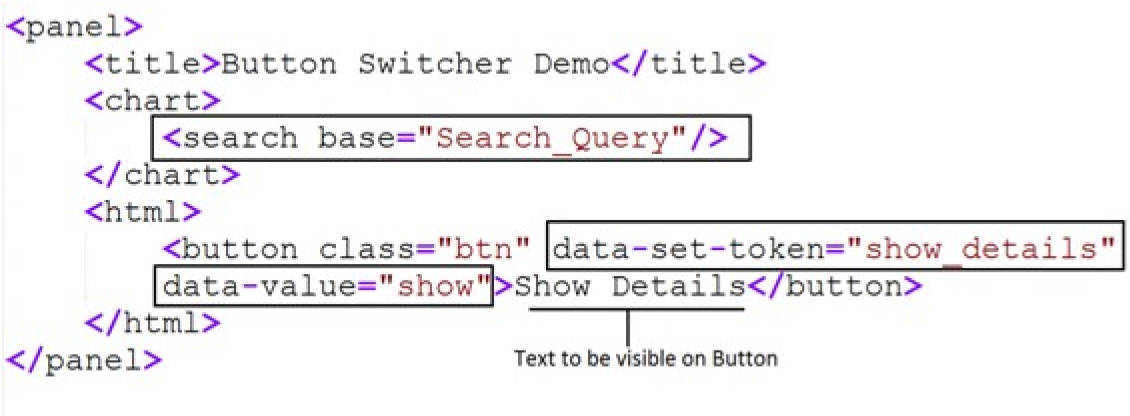
```
<a href="#" data-unset-token="test_token "> Button Switcher 2</a>
```



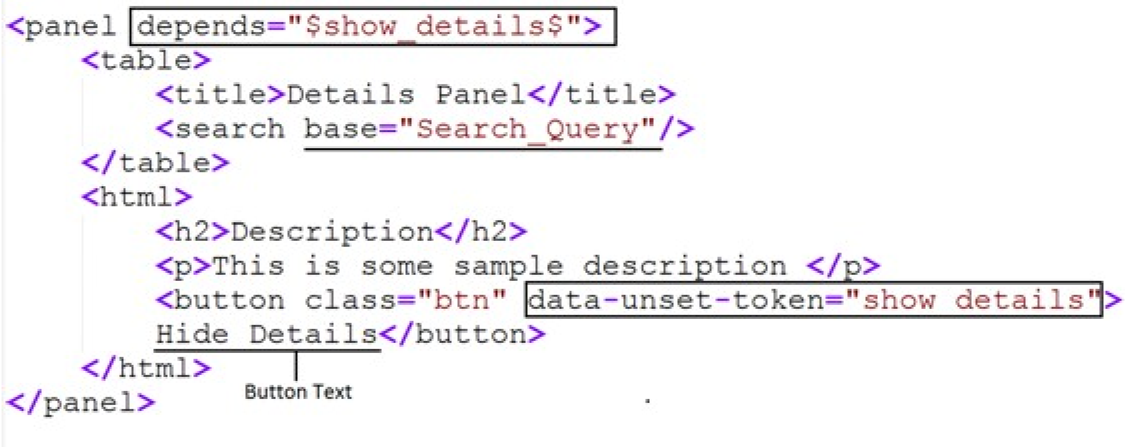
```
<a href="#" data-token-json= '{“token1": "value 1",
"token2": "value 2", "token3": null}'> Button Switcher 3</a>
```



```
<search id="Search_Query">
    <query>index=_internal | timechart count by sourcetype</query>
</search>
```

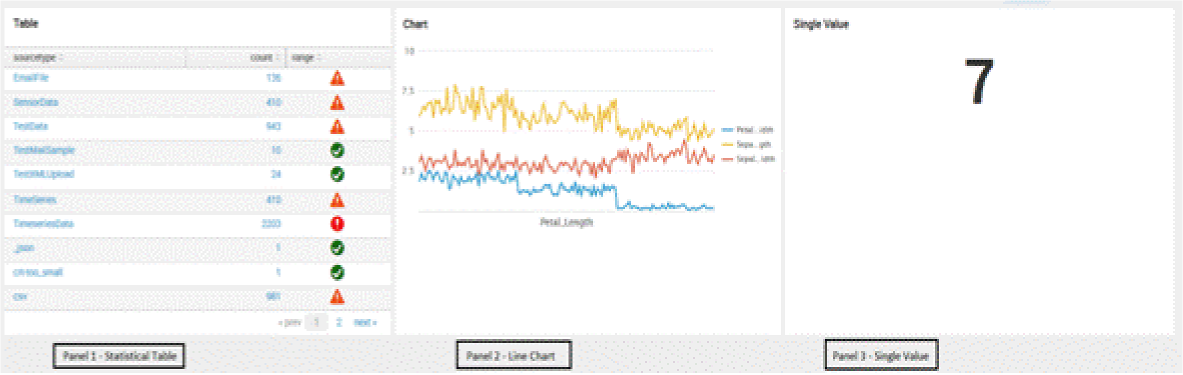


```
<panel>
    <title>Button Switcher Demo</title>
    <chart>
        <search base="Search_Query"/>
    </chart>
    <html>
        <button class="btn" data-set-token="show_details"
        data-value="show">Show Details</button>
    </html>
</panel>
```



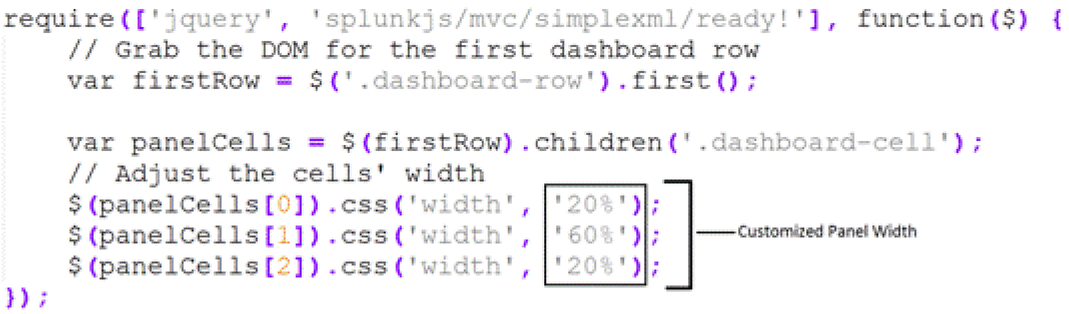
```
<panel depends="$show_details$">
    <table>
        <title>Details Panel</title>
        <search base="Search_Query"/>
    </table>
    <html>
        <h2>Description</h2>
        <p>This is some sample description </p>
        <button class="btn" data-unset-token="show details">
        Hide Details</button>
    </html>
</panel>
```

Chapter 9: Advanced Dashboard Customization

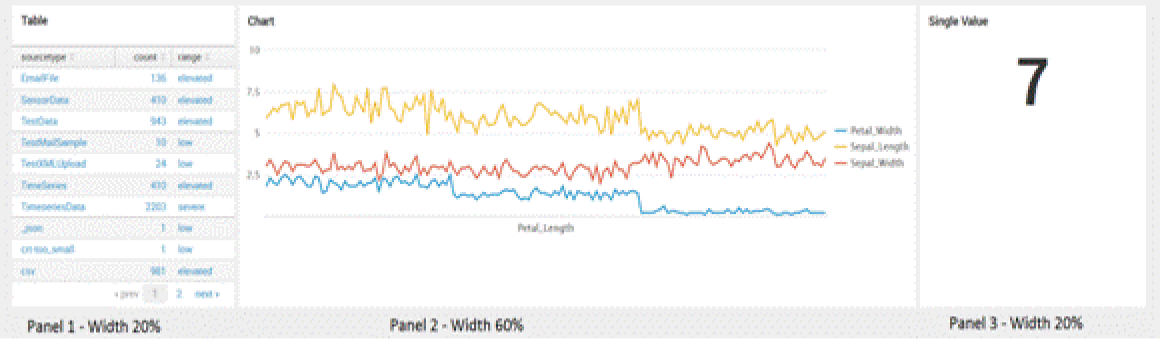


Table

sourcetype	count	range
EmailFile	136	⚠
SensorData	410	⚠
TestData	943	⚠
TestMailSample	10	✓
TestXMLUpload	24	✓
TimeSeries	410	⚠
TimeseriesData	2203	❗
_json	1	✓
cri-too_small	1	✓
csv	981	⚠

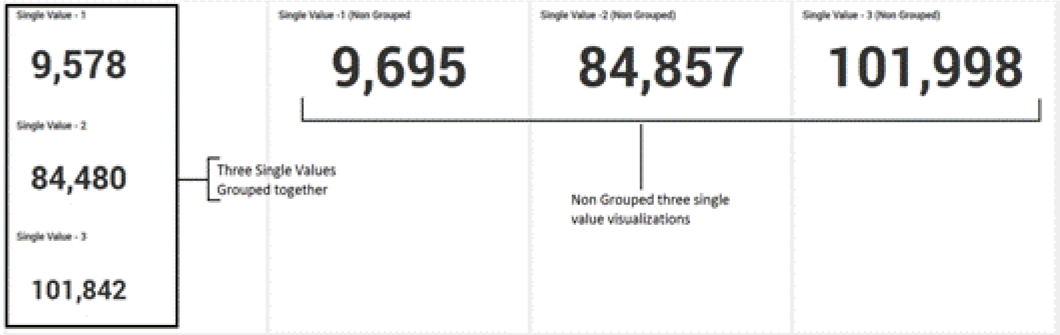


```
require(['jquery', 'splunkjs/mvc/simplexml/ready!'], function($) {
    // Grab the DOM for the first dashboard row
    var firstRow = $('.dashboard-row').first();

    var panelCells = $(firstRow).children('.dashboard-cell');
    // Adjust the cells' width
    $(panelCells[0]).css('width', '20%');
    $(panelCells[1]).css('width', '60%');
    $(panelCells[2]).css('width', '20%');
});
```

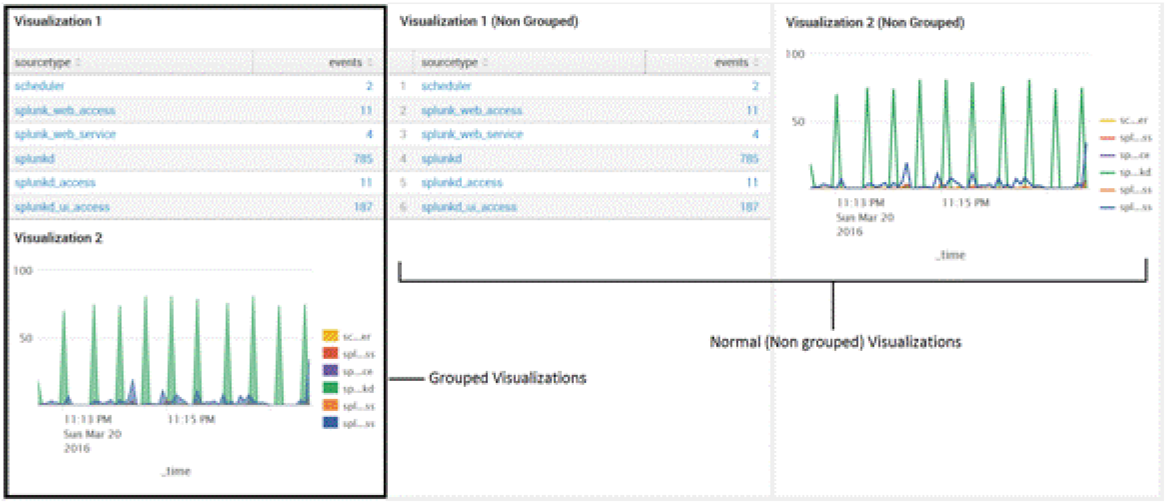


Table

sourcetype	count	range
EmailFile	136	elevated
SensorData	410	elevated
TestData	943	elevated
TestMailSample	10	low
TestXMLUpload	24	low
TimeSeries	410	elevated
TimeseriesData	2203	severe
_json	1	low
cri-too_small	1	low
csv	981	elevated



Single Value - 1
9,578
Single Value - 2
84,480
Single Value - 3
101,842
Three Single Values Grouped together
Single Value -1 (Non Grouped
9,695
Single Value -2 (Non Grouped)
84,857
Single Value - 3 (Non Grouped)
101,998
Non Grouped three single value visualizations



Visualization 1

sourcetype	events
scheduler	2
splunk_web_access	11
splunk_web_service	4
splunkd	785
splunkd_access	11
splunkd_ui_access	187

Visualization 2

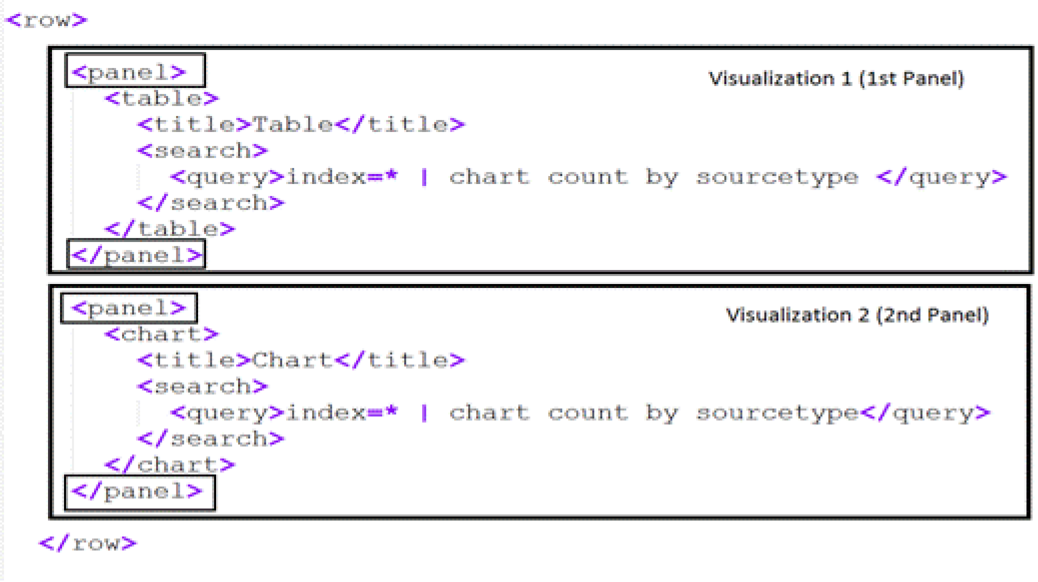
Grouped Visualizations

Visualization 1 (Non Grouped)

	sourcetype	events
1	scheduler	2
2	splunk_web_access	11
3	splunk_web_service	4
4	splunkd	785
5	splunkd_access	11
6	splunkd_ui_access	187

Visualization 2 (Non Grouped)

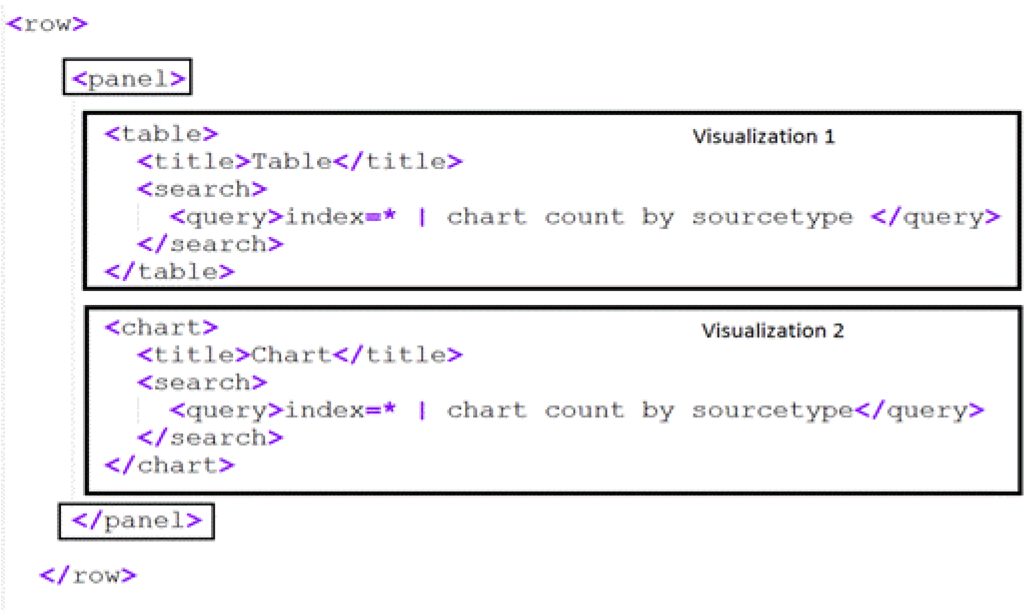
Normal (Non grouped) Visualizations



```
<row>
  <panel>
    <table>
      <title>Table</title>
      <search>
        <query>index=* | chart count by sourcetype </query>
      </search>
    </table>
  </panel>
  <panel>
    <chart>
      <title>Chart</title>
      <search>
        <query>index=* | chart count by sourcetype</query>
      </search>
    </chart>
  </panel>
</row>
```

Visualization 1 (1st Panel)

