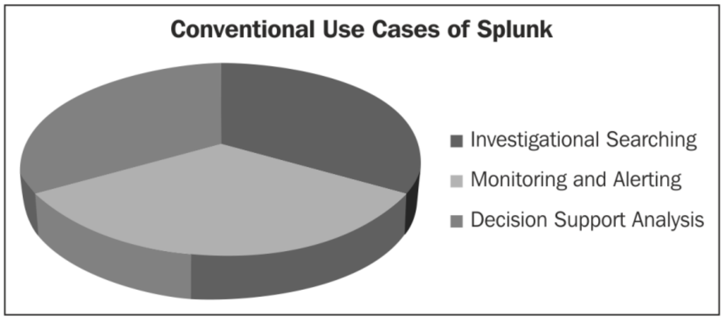
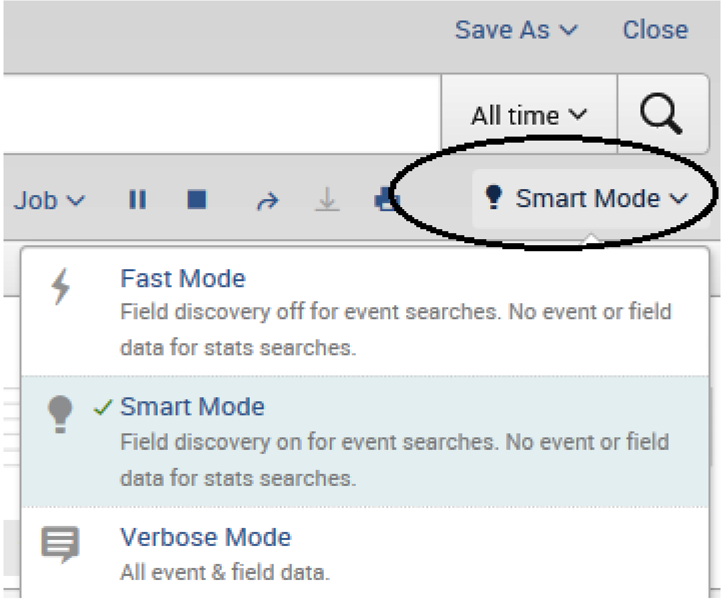
Chapter 1, *The Application of Splunk*



Chapter 2, *Advanced Searching*



Fast Mode

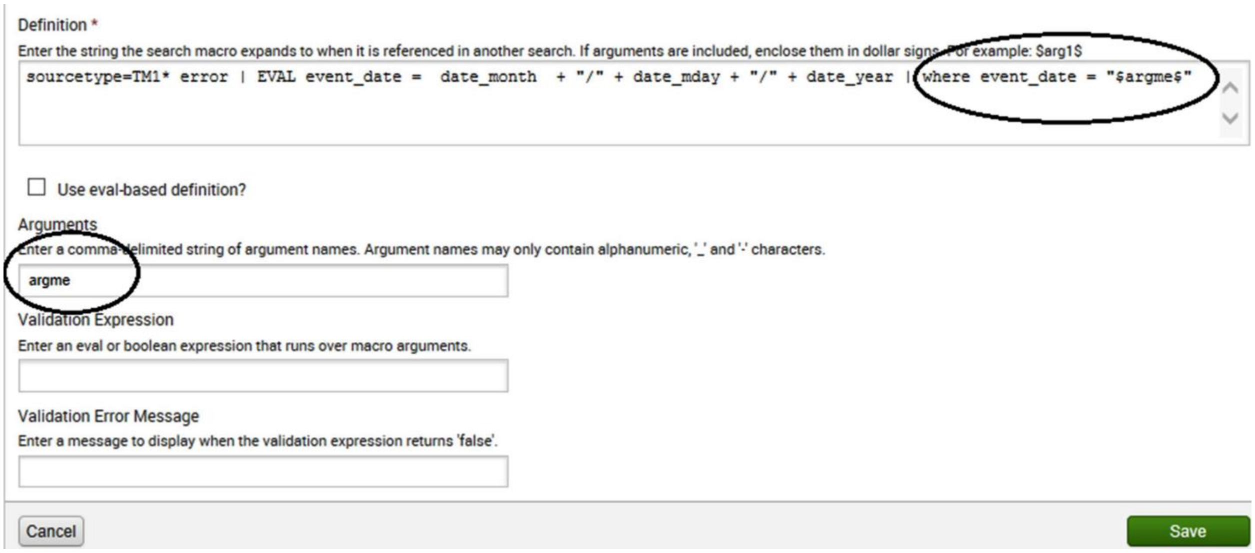
Field discovery off for event searches. No event or field data for stats searches.

✓ Smart Mode

Field discovery on for event searches. No event or field data for stats searches.

Verbose Mode

All event & field data.



Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
sourcetype=TM1* error | EVAL event_date =  date_month  + "/" + date_mday + "/" + date_year | where event_date = "$argme$"
```

☐ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

argme

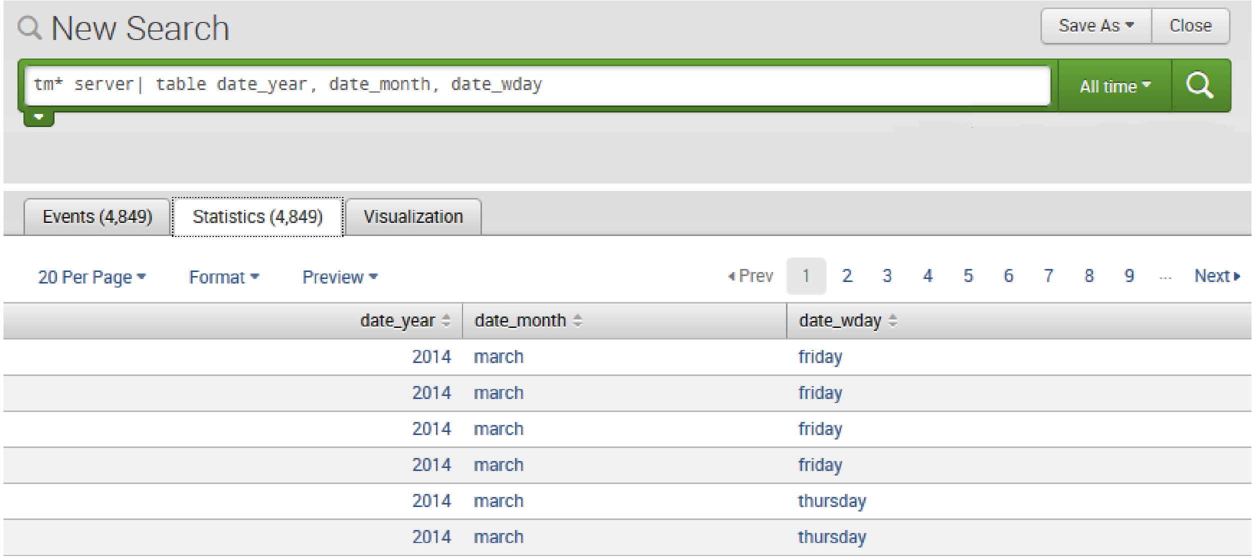
Validation Expression

Enter an eval or boolean expression that runs over macro arguments.

Validation Error Message

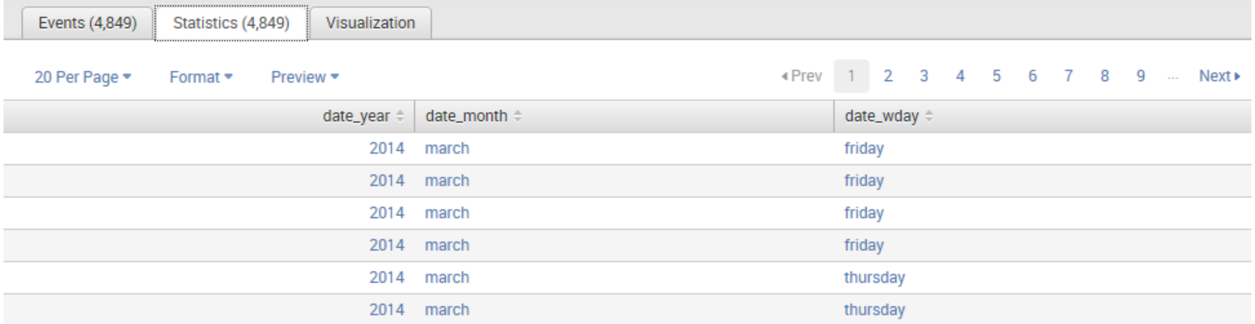
Enter a message to display when the validation expression returns 'false'.

Chapter 3, *Mastering Tables, Charts, and Fields*

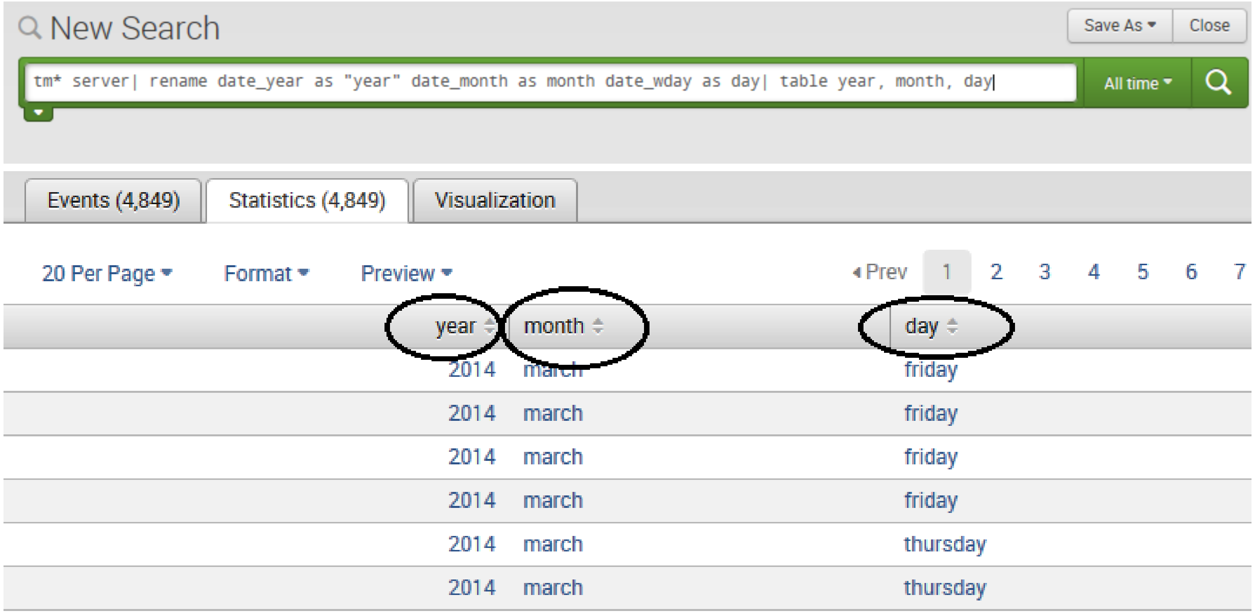


```
tm* server| table date_year, date_month, date_wday
```

date_year	date_month	date_wday
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	thursday
2014	march	thursday

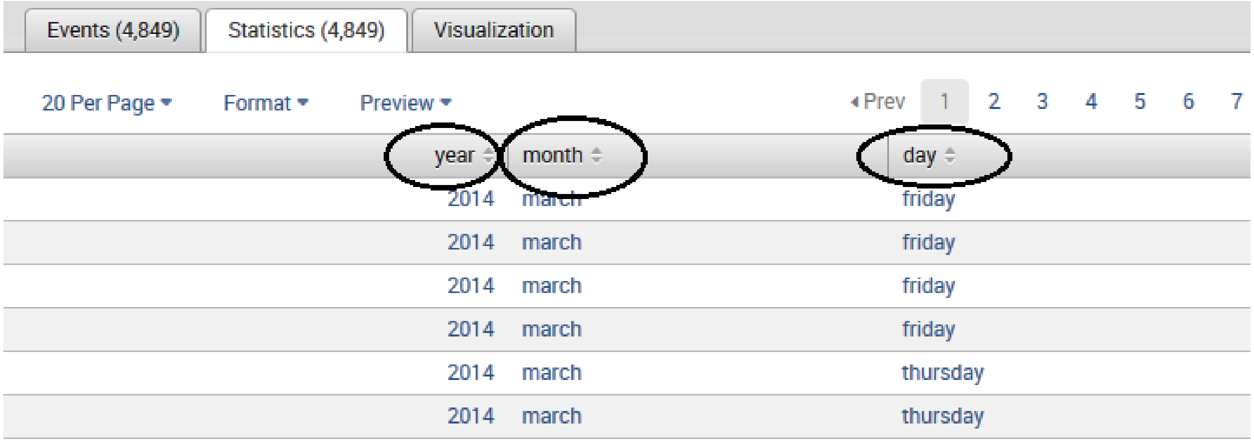


date_year	date_month	date_wday
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	thursday
2014	march	thursday

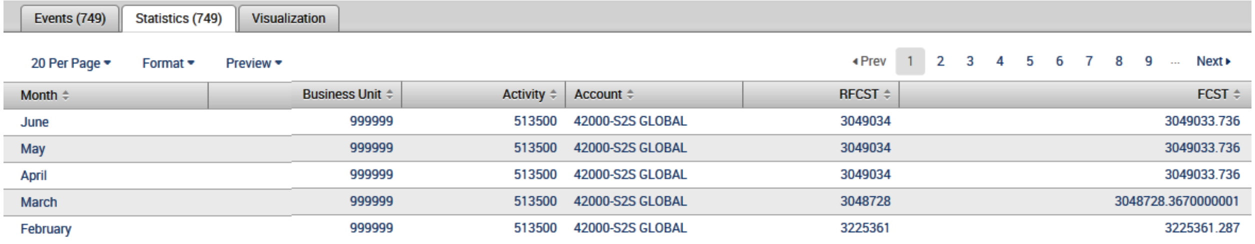