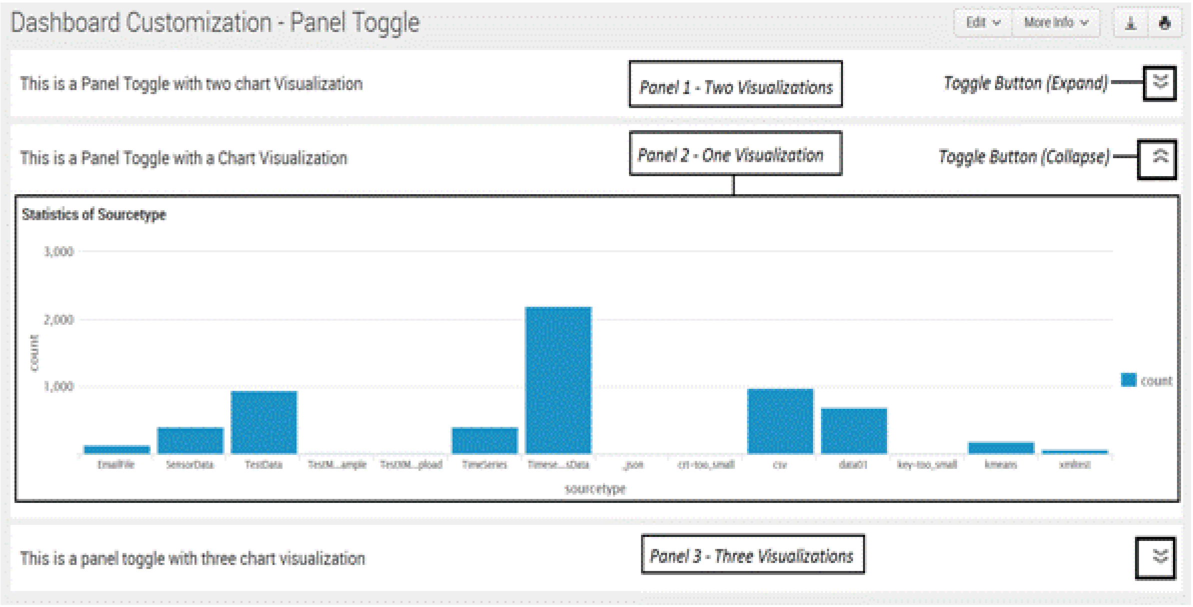
Visualization 2 (2nd Panel)



```
<row>
    <panel>
      <table>
        <title>Table</title>
        <search>
          <query>index=* | chart count by sourcetype </query>
        </search>
      </table>
      <chart>
        <title>Chart</title>
        <search>
          <query>index=* | chart count by sourcetype</query>
        </search>
      </chart>
    </panel>
  </row>
```

Visualization 1

Visualization 2



Dashboard Customization - Panel Toggle

This is a Panel Toggle with two chart Visualization

Panel 1 - Two Visualizations

Toggle Button (Expand)

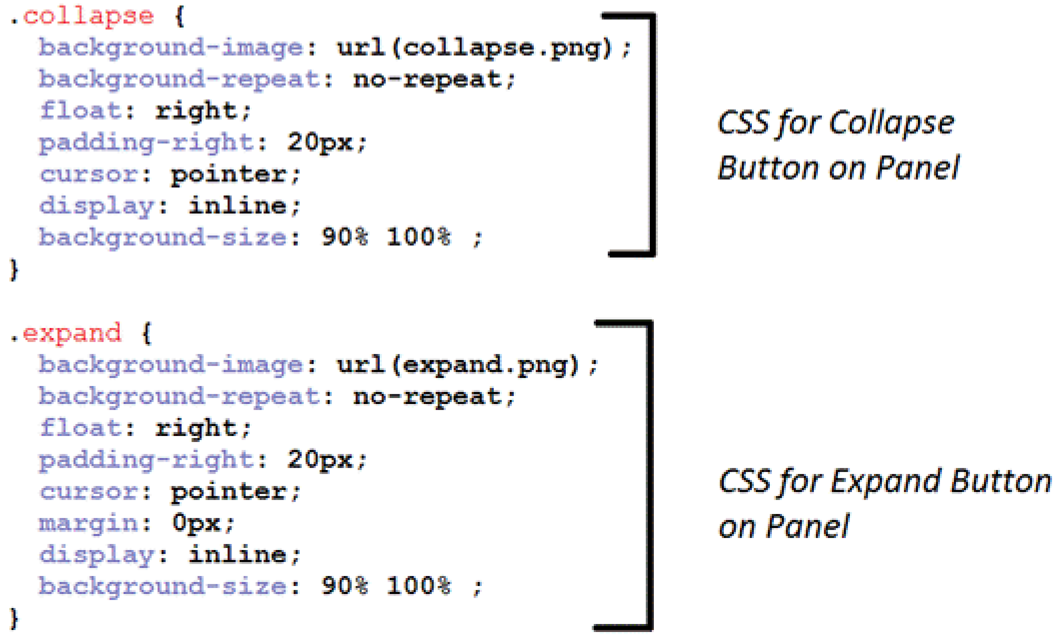
This is a Panel Toggle with a Chart Visualization

Panel 2 - One Visualization

Toggle Button (Collapse)

This is a panel toggle with three chart visualization

Panel 3 - Three Visualizations

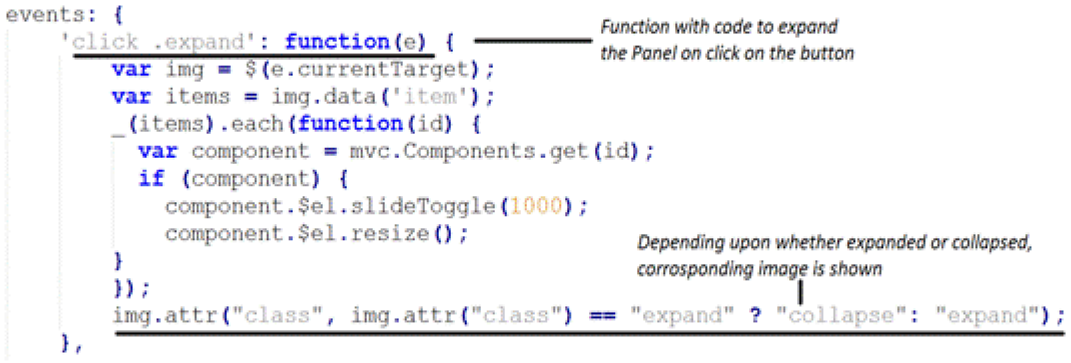


```
.collapse {
  background-image: url(collapse.png);
  background-repeat: no-repeat;
  float: right;
  padding-right: 20px;
  cursor: pointer;
  display: inline;
  background-size: 90% 100% ;
}
```

CSS for Collapse Button on Panel

```
.expand {
  background-image: url(expand.png);
  background-repeat: no-repeat;
  float: right;
  padding-right: 20px;
  cursor: pointer;
  margin: 0px;
  display: inline;
  background-size: 90% 100% ;
}
```

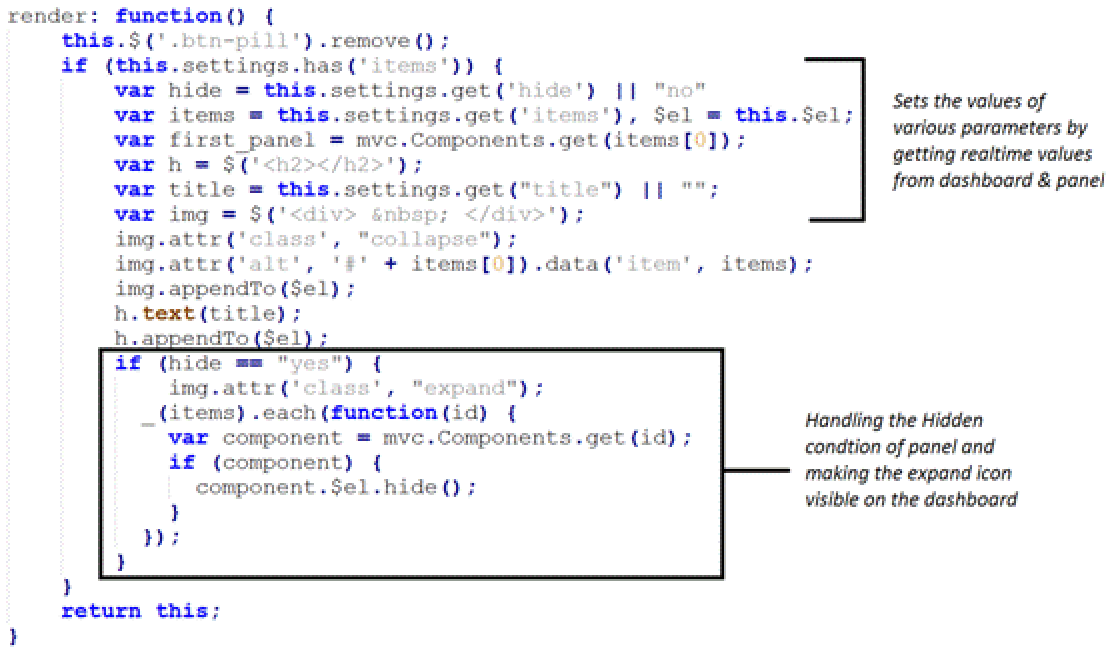
CSS for Expand Button on Panel



```
events: {
    'click .expand': function(e) {
        var img = $(e.currentTarget);
        var items = img.data('item');
        _(items).each(function(id) {
          var component = mvc.Components.get(id);
          if (component) {
            component.$el.slideToggle(1000);
            component.$el.resize();
          }
        });
        img.attr("class", img.attr("class") == "expand" ? "collapse": "expand");
    },
```

Function with code to expand the Panel on click on the button

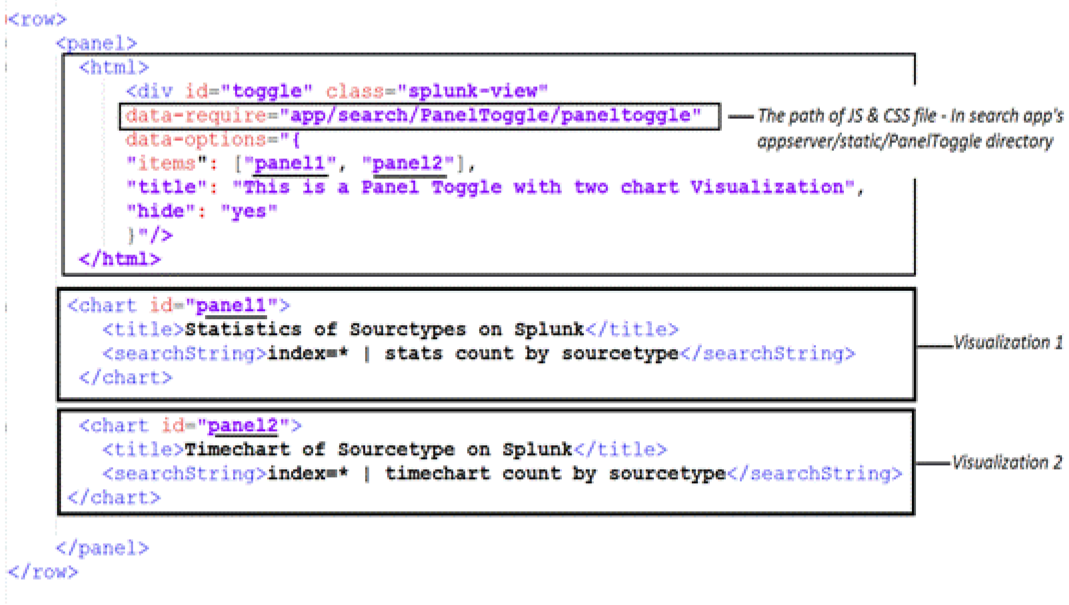
Depending upon whether expanded or collapsed, corrosponding image is shown



```
render: function() {
    this.$('.btn-pill').remove();
    if (this.settings.has('items')) {
        var hide = this.settings.get('hide') || "no"
        var items = this.settings.get('items'), $el = this.$el;
        var first_panel = mvc.Components.get(items[0]);
        var h = $('<h2></h2>');
        var title = this.settings.get("title") || "";
        var img = $('<div> &nbsp; </div>');
        img.attr('class', "collapse");
        img.attr('alt', '#' + items[0]).data('item', items);
        img.appendTo($el);
        h.text(title);
        h.appendTo($el);
        if (hide == "yes") {
            img.attr('class', "expand");
          _(items).each(function(id) {
            var component = mvc.Components.get(id);
            if (component) {
              component.$el.hide();
            }
          });
        }
    }
    return this;
}
```

Sets the values of various parameters by getting realtime values from dashboard & panel

Handling the Hidden condtion of panel and making the expand icon visible on the dashboard

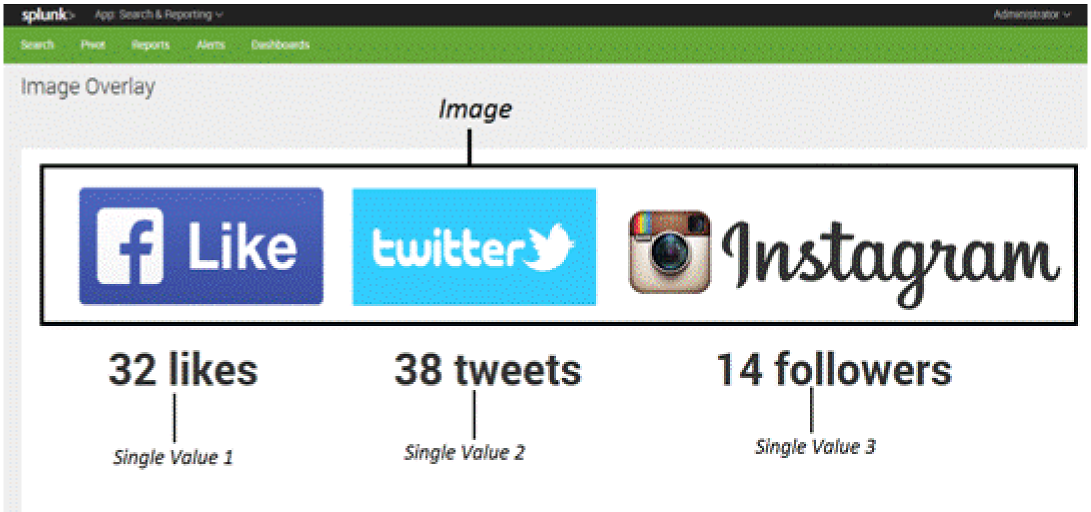


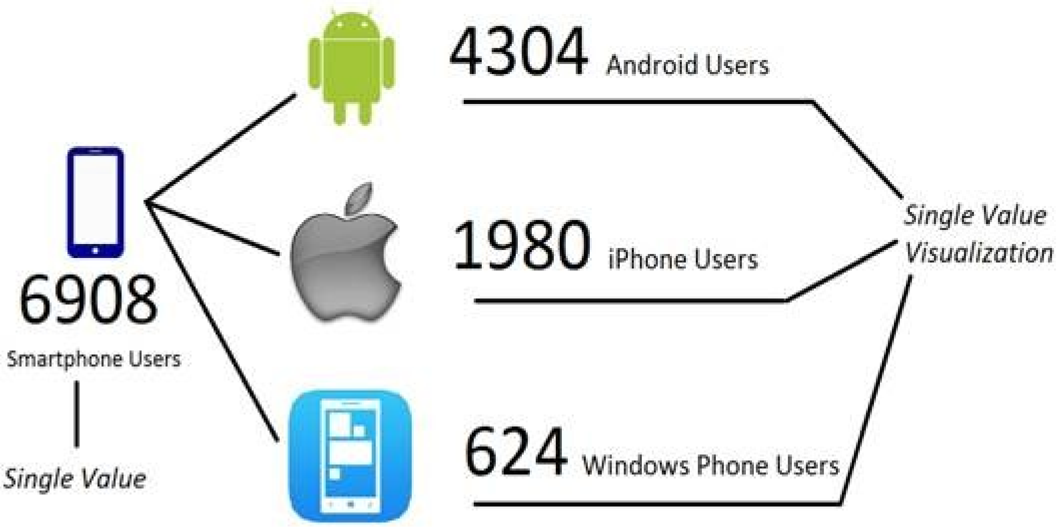
```
<row>
    <panel>
     <html>
        <div id="toggle" class="splunk-view"
        data-require="app/search/PanelToggle/paneltoggle"
        data-options="{
        "items": ["panel1", "panel2"],
        "title": "This is a Panel Toggle with two chart Visualization",
        "hide": "yes"
        }"/>
     </html>
    <chart id="panel1">
       <title>Statistics of Sourctypes on Splunk</title>
       <searchString>index=* | stats count by sourcetype</searchString>
     </chart>
     <chart id="panel2">
       <title>Timechart of Sourcetype on Splunk</title>
       <searchString>index=* | timechart count by sourcetype</searchString>
    </chart>
    </panel>
</row>
```

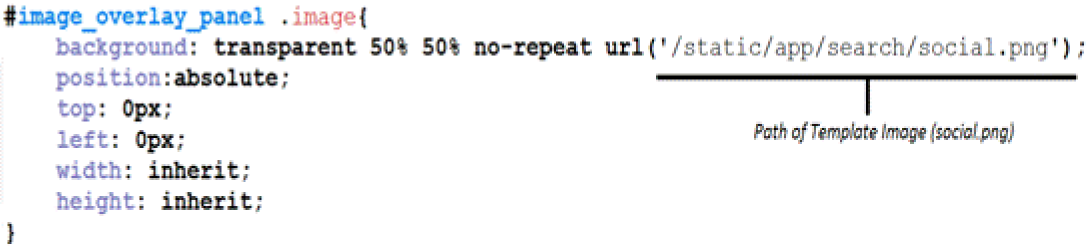
The path of JS & CSS file - In search app's appserver/static/PanelToggle directory