```
tm* server| rename date_year as "year" date_month as month date_wday as day| table year, month, day
```

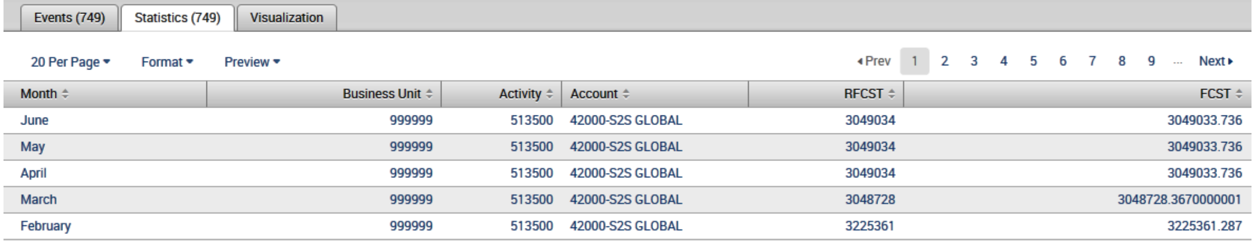
year	month	day
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	thursday
2014	march	thursday



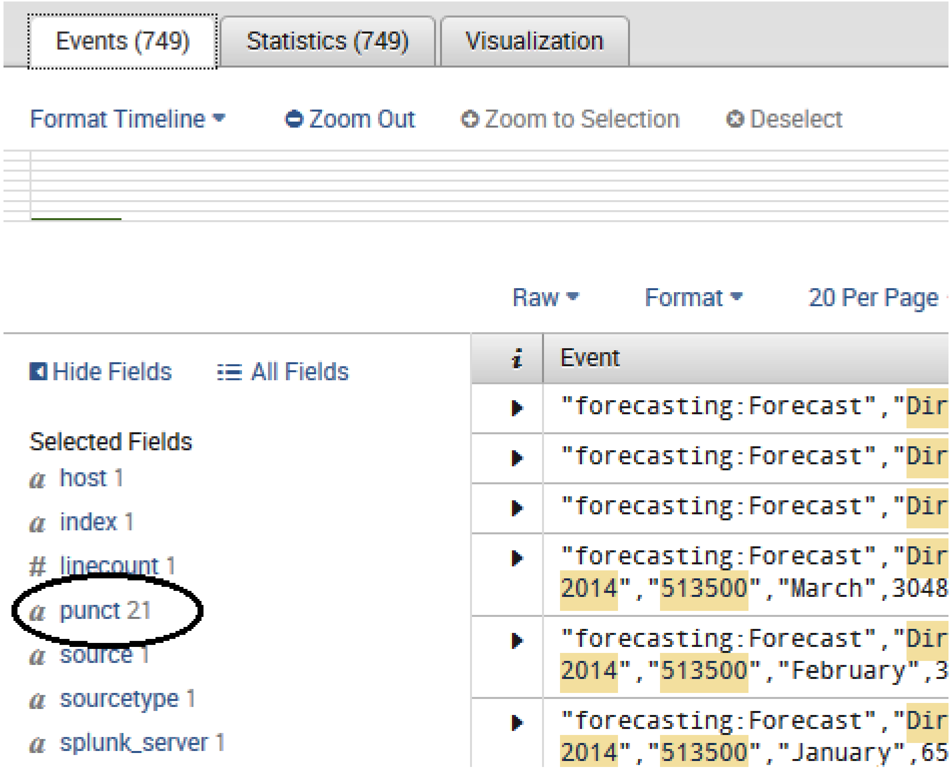
year	month	day
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	friday
2014	march	thursday
2014	march	thursday



Month	Business Unit	Activity	Account	RFCST	FCST
June	999999	513500	42000-S2S GLOBAL	3049034	3049033.736
May	999999	513500	42000-S2S GLOBAL	3049034	3049033.736
April	999999	513500	42000-S2S GLOBAL	3049034	3049033.736
March	999999	513500	42000-S2S GLOBAL	3048728	3048728.3670000001
February	999999	513500	42000-S2S GLOBAL	3225361	3225361.287



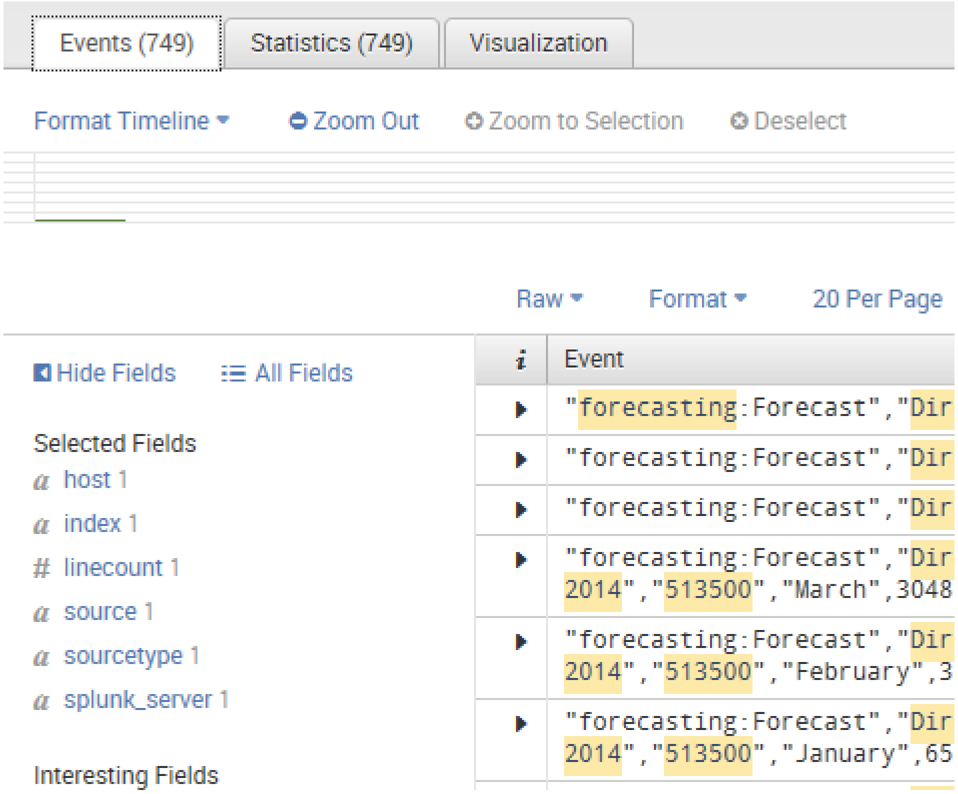
Month	Business Unit	Activity	Account	RFCST	FCST
June	999999	513500	42000-S2S GLOBAL	3049034	3049033.736
May	999999	513500	42000-S2S GLOBAL	3049034	3049033.736
April	999999	513500	42000-S2S GLOBAL	3049034	3049033.736
March	999999	513500	42000-S2S GLOBAL	3048728	3048728.3670000001
February	999999	513500	42000-S2S GLOBAL	3225361	3225361.287



Selected Fields

a	host 1
a	index 1
#	linecount 1
a	punct 21
a	source 1
a	sourcetype 1
a	splunk_server 1

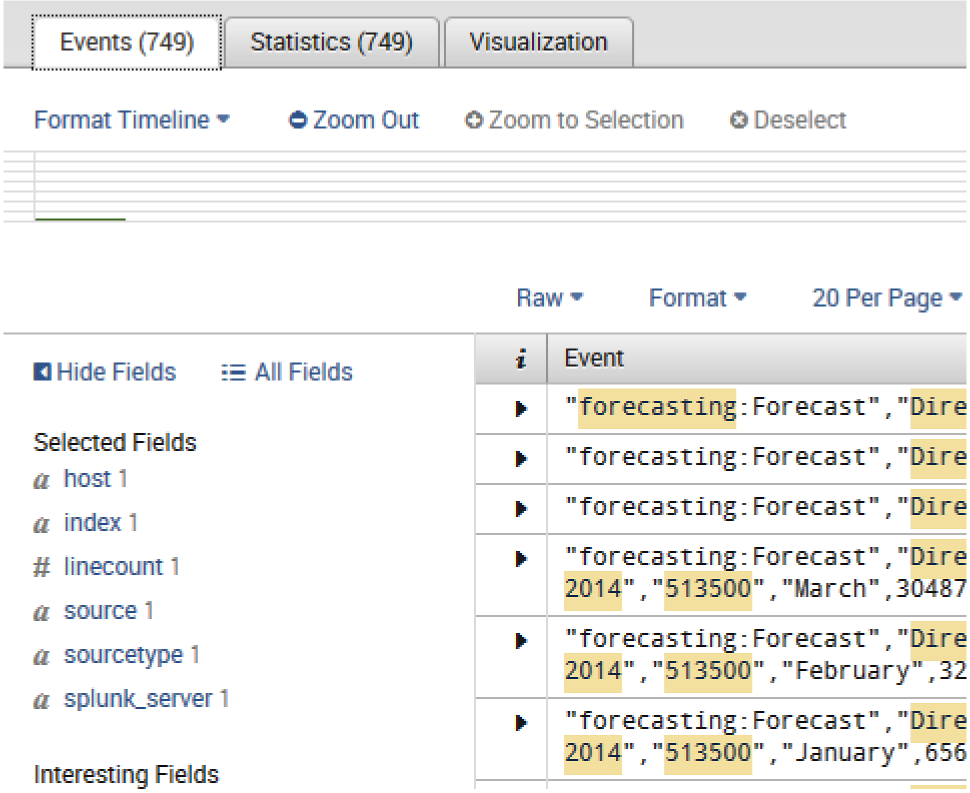
```
"forecasting:Forecast","Dir
"forecasting:Forecast","Dir
"forecasting:Forecast","Dir
"forecasting:Forecast","Dir
2014","513500","March",3048
"forecasting:Forecast","Dir
2014","513500","February",3
"forecasting:Forecast","Dir
2014","513500","January",65
```



Selected Fields
a host 1
a index 1
# linecount 1
a source 1
a sourcetype 1
a splunk_server 1

Interesting Fields

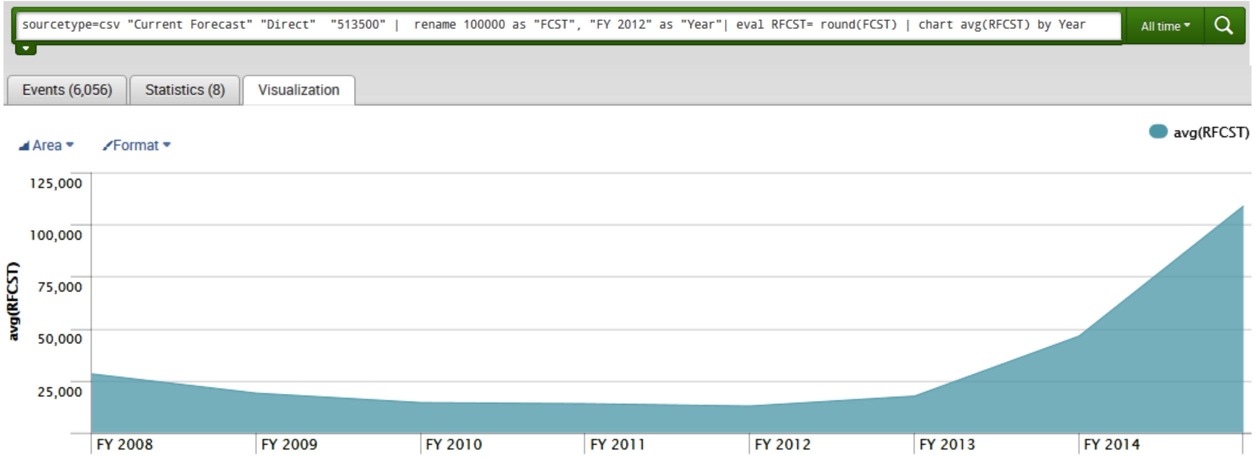
```
i  Event
   "forecasting:Forecast","Dir
   "forecasting:Forecast","Dir
   "forecasting:Forecast","Dir
   "forecasting:Forecast","Dir
   2014","513500","March",3048
   "forecasting:Forecast","Dir
   2014","513500","February",3
   "forecasting:Forecast","Dir
   2014","513500","January",65
```


Events (749)
Statistics (749)
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
Raw
Format
20 Per Page
Hide Fields
All Fields

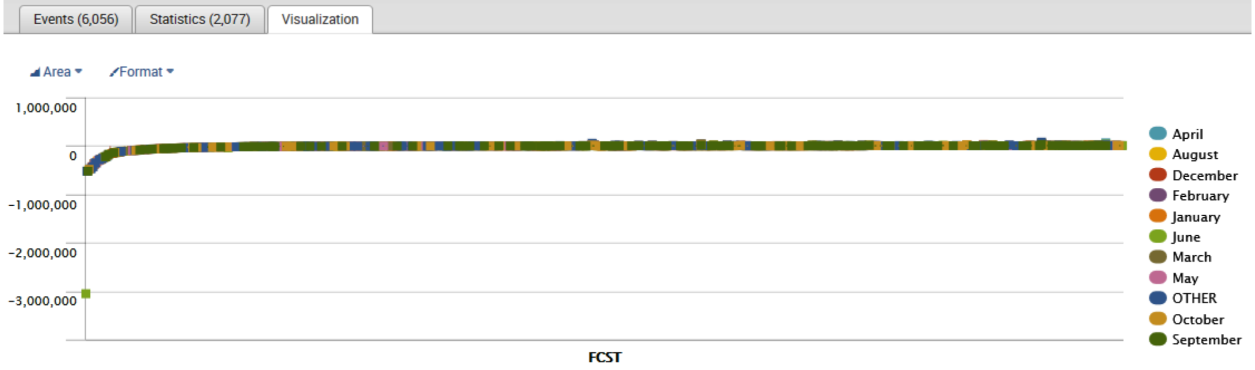
Selected Fields
a host 1
a index 1
# linecount 1
a source 1
a sourcetype 1
a splunk_server 1

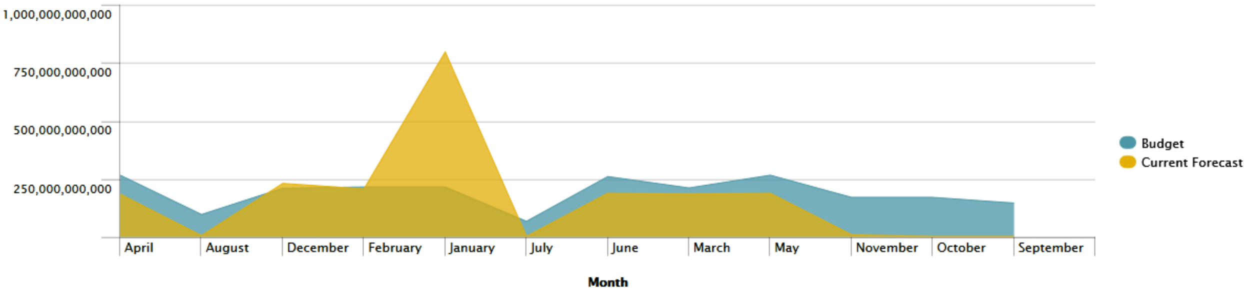
Interesting Fields

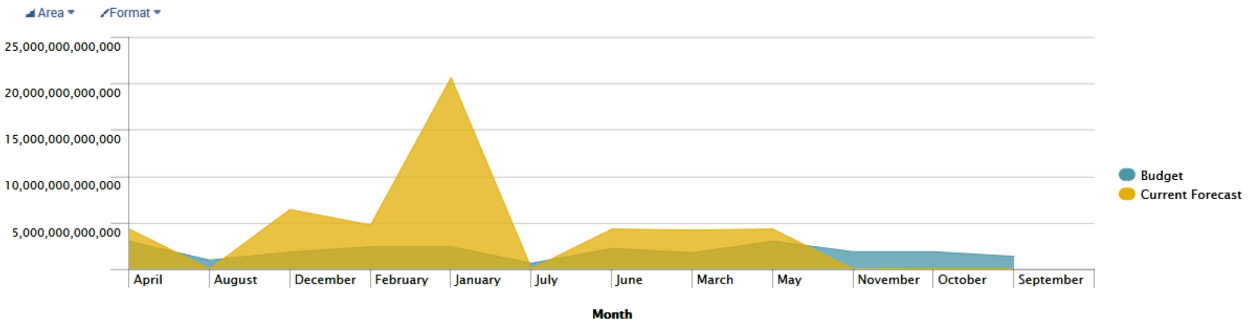
```
i  Event
   "forecasting:Forecast","Dire
   "forecasting:Forecast","Dire
   "forecasting:Forecast","Dire
   "forecasting:Forecast","Dire
   2014","513500","March",30487
   "forecasting:Forecast","Dire
   2014","513500","February",32
   "forecasting:Forecast","Dire
   2014","513500","January",656
```

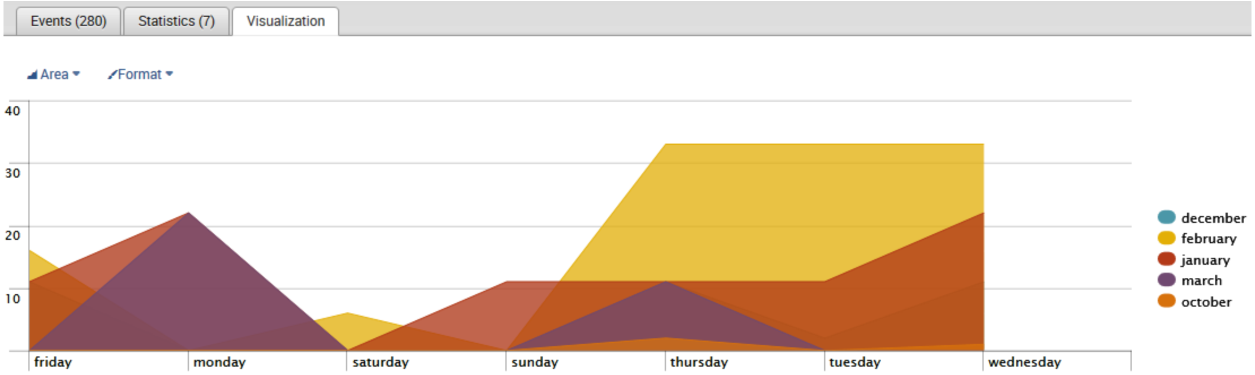


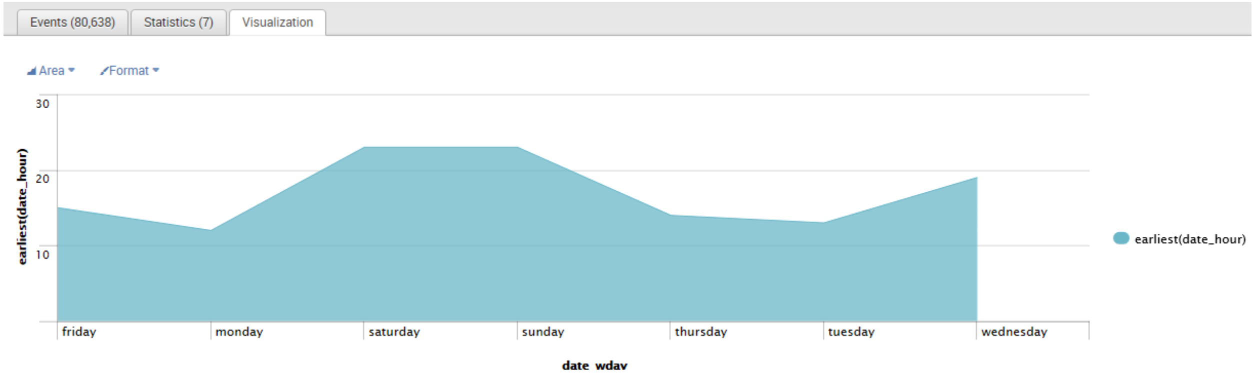
```
sourcetype=csv "Current Forecast" "Direct"  "513500" |  rename 100000 as "FCST", "FY 2012" as "Year"| eval RFCST= round(FCST) | chart avg(RFCST) by Year
```

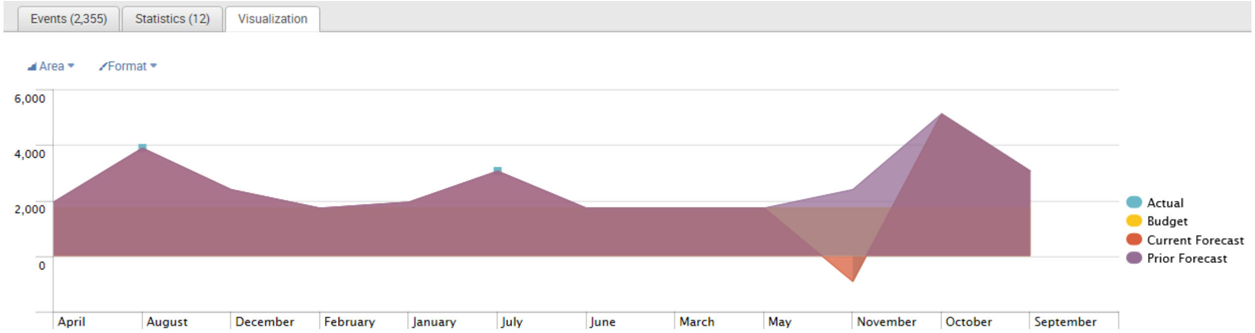


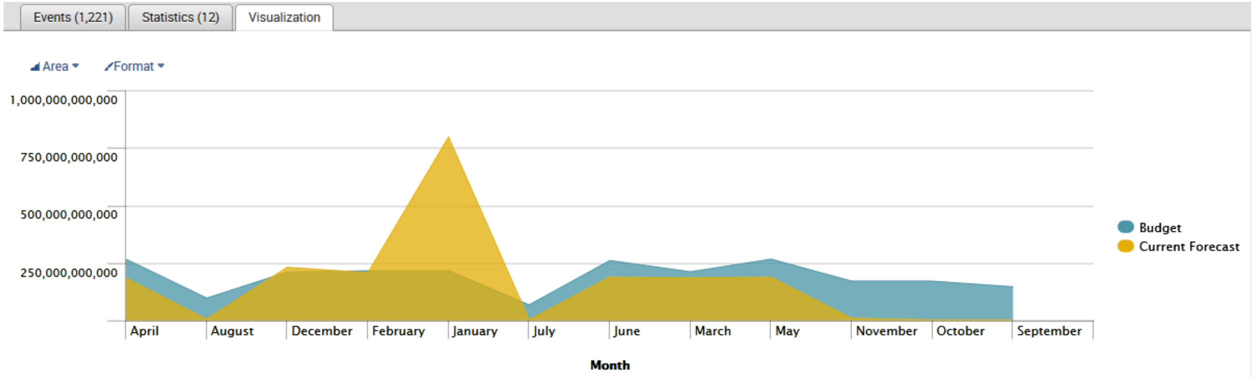


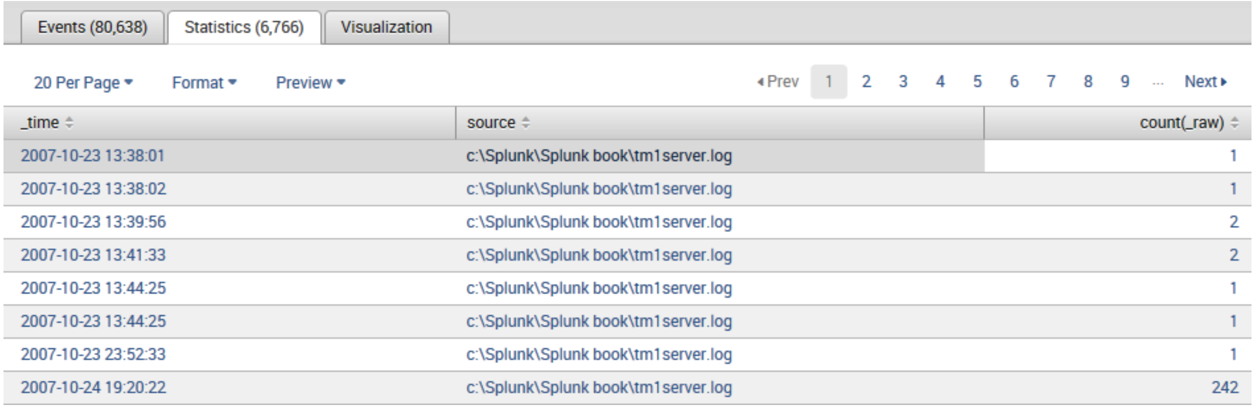



Events (280)
Statistics (7)
Visualization
Area
Format
40
30
20
10
friday
monday
saturday
sunday
thursday
tuesday
wednesday
december
february
january
march
october

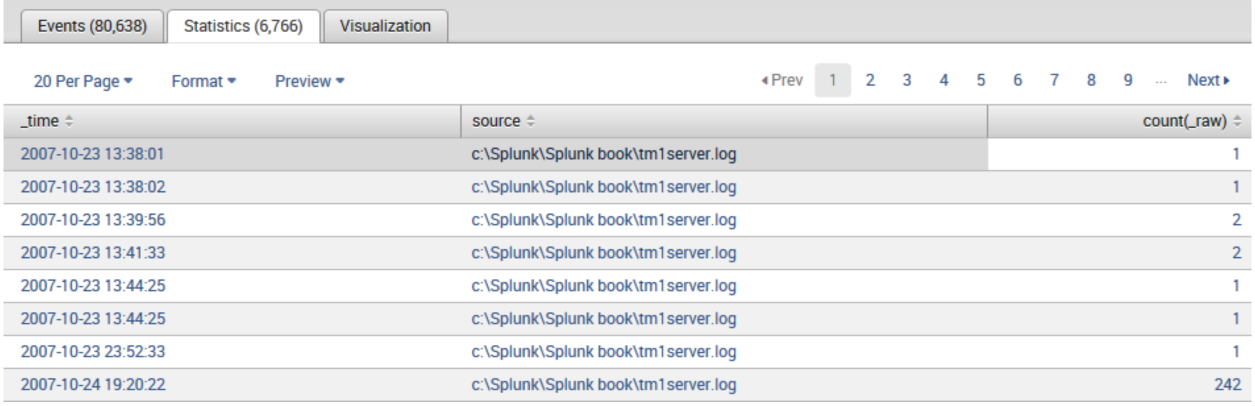

Events (80,638)
Statistics (7)
Visualization
Area
Format
earliest(date_hour)
30
20
10
friday
monday
saturday
sunday
thursday
tuesday
wednesday
date_wday
earliest(date_hour)


Events (2,355)
Statistics (12)
Visualization
Area
Format
6,000
4,000
2,000
0
April
August
December
February
January
July
June
March
May
November
October
September
Actual
Budget
Current Forecast
Prior Forecast

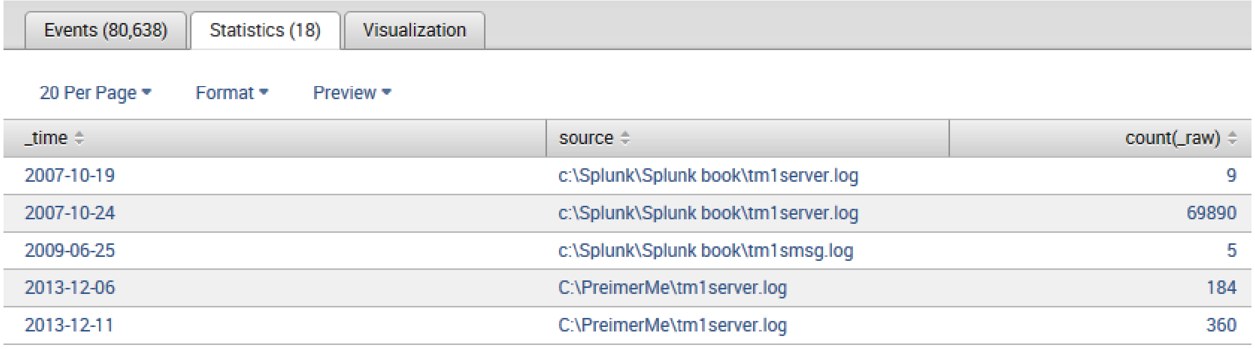

Events (1,221)
Statistics (12)
Visualization
Area
Format
1,000,000,000,000
750,000,000,000
500,000,000,000
250,000,000,000
April
August
December
February
January
July
June
March
May
November
October
September
Month
Budget
Current Forecast



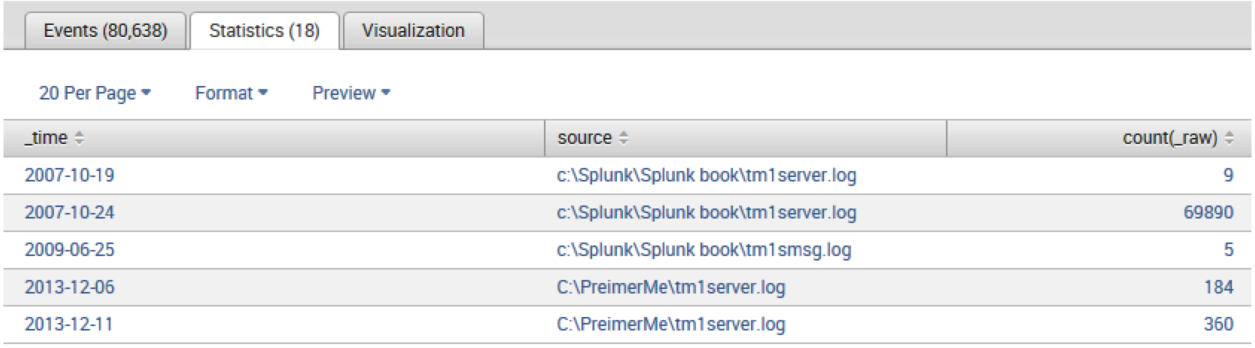
_time	source	count(_raw)
2007-10-23 13:38:01	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 13:38:02	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 13:39:56	c:\Splunk\Splunk book\tm1server.log	2
2007-10-23 13:41:33	c:\Splunk\Splunk book\tm1server.log	2
2007-10-23 13:44:25	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 13:44:25	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 23:52:33	c:\Splunk\Splunk book\tm1server.log	1
2007-10-24 19:20:22	c:\Splunk\Splunk book\tm1server.log	242



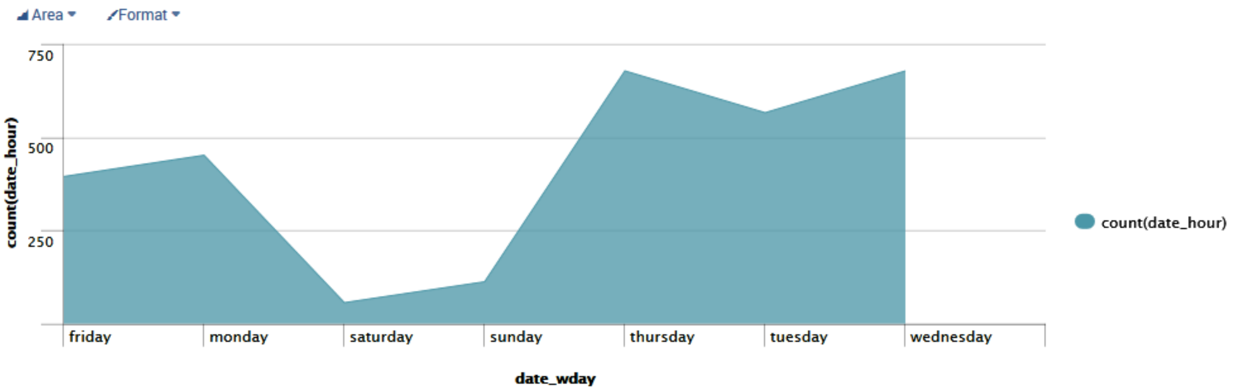
_time	source	count(_raw)
2007-10-23 13:38:01	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 13:38:02	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 13:39:56	c:\Splunk\Splunk book\tm1server.log	2
2007-10-23 13:41:33	c:\Splunk\Splunk book\tm1server.log	2
2007-10-23 13:44:25	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 13:44:25	c:\Splunk\Splunk book\tm1server.log	1
2007-10-23 23:52:33	c:\Splunk\Splunk book\tm1server.log	1
2007-10-24 19:20:22	c:\Splunk\Splunk book\tm1server.log	242

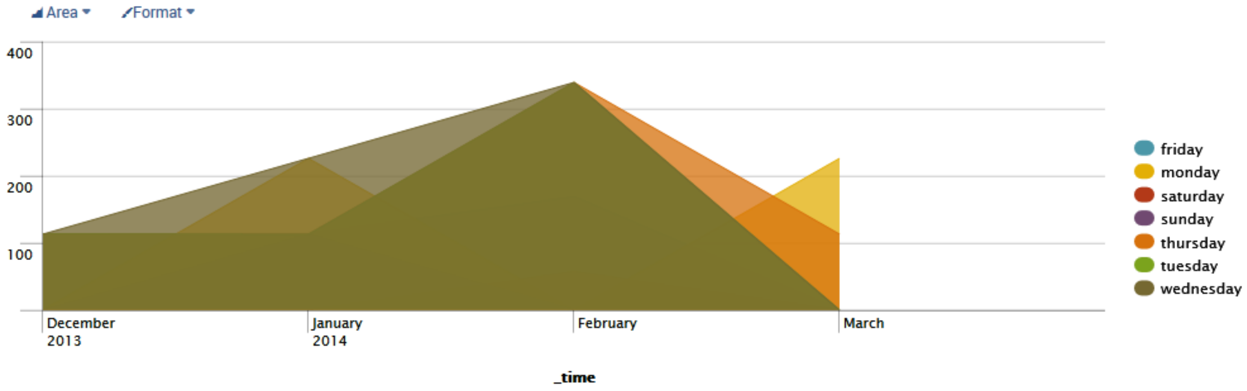


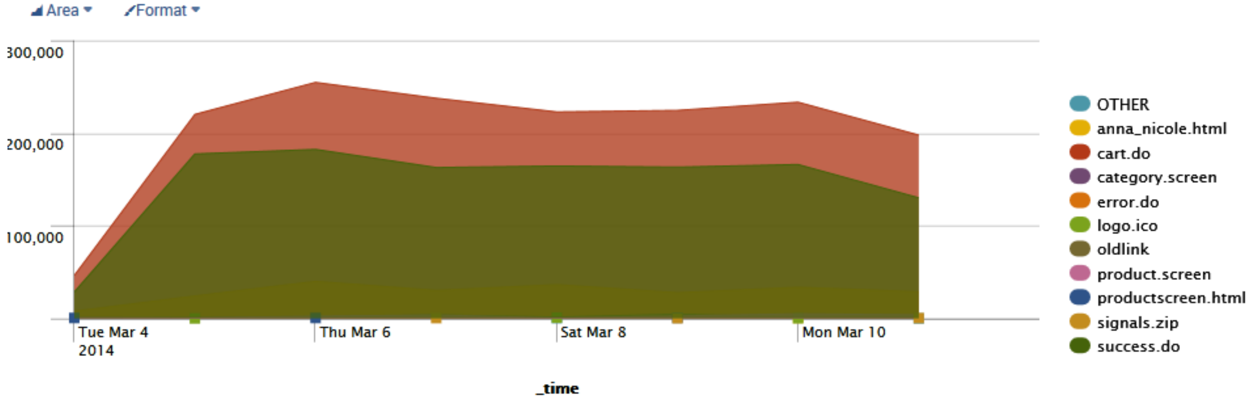
_time	source	count(_raw)
2007-10-19	c:\Splunk\Splunk book\tm1server.log	9
2007-10-24	c:\Splunk\Splunk book\tm1server.log	69890
2009-06-25	c:\Splunk\Splunk book\tm1smsg.log	5
2013-12-06	C:\PreimerMe\tm1server.log	184
2013-12-11	C:\PreimerMe\tm1server.log	360

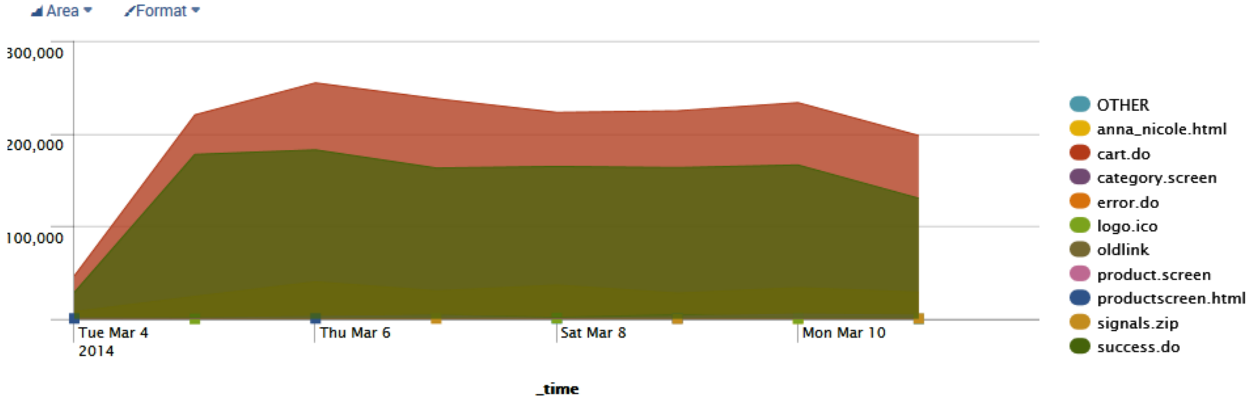


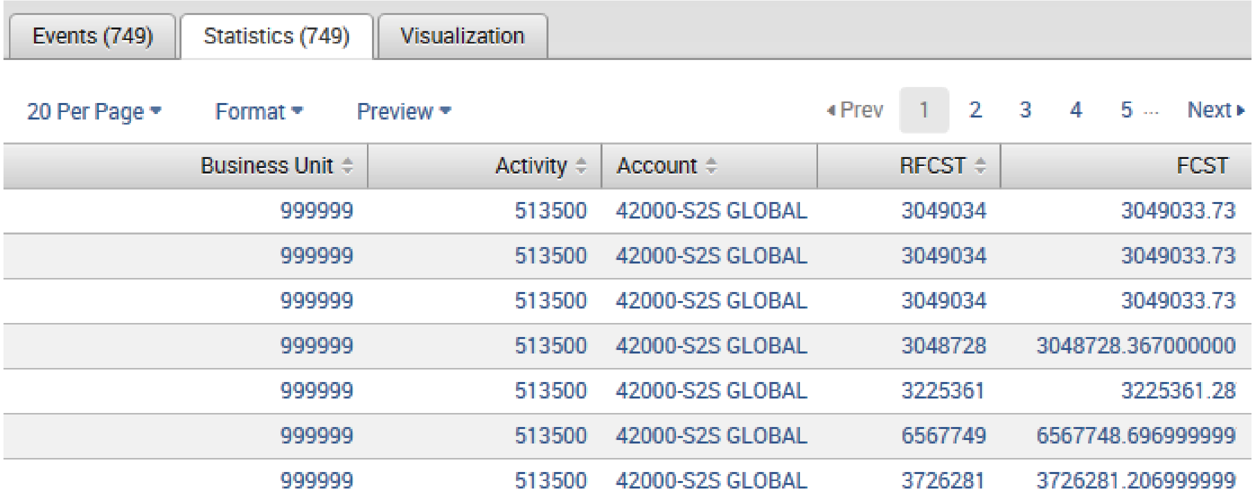
_time	source	count(_raw)
2007-10-19	c:\Splunk\Splunk book\tm1server.log	9
2007-10-24	c:\Splunk\Splunk book\tm1server.log	69890
2009-06-25	c:\Splunk\Splunk book\tm1smsg.log	5
2013-12-06	C:\PreimerMe\tm1server.log	184
2013-12-11	C:\PreimerMe\tm1server.log	360


Area
Format
750
500
250
count(date_hour)
friday
monday
saturday
sunday
thursday
tuesday
wednesday
date_wday
● count(date_hour)

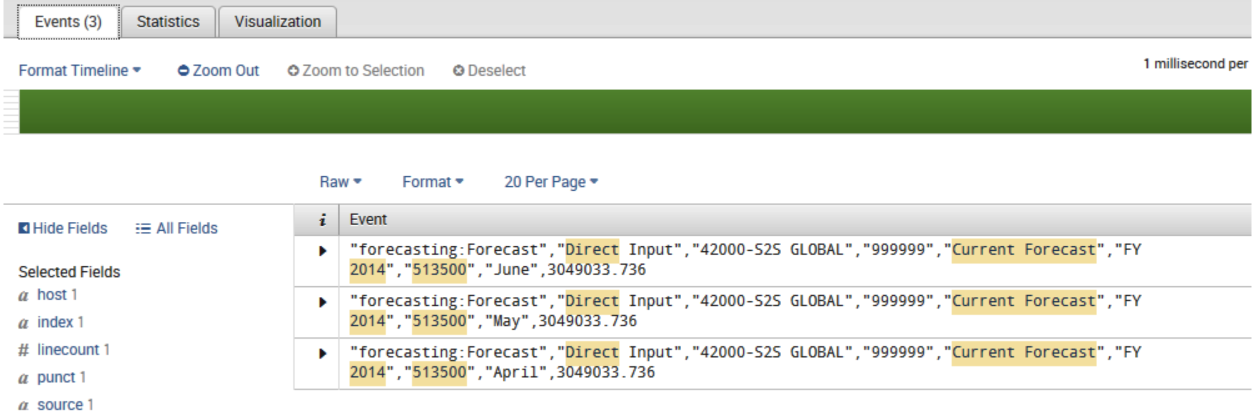

Area
Format
400
300
200
100
December
2013
January
2014
February
March
_time
● friday
● monday
● saturday
● sunday
● thursday
● tuesday
● wednesday


Area
Format
300,000
200,000
100,000
Tue Mar 4
2014
Thu Mar 6
Sat Mar 8
Mon Mar 10
_time
● OTHER
● anna_nicole.html
● cart.do
● category.screen
● error.do
● logo.ico
● oldlink
● product.screen
● productscreen.html
● signals.zip
● success.do

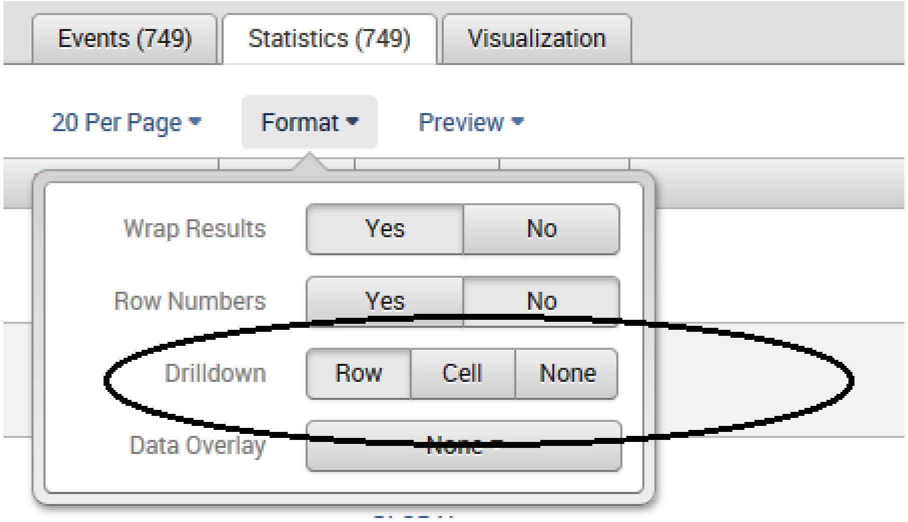

Area
Format
300,000
200,000
100,000
Tue Mar 4
2014
Thu Mar 6
Sat Mar 8
Mon Mar 10
_time
● OTHER
● anna_nicole.html
● cart.do
● category.screen
● error.do
● logo.ico
● oldlink
● product.screen
● productscreen.html
● signals.zip
● success.do



Business Unit	Activity	Account	RFCST	FCST
999999	513500	42000-S2S GLOBAL	3049034	3049033.73
999999	513500	42000-S2S GLOBAL	3049034	3049033.73
999999	513500	42000-S2S GLOBAL	3049034	3049033.73
999999	513500	42000-S2S GLOBAL	3048728	3048728.367000000
999999	513500	42000-S2S GLOBAL	3225361	3225361.28
999999	513500	42000-S2S GLOBAL	6567749	6567748.696999999
999999	513500	42000-S2S GLOBAL	3726281	3726281.206999999



```
"forecasting:Forecast","Direct Input","42000-S2S GLOBAL","999999","Current Forecast","FY
2014","513500","June",3049033.736
"forecasting:Forecast","Direct Input","42000-S2S GLOBAL","999999","Current Forecast","FY
2014","513500","May",3049033.736
"forecasting:Forecast","Direct Input","42000-S2S GLOBAL","999999","Current Forecast","FY
2014","513500","April",3049033.736
```

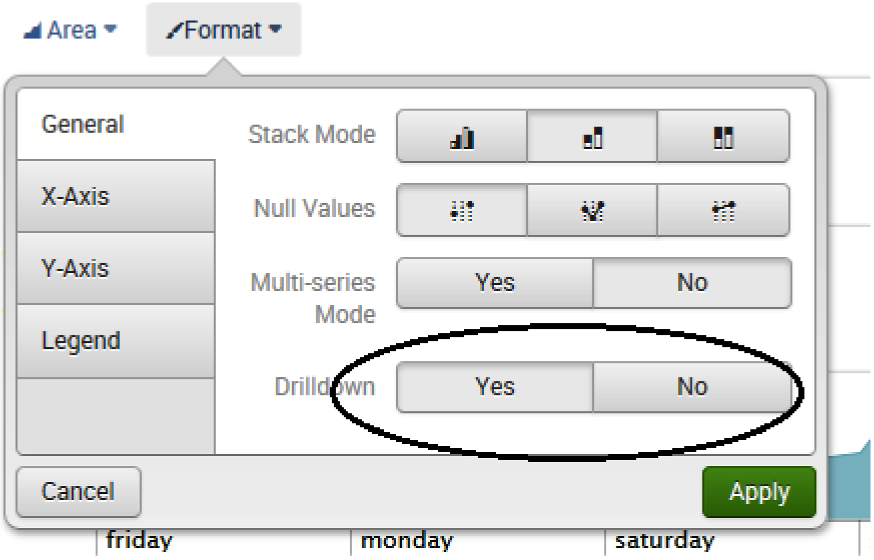


Wrap Results: Yes | No

Row Numbers: Yes | No

Drilldown: Row | Cell | None

Data Overlay: None

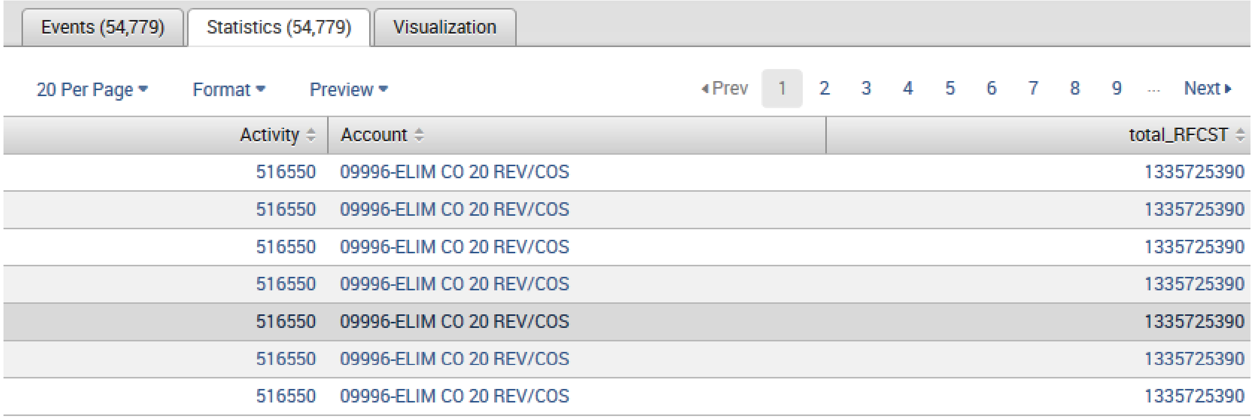


Stack Mode

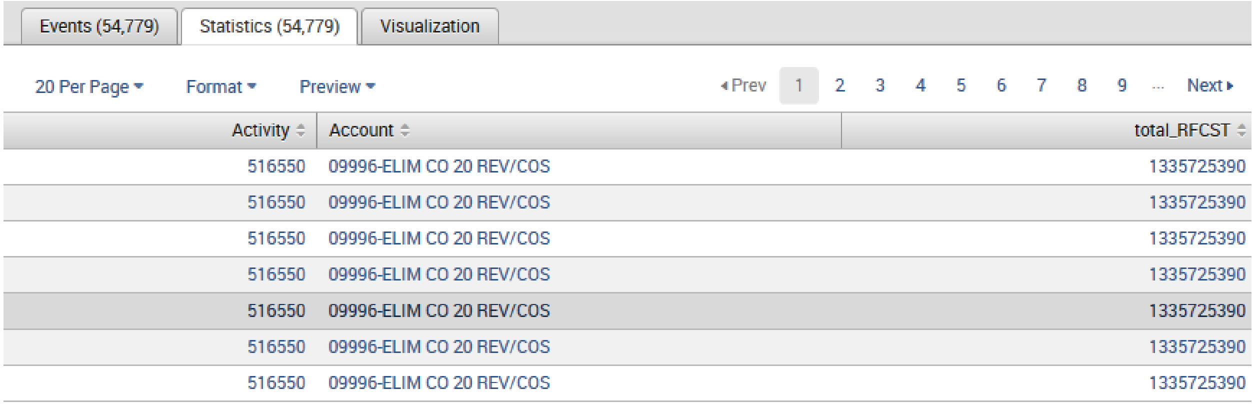
Null Values

Multi-series Mode: Yes | No

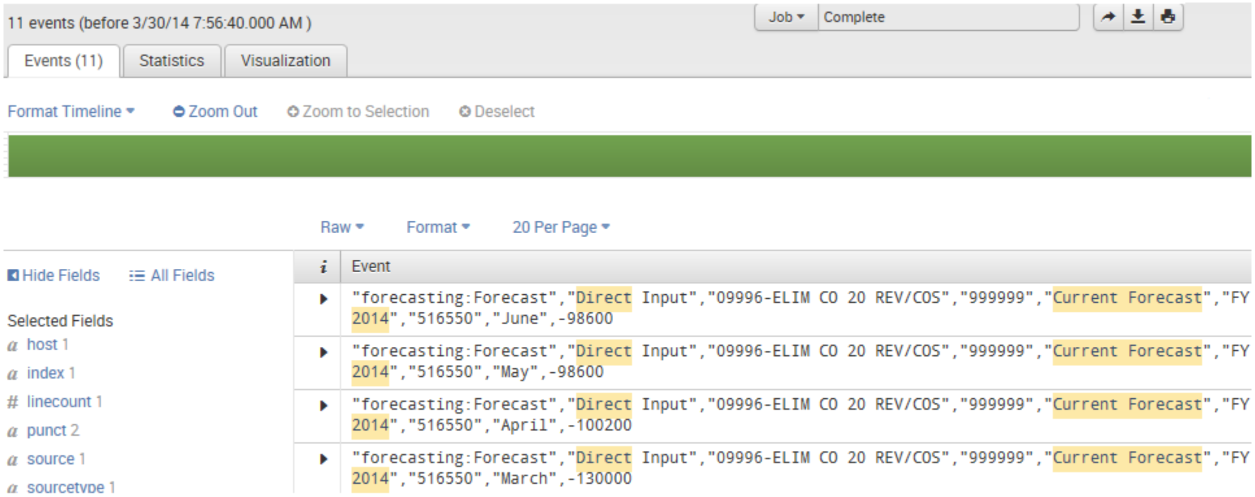
Drilldown: Yes | No



Activity	Account	total_RFCST
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390



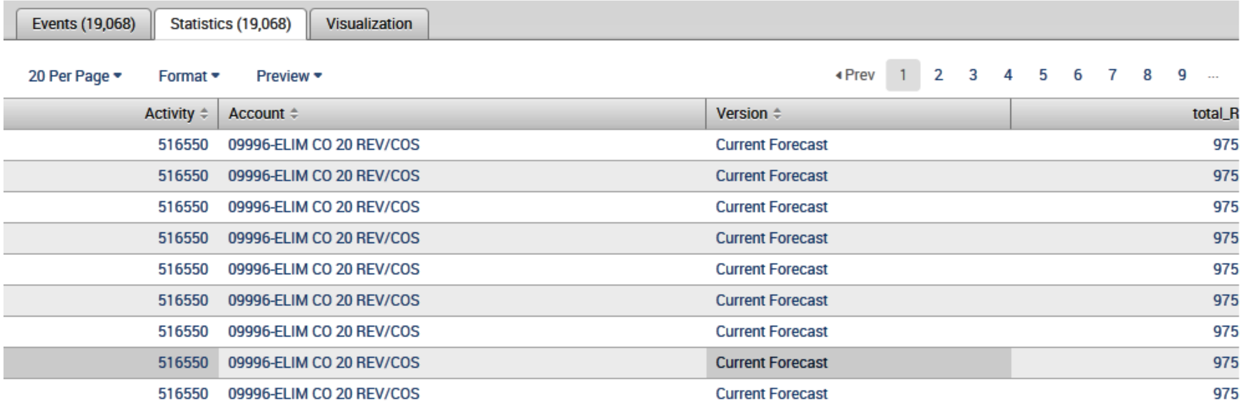
Activity	Account	total_RFCST
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390
516550	09996-ELIM CO 20 REV/COS	1335725390



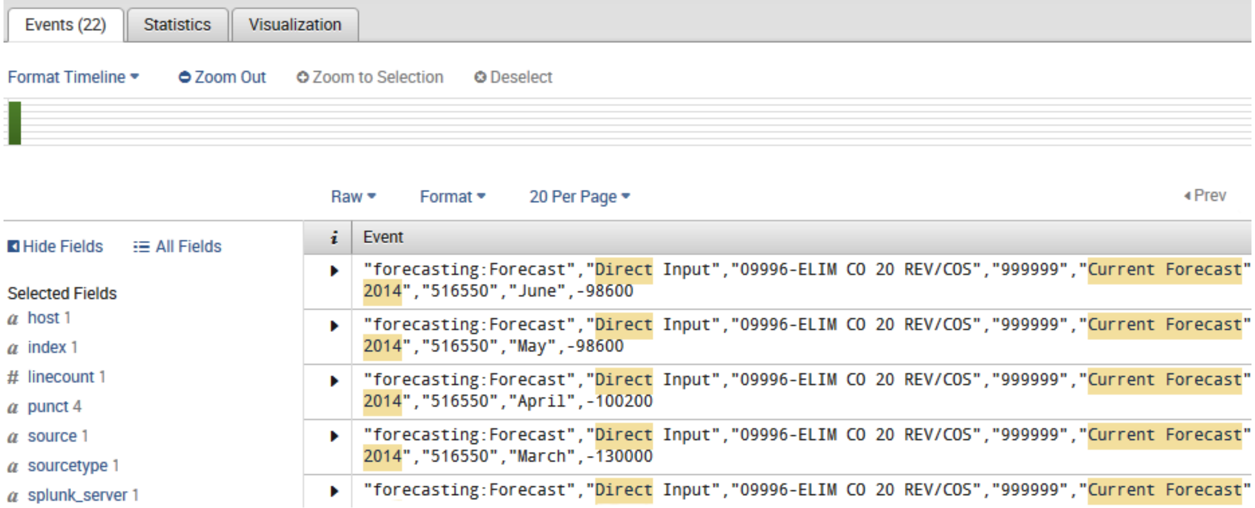
11 events (before 3/30/14 7:56:40.000 AM)

Selected Fields
- host 1
- index 1
- linecount 1
- punct 2
- source 1
- sourcetype 1

```
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast","FY
2014","516550","June",-98600
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast","FY
2014","516550","May",-98600
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast","FY
2014","516550","April",-100200
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast","FY
2014","516550","March",-130000
```

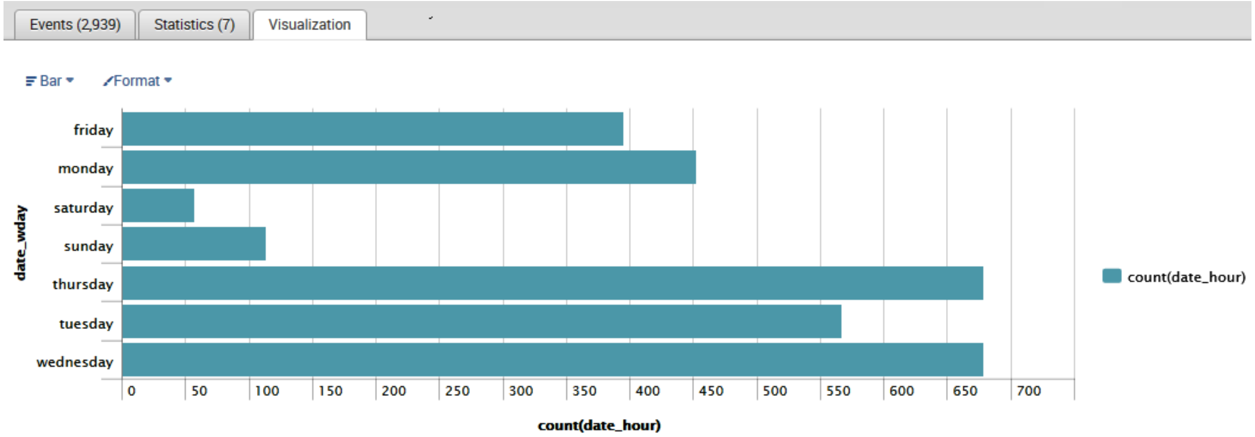


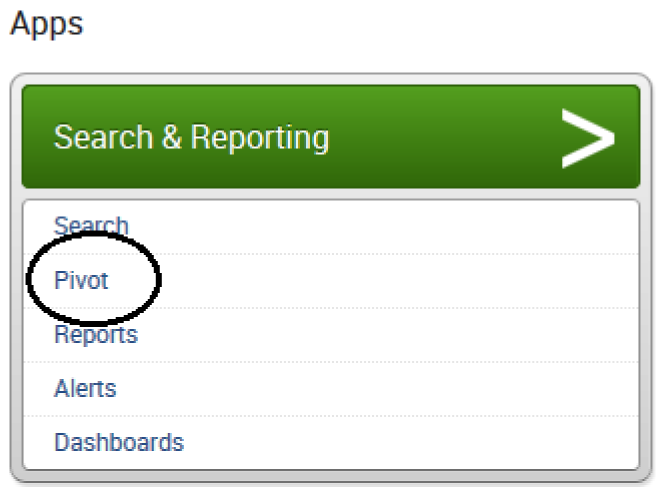
Activity	Account	Version	total_R
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975
516550	09996-ELIM CO 20 REV/COS	Current Forecast	975

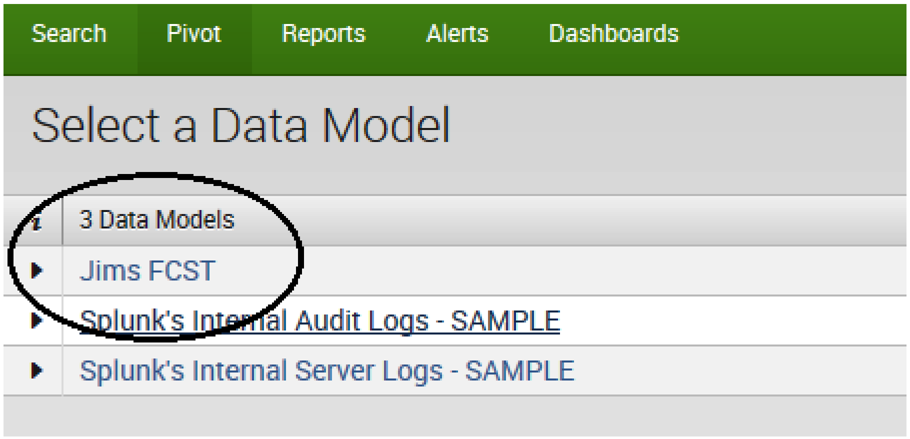


Selected Fields
- host 1
- index 1
- linecount 1
- punct 4
- source 1
- sourcetype 1
- splunk_server 1