Visualization 1

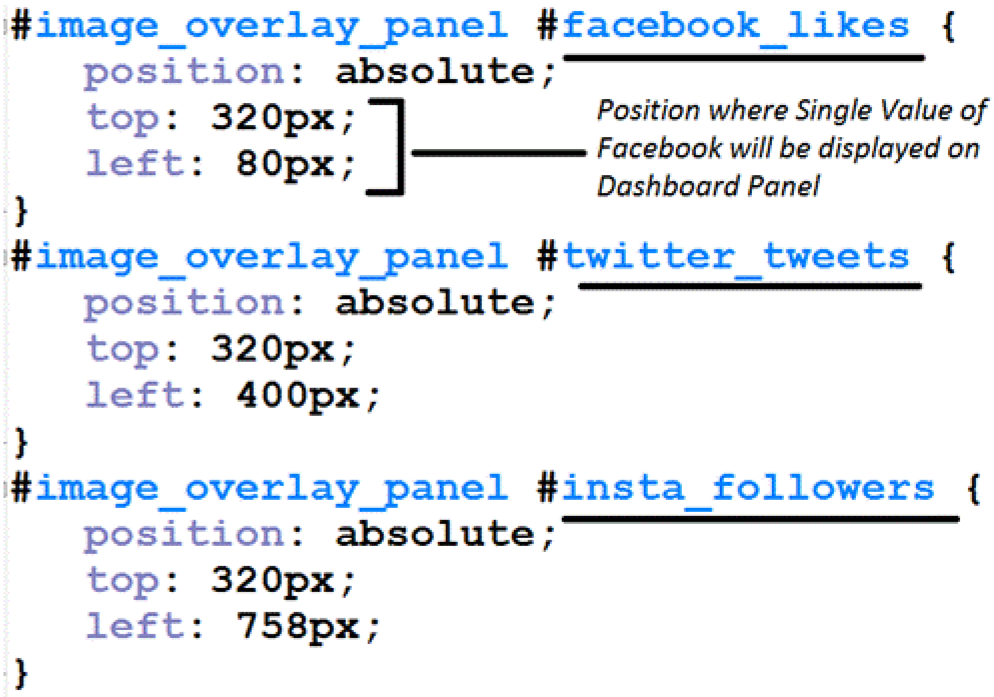
Visualization 2





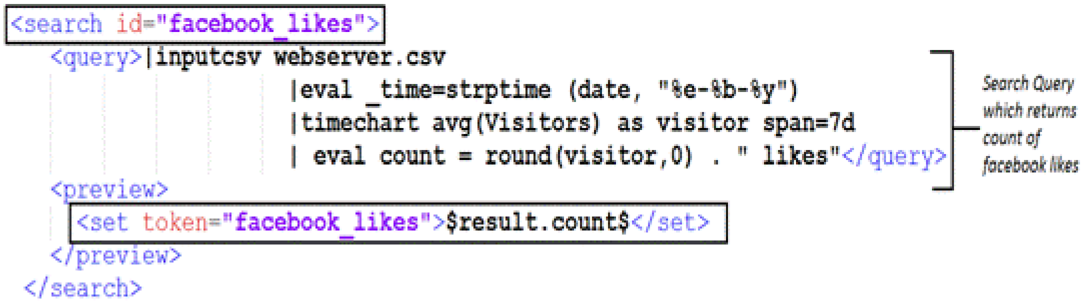


```
#image_overlay_panel .image{
    background: transparent 50% 50% no-repeat url('/static/app/search/social.png');
    position:absolute;
    top: 0px;
    left: 0px;
    width: inherit;
    height: inherit;
}
```



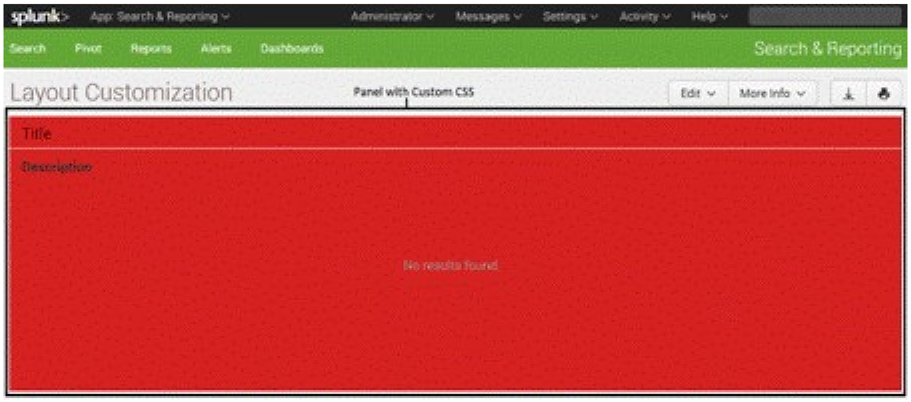
```
#image_overlay_panel #facebook_likes {
   position: absolute;
   top: 320px;
   left: 80px;
}
#image_overlay_panel #twitter_tweets {
   position: absolute;
   top: 320px;
   left: 400px;
}
#image_overlay_panel #insta_followers {
   position: absolute;
   top: 320px;
   left: 758px;
}
```

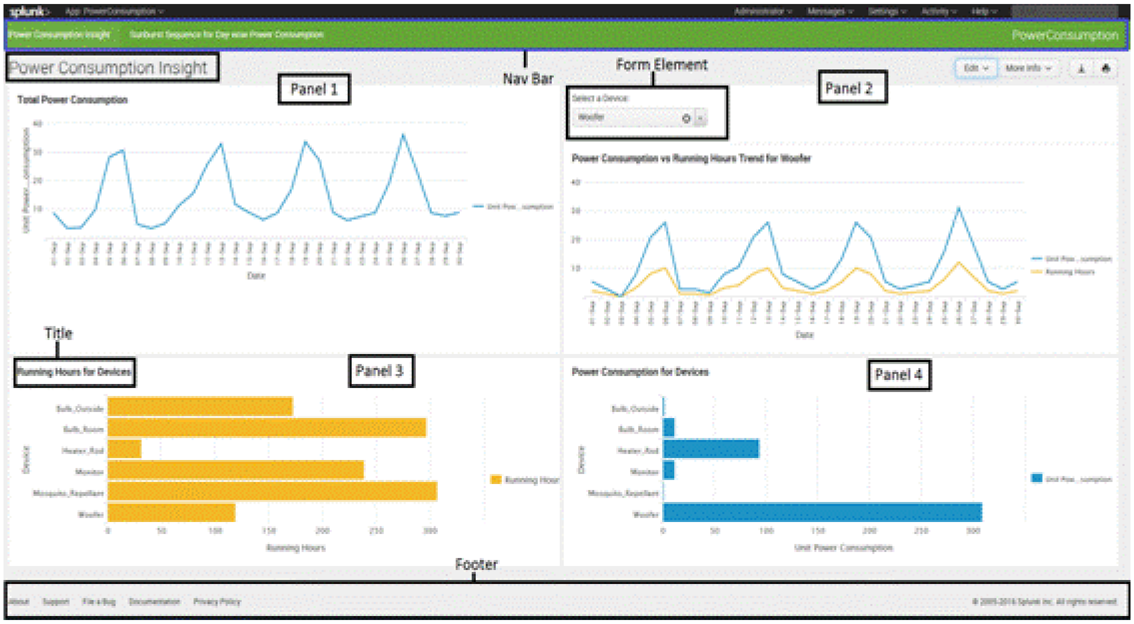
Position where Single Value of Facebook will be displayed on Dashboard Panel

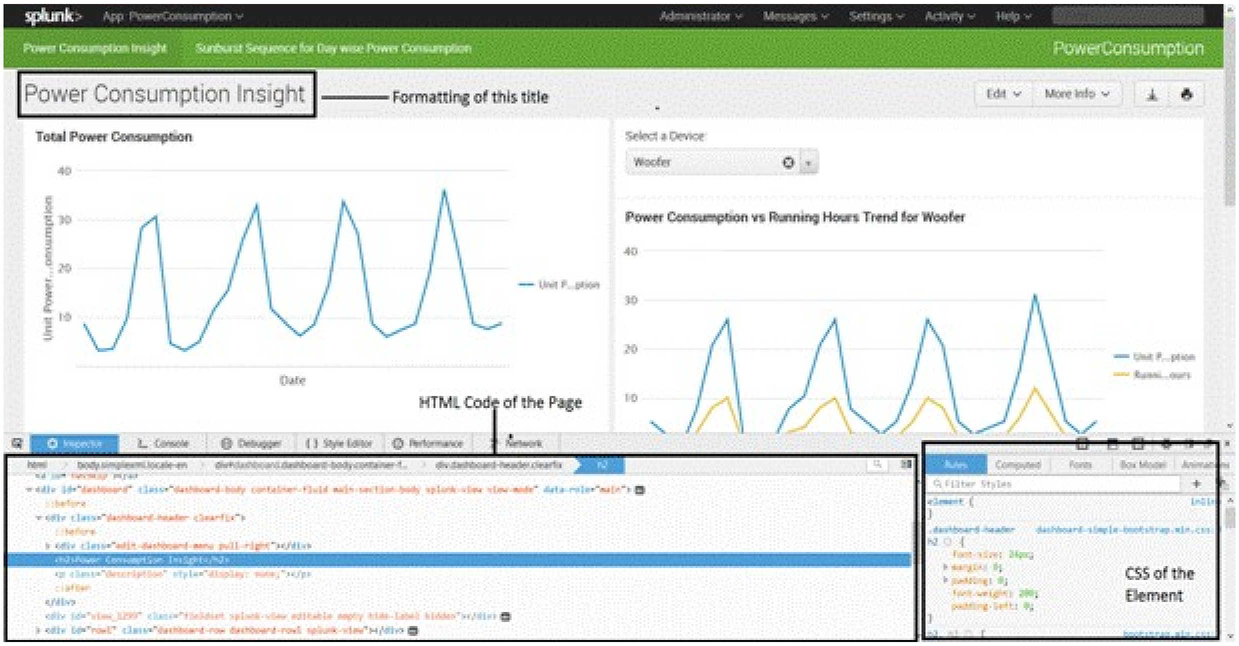


```
<search id="facebook_likes">
  <query>|inputcsv webserver.csv
              |eval _time=strptime (date, "%e-%b-%y")
              |timechart avg(Visitors) as visitor span=7d
              | eval count = round(visitor,0) . " likes"</query>
  <preview>
    <set token="facebook_likes">$result.count$</set>
  </preview>
</search>
```

Search Query which returns count of facebook likes

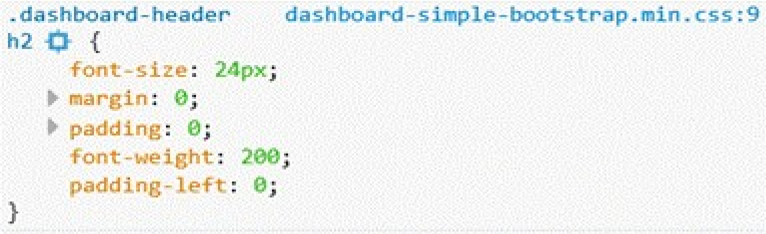




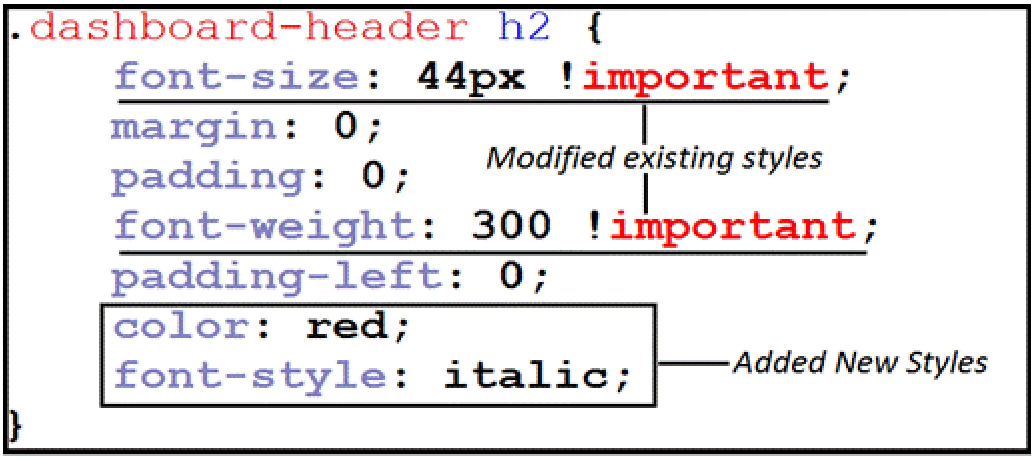


```
▾ <div id="dashboard" class="dashboard-body container-fluid main-section-body splunk-view view-mode" data-role="main">
    ::before
  ▾ <div class="dashboard-header clearfix">
      ::before
    ▸ <div class="edit-dashboard-menu pull-right"></div>
      <h2>Power Consumption Insight</h2>
      <p class="description" style="display: none;"></p>
      ::after
    </div>
    <div id="view_1299" class="fieldset splunk-view editable empty hide-label hidden"></div>
  ▸ <div id="row1" class="dashboard-row dashboard-row1 splunk-view"></div>
```

```
element {
}
.dashboard-header     dashboard-simple-bootstrap.min.css:9
h2 {
    font-size: 24px;
  ▸ margin: 0;
  ▸ padding: 0;
    font-weight: 200;
    padding-left: 0;
}
```



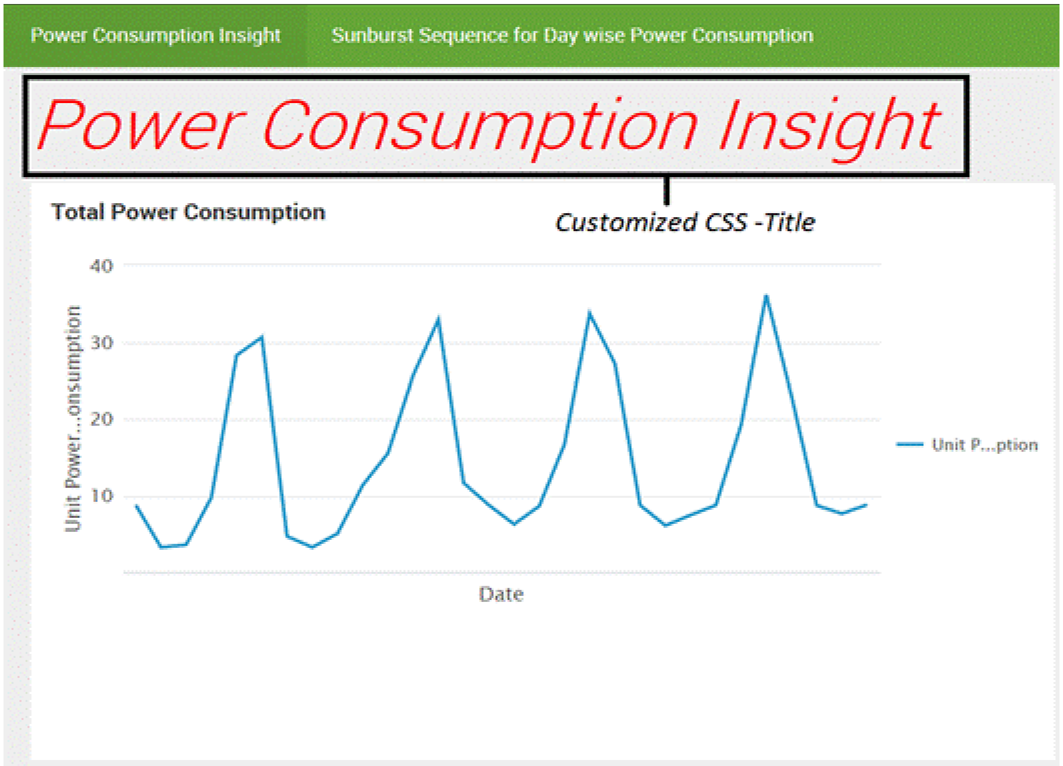
```
.dashboard-header     dashboard-simple-bootstrap.min.css:9
h2 {
    font-size: 24px;
  ▸ margin: 0;
  ▸ padding: 0;
    font-weight: 200;
    padding-left: 0;
}
```



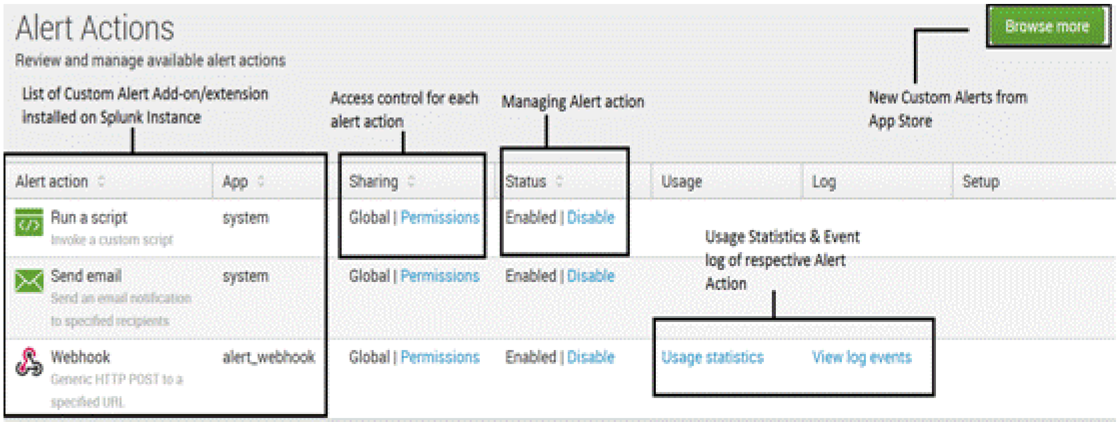
```
.dashboard-header h2 {
    font-size: 44px !important;
    margin: 0;
    padding: 0;
    font-weight: 300 !important;
    padding-left: 0;
    color: red;
    font-style: italic;
}
```

Modified existing styles

Added New Styles


Power Consumption Insight
Sunburst Sequence for Day wise Power Consumption
Power Consumption Insight
Total Power Consumption
40
30
20
10
Unit Power...onsumption
Date
Unit P...ption