```
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast"
2014","516550","June",-98600
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast"
2014","516550","May",-98600
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast"
2014","516550","April",-100200
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast"
2014","516550","March",-130000
"forecasting:Forecast","Direct Input","09996-ELIM CO 20 REV/COS","999999","Current Forecast"
```



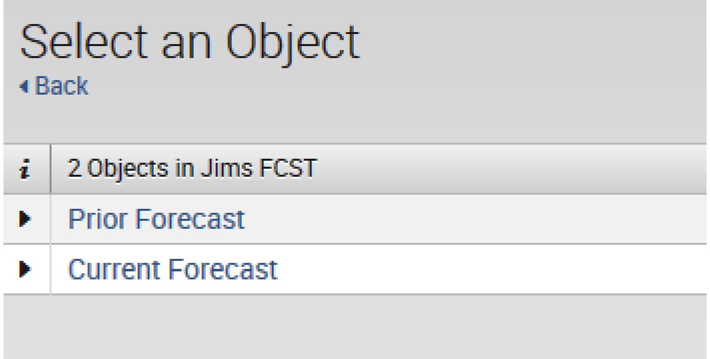




Select a Data Model

3 Data Models

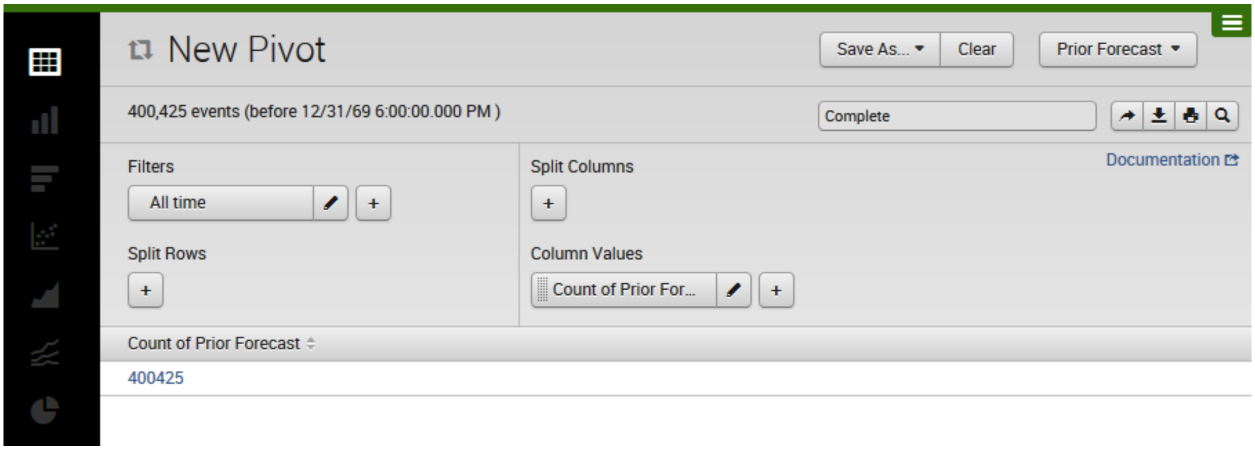
- Jims FCST
- Splunk's Internal Audit Logs - SAMPLE
- Splunk's Internal Server Logs - SAMPLE



Select an Object

2 Objects in Jims FCST

- Prior Forecast
- Current Forecast



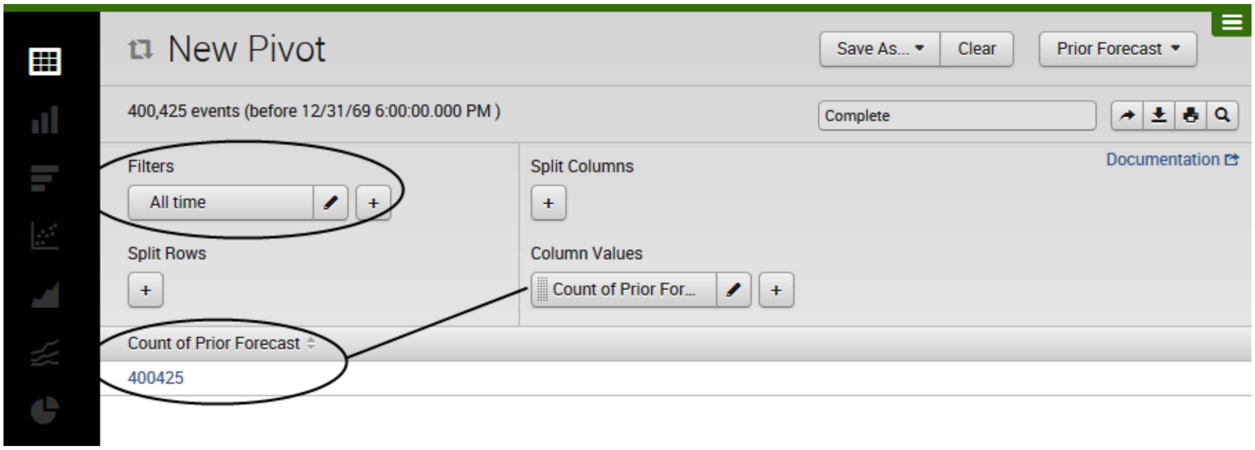
New Pivot

400,425 events (before 12/31/69 6:00:00.000 PM)

Filters: All time

Column Values: Count of Prior For...

Count of Prior Forecast
400425



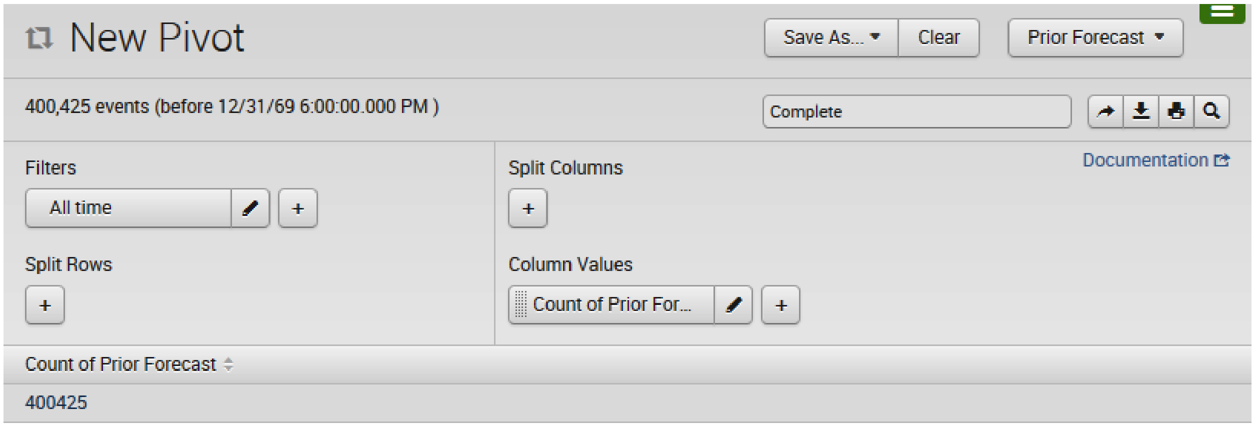
New Pivot

400,425 events (before 12/31/69 6:00:00.000 PM)

Filters: All time

Column Values: Count of Prior For...

Count of Prior Forecast
400425



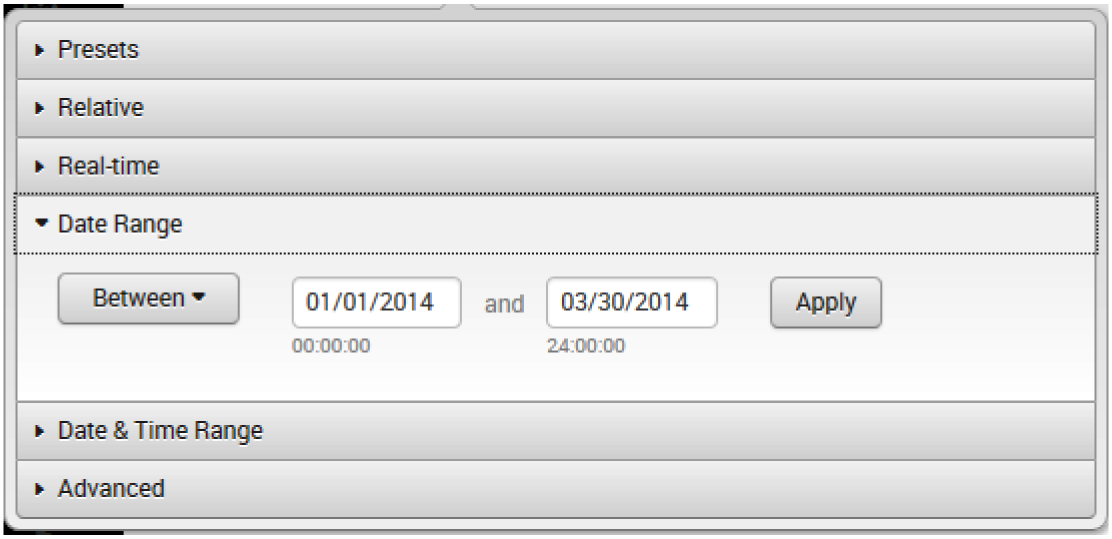
New Pivot

400,425 events (before 12/31/69 6:00:00.000 PM)

Filters: All time

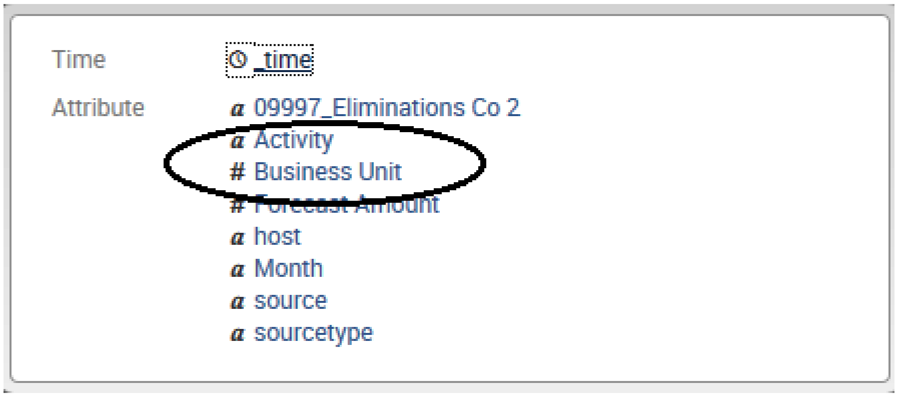
Column Values: Count of Prior For...

Count of Prior Forecast
400425



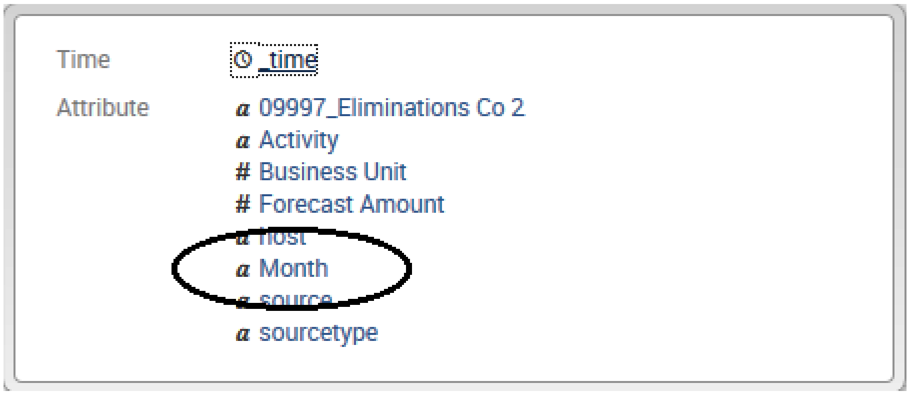
Between 01/01/2014 and 03/30/2014

00:00:00 24:00:00



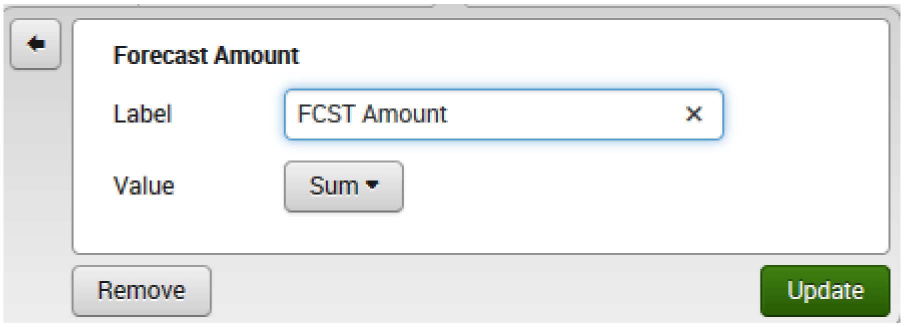
Time ⏱ _time

Attribute
a 09997_Eliminations Co 2
a Activity
Business Unit
Forecast Amount
a host
a Month
a source
a sourcetype



Time ⏱ _time

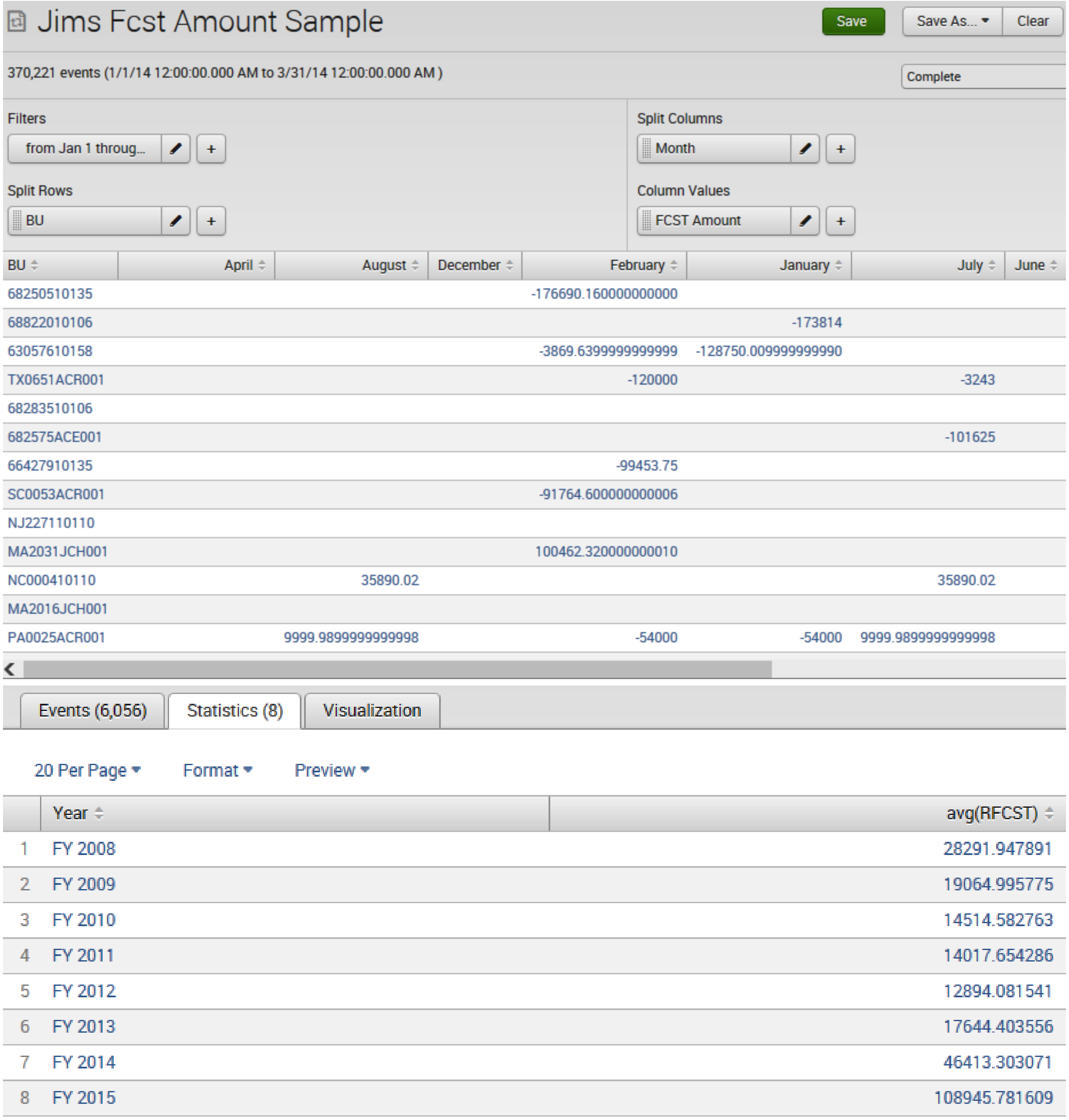
Attribute
a 09997_Eliminations Co 2
a Activity
Business Unit
Forecast Amount
a host
a Month
a source
a sourcetype



Forecast Amount

Label: FCST Amount ×

Value: Sum

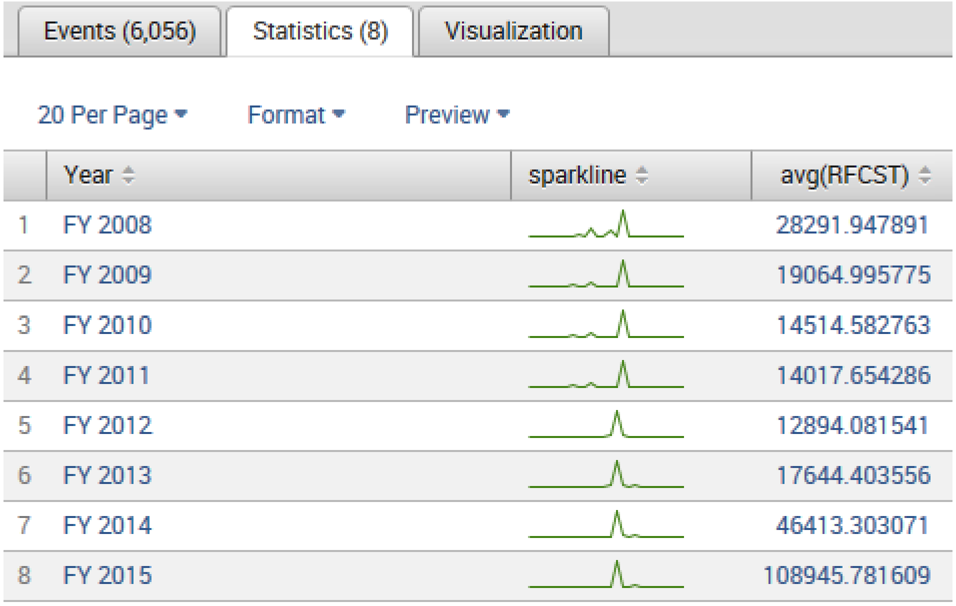


Jims Fcst Amount Sample

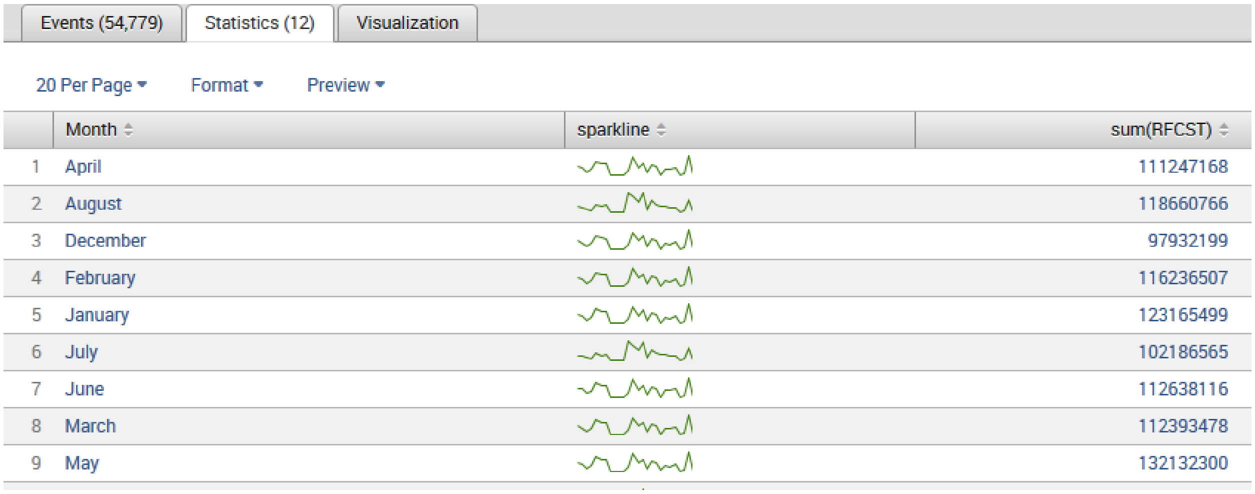
370,221 events (1/1/14 12:00:00.000 AM to 3/31/14 12:00:00.000 AM)

BU	April	August	December	February	January	July	June
68250510135				-176690.160000000000			
68822010106					-173814		
63057610158				-3869.6399999999999	-128750.009999999990		
TX0651ACR001				-120000		-3243	
68283510106							
682575ACE001						-101625	
66427910135				-99453.75			
SC0053ACR001				-91764.600000000006			
NJ227110110							
MA2031JCH001				100462.320000000010			
NC000410110		35890.02				35890.02	
MA2016JCH001							
PA0025ACR001		9999.9899999999998		-54000	-54000	9999.9899999999998	

	Year	avg(RFCST)
1	FY 2008	28291.947891
2	FY 2009	19064.995775
3	FY 2010	14514.582763
4	FY 2011	14017.654286
5	FY 2012	12894.081541
6	FY 2013	17644.403556
7	FY 2014	46413.303071
8	FY 2015	108945.781609

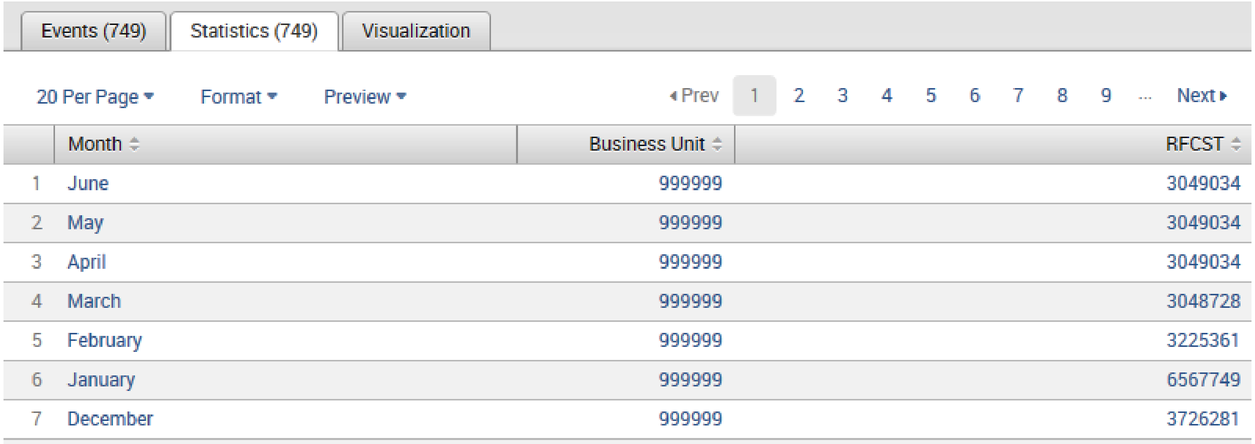


	Year	sparkline	avg(RFCST)
1	FY 2008		28291.947891
2	FY 2009		19064.995775
3	FY 2010		14514.582763
4	FY 2011		14017.654286
5	FY 2012		12894.081541
6	FY 2013		17644.403556
7	FY 2014		46413.303071
8	FY 2015		108945.781609

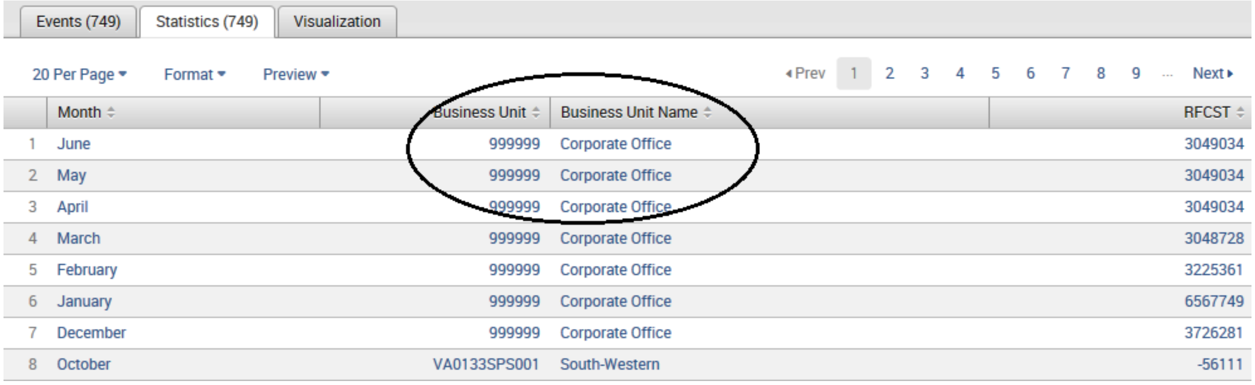


	Month	sparkline	sum(RFCST)
1	April		111247168
2	August		118660766
3	December		97932199
4	February		116236507
5	January		123165499
6	July		102186565
7	June		112638116
8	March		112393478
9	May		132132300

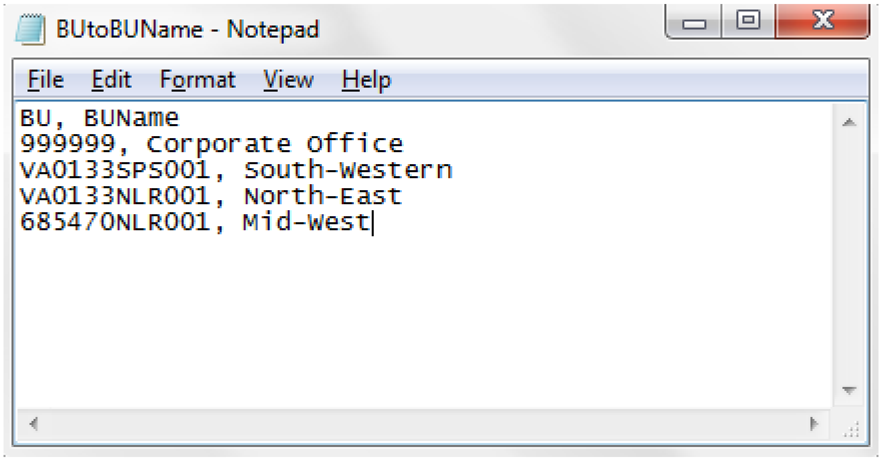
Chapter 4, *Lookups*



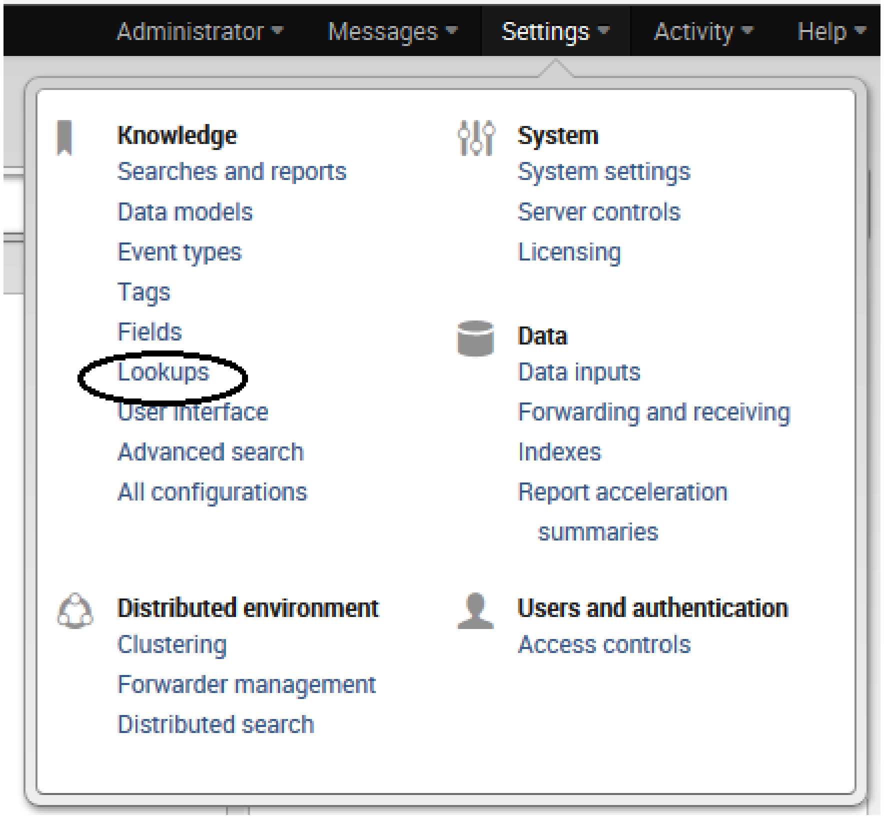
	Month	Business Unit	RFCST
1	June	999999	3049034
2	May	999999	3049034
3	April	999999	3049034
4	March	999999	3048728
5	February	999999	3225361
6	January	999999	6567749
7	December	999999	3726281

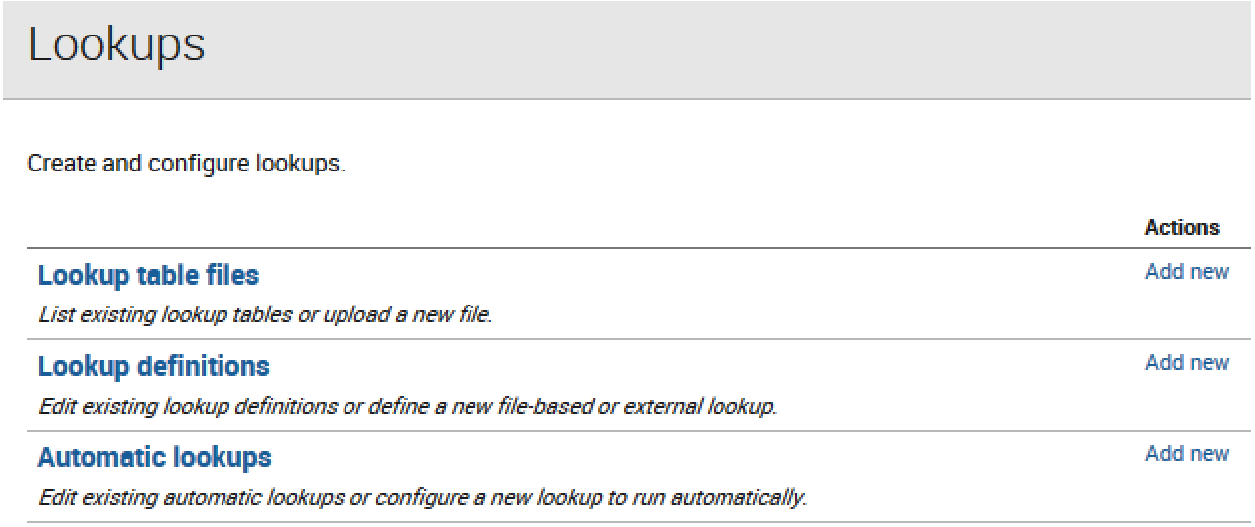


	Month	Business Unit	Business Unit Name	RFCST
1	June	999999	Corporate Office	3049034
2	May	999999	Corporate Office	3049034
3	April	999999	Corporate Office	3049034
4	March	999999	Corporate Office	3048728
5	February	999999	Corporate Office	3225361
6	January	999999	Corporate Office	6567749
7	December	999999	Corporate Office	3726281
8	October	VA0133SPS001	South-Western	-56111