Customized CSS -Title



Alert Actions

Review and manage available alert actions

List of Custom Alert Add-on/extension installed on Splunk Instance

Access control for each alert action

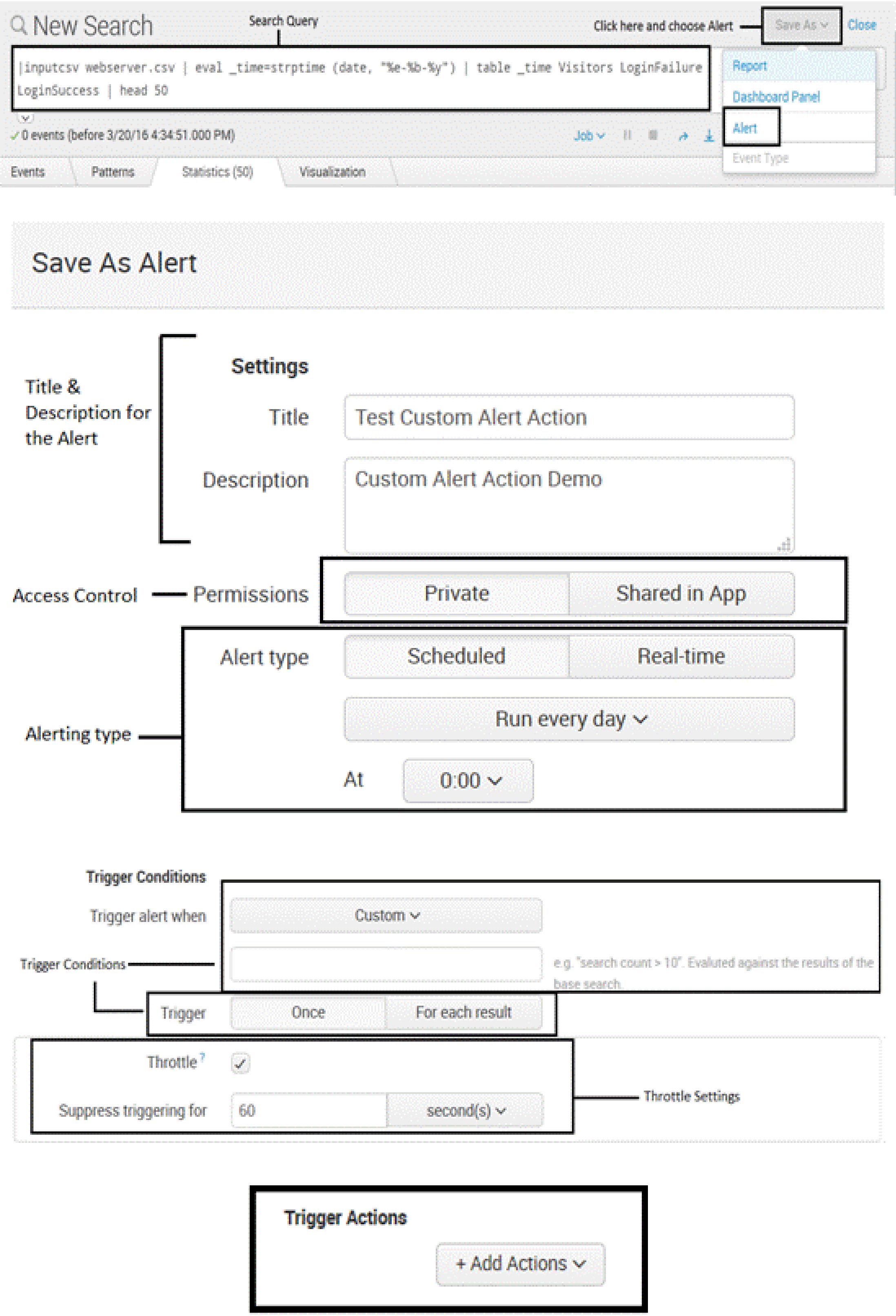
Managing Alert action

New Custom Alerts from App Store

Browse more

Alert action	App	Sharing	Status	Usage	Log	Setup
Run a script Invoke a custom script	system	Global | Permissions	Enabled | Disable			
Send email Send an email notification to specified recipients	system	Global | Permissions	Enabled | Disable			
Webhook Generic HTTP POST to a specified URL	alert_webhook	Global | Permissions	Enabled | Disable	Usage statistics	View log events	

Usage Statistics & Event log of respective Alert Action



```
|inputcsv webserver.csv | eval _time=strptime (date, "%e-%b-%y") | table _time Visitors LoginFailure
LoginSuccess | head 50
```

✓ 0 events (before 3/20/16 4:34:51.000 PM)

Save As Alert

Settings

Title: Test Custom Alert Action

Description: Custom Alert Action Demo

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every day

At 0:00

Trigger Conditions

Trigger alert when: Custom

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

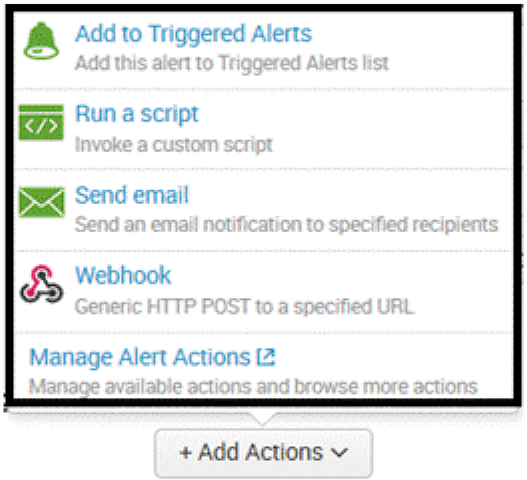
Trigger: Once | For each result

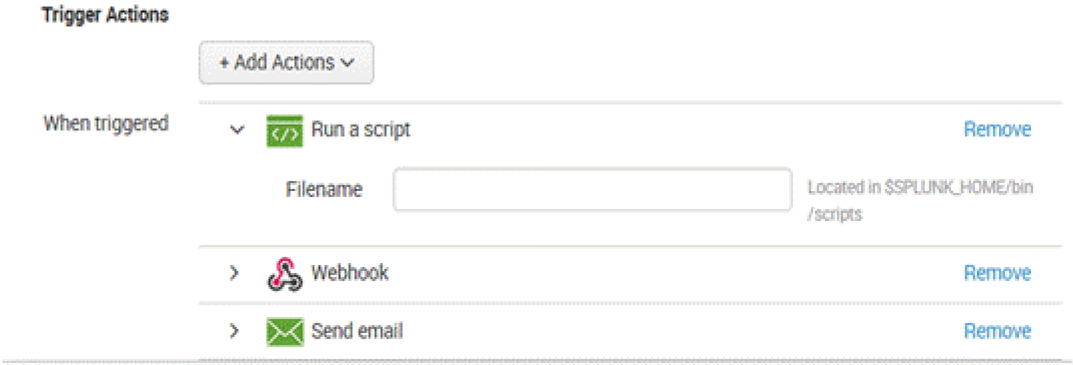
Throttle ☑

Suppress triggering for: 60 second(s)

Trigger Actions

+ Add Actions


Add to Triggered Alerts
Add this alert to Triggered Alerts list
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
+ Add Actions



Trigger Actions

When triggered

Run a script

Filename

Located in $SPLUNK_HOME/bin/scripts

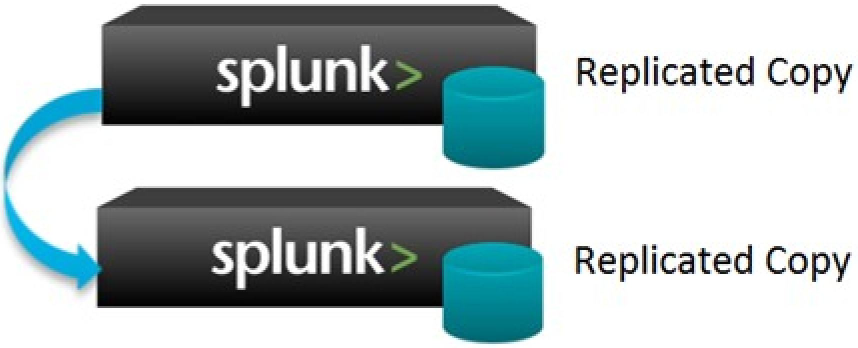
Webhook

Send email

Chapter 10: Tweaking Splunk

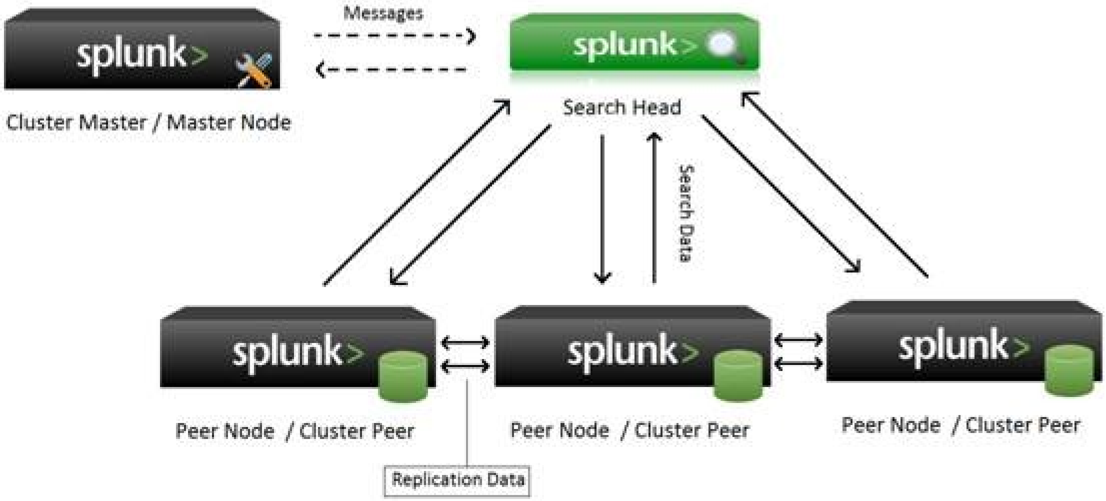
Cluster Master / Master Node

Peer Node / Cluster Peer

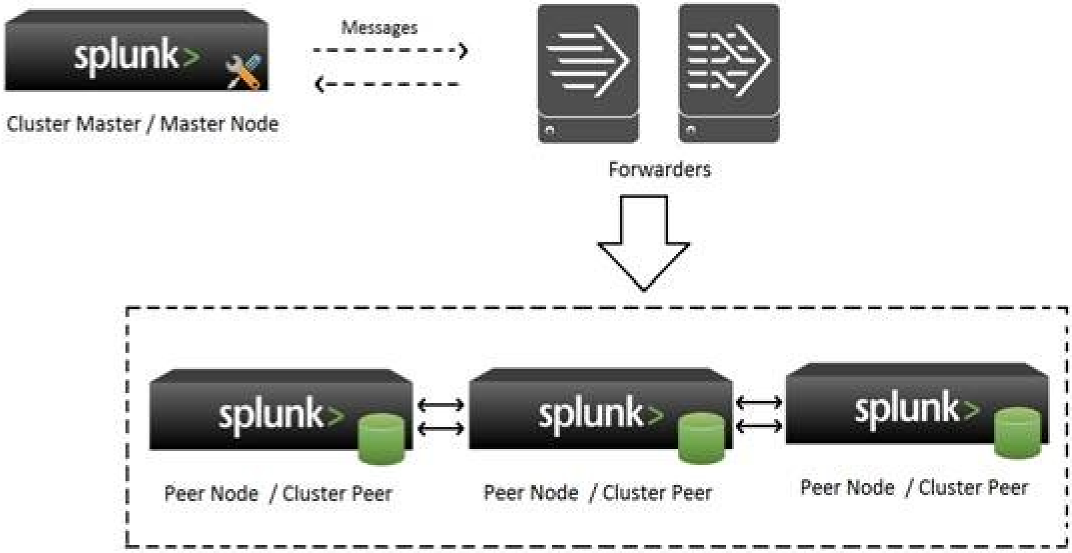


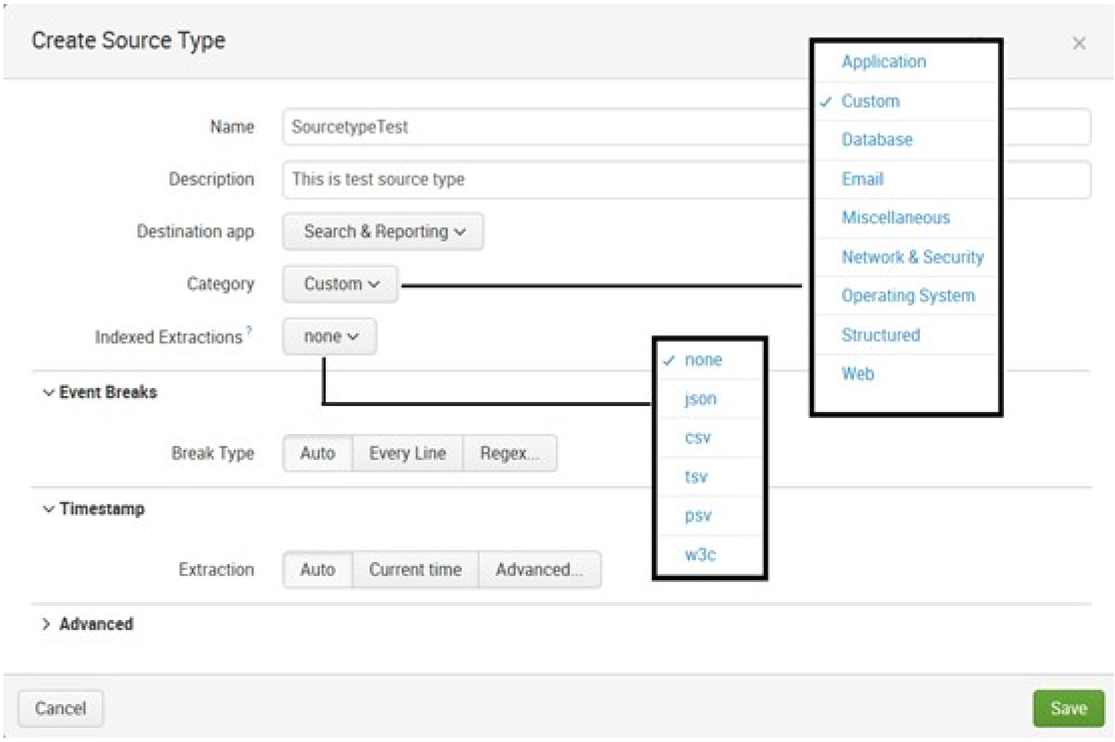
Peer Replication

Search Head



Distributed Splunk Environment with Replication Factor as 3





Create Source Type

Name: SourcetypeTest

Description: This is test source type

Destination app: Search & Reporting

Category: Custom

Indexed Extractions: none

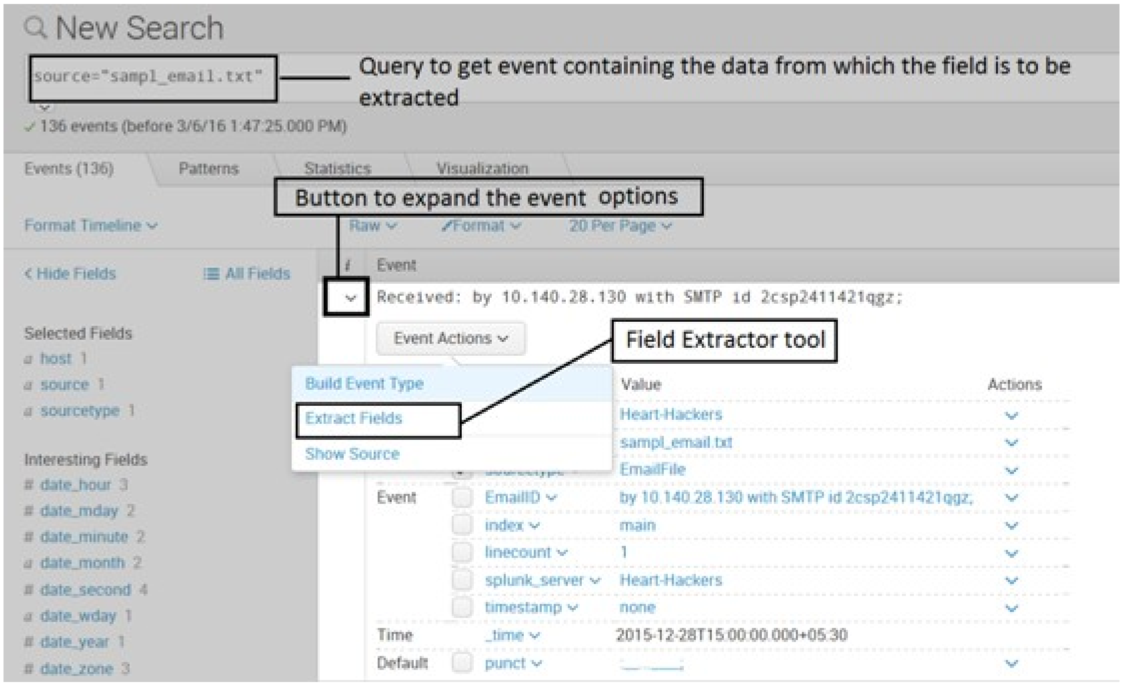
Event Breaks

Break Type: Auto | Every Line | Regex...

Timestamp

Extraction: Auto | Current time | Advanced...