```
BU, BUName
999999, Corporate Office
VA0133SPS001, South-Western
VA0133NLR001, North-East
685470NLR001, Mid-West
```

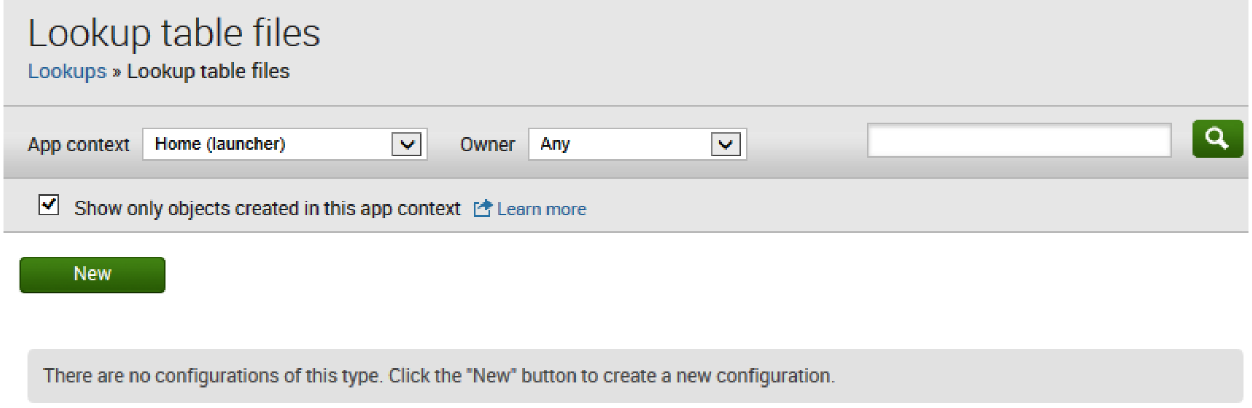




Lookups

Create and configure lookups.

	Actions
Lookup table files *List existing lookup tables or upload a new file.*	Add new
Lookup definitions *Edit existing lookup definitions or define a new file-based or external lookup.*	Add new
Automatic lookups *Edit existing automatic lookups or configure a new lookup to run automatically.*	Add new



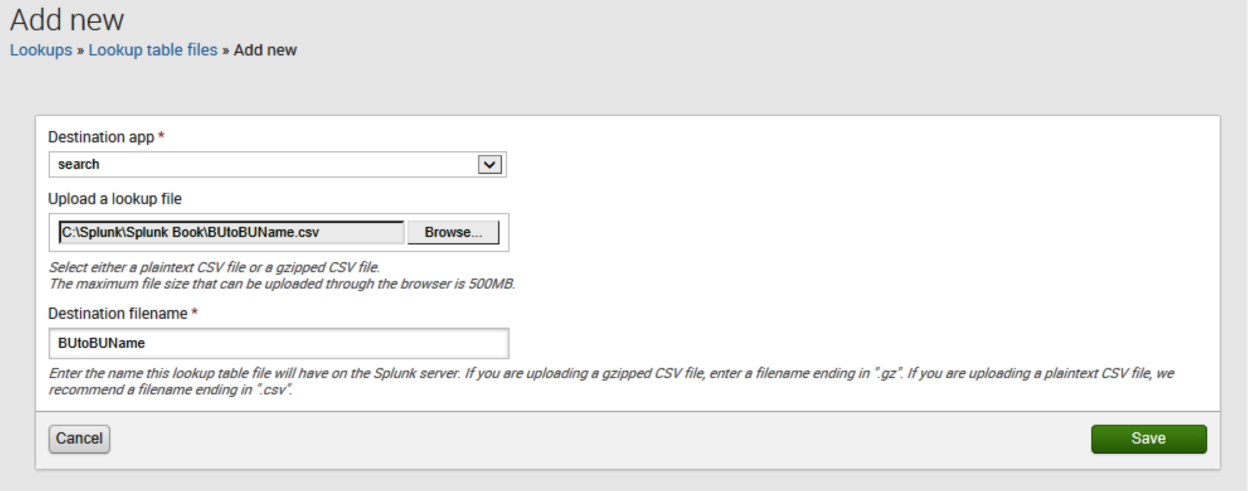
Lookup table files

Lookups » Lookup table files

App context: Home (launcher)   Owner: Any

☑ Show only objects created in this app context   Learn more

There are no configurations of this type. Click the "New" button to create a new configuration.



Add new

Lookups » Lookup table files » Add new

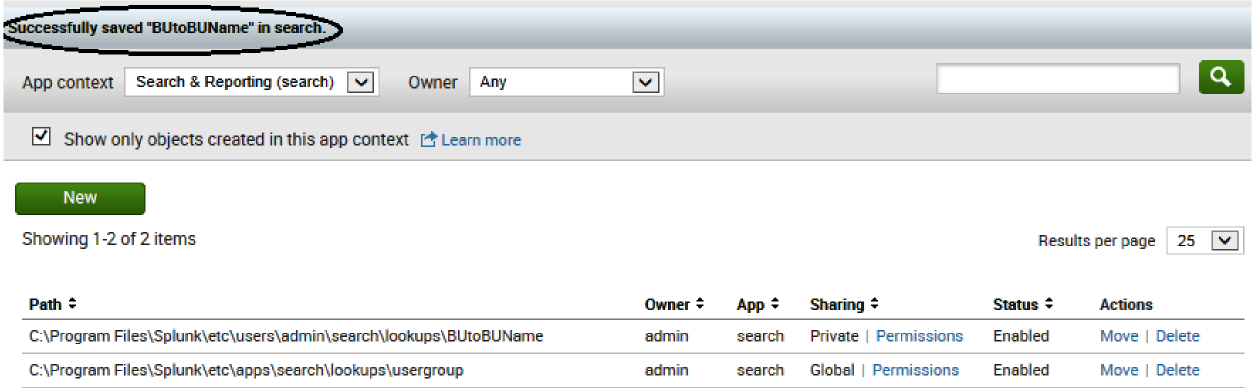
Destination app *: search

Upload a lookup file: C:\Splunk\Splunk Book\BUtoBUName.csv   Browse...

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

Destination filename *: BUtoBUName

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv".



Successfully saved "BUtoBUName" in search.

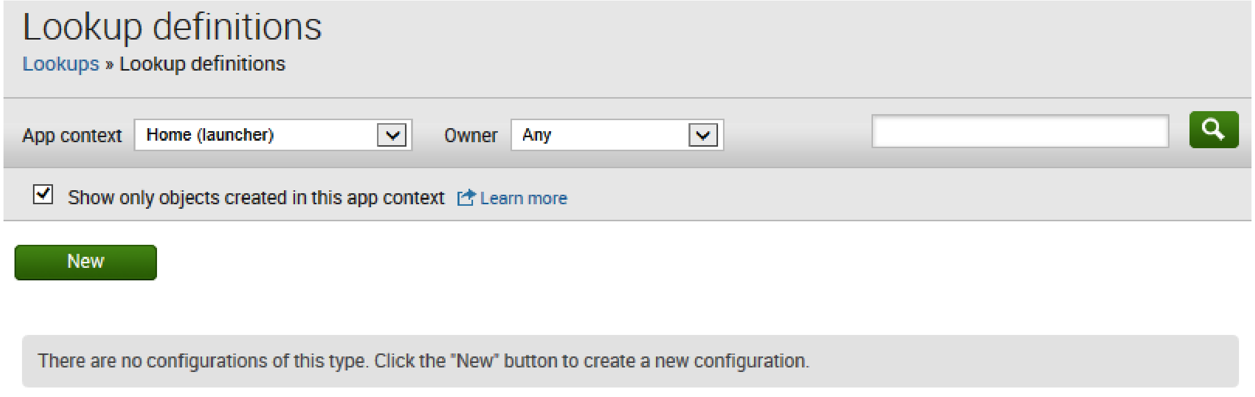
App context: Search & Reporting (search) Owner: Any

☑ Show only objects created in this app context Learn more

Showing 1-2 of 2 items

Results per page: 25

Path	Owner	App	Sharing	Status	Actions
C:\Program Files\Splunk\etc\users\admin\search\lookups\BUtoBUName	admin	search	Private | Permissions	Enabled	Move | Delete
C:\Program Files\Splunk\etc\apps\search\lookups\usergroup	admin	search	Global | Permissions	Enabled	Move | Delete



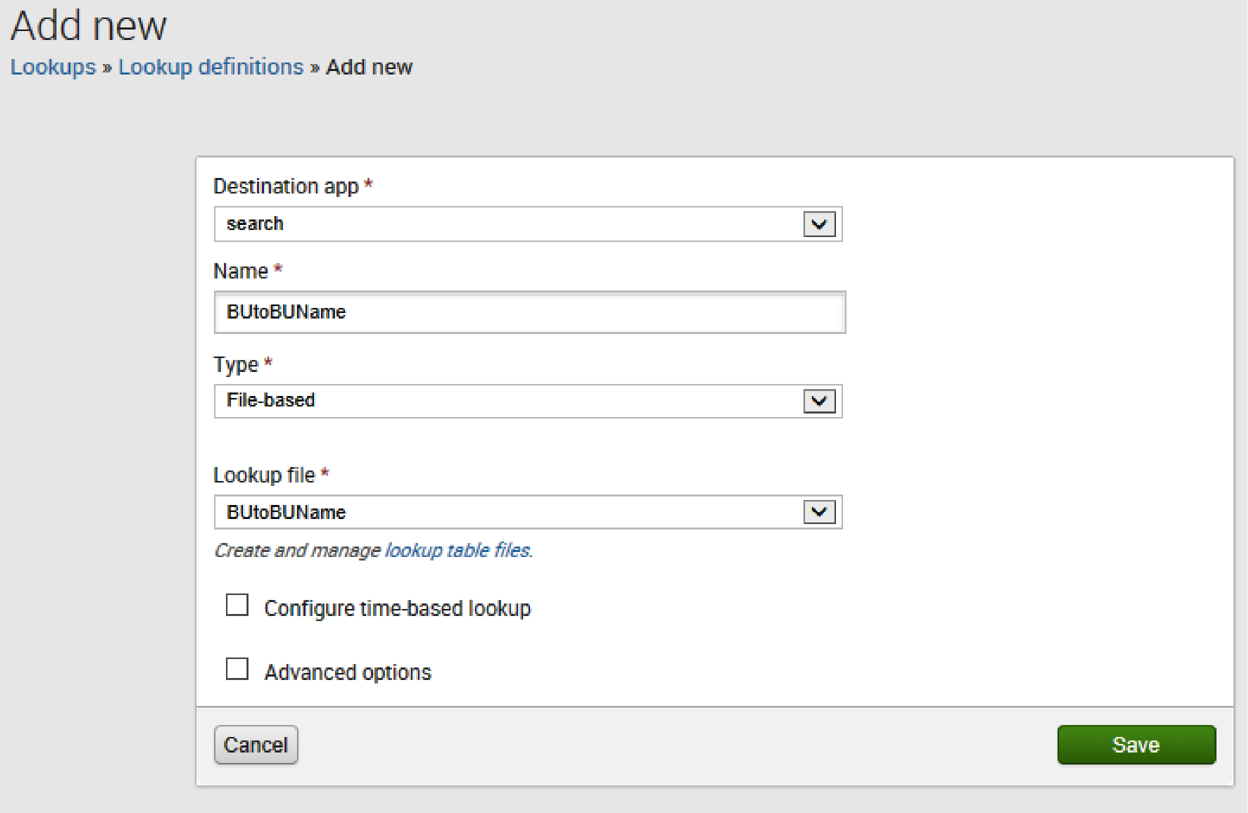
Lookup definitions

Lookups » Lookup definitions

App context: Home (launcher) Owner: Any

☑ Show only objects created in this app context Learn more

There are no configurations of this type. Click the "New" button to create a new configuration.



Add new

Lookups » Lookup definitions » Add new

Destination app *: search

Name *: BUtoBUName

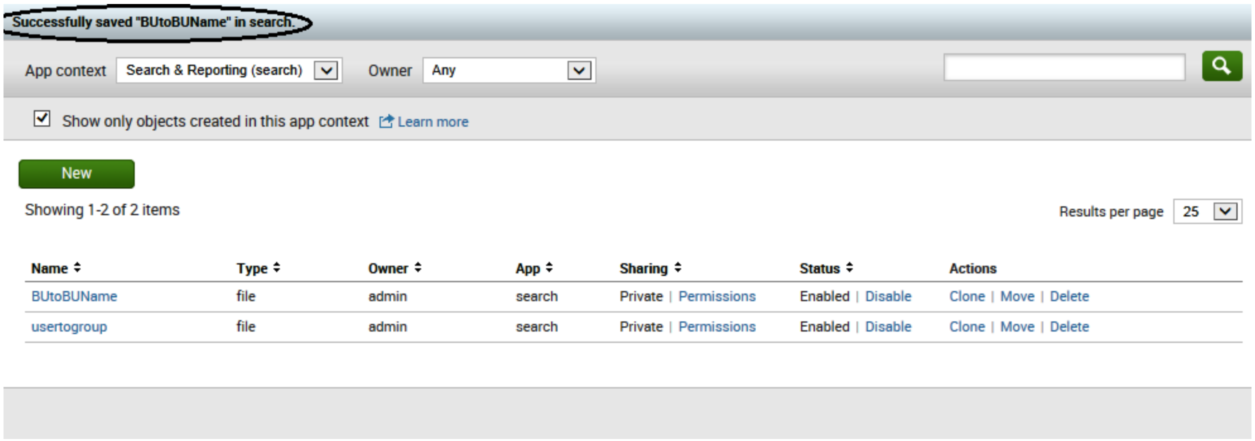
Type *: File-based

Lookup file *: BUtoBUName

Create and manage lookup table files.

□ Configure time-based lookup

□ Advanced options



Successfully saved "BUtoBUName" in search.

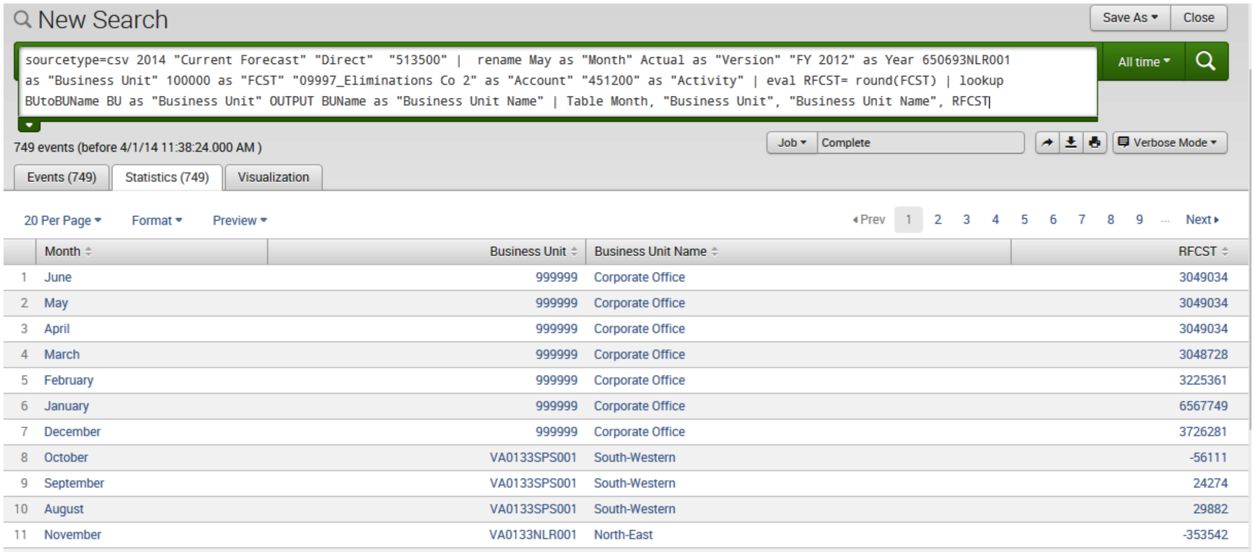
App context: Search & Reporting (search)   Owner: Any

☑ Show only objects created in this app context

Showing 1-2 of 2 items

Results per page: 25

Name	Type	Owner	App	Sharing	Status	Actions
BUtoBUName	file	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete
usertogroup	file	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete

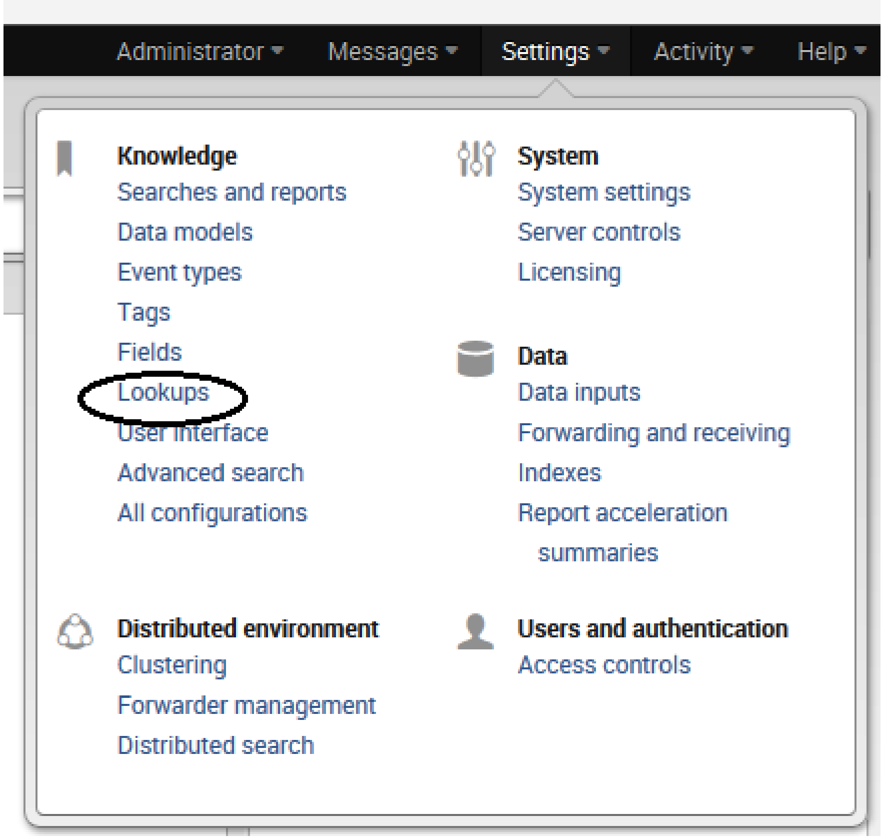


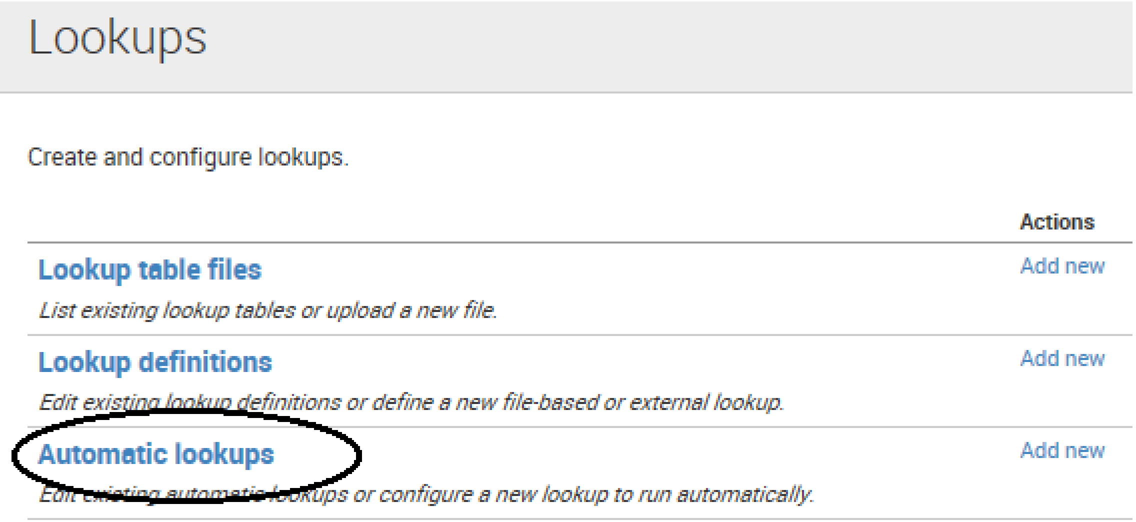
```
sourcetype=csv 2014 "Current Forecast" "Direct"  "513500" |  rename May as "Month" Actual as "Version" "FY 2012" as Year 650693NLR001
as "Business Unit" 100000 as "FCST" "09997_Eliminations Co 2" as "Account" "451200" as "Activity" | eval RFCST= round(FCST) | lookup
BUtoBUName BU as "Business Unit" OUTPUT BUName as "Business Unit Name" | Table Month, "Business Unit", "Business Unit Name", RFCST
```

749 events (before 4/1/14 11:38:24.000 AM)

Job: Complete   Verbose Mode

	Month	Business Unit	Business Unit Name	RFCST
1	June	999999	Corporate Office	3049034
2	May	999999	Corporate Office	3049034
3	April	999999	Corporate Office	3049034
4	March	999999	Corporate Office	3048728
5	February	999999	Corporate Office	3225361
6	January	999999	Corporate Office	6567749
7	December	999999	Corporate Office	3726281
8	October	VA0133SPS001	South-Western	-56111
9	September	VA0133SPS001	South-Western	24274
10	August	VA0133SPS001	South-Western	29882
11	November	VA0133NLR001	North-East	-353542

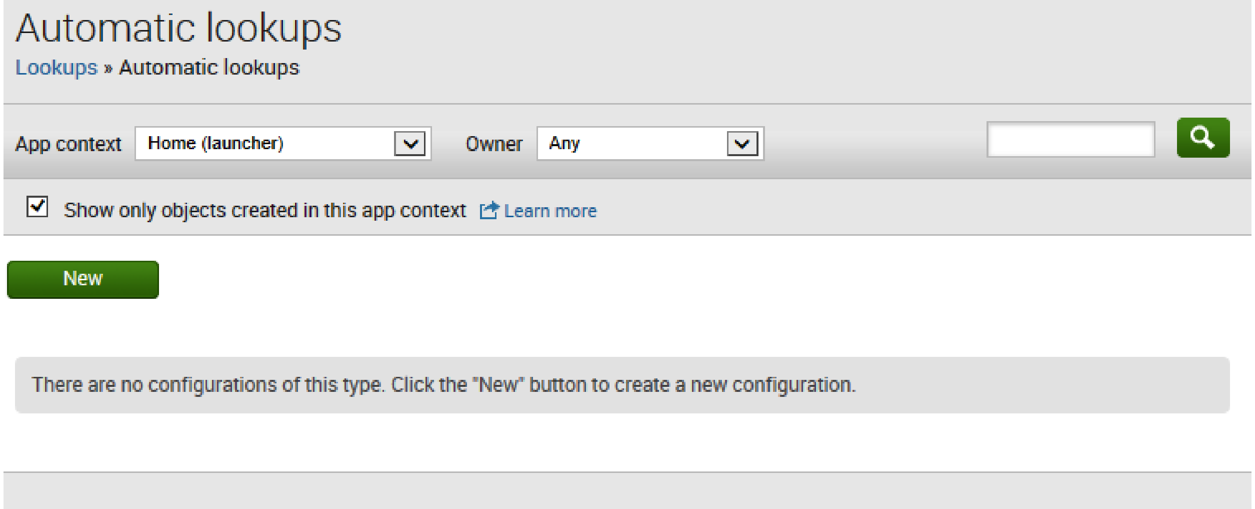




Lookups

Create and configure lookups.

	Actions
Lookup table files *List existing lookup tables or upload a new file.*	Add new
Lookup definitions *Edit existing lookup definitions or define a new file-based or external lookup.*	Add new
Automatic lookups *Edit existing automatic lookups or configure a new lookup to run automatically.*	Add new



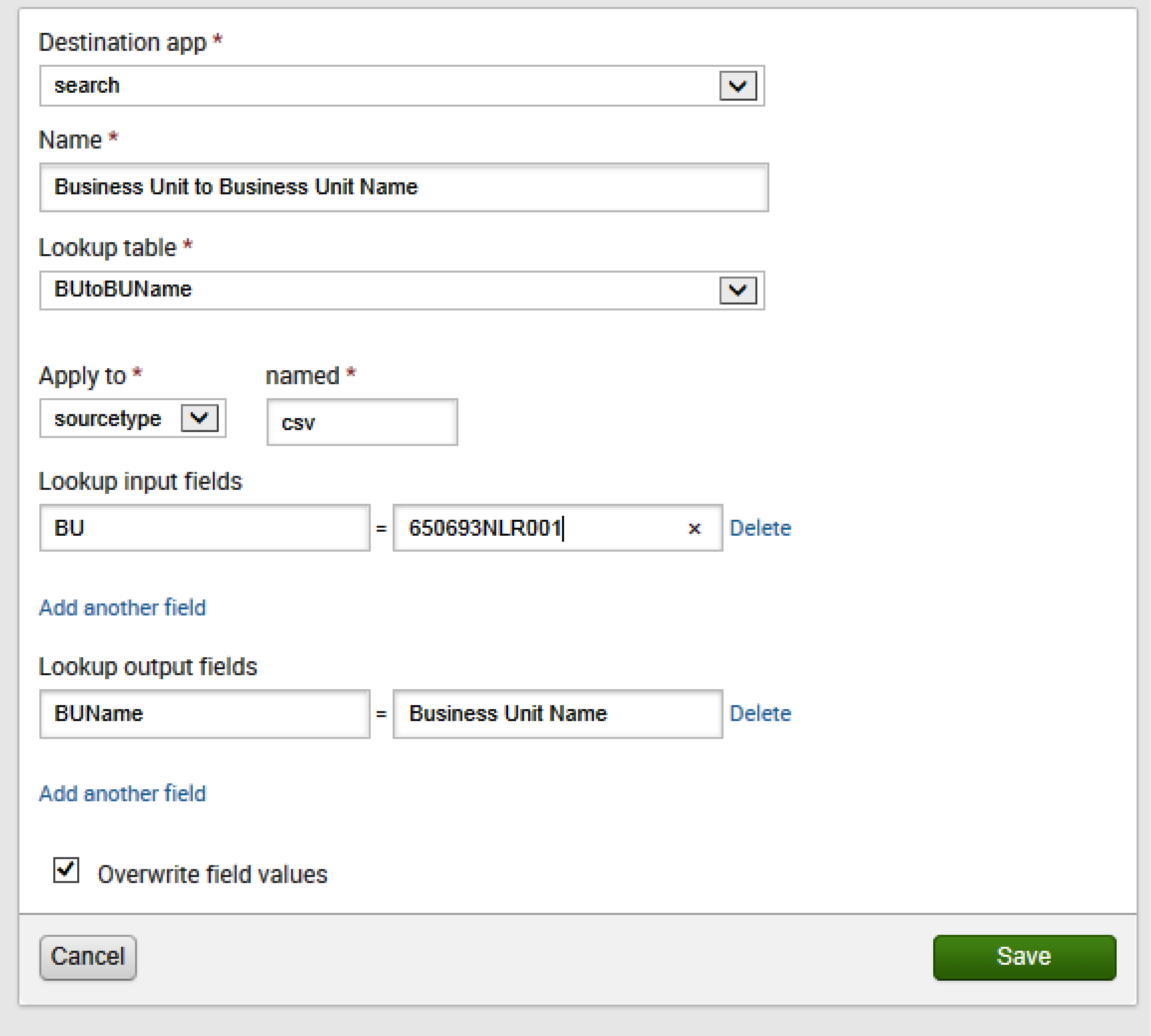
Automatic lookups

Lookups » Automatic lookups

App context: Home (launcher) | Owner: Any

☑ Show only objects created in this app context Learn more

There are no configurations of this type. Click the "New" button to create a new configuration.



Destination app *: search

Name *: Business Unit to Business Unit Name

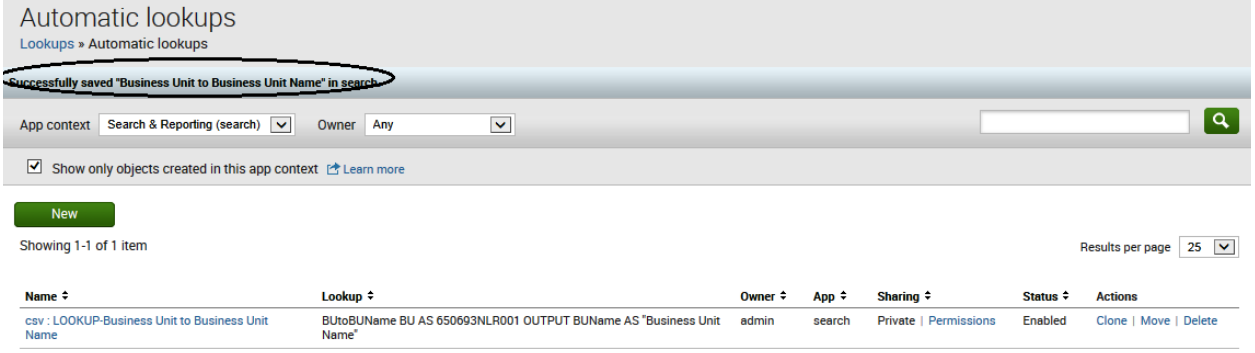
Lookup table *: BUtoBUName

Apply to *: sourcetype | named *: csv

Lookup input fields: BU = 650693NLR001

Lookup output fields: BUName = Business Unit Name

☑ Overwrite field values



Automatic lookups

Lookups » Automatic lookups

Successfully saved "Business Unit to Business Unit Name" in search

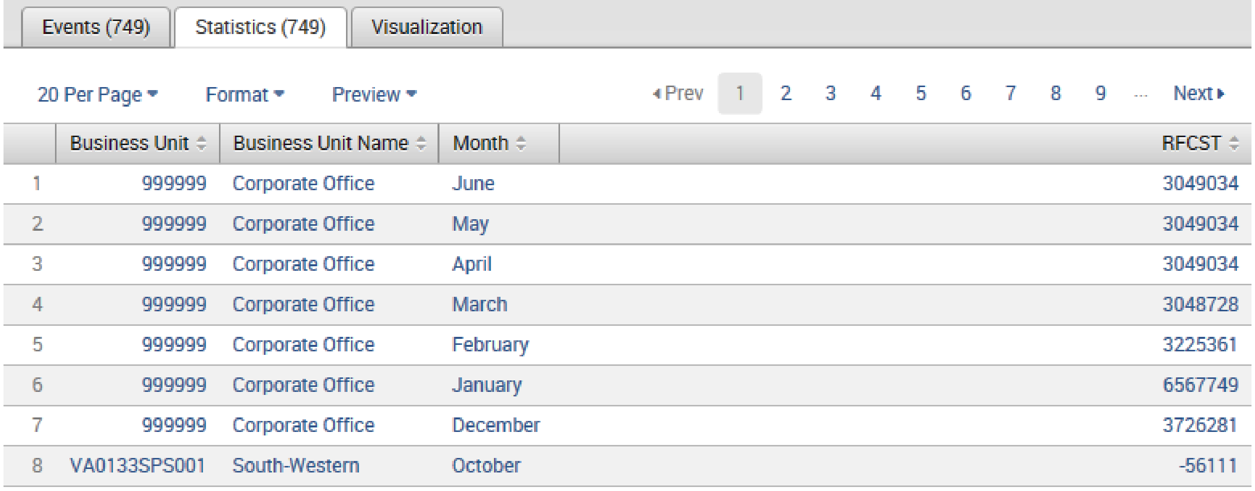
App context: Search & Reporting (search)   Owner: Any

☑ Show only objects created in this app context Learn more

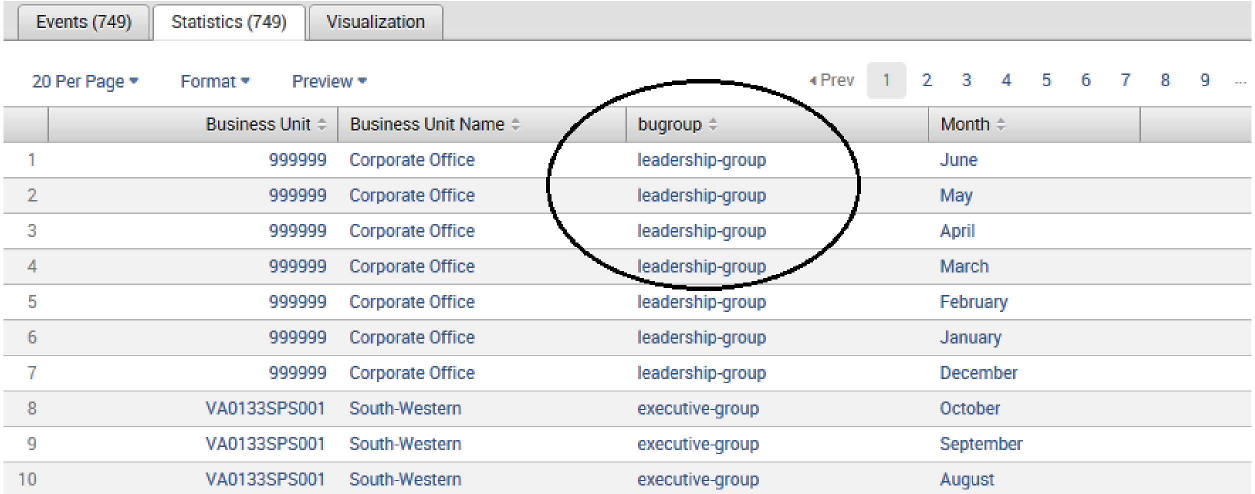
Showing 1-1 of 1 item

Results per page 25

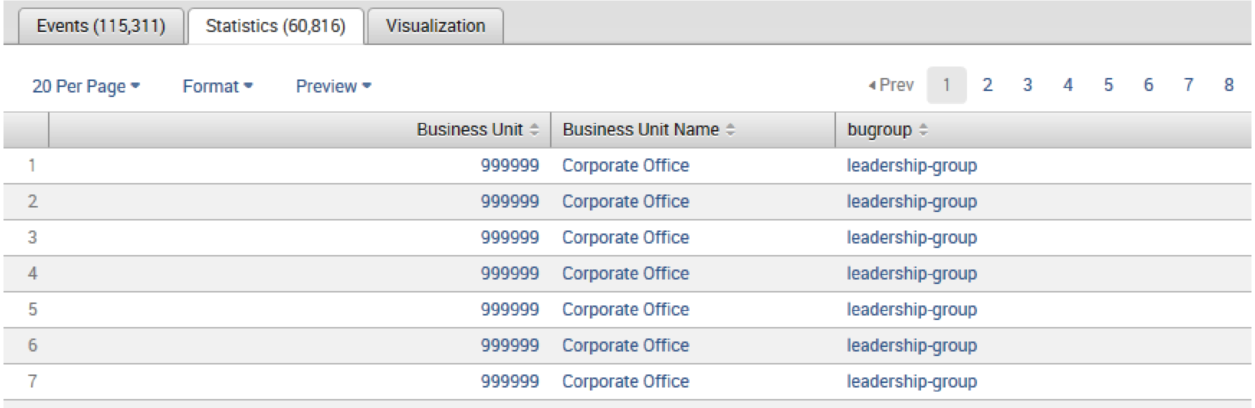
Name	Lookup	Owner	App	Sharing	Status	Actions
csv : LOOKUP-Business Unit to Business Unit Name	BUtoBUName BU AS 650693NLR001 OUTPUT BUName AS "Business Unit Name"	admin	search	Private | Permissions	Enabled	Clone | Move | Delete



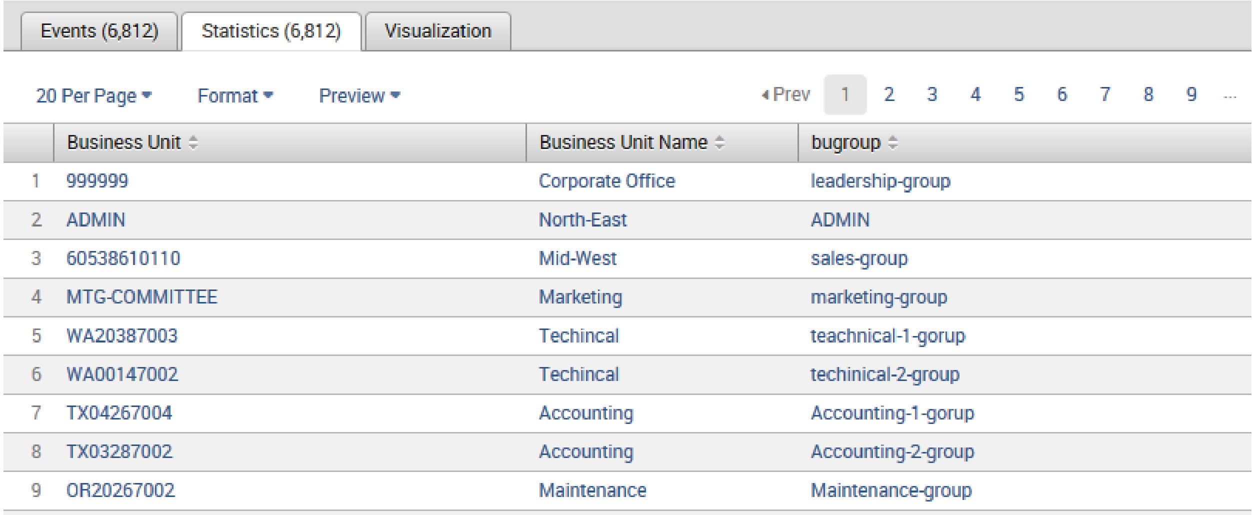
	Business Unit	Business Unit Name	Month	RFCST
1	999999	Corporate Office	June	3049034
2	999999	Corporate Office	May	3049034
3	999999	Corporate Office	April	3049034
4	999999	Corporate Office	March	3048728
5	999999	Corporate Office	February	3225361
6	999999	Corporate Office	January	6567749
7	999999	Corporate Office	December	3726281
8	VA0133SPS001	South-Western	October	-56111



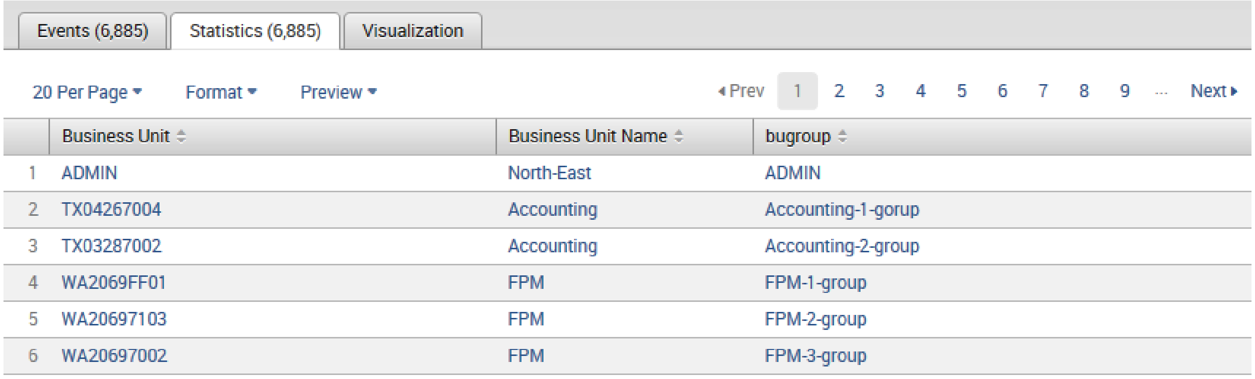
	Business Unit	Business Unit Name	bugroup	Month
1	999999	Corporate Office	leadership-group	June
2	999999	Corporate Office	leadership-group	May
3	999999	Corporate Office	leadership-group	April
4	999999	Corporate Office	leadership-group	March
5	999999	Corporate Office	leadership-group	February
6	999999	Corporate Office	leadership-group	January
7	999999	Corporate Office	leadership-group	December
8	VA0133SPS001	South-Western	executive-group	October
9	VA0133SPS001	South-Western	executive-group	September
10	VA0133SPS001	South-Western	executive-group	August



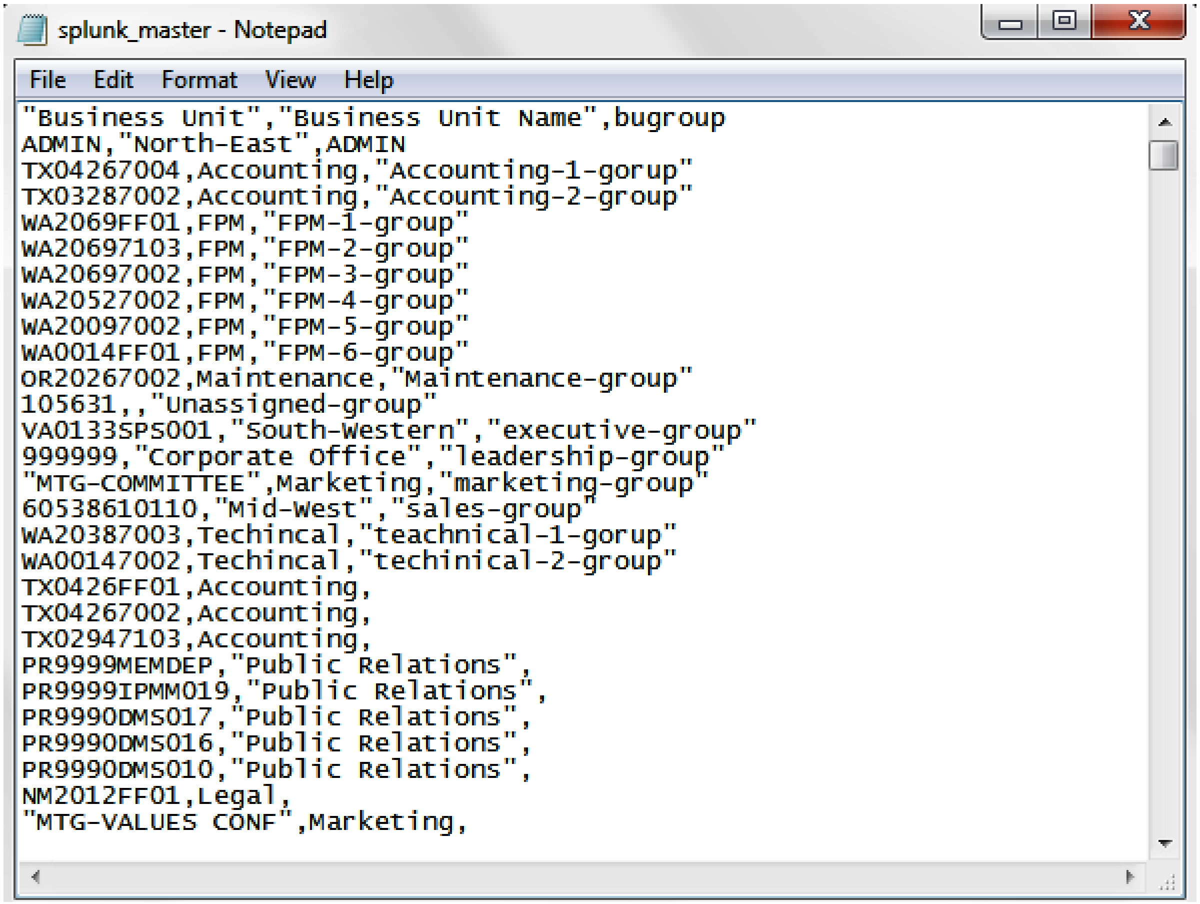
	Business Unit	Business Unit Name	bugroup
1	999999	Corporate Office	leadership-group
2	999999	Corporate Office	leadership-group
3	999999	Corporate Office	leadership-group
4	999999	Corporate Office	leadership-group
5	999999	Corporate Office	leadership-group
6	999999	Corporate Office	leadership-group
7	999999	Corporate Office	leadership-group



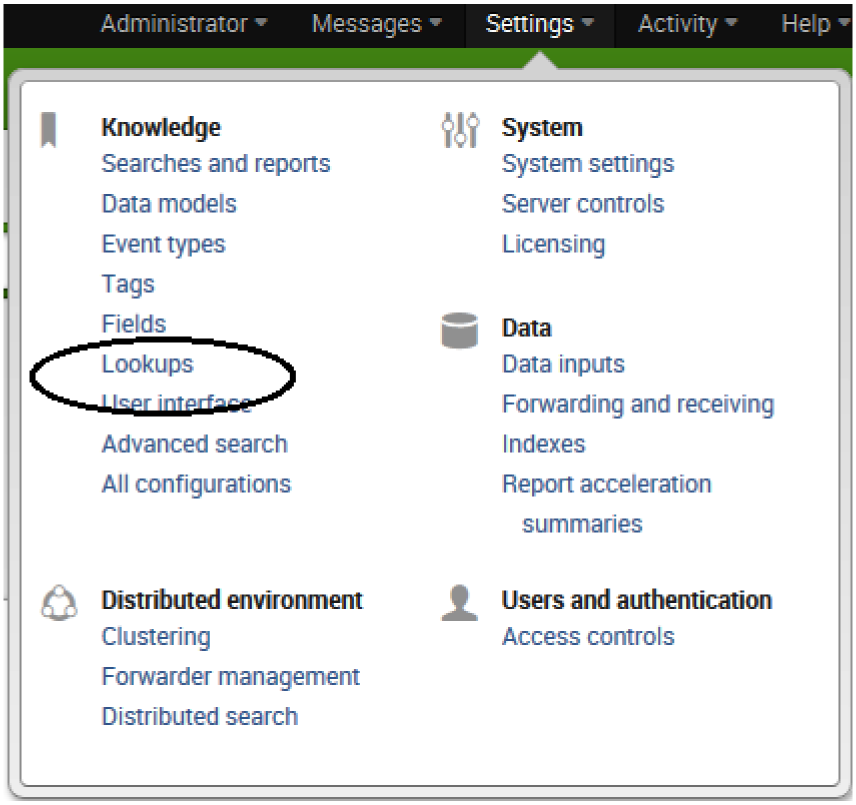
	Business Unit	Business Unit Name	bugroup
1	999999	Corporate Office	leadership-group
2	ADMIN	North-East	ADMIN
3	60538610110	Mid-West	sales-group
4	MTG-COMMITTEE	Marketing	marketing-group
5	WA20387003	Techincal	teachnical-1-gorup
6	WA00147002	Techincal	techinical-2-group
7	TX04267004	Accounting	Accounting-1-gorup
8	TX03287002	Accounting	Accounting-2-group
9	OR20267002	Maintenance	Maintenance-group

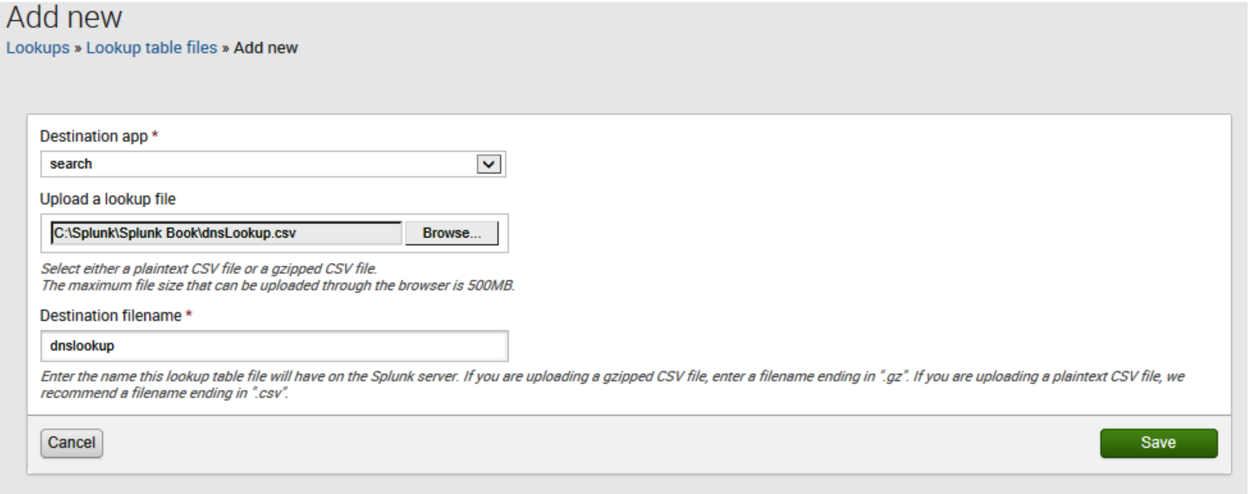


	Business Unit	Business Unit Name	bugroup
1	ADMIN	North-East	ADMIN
2	TX04267004	Accounting	Accounting-1-gorup
3	TX03287002	Accounting	Accounting-2-group
4	WA2069FF01	FPM	FPM-1-group
5	WA20697103	FPM	FPM-2-group
6	WA20697002	FPM	FPM-3-group