Advanced



New Search

```
source="sampl_email.txt"
```

Query to get event containing the data from which the field is to be extracted

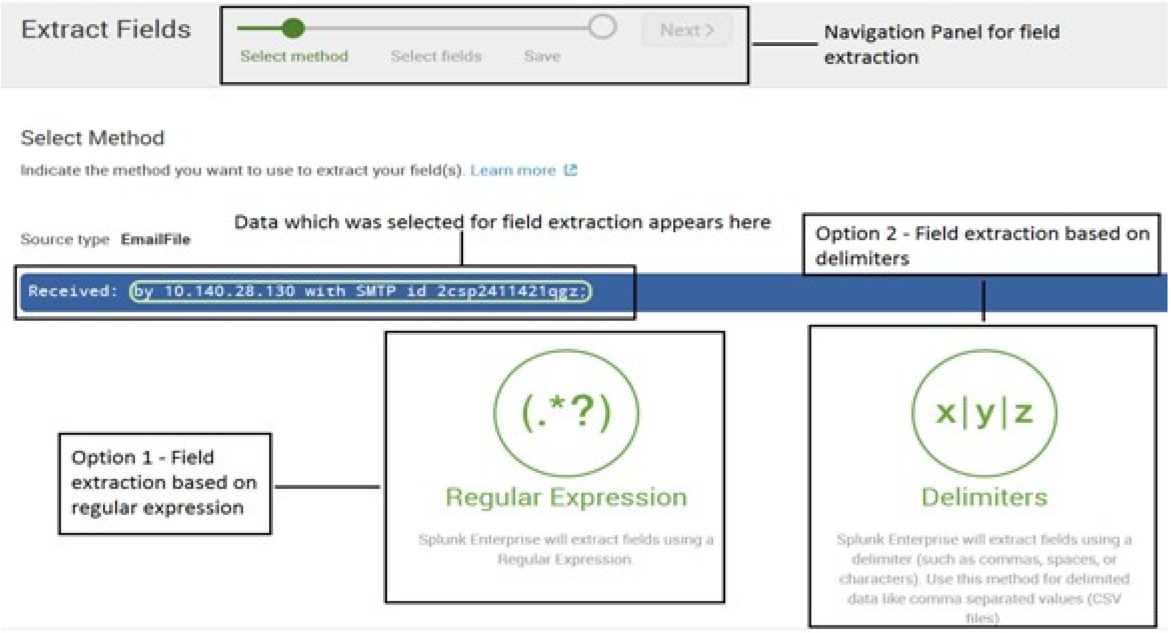
✓ 136 events (before 3/6/16 1:47:25.000 PM)

Button to expand the event options

```
Received: by 10.140.28.130 with SMTP id 2csp2411421qgz;
```

Field Extractor tool

		Value	Actions
		Heart-Hackers	⌄
		sampl_email.txt	⌄
	sourcetype	EmailFile	⌄
Event	EmailID	by 10.140.28.130 with SMTP id 2csp2411421qgz;	⌄
	index	main	⌄
	linecount	1	⌄
	splunk_server	Heart-Hackers	⌄
	timestamp	none	⌄
Time	_time	2015-12-28T15:00:00.000+05:30	
Default	punct	:_.._.._;	⌄



Navigation Panel for field extraction

Select Method

Indicate the method you want to use to extract your field(s). Learn more

Source type EmailFile

Data which was selected for field extraction appears here

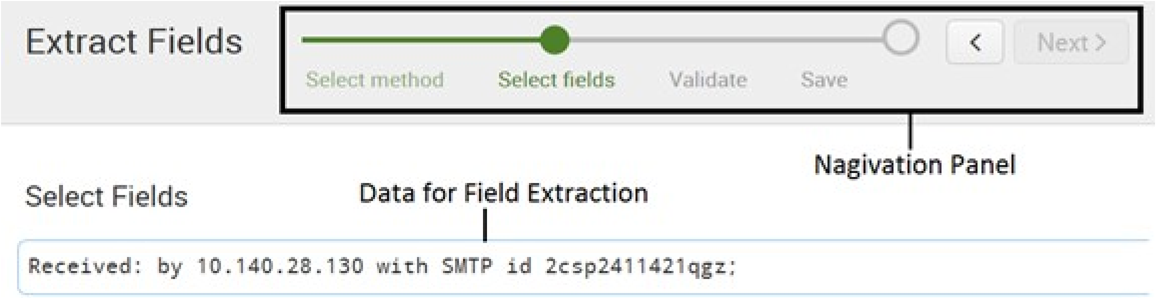
Option 2 - Field extraction based on delimiters

```
Received: by 10.140.28.130 with SMTP id 2csp2411421qgz;
```

Option 1 - Field extraction based on regular expression

Splunk Enterprise will extract fields using a Regular Expression.

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

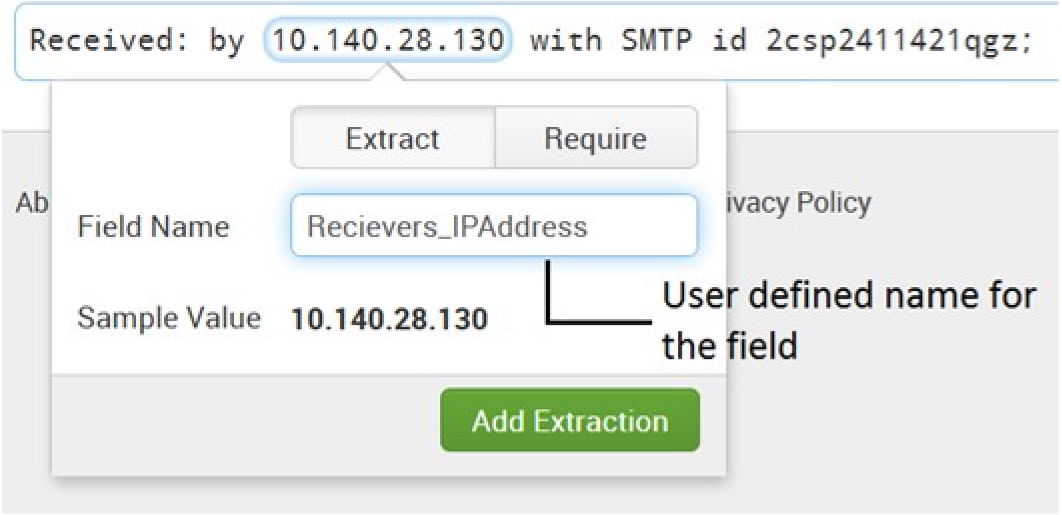


Nagivation Panel

Select Fields

Data for Field Extraction

```
Received: by 10.140.28.130 with SMTP id 2csp2411421qgz;
```

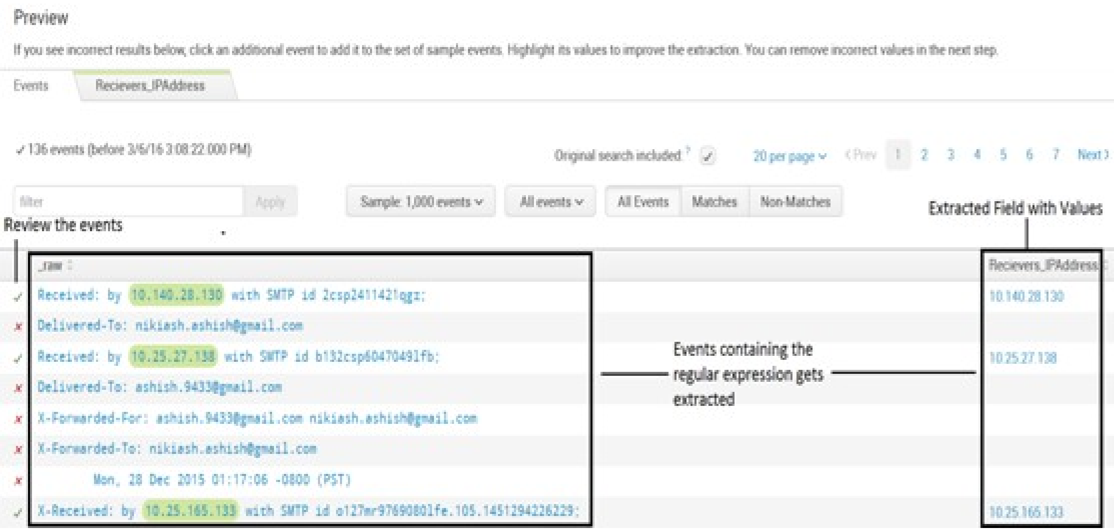


```
Received: by 10.140.28.130 with SMTP id 2csp2411421qgz;
```

Field Name: Recievers_IPAddress

Sample Value: 10.140.28.130

User defined name for the field



Preview

If you see incorrect results below, click an additional event to add it to the set of sample events. Highlight its values to improve the extraction. You can remove incorrect values in the next step.

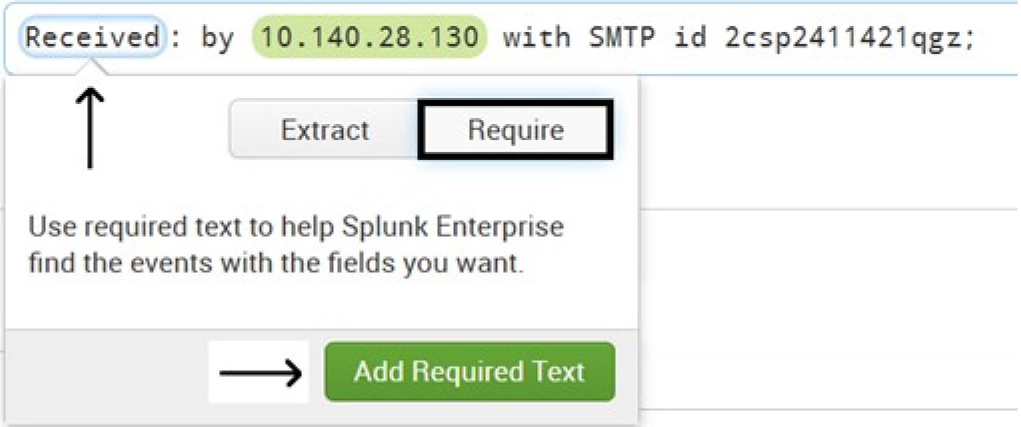
✓ 136 events (before 3/6/16 3:08:22.000 PM)

Review the events

Extracted Field with Values

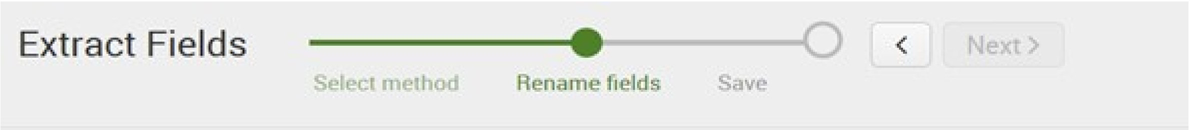
	_raw	Recievers_IPAddress
✓	Received: by 10.140.28.130 with SMTP id 2csp2411421qgz;	10.140.28.130
✗	Delivered-To: nikiash.ashish@gmail.com	
✓	Received: by 10.25.27.138 with SMTP id b132csp60470491fb;	10.25.27.138
✗	Delivered-To: ashish.9433@gmail.com	
✗	X-Forwarded-For: ashish.9433@gmail.com nikiash.ashish@gmail.com	
✗	X-Forwarded-To: nikiash.ashish@gmail.com	
✗	Mon, 28 Dec 2015 01:17:06 -0800 (PST)	
✓	X-Received: by 10.25.165.133 with SMTP id o127mr97690801fe.105.1451294226229;	10.25.165.133

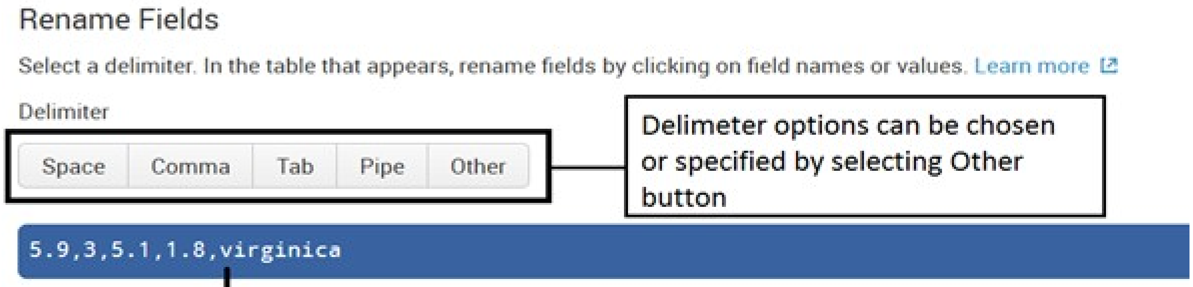
Events containing the regular expression gets extracted



```
Received: by 10.140.28.130 with SMTP id 2csp2411421qgz;
```

Use required text to help Splunk Enterprise find the events with the fields you want.





Rename Fields

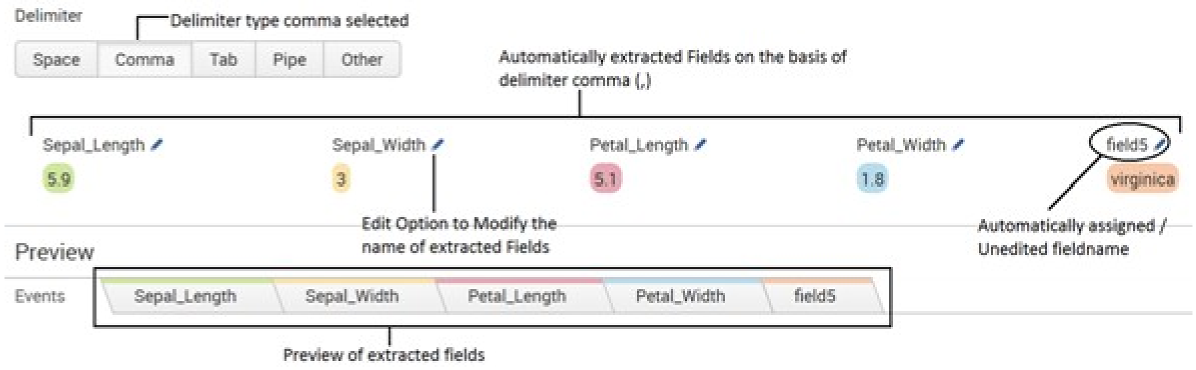
Select a delimiter. In the table that appears, rename fields by clicking on field names or values. Learn more

Delimiter

Delimeter options can be chosen or specified by selecting Other button

```
5.9,3,5.1,1.8,virginica
```

Data for which fields are to be extracted



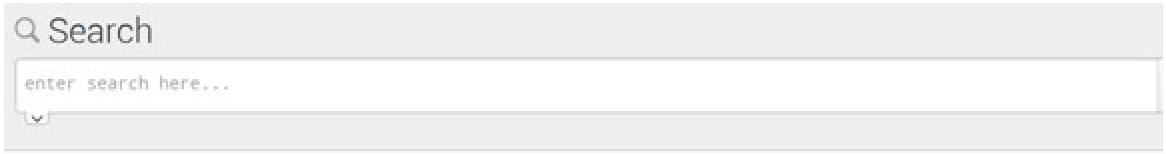
Delimiter type comma selected

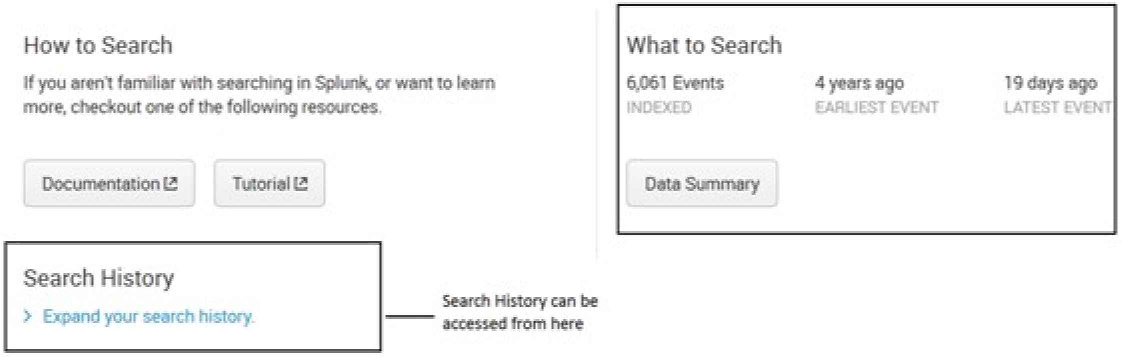
Automatically extracted Fields on the basis of delimiter comma (,)

Edit Option to Modify the name of extracted Fields

Automatically assigned / Unedited fieldname

Preview of extracted fields





How to Search

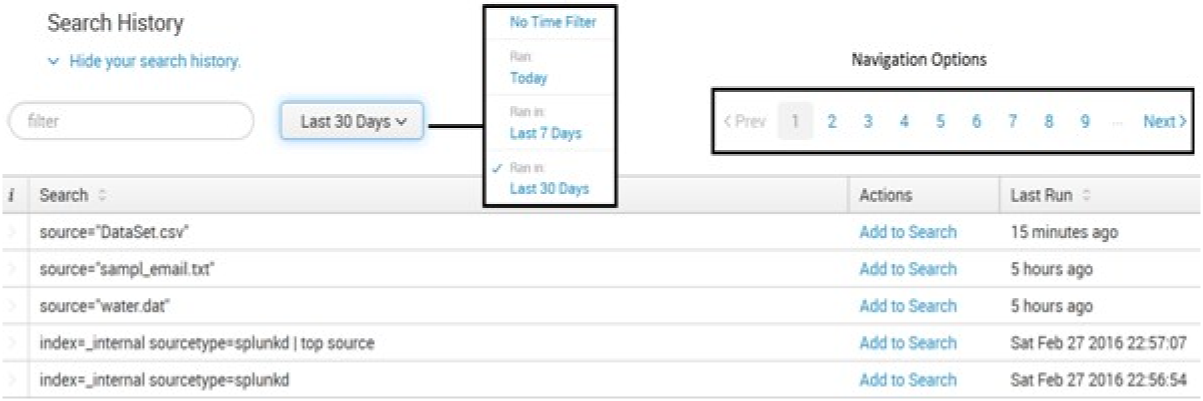
If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.