```
"Business Unit","Business Unit Name",bugroup
ADMIN,"North-East",ADMIN
TX04267004,Accounting,"Accounting-1-gorup"
TX03287002,Accounting,"Accounting-2-group"
WA2069FF01,FPM,"FPM-1-group"
WA20697103,FPM,"FPM-2-group"
WA20697002,FPM,"FPM-3-group"
WA20527002,FPM,"FPM-4-group"
WA20097002,FPM,"FPM-5-group"
WA0014FF01,FPM,"FPM-6-group"
OR20267002,Maintenance,"Maintenance-group"
105631,,"Unassigned-group"
VA0133SPS001,"South-Western","executive-group"
999999,"Corporate Office","leadership-group"
"MTG-COMMITTEE",Marketing,"marketing-group"
60538610110,"Mid-West","sales-group"
WA20387003,Techincal,"teachnical-1-gorup"
WA00147002,Techincal,"techinical-2-group"
TX0426FF01,Accounting,
TX04267002,Accounting,
TX02947103,Accounting,
PR9999MEMDEP,"Public Relations",
PR9999IPMM019,"Public Relations",
PR9990DMS017,"Public Relations",
PR9990DMS016,"Public Relations",
PR9990DMS010,"Public Relations",
NM2012FF01,Legal,
"MTG-VALUES CONF",Marketing,
```





Add new

Lookups » Lookup table files » Add new

Destination app *

search

Upload a lookup file

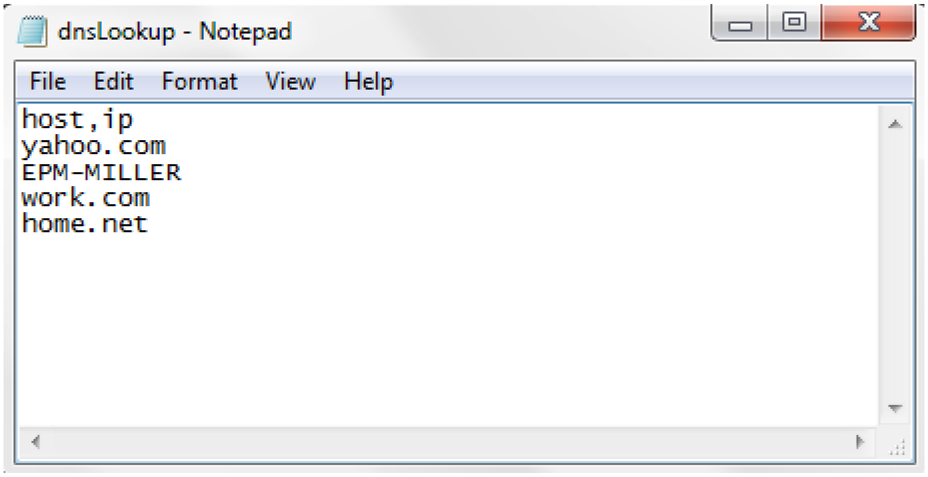
C:\Splunk\Splunk Book\dnsLookup.csv

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

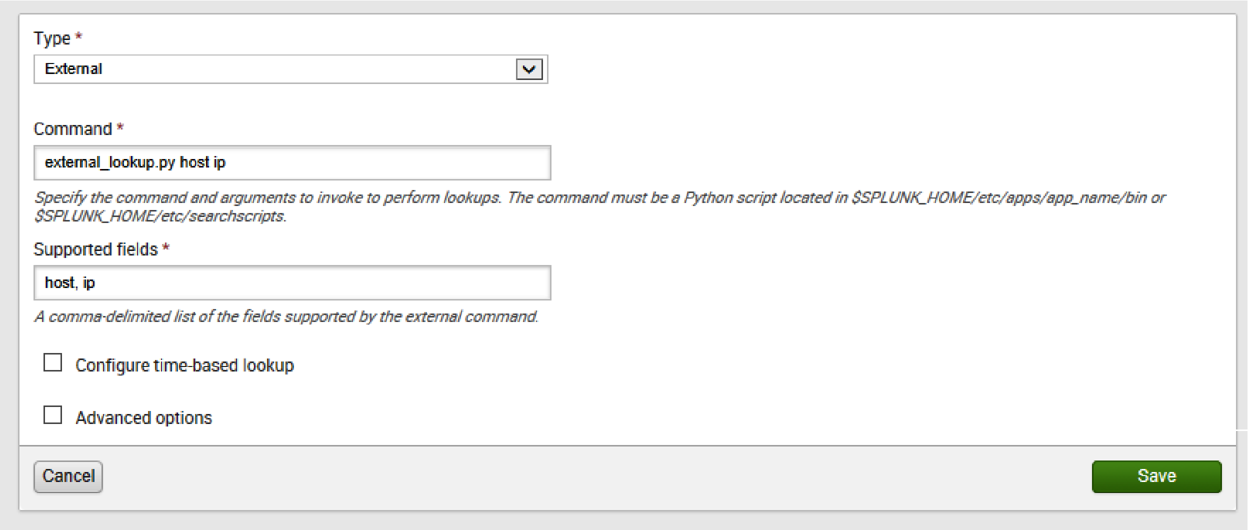
Destination filename *

dnslookup

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv".



```
host,ip
yahoo.com
EPM-MILLER
work.com
home.net
```



Type *

External

Command *

external_lookup.py host ip

Specify the command and arguments to invoke to perform lookups. The command must be a Python script located in $SPLUNK_HOME/etc/apps/app_name/bin or $SPLUNK_HOME/etc/searchscripts.

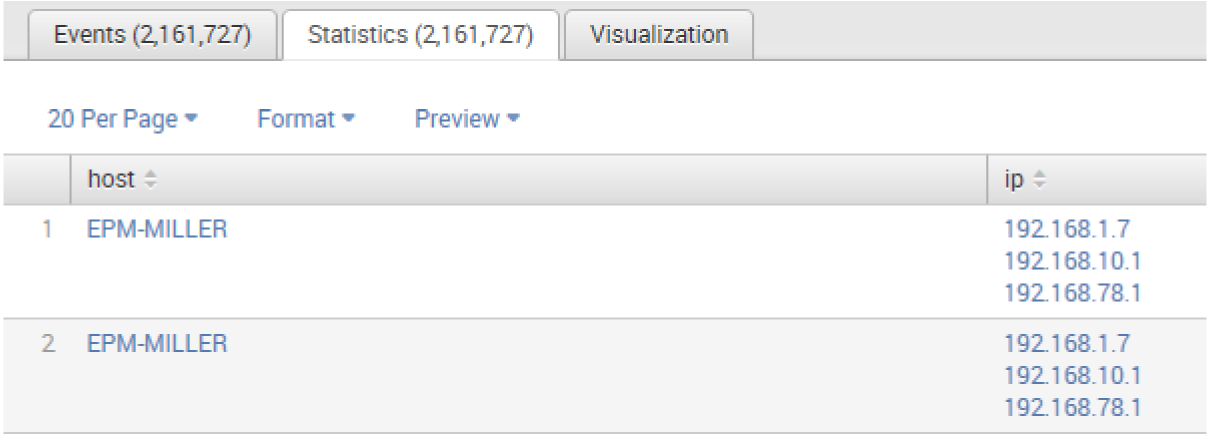
Supported fields *

host, ip

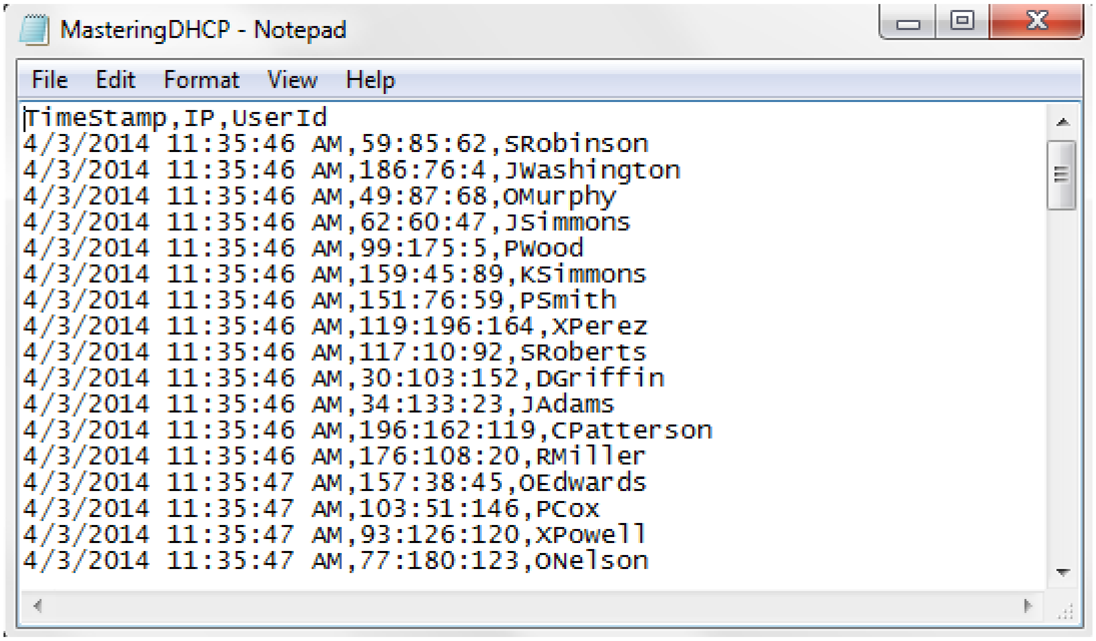
A comma-delimited list of the fields supported by the external command.

□ Configure time-based lookup

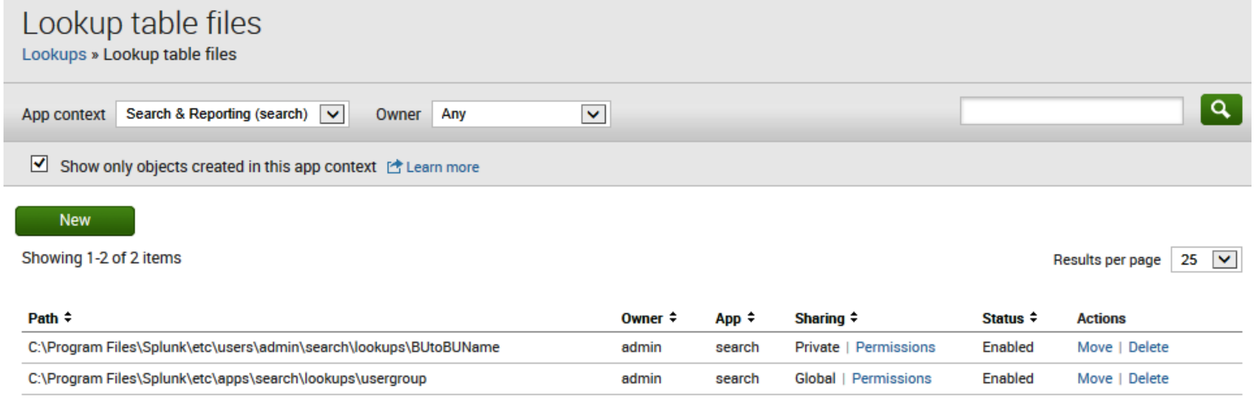
□ Advanced options



	host	ip
1	EPM-MILLER	192.168.1.7 192.168.10.1 192.168.78.1
2	EPM-MILLER	192.168.1.7 192.168.10.1 192.168.78.1