What to Search

6,061 Events	4 years ago	19 days ago
INDEXED	EARLIEST EVENT	LATEST EVENT

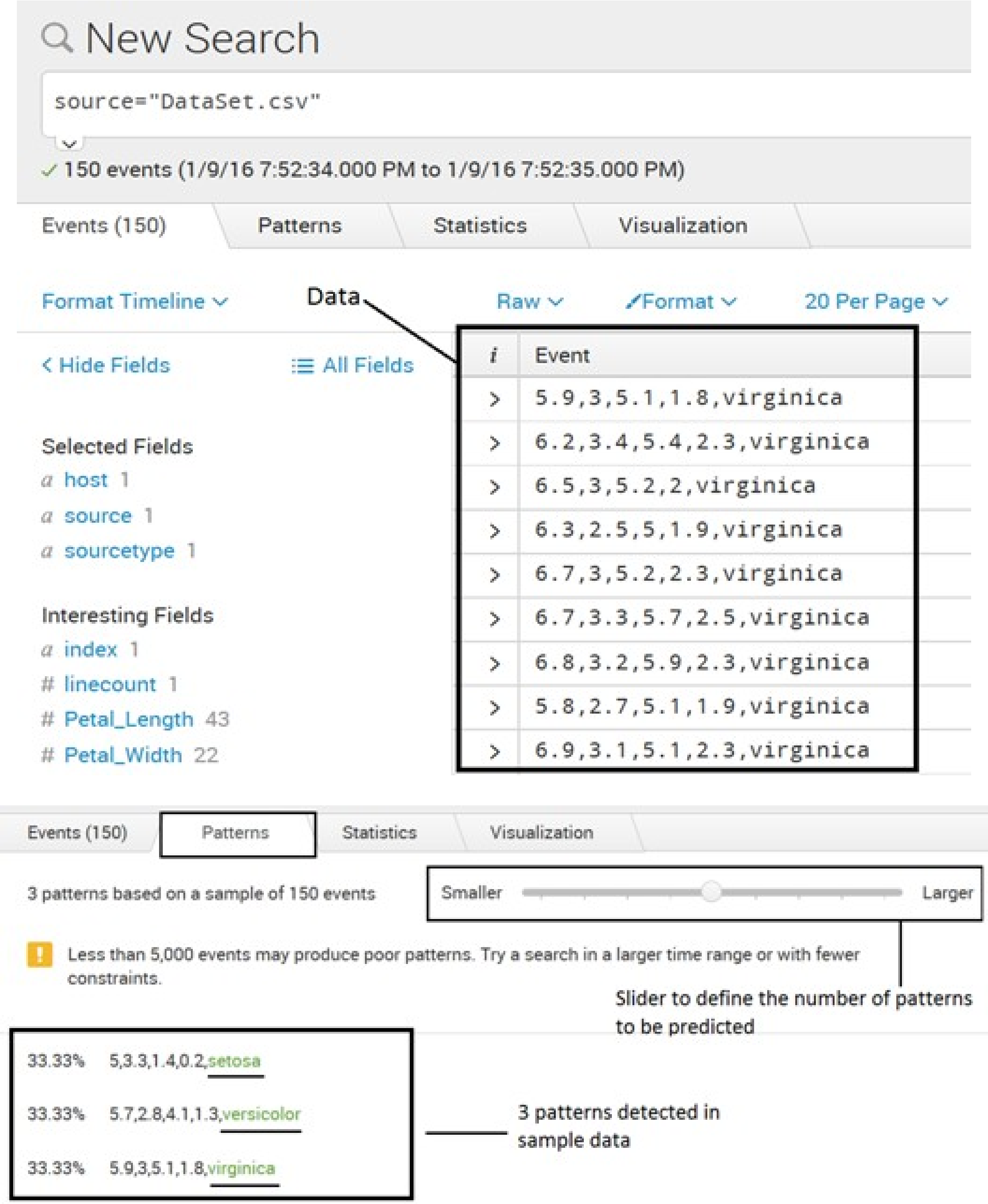
Search History

Search History can be accessed from here



Navigation Options

i	Search	Actions	Last Run
	source="DataSet.csv"	Add to Search	15 minutes ago
	source="sampl_email.txt"	Add to Search	5 hours ago
	source="water.dat"	Add to Search	5 hours ago
	index=_internal sourcetype=splunkd | top source	Add to Search	Sat Feb 27 2016 22:57:07
	index=_internal sourcetype=splunkd	Add to Search	Sat Feb 27 2016 22:56:54



```
source="DataSet.csv"
```

✓ 150 events (1/9/16 7:52:34.000 PM to 1/9/16 7:52:35.000 PM)

Data

```
5.9,3,5.1,1.8,virginica
6.2,3.4,5.4,2.3,virginica
6.5,3,5.2,2,virginica
6.3,2.5,5,1.9,virginica
6.7,3,5.2,2.3,virginica
6.7,3.3,5.7,2.5,virginica
6.8,3.2,5.9,2.3,virginica
5.8,2.7,5.1,1.9,virginica
6.9,3.1,5.1,2.3,virginica
```

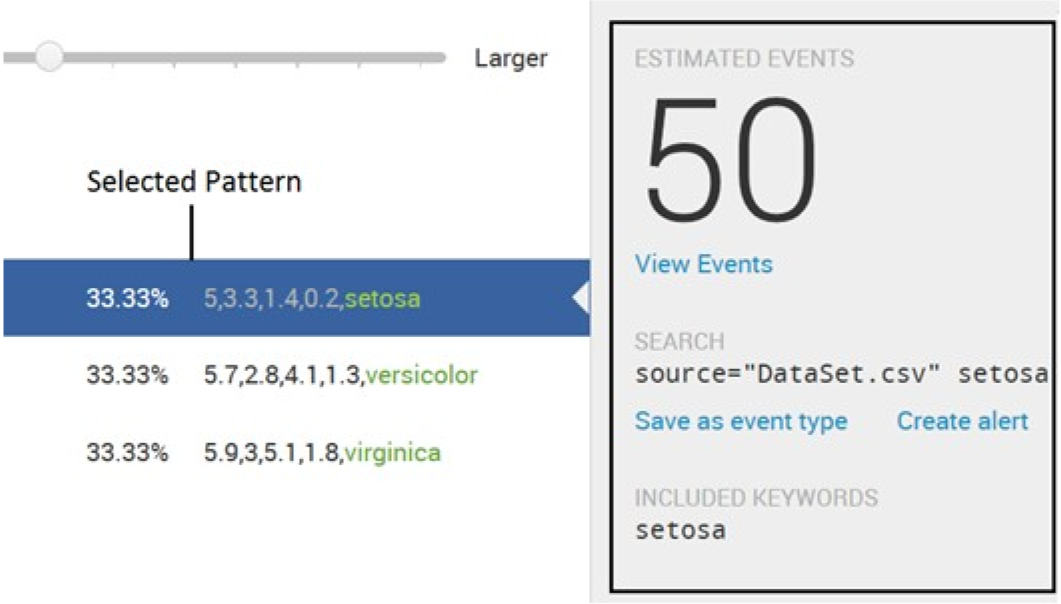
3 patterns based on a sample of 150 events

! Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.

Slider to define the number of patterns to be predicted

```
33.33%   5,3.3,1.4,0.2,setosa
33.33%   5.7,2.8,4.1,1.3,versicolor
33.33%   5.9,3,5.1,1.8,virginica
```

3 patterns detected in sample data



33.33% 5,3.3,1.4,0.2,setosa

33.33% 5.7,2.8,4.1,1.3,versicolor

33.33% 5.9,3,5.1,1.8,virginica

ESTIMATED EVENTS

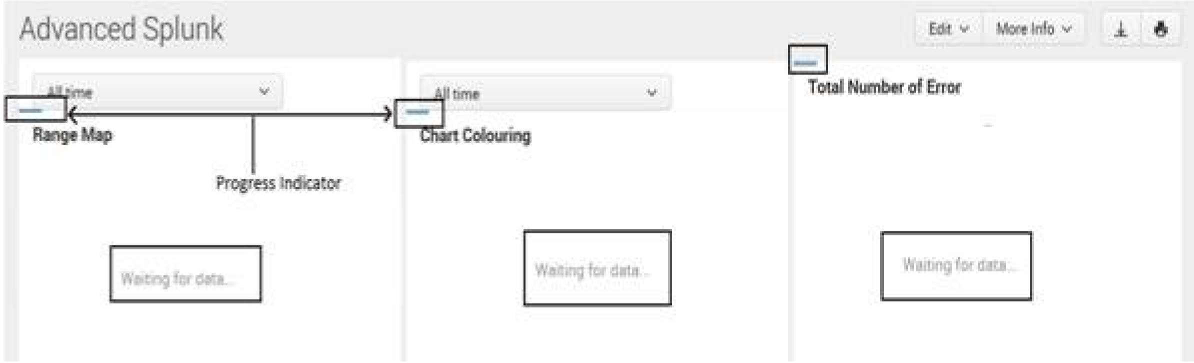
50

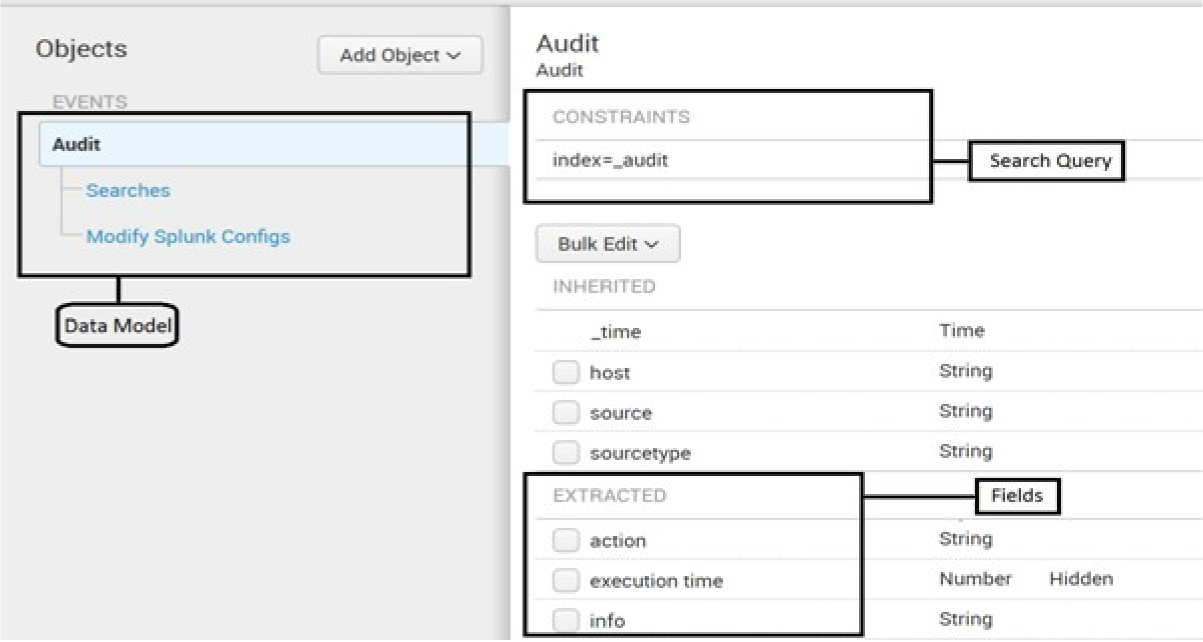
SEARCH

```
source="DataSet.csv" setosa
```

INCLUDED KEYWORDS

setosa

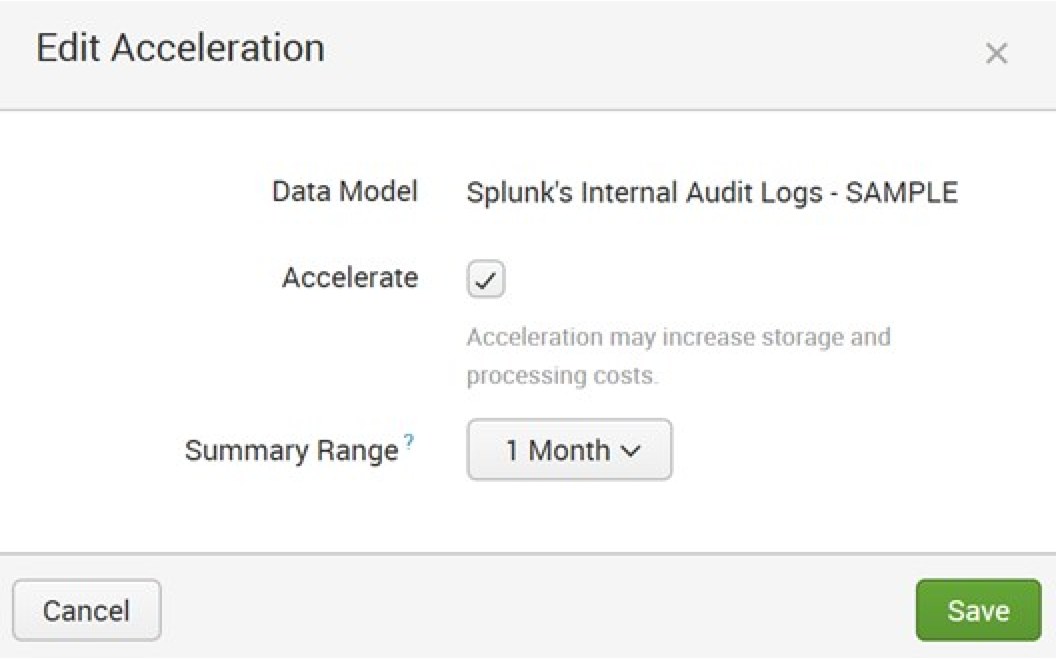




CONSTRAINTS

index=_audit

INHERITED	
_time	Time
□ host	String
□ source	String
□ sourcetype	String
EXTRACTED	
□ action	String
□ execution time	Number Hidden
□ info	String



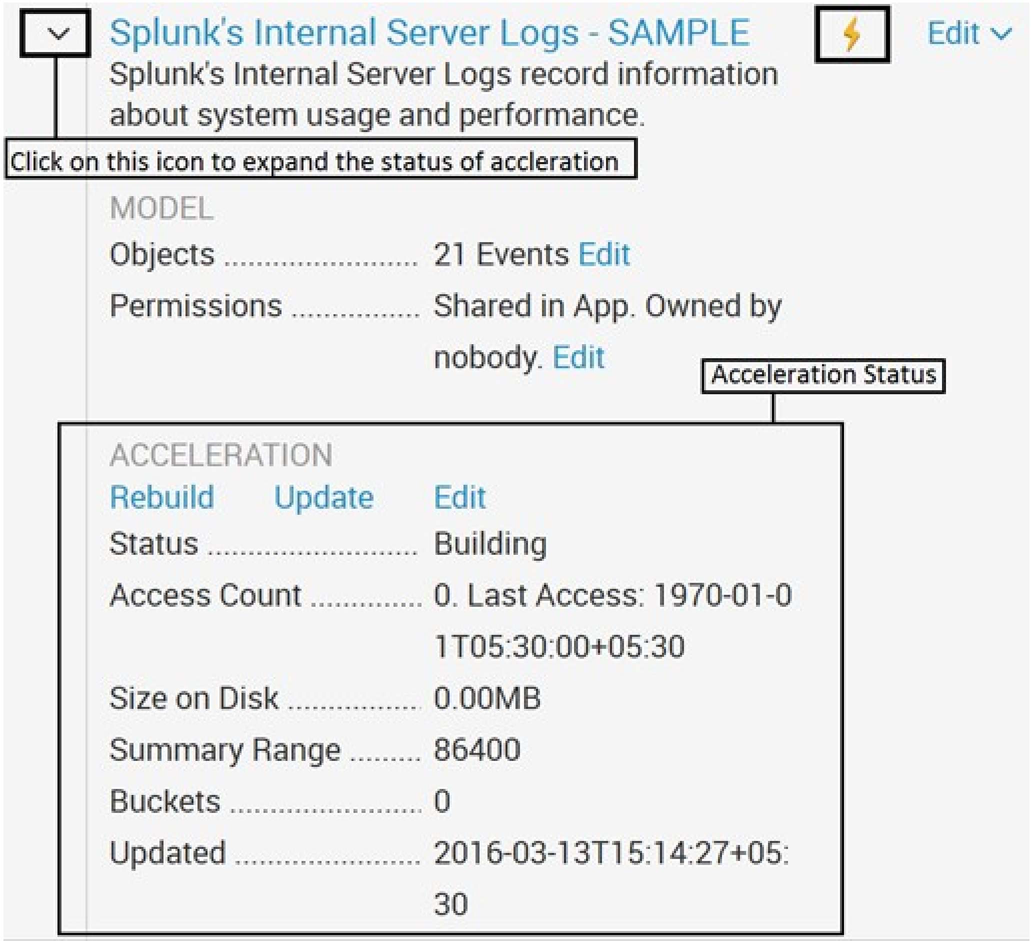
Edit Acceleration

Data Model: Splunk's Internal Audit Logs - SAMPLE

Accelerate: ☑

Acceleration may increase storage and processing costs.

Summary Range ?: 1 Month



Splunk's Internal Server Logs - SAMPLE

Splunk's Internal Server Logs record information about system usage and performance.