```
TimeStamp,IP,UserId
4/3/2014 11:35:46 AM,59:85:62,SRobinson
4/3/2014 11:35:46 AM,186:76:4,JWashington
4/3/2014 11:35:46 AM,49:87:68,OMurphy
4/3/2014 11:35:46 AM,62:60:47,JSimmons
4/3/2014 11:35:46 AM,99:175:5,PWood
4/3/2014 11:35:46 AM,159:45:89,KSimmons
4/3/2014 11:35:46 AM,151:76:59,PSmith
4/3/2014 11:35:46 AM,119:196:164,XPerez
4/3/2014 11:35:46 AM,117:10:92,SRoberts
4/3/2014 11:35:46 AM,30:103:152,DGriffin
4/3/2014 11:35:46 AM,34:133:23,JAdams
4/3/2014 11:35:46 AM,196:162:119,CPatterson
4/3/2014 11:35:46 AM,176:108:20,RMiller
4/3/2014 11:35:47 AM,157:38:45,OEdwards
4/3/2014 11:35:47 AM,103:51:146,PCox
4/3/2014 11:35:47 AM,93:126:120,XPowell
4/3/2014 11:35:47 AM,77:180:123,ONelson
```


Lookup table files

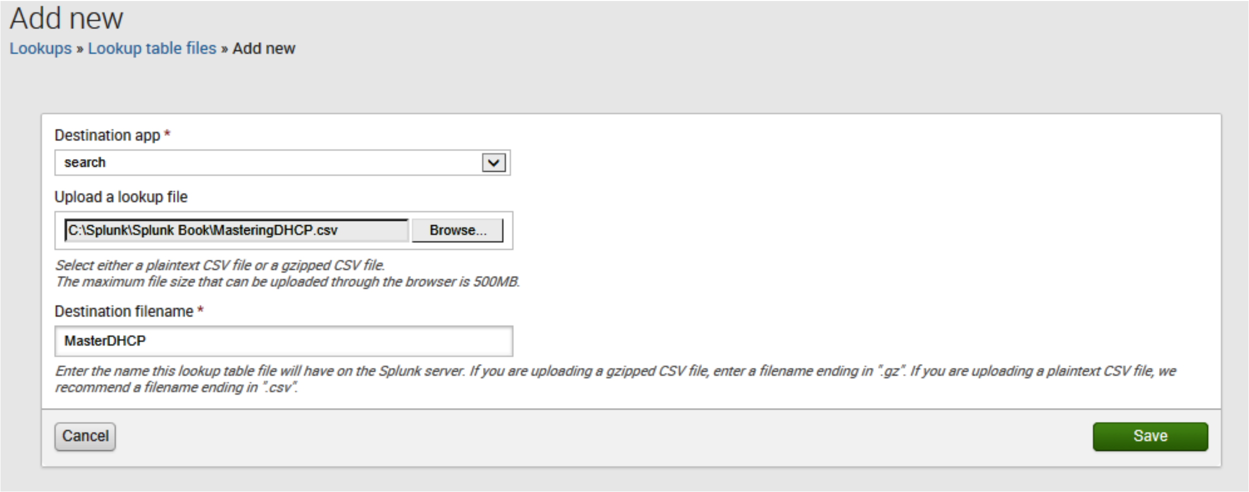
Lookups » Lookup table files

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

☑ Show only objects created in this app context Learn more

Showing 1-2 of 2 items Results per page 25

Path	Owner	App	Sharing	Status	Actions
C:\Program Files\Splunk\etc\users\admin\search\lookups\BUtoBUName	admin	search	Private | Permissions	Enabled	Move | Delete
C:\Program Files\Splunk\etc\apps\search\lookups\usergroup	admin	search	Global | Permissions	Enabled	Move | Delete



Add new

Lookups » Lookup table files » Add new

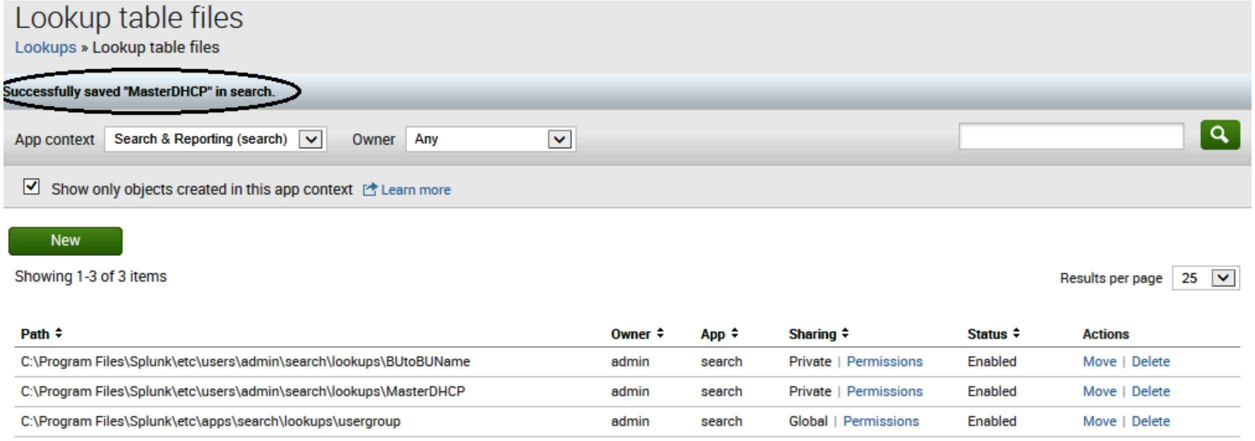
Destination app *: search

Upload a lookup file: C:\Splunk\Splunk Book\MasteringDHCP.csv

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

Destination filename *: MasterDHCP

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, we recommend a filename ending in ".csv".



Lookup table files

Lookups » Lookup table files

Successfully saved "MasterDHCP" in search.

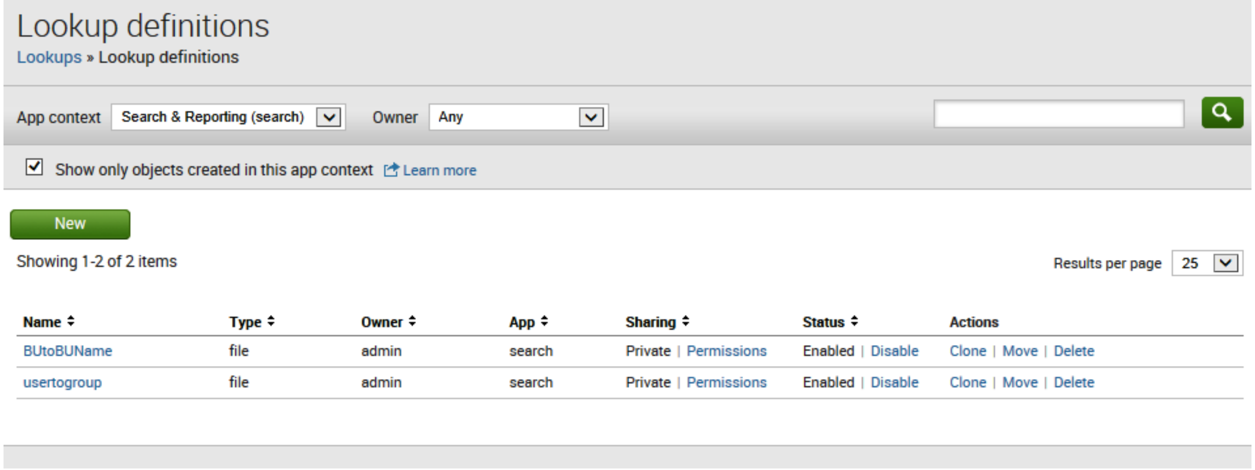
App context: Search & Reporting (search) Owner: Any

☑ Show only objects created in this app context

Showing 1-3 of 3 items

Results per page: 25

Path	Owner	App	Sharing	Status	Actions
C:\Program Files\Splunk\etc\users\admin\search\lookups\BUtoBUName	admin	search	Private | Permissions	Enabled	Move | Delete
C:\Program Files\Splunk\etc\users\admin\search\lookups\MasterDHCP	admin	search	Private | Permissions	Enabled	Move | Delete
C:\Program Files\Splunk\etc\apps\search\lookups\usergroup	admin	search	Global | Permissions	Enabled	Move | Delete



Lookup definitions

Lookups » Lookup definitions

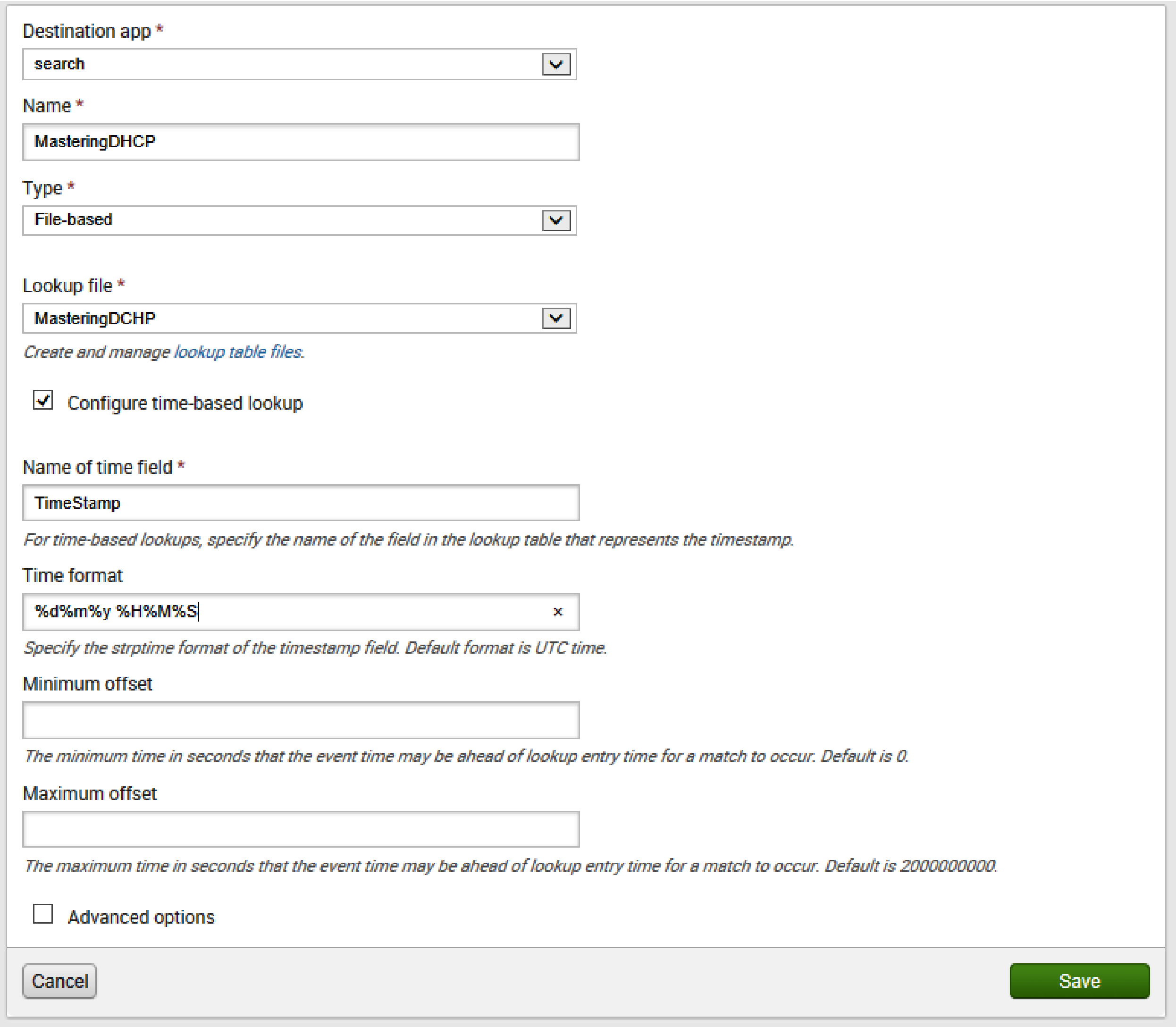
App context: Search & Reporting (search) Owner: Any

☑ Show only objects created in this app context

Showing 1-2 of 2 items

Results per page: 25

Name	Type	Owner	App	Sharing	Status	Actions
BUtoBUName	file	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete
usertogroup	file	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete



Destination app *

search

Name *

MasteringDHCP

Type *

File-based

Lookup file *

MasteringDCHP

Create and manage lookup table files.

☑ Configure time-based lookup

Name of time field *

TimeStamp

For time-based lookups, specify the name of the field in the lookup table that represents the timestamp.

Time format

%d%m%y %H%M%S

Specify the strptime format of the timestamp field. Default format is UTC time.

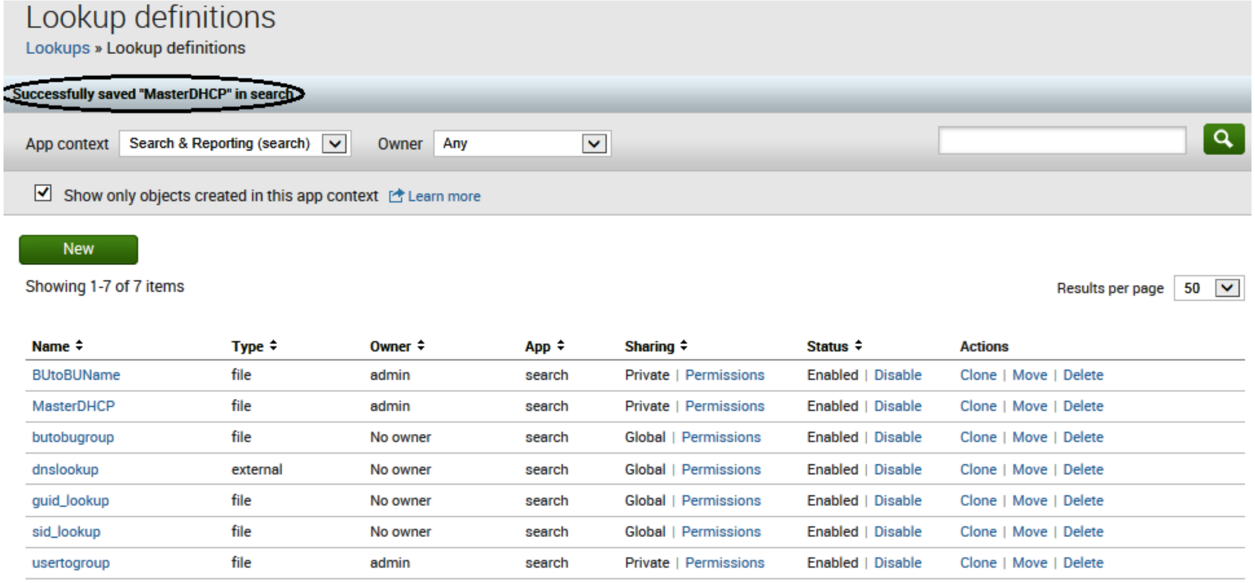
Minimum offset

The minimum time in seconds that the event time may be ahead of lookup entry time for a match to occur. Default is 0.

Maximum offset

The maximum time in seconds that the event time may be ahead of lookup entry time for a match to occur. Default is 2000000000.

□ Advanced options



Lookup definitions

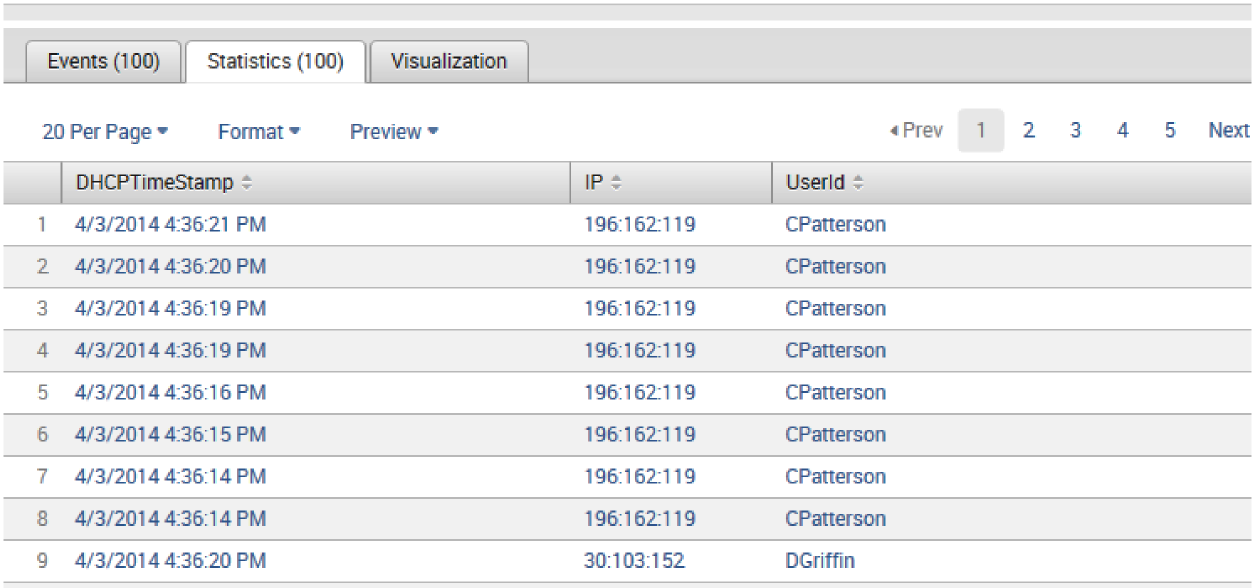
Lookups » Lookup definitions

Successfully saved "MasterDHCP" in search

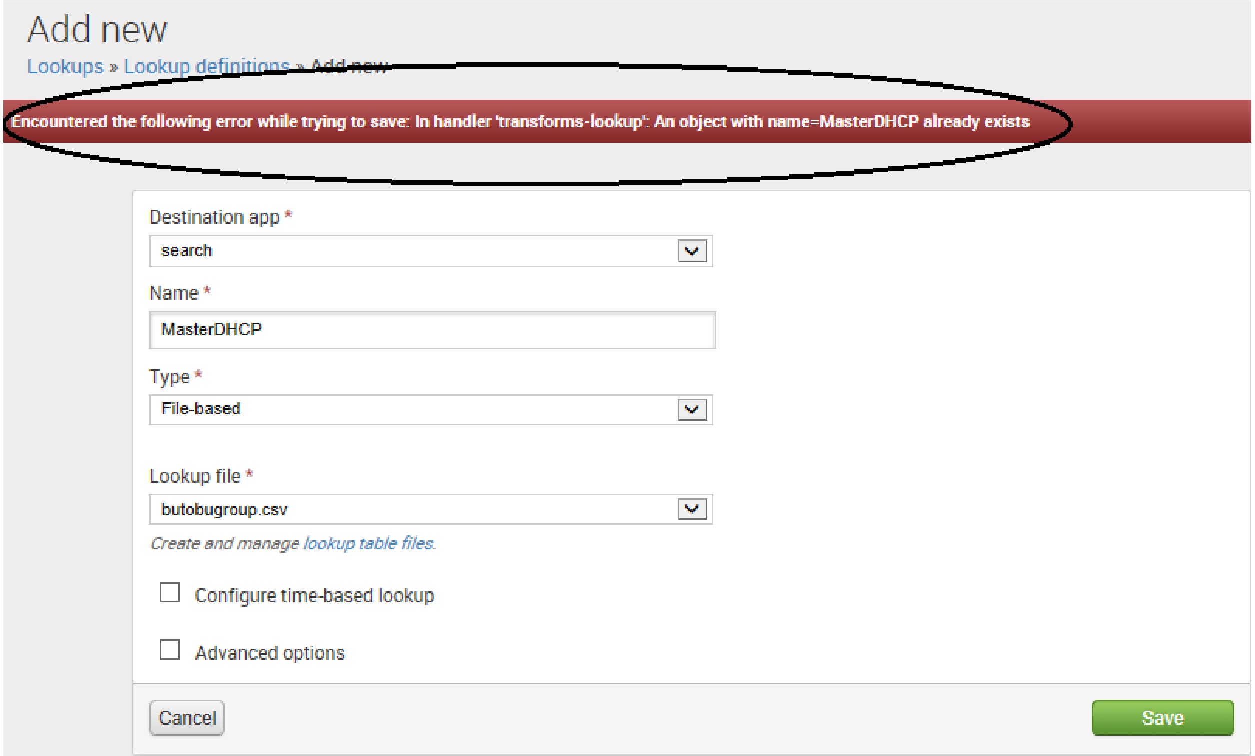
☑ Show only objects created in this app context

Showing 1-7 of 7 items

Name	Type	Owner	App	Sharing	Status	Actions
BUtoBUName	file	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete
MasterDHCP	file	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete
butobugroup	file	No owner	search	Global | Permissions	Enabled | Disable	Clone | Move | Delete
dnslookup	external	No owner	search	Global | Permissions	Enabled | Disable	Clone | Move | Delete
guid_lookup	file	No owner	search	Global | Permissions	Enabled | Disable	Clone | Move | Delete
sid_lookup	file	No owner	search	Global | Permissions	Enabled | Disable	Clone | Move | Delete
usertogroup	file	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete



	DHCPTimeStamp	IP	UserId
1	4/3/2014 4:36:21 PM	196:162:119	CPatterson
2	4/3/2014 4:36:20 PM	196:162:119	CPatterson
3	4/3/2014 4:36:19 PM	196:162:119	CPatterson
4	4/3/2014 4:36:19 PM	196:162:119	CPatterson
5	4/3/2014 4:36:16 PM	196:162:119	CPatterson
6	4/3/2014 4:36:15 PM	196:162:119	CPatterson
7	4/3/2014 4:36:14 PM	196:162:119	CPatterson
8	4/3/2014 4:36:14 PM	196:162:119	CPatterson
9	4/3/2014 4:36:20 PM	30:103:152	DGriffin



Add new

Lookups » Lookup definitions » Add new

Encountered the following error while trying to save: In handler 'transforms-lookup': An object with name=MasterDHCP already exists

Destination app *: search

Name *: MasterDHCP

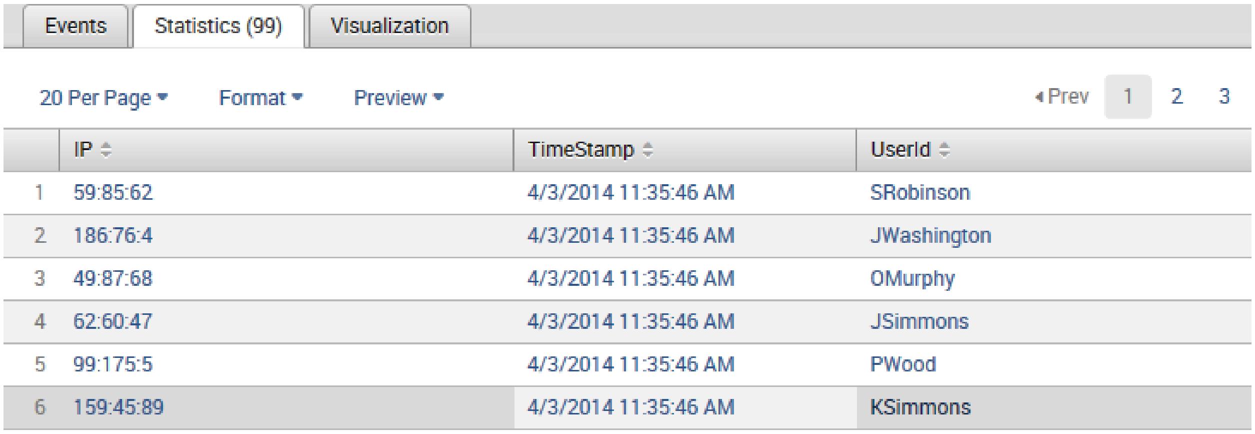
Type *: File-based

Lookup file *: butobugroup.csv

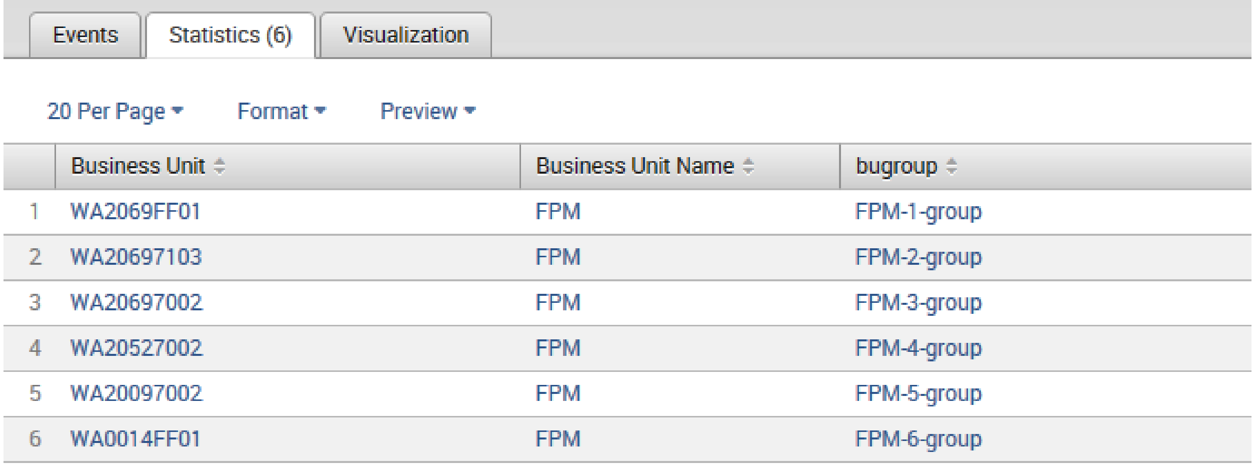
Create and manage lookup table files.

□ Configure time-based lookup

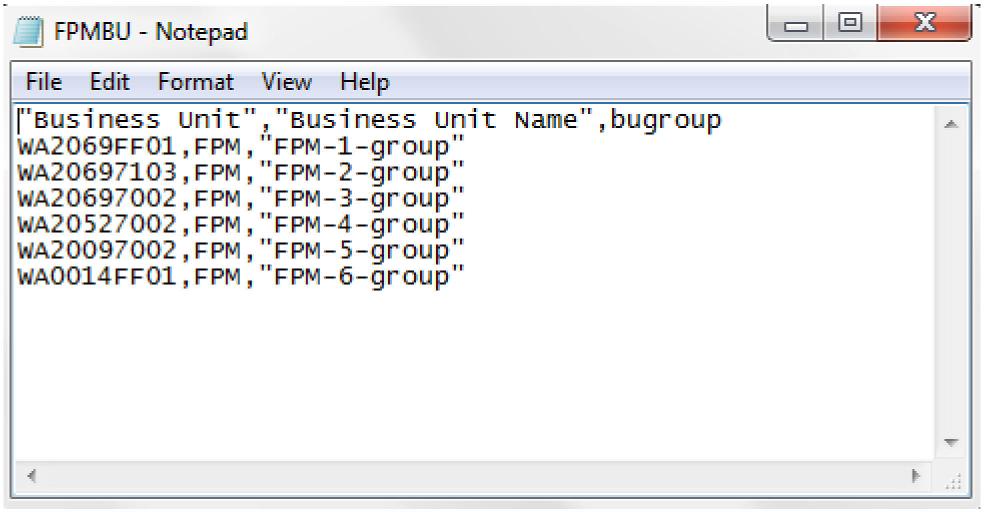
□ Advanced options



	IP	TimeStamp	UserId
1	59:85:62	4/3/2014 11:35:46 AM	SRobinson
2	186:76:4	4/3/2014 11:35:46 AM	JWashington
3	49:87:68	4/3/2014 11:35:46 AM	OMurphy
4	62:60:47	4/3/2014 11:35:46 AM	JSimmons
5	99:175:5	4/3/2014 11:35:46 AM	PWood
6	159:45:89	4/3/2014 11:35:46 AM	KSimmons

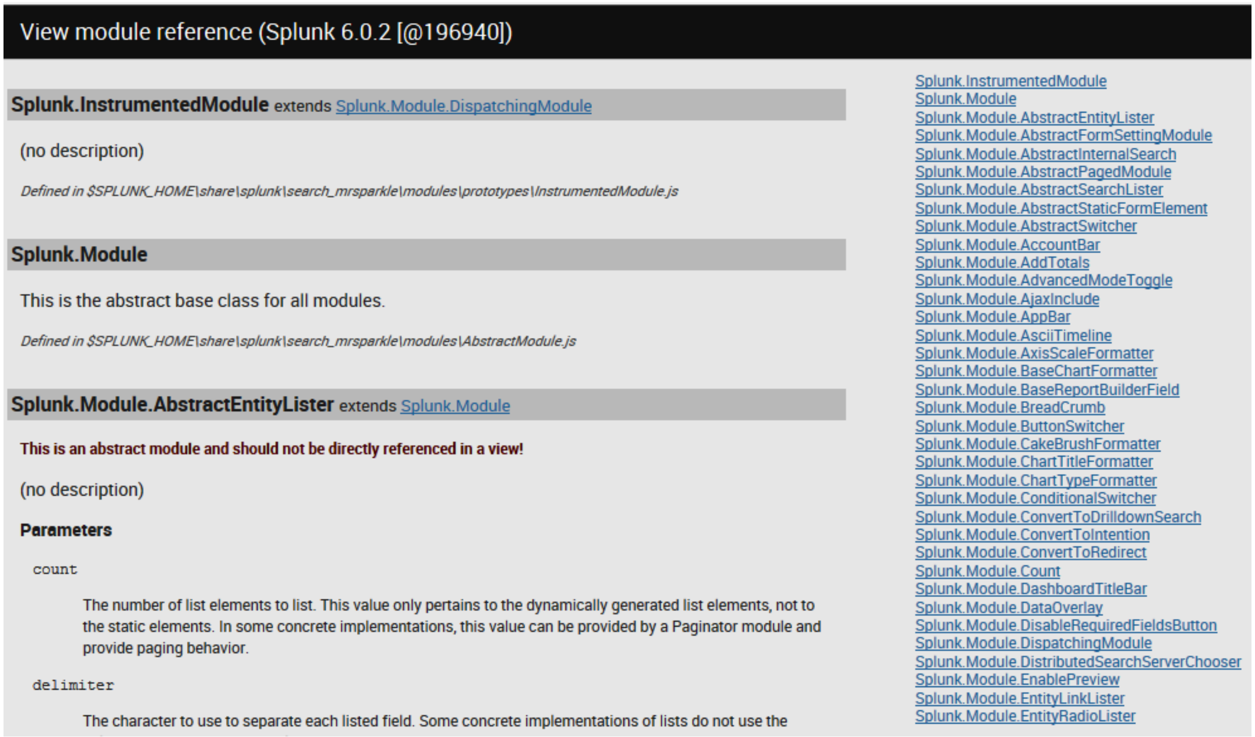


	Business Unit	Business Unit Name	bugroup
1	WA2069FF01	FPM	FPM-1-group
2	WA20697103	FPM	FPM-2-group
3	WA20697002	FPM	FPM-3-group
4	WA20527002	FPM	FPM-4-group
5	WA20097002	FPM	FPM-5-group
6	WA0014FF01	FPM	FPM-6-group