Click on this icon to expand the status of accleration

MODEL

Objects .... 21 Events Edit

Permissions .... Shared in App. Owned by nobody. Edit

Acceleration Status

ACCELERATION

Rebuild Update Edit

Status .... Building

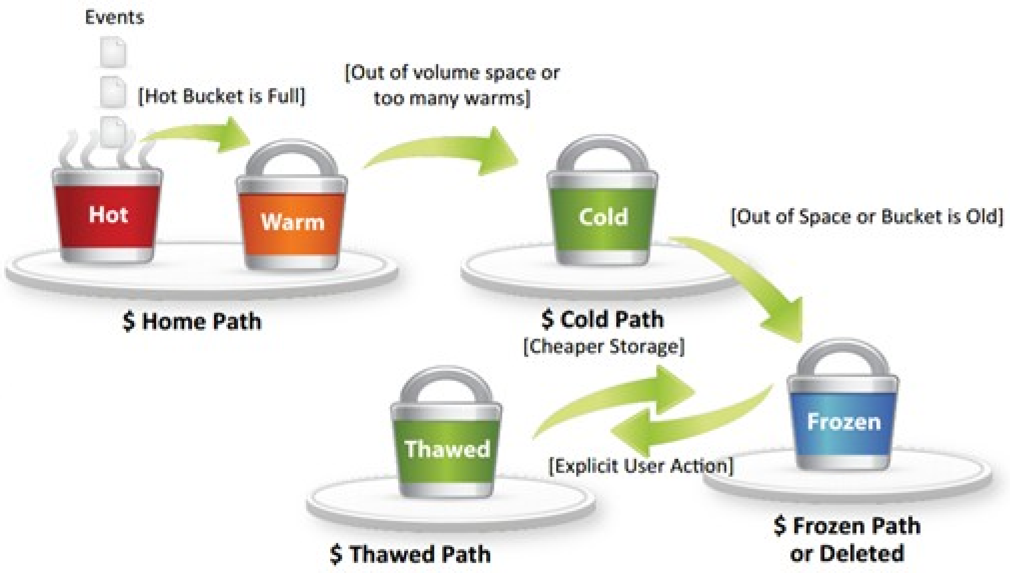
Access Count .... 0. Last Access: 1970-01-01T05:30:00+05:30

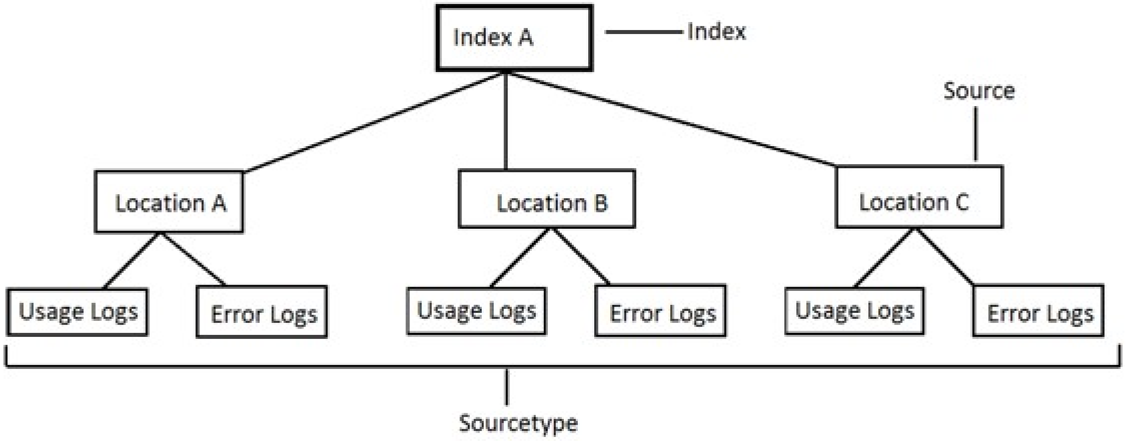
Size on Disk 0.00MB

Summary Range 86400

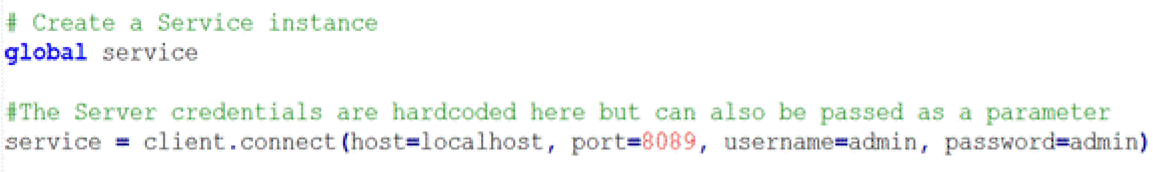
Buckets 0

Updated .... 2016-03-13T15:14:27+05:30

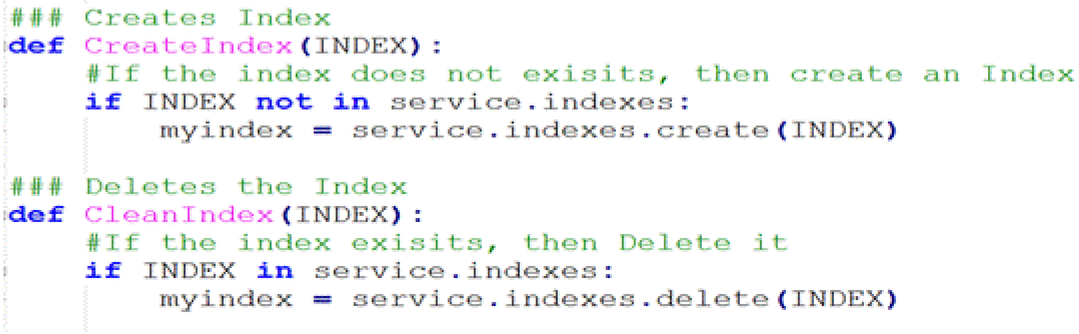

Events
[Hot Bucket is Full]
[Out of volume space or too many warms]
Hot
Warm
Cold
[Out of Space or Bucket is Old]
$ Home Path
$ Cold Path
[Cheaper Storage]
Thawed
Frozen
[Explicit User Action]
$ Thawed Path
$ Frozen Path or Deleted


Index A
Index
Source
Location A
Location B
Location C
Usage Logs
Error Logs
Usage Logs
Error Logs
Usage Logs
Error Logs
Sourcetype

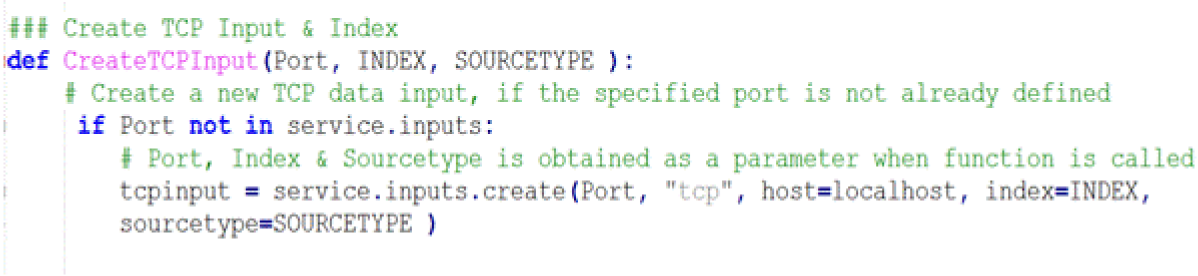
Chapter 11: Enterprise Integration with Splunk



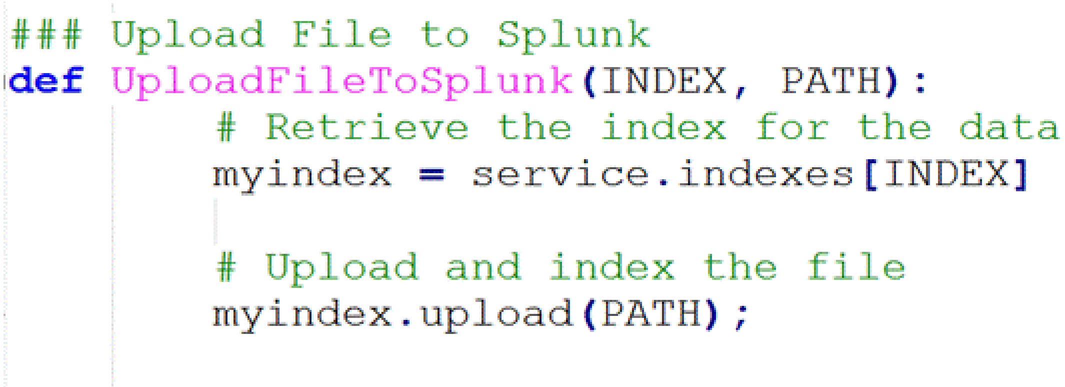
```
# Create a Service instance
global service

#The Server credentials are hardcoded here but can also be passed as a parameter
service = client.connect(host=localhost, port=8089, username=admin, password=admin)
```



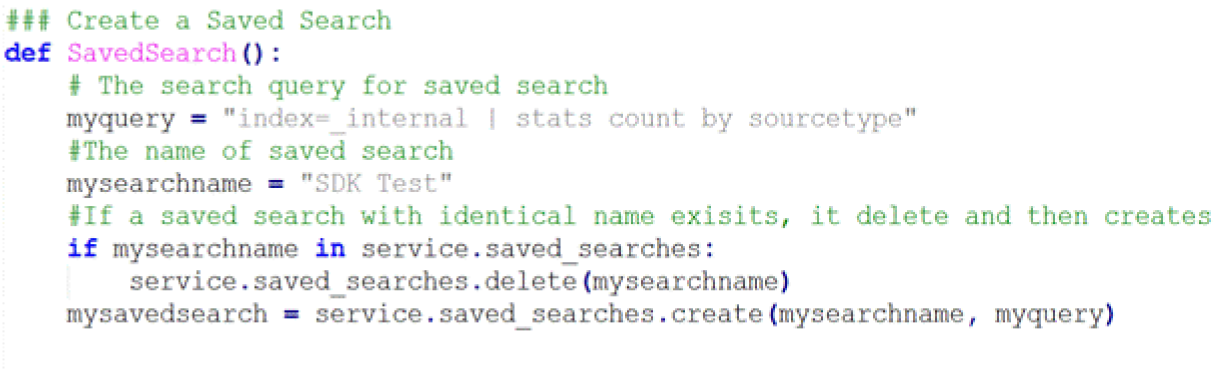
```
### Creates Index
def CreateIndex(INDEX):
    #If the index does not exisits, then create an Index
    if INDEX not in service.indexes:
        myindex = service.indexes.create(INDEX)

### Deletes the Index
def CleanIndex(INDEX):
    #If the index exisits, then Delete it
    if INDEX in service.indexes:
        myindex = service.indexes.delete(INDEX)
```



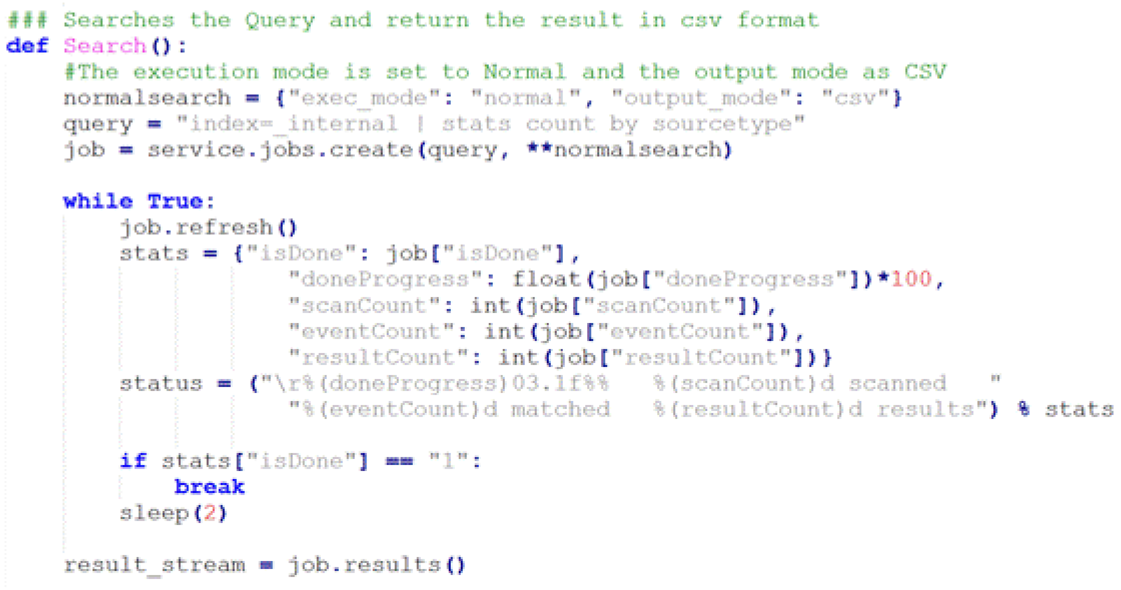
```
### Create TCP Input & Index
def CreateTCPInput(Port, INDEX, SOURCETYPE ):
    # Create a new TCP data input, if the specified port is not already defined
     if Port not in service.inputs:
        # Port, Index & Sourcetype is obtained as a parameter when function is called
        tcpinput = service.inputs.create(Port, "tcp", host=localhost, index=INDEX,
        sourcetype=SOURCETYPE )
```



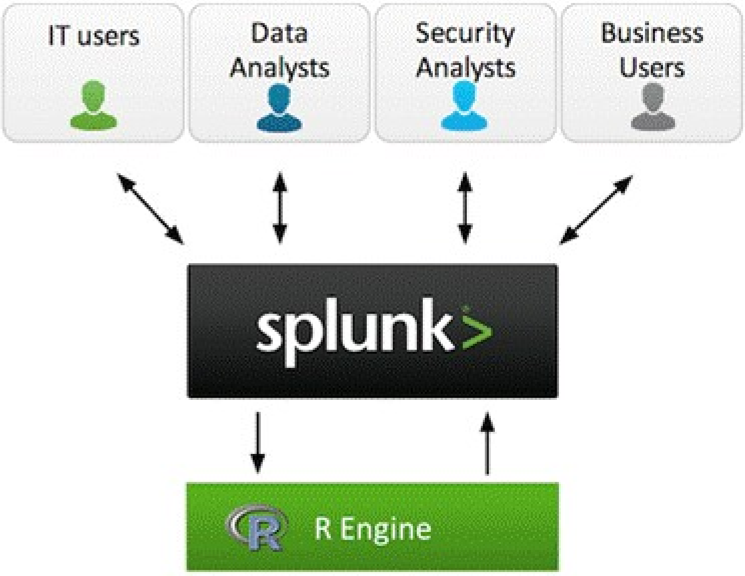
```
### Upload File to Splunk
def UploadFileToSplunk(INDEX, PATH):
        # Retrieve the index for the data
        myindex = service.indexes[INDEX]

        # Upload and index the file
        myindex.upload(PATH);
```

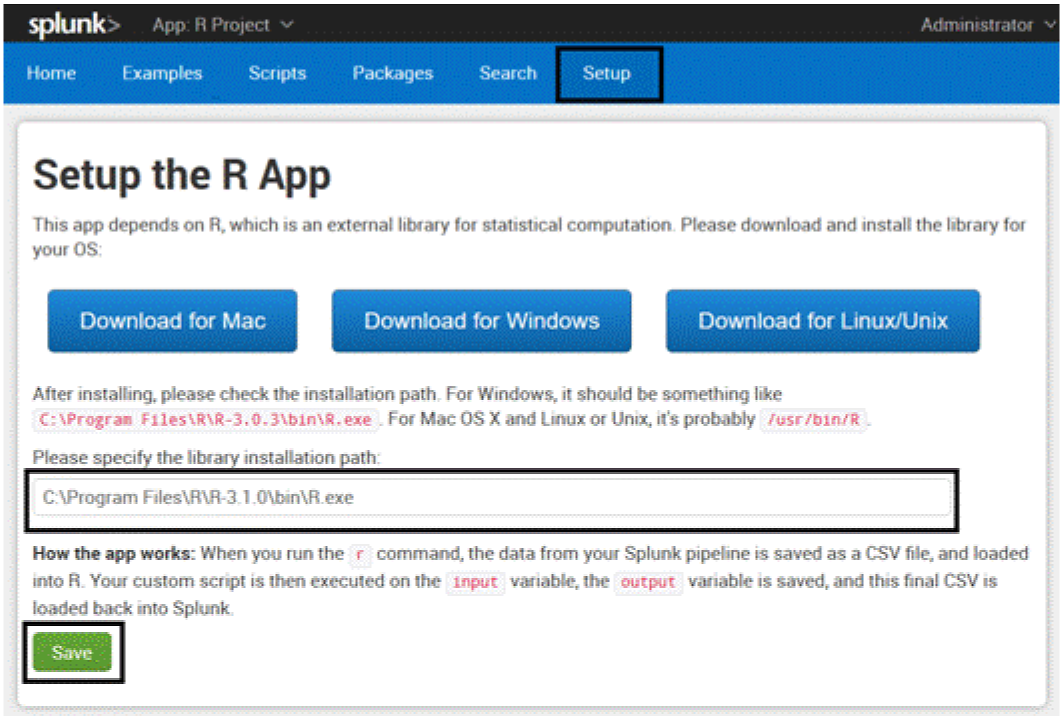


```
### Create a Saved Search
def SavedSearch():
    # The search query for saved search
    myquery = "index=_internal | stats count by sourcetype"
    #The name of saved search
    mysearchname = "SDK Test"
    #If a saved search with identical name exisits, it delete and then creates
    if mysearchname in service.saved_searches:
        service.saved_searches.delete(mysearchname)
    mysavedsearch = service.saved_searches.create(mysearchname, myquery)
```



```
### Searches the Query and return the result in csv format
def Search():
    #The execution mode is set to Normal and the output mode as CSV
    normalsearch = {"exec_mode": "normal", "output_mode": "csv"}
    query = "index=_internal | stats count by sourcetype"
    job = service.jobs.create(query, **normalsearch)

    while True:
        job.refresh()
        stats = {"isDone": job["isDone"],
                    "doneProgress": float(job["doneProgress"])*100,
                    "scanCount": int(job["scanCount"]),
                    "eventCount": int(job["eventCount"]),
                    "resultCount": int(job["resultCount"])}
        status = ("\r%(doneProgress)03.1f%%    %(scanCount)d scanned    "
                    "%(eventCount)d matched    %(resultCount)d results") % stats

        if stats["isDone"] == "1":
            break
        sleep(2)

    result_stream = job.results()
```





Setup the R App

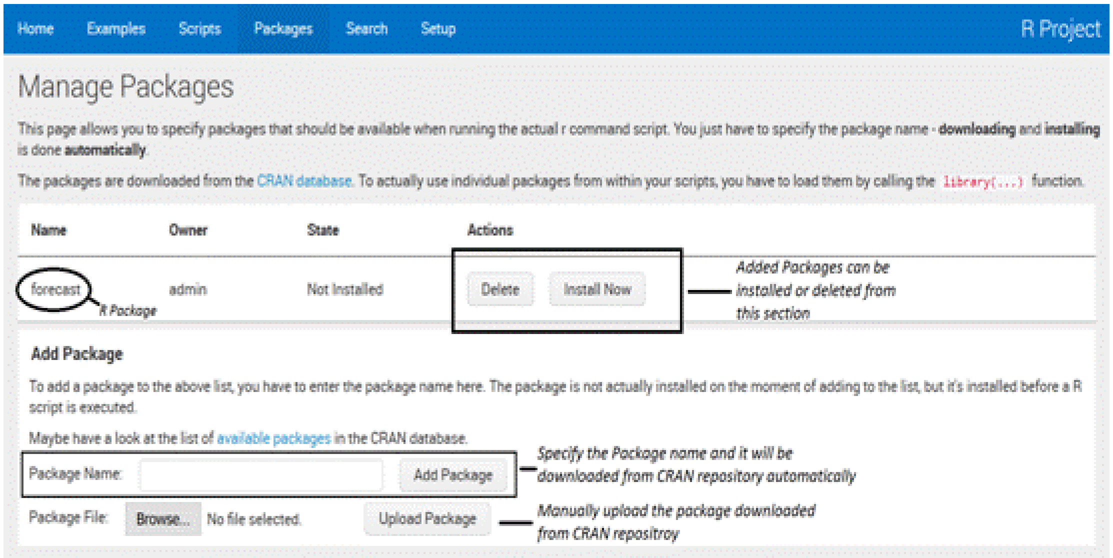
This app depends on R, which is an external library for statistical computation. Please download and install the library for your OS:

After installing, please check the installation path. For Windows, it should be something like `C:\Program Files\R\R-3.0.3\bin\R.exe`. For Mac OS X and Linux or Unix, it's probably `/usr/bin/R`.

Please specify the library installation path:

C:\Program Files\R\R-3.1.0\bin\R.exe

How the app works: When you run the `r` command, the data from your Splunk pipeline is saved as a CSV file, and loaded into R. Your custom script is then executed on the `input` variable, the `output` variable is saved, and this final CSV is loaded back into Splunk.



Manage Packages

This page allows you to specify packages that should be available when running the actual r command script. You just have to specify the package name - **downloading** and **installing** is done **automatically**.

The packages are downloaded from the CRAN database. To actually use individual packages from within your scripts, you have to load them by calling the `library(...)` function.

Name	Owner	State	Actions
forecast	admin	Not Installed	Delete Install Now

R Package

Added Packages can be installed or deleted from this section

Add Package

To add a package to the above list, you have to enter the package name here. The package is not actually installed on the moment of adding to the list, but it's installed before a R script is executed.

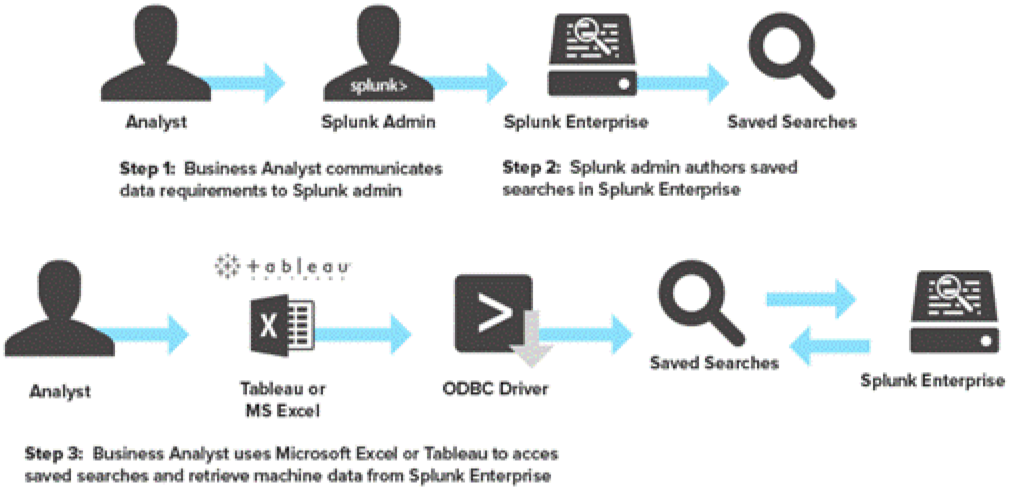
Maybe have a look at the list of available packages in the CRAN database.

Package Name: Add Package

Specify the Package name and it will be downloaded from CRAN repository automatically

Package File: Browse... No file selected. Upload Package

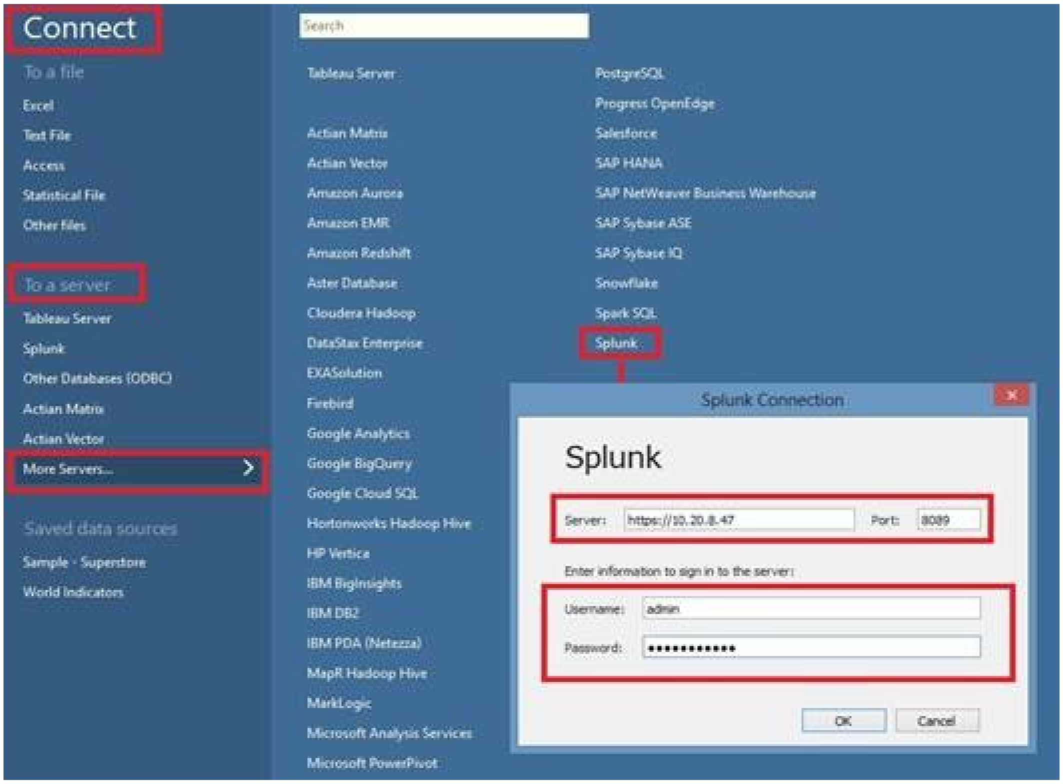
Manually upload the package downloaded from CRAN repositroy



Step 1: Business Analyst communicates data requirements to Splunk admin

Step 2: Splunk admin authors saved searches in Splunk Enterprise

Step 3: Business Analyst uses Microsoft Excel or Tableau to acces saved searches and retrieve machine data from Splunk Enterprise



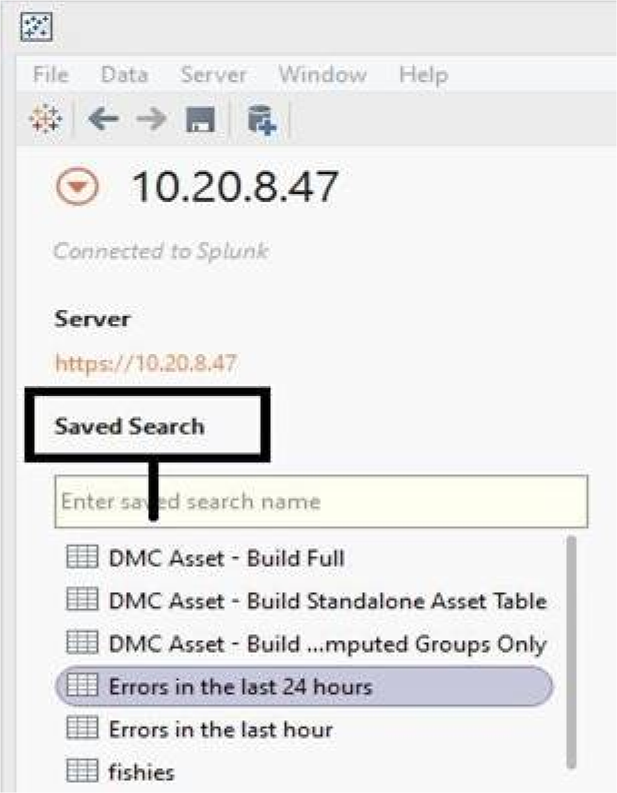
Splunk

Server: https://10.20.8.47 Port: 8089

Enter information to sign in to the server:

Username: admin

Password: ●●●●●●●●●●●●



10.20.8.47

Connected to Splunk

Server

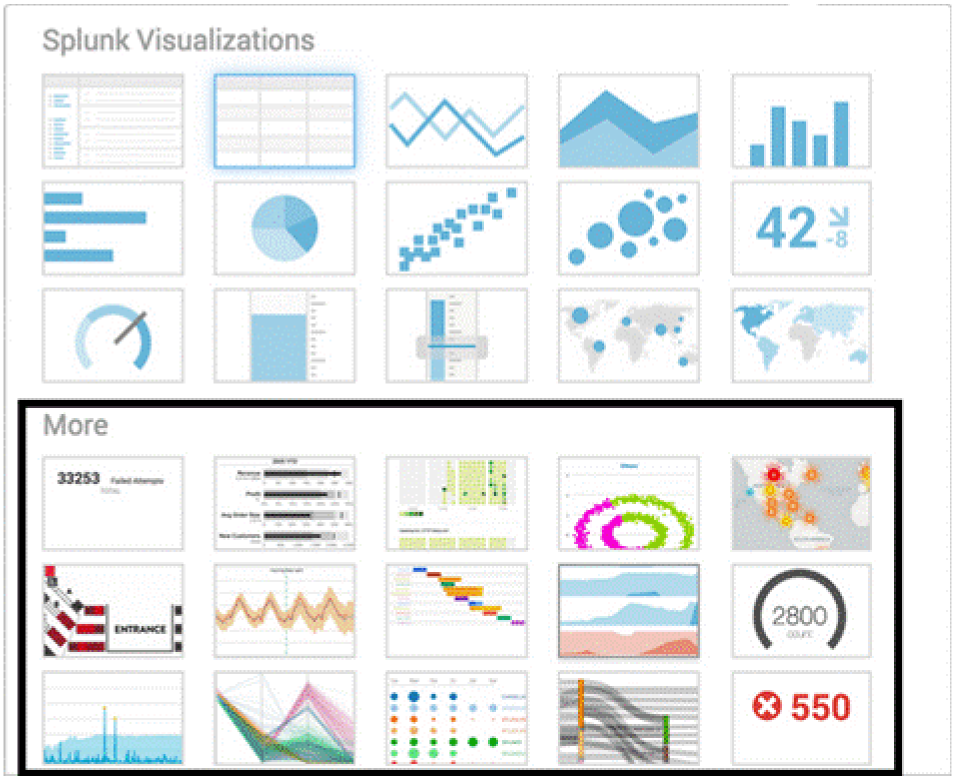
https://10.20.8.47

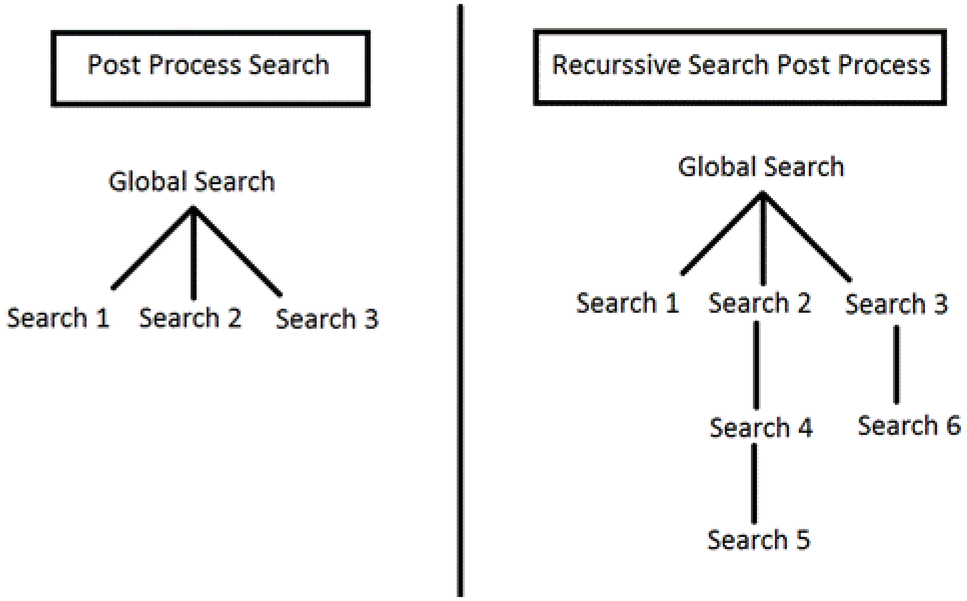
Saved Search

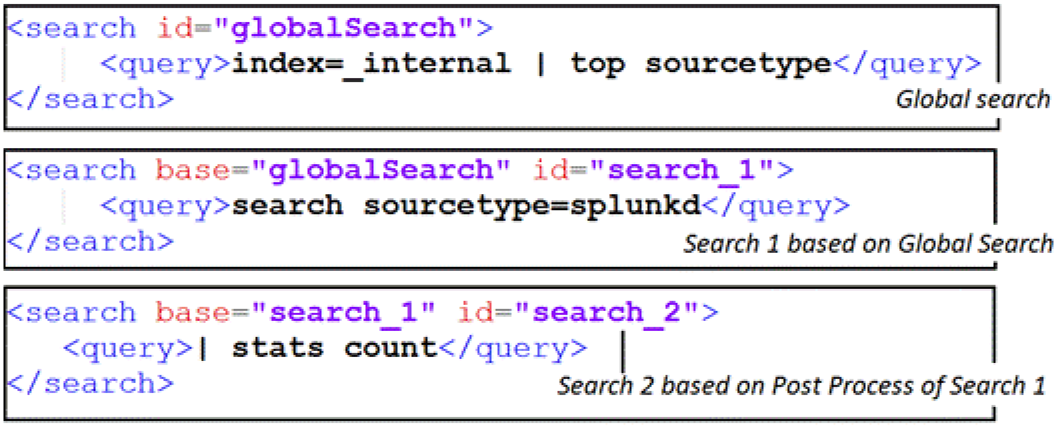
Enter saved search name

- DMC Asset - Build Full
- DMC Asset - Build Standalone Asset Table
- DMC Asset - Build ...mputed Groups Only
- Errors in the last 24 hours
- Errors in the last hour
- fishies

Chapter 12: What's Next? Splunk 6.4







```
<search id="globalSearch">
    <query>index=_internal | top sourcetype</query>
</search>
```

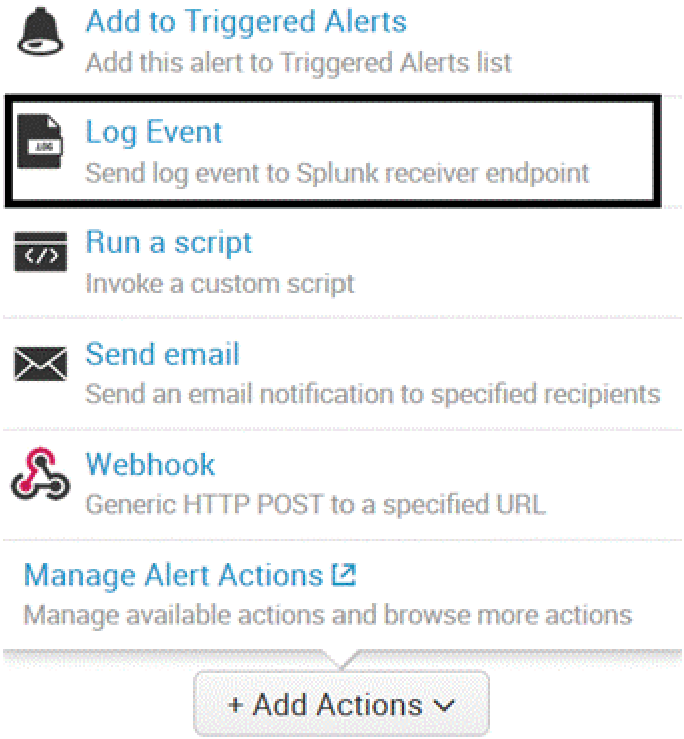
Global search

```
<search base="globalSearch" id="search_1">
    <query>search sourcetype=splunkd</query>
</search>
```

Search 1 based on Global Search

```
<search base="search_1" id="search_2">
  <query>| stats count</query>
</search>
```

Search 2 based on Post Process of Search 1



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