```
"Business Unit","Business Unit Name",bugroup
WA2069FF01,FPM,"FPM-1-group"
WA20697103,FPM,"FPM-2-group"
WA20697002,FPM,"FPM-3-group"
WA20527002,FPM,"FPM-4-group"
WA20097002,FPM,"FPM-5-group"
WA0014FF01,FPM,"FPM-6-group"
```

Chapter 5, *Progressive Dashboards*



View module reference (Splunk 6.0.2 [@196940])

Splunk.InstrumentedModule extends Splunk.Module.DispatchingModule

(no description)

Defined in $SPLUNK_HOME\share\splunk\search_mrsparkle\modules\prototypes\InstrumentedModule.js

Splunk.Module

This is the abstract base class for all modules.

Defined in $SPLUNK_HOME\share\splunk\search_mrsparkle\modules\AbstractModule.js

Splunk.Module.AbstractEntityLister extends Splunk.Module

This is an abstract module and should not be directly referenced in a view!

(no description)

Parameters

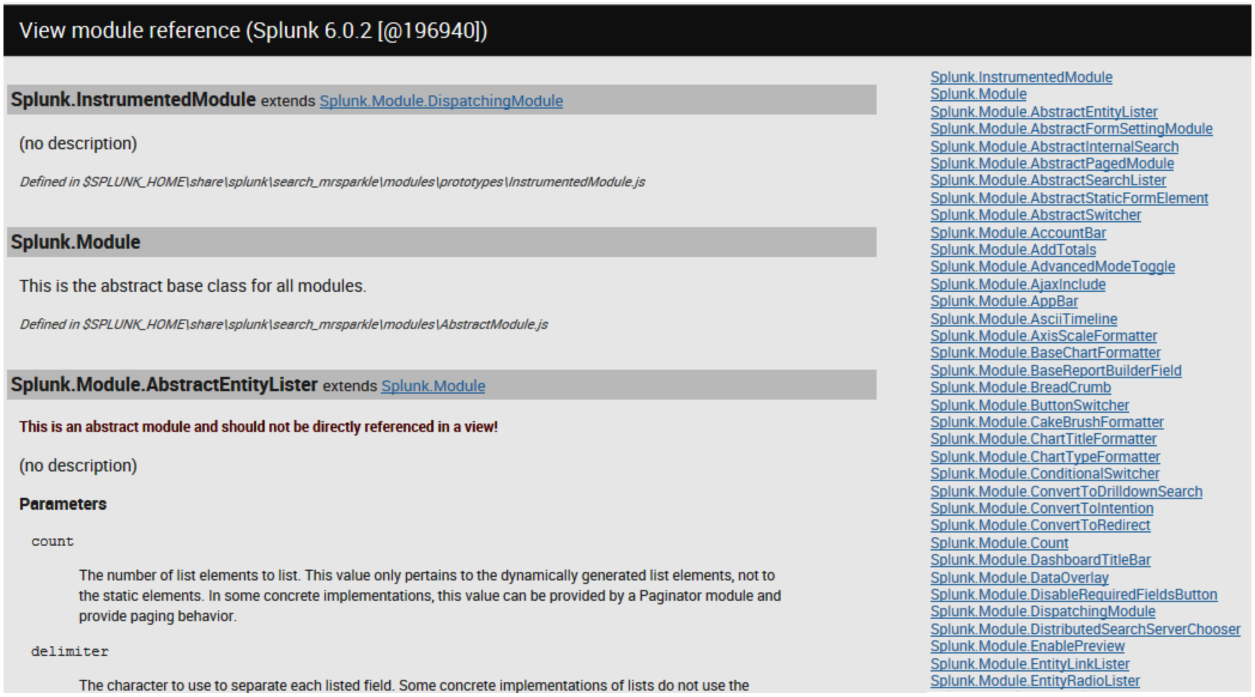
`count`

The number of list elements to list. This value only pertains to the dynamically generated list elements, not to the static elements. In some concrete implementations, this value can be provided by a Paginator module and provide paging behavior.

`delimiter`

The character to use to separate each listed field. Some concrete implementations of lists do not use the

Splunk.InstrumentedModule
Splunk.Module
Splunk.Module.AbstractEntityLister
Splunk.Module.AbstractFormSettingModule
Splunk.Module.AbstractInternalSearch
Splunk.Module.AbstractPagedModule
Splunk.Module.AbstractSearchLister
Splunk.Module.AbstractStaticFormElement
Splunk.Module.AbstractSwitcher
Splunk.Module.AccountBar
Splunk.Module.AddTotals
Splunk.Module.AdvancedModeToggle
Splunk.Module.AjaxInclude
Splunk.Module.AppBar
Splunk.Module.AsciiTimeline
Splunk.Module.AxisScaleFormatter
Splunk.Module.BaseChartFormatter
Splunk.Module.BaseReportBuilderField
Splunk.Module.BreadCrumb
Splunk.Module.ButtonSwitcher
Splunk.Module.CakeBrushFormatter
Splunk.Module.ChartTitleFormatter
Splunk.Module.ChartTypeFormatter
Splunk.Module.ConditionalSwitcher
Splunk.Module.ConvertToDrilldownSearch
Splunk.Module.ConvertToIntention
Splunk.Module.ConvertToRedirect
Splunk.Module.Count
Splunk.Module.DashboardTitleBar
Splunk.Module.DataOverlay
Splunk.Module.DisableRequiredFieldsButton
Splunk.Module.DispatchingModule
Splunk.Module.DistributedSearchServerChooser
Splunk.Module.EnablePreview
Splunk.Module.EntityLinkLister
Splunk.Module.EntityRadioLister



View module reference (Splunk 6.0.2 [@196940])

Splunk.InstrumentedModule extends Splunk.Module.DispatchingModule

(no description)

Defined in $SPLUNK_HOME\share\splunk\search_mrsparkle\modules\prototypes\InstrumentedModule.js

Splunk.Module

This is the abstract base class for all modules.

Defined in $SPLUNK_HOME\share\splunk\search_mrsparkle\modules\AbstractModule.js

Splunk.Module.AbstractEntityLister extends Splunk.Module

This is an abstract module and should not be directly referenced in a view!

(no description)

Parameters

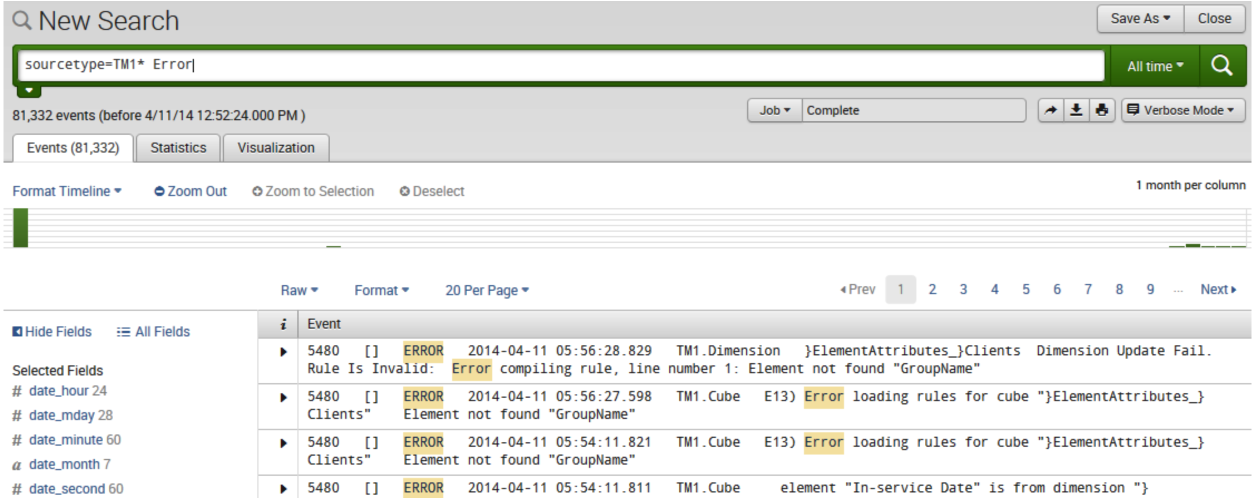
`count`

The number of list elements to list. This value only pertains to the dynamically generated list elements, not to the static elements. In some concrete implementations, this value can be provided by a Paginator module and provide paging behavior.

`delimiter`

The character to use to separate each listed field. Some concrete implementations of lists do not use the

- Splunk.InstrumentedModule
- Splunk.Module
- Splunk.Module.AbstractEntityLister
- Splunk.Module.AbstractFormSettingModule
- Splunk.Module.AbstractInternalSearch
- Splunk.Module.AbstractPagedModule
- Splunk.Module.AbstractSearchLister
- Splunk.Module.AbstractStaticFormElement
- Splunk.Module.AbstractSwitcher
- Splunk.Module.AccountBar
- Splunk.Module.AddTotals
- Splunk.Module.AdvancedModeToggle
- Splunk.Module.AjaxInclude
- Splunk.Module.AppBar
- Splunk.Module.AsciiTimeline
- Splunk.Module.AxisScaleFormatter
- Splunk.Module.BaseChartFormatter
- Splunk.Module.BaseReportBuilderField
- Splunk.Module.BreadCrumb
- Splunk.Module.ButtonSwitcher
- Splunk.Module.CakeBrushFormatter
- Splunk.Module.ChartTitleFormatter
- Splunk.Module.ChartTypeFormatter
- Splunk.Module.ConditionalSwitcher
- Splunk.Module.ConvertToDrilldownSearch
- Splunk.Module.ConvertToIntention
- Splunk.Module.ConvertToRedirect
- Splunk.Module.Count
- Splunk.Module.DashboardTitleBar
- Splunk.Module.DataOverlay
- Splunk.Module.DisableRequiredFieldsButton
- Splunk.Module.DispatchingModule
- Splunk.Module.DistributedSearchServerChooser
- Splunk.Module.EnablePreview
- Splunk.Module.EntityLinkLister
- Splunk.Module.EntityRadioLister



```
sourcetype=TM1* Error
```

81,332 events (before 4/11/14 12:52:24.000 PM)

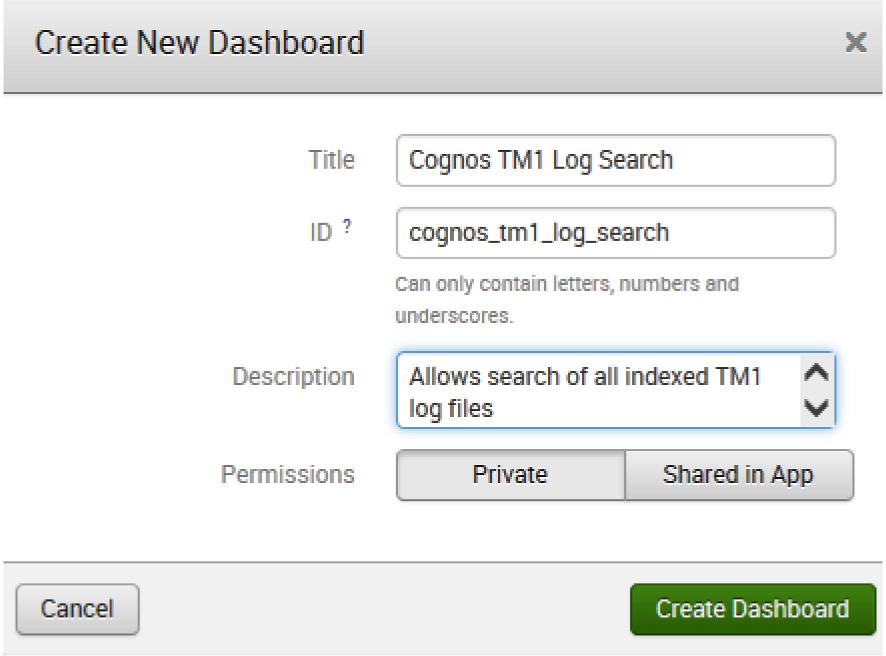
Complete

Selected Fields

- # date_hour 24
- # date_mday 28
- # date_minute 60
- a date_month 7
- # date_second 60

Event

```
5480   []   ERROR   2014-04-11 05:56:28.829   TM1.Dimension   }ElementAttributes_}Clients  Dimension Update Fail.
Rule Is Invalid:  Error compiling rule, line number 1: Element not found "GroupName"
5480   []   ERROR   2014-04-11 05:56:27.598   TM1.Cube    E13) Error loading rules for cube "}ElementAttributes_}
Clients"   Element not found "GroupName"
5480   []   ERROR   2014-04-11 05:54:11.821   TM1.Cube    E13) Error loading rules for cube "}ElementAttributes_}
Clients"   Element not found "GroupName"
5480   []   ERROR   2014-04-11 05:54:11.811   TM1.Cube     element "In-service Date" is from dimension "}
```



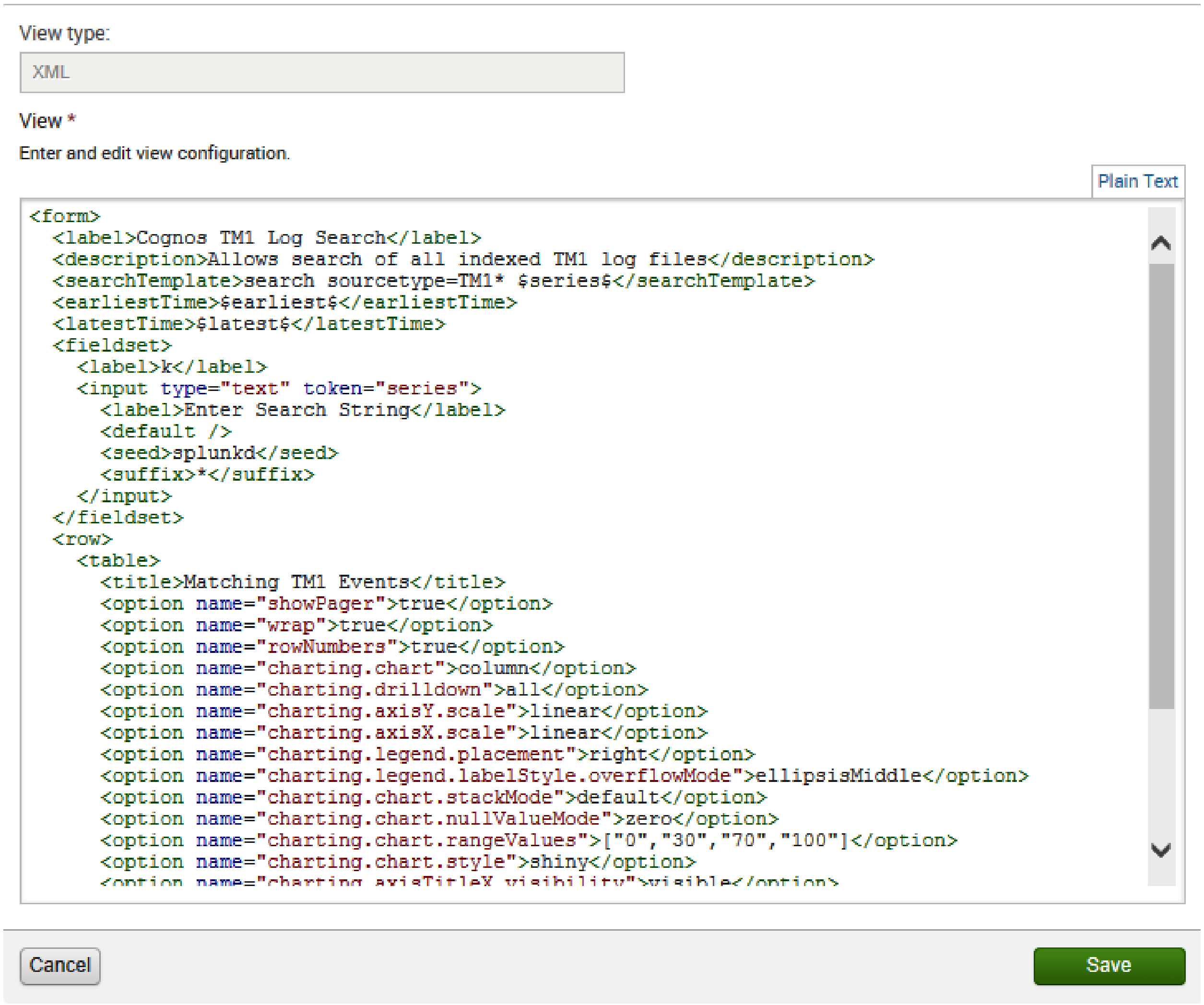
Title: Cognos TM1 Log Search

ID ?: cognos_tm1_log_search

Can only contain letters, numbers and underscores.

Description: Allows search of all indexed TM1 log files

Permissions: Private | Shared in App

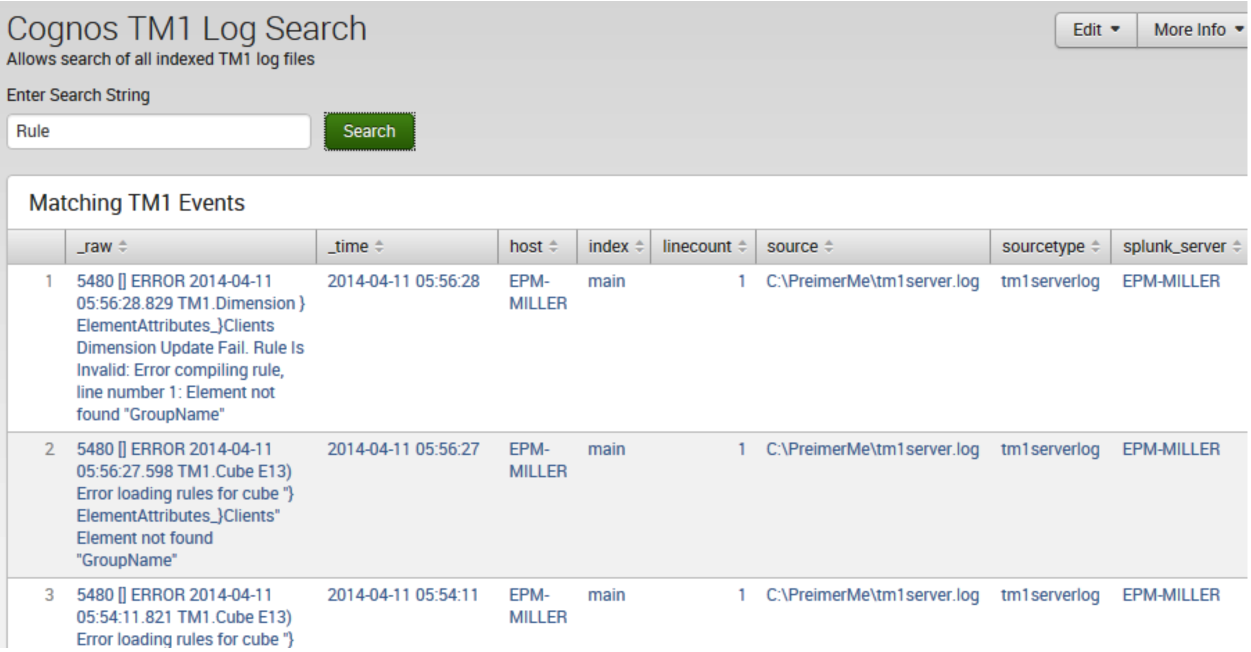


View type: XML

View *

Enter and edit view configuration.

```
<form>
  <label>Cognos TM1 Log Search</label>
  <description>Allows search of all indexed TM1 log files</description>
  <searchTemplate>search sourcetype=TM1* $series$</searchTemplate>
  <earliestTime>$earliest$</earliestTime>
  <latestTime>$latest$</latestTime>
  <fieldset>
    <label>k</label>
    <input type="text" token="series">
      <label>Enter Search String</label>
      <default />
      <seed>splunkd</seed>
      <suffix>*</suffix>
    </input>
  </fieldset>
  <row>
    <table>
      <title>Matching TM1 Events</title>
      <option name="showPager">true</option>
      <option name="wrap">true</option>
      <option name="rowNumbers">true</option>
      <option name="charting.chart">column</option>
      <option name="charting.drilldown">all</option>
      <option name="charting.axisY.scale">linear</option>
      <option name="charting.axisX.scale">linear</option>
      <option name="charting.legend.placement">right</option>
      <option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>
      <option name="charting.chart.stackMode">default</option>
      <option name="charting.chart.nullValueMode">zero</option>
      <option name="charting.chart.rangeValues">["0","30","70","100"]</option>
      <option name="charting.chart.style">shiny</option>
      <option name="charting.axisTitleX.visibility">visible</option>
```



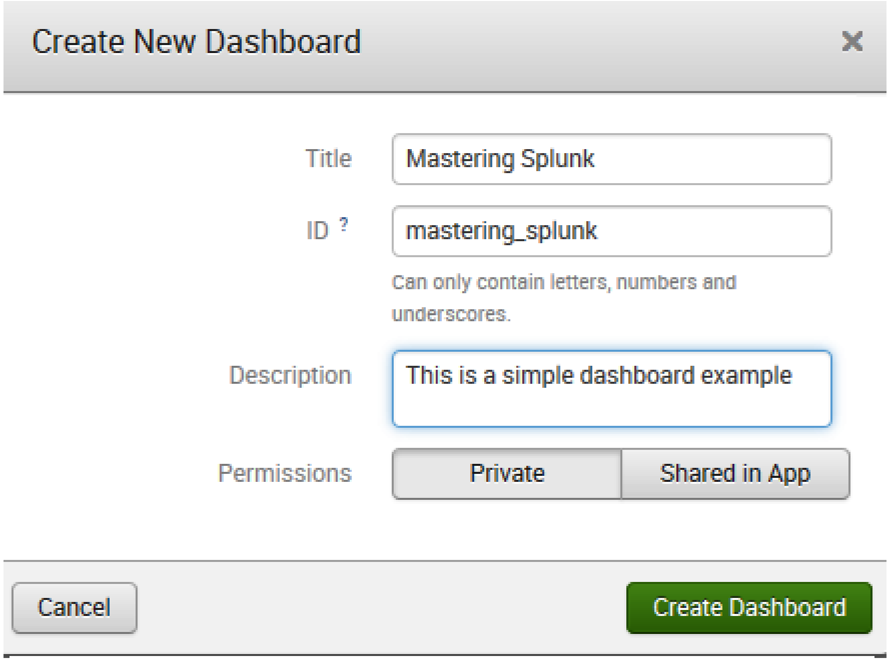
Cognos TM1 Log Search

Allows search of all indexed TM1 log files

Enter Search String: Rule

Matching TM1 Events

	_raw	_time	host	index	linecount	source	sourcetype	splunk_server
1	5480 [] ERROR 2014-04-11 05:56:28.829 TM1.Dimension } ElementAttributes_}Clients Dimension Update Fail. Rule Is Invalid: Error compiling rule, line number 1: Element not found "GroupName"	2014-04-11 05:56:28	EPM-MILLER	main	1	C:\PreimerMe\tm1server.log	tm1serverlog	EPM-MILLER
2	5480 [] ERROR 2014-04-11 05:56:27.598 TM1.Cube E13) Error loading rules for cube "} ElementAttributes_}Clients" Element not found "GroupName"	2014-04-11 05:56:27	EPM-MILLER	main	1	C:\PreimerMe\tm1server.log	tm1serverlog	EPM-MILLER
3	5480 [] ERROR 2014-04-11 05:54:11.821 TM1.Cube E13) Error loading rules for cube "}	2014-04-11 05:54:11	EPM-MILLER	main	1	C:\PreimerMe\tm1server.log	tm1serverlog	EPM-MILLER



Create New Dashboard

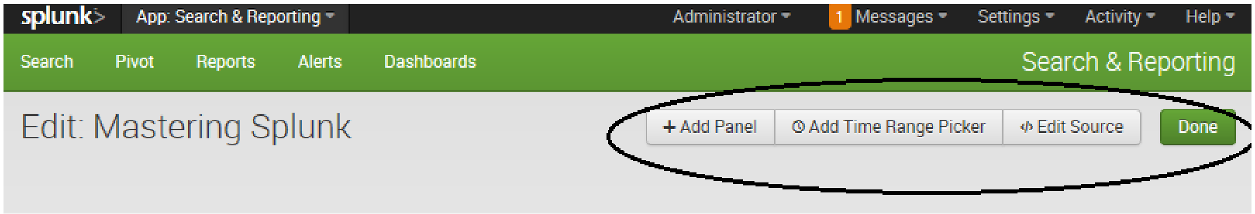
Title: Mastering Splunk

ID ?: mastering_splunk

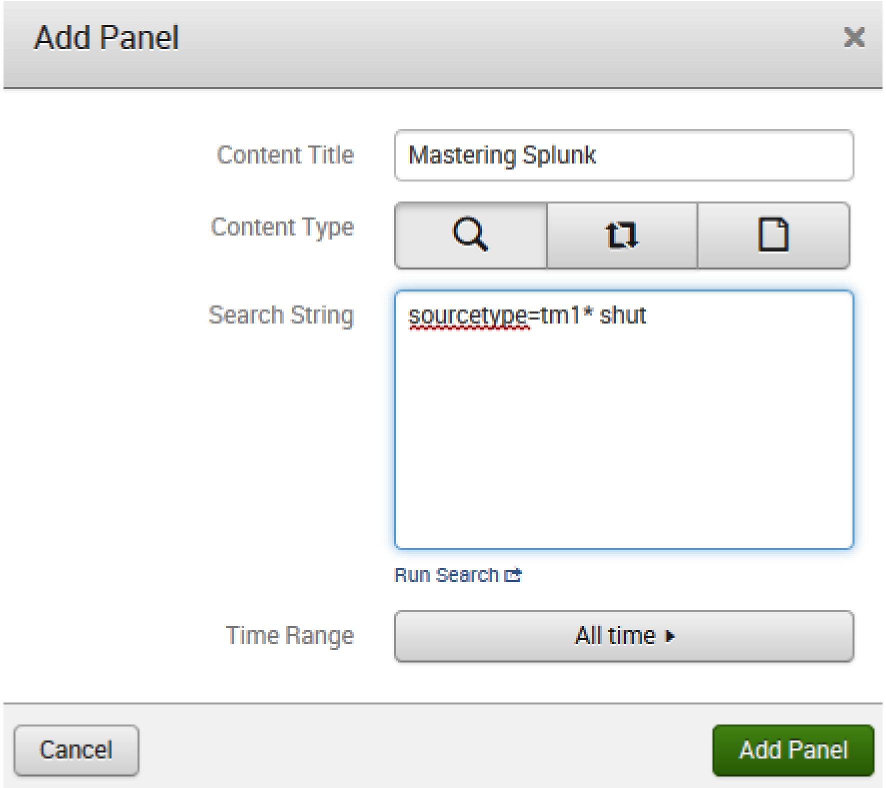
Can only contain letters, numbers and underscores.

Description: This is a simple dashboard example

Permissions: Private | Shared in App



Edit: Mastering Splunk

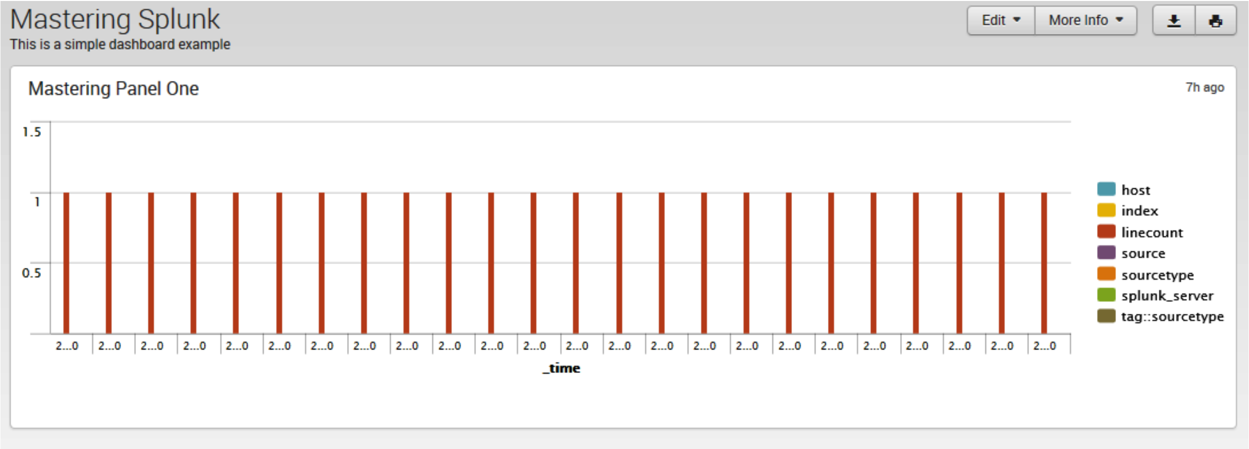


Content Title: Mastering Splunk

Content Type

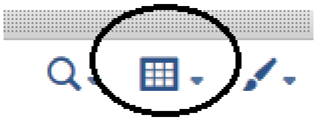
Search String: sourcetype=tm1* shut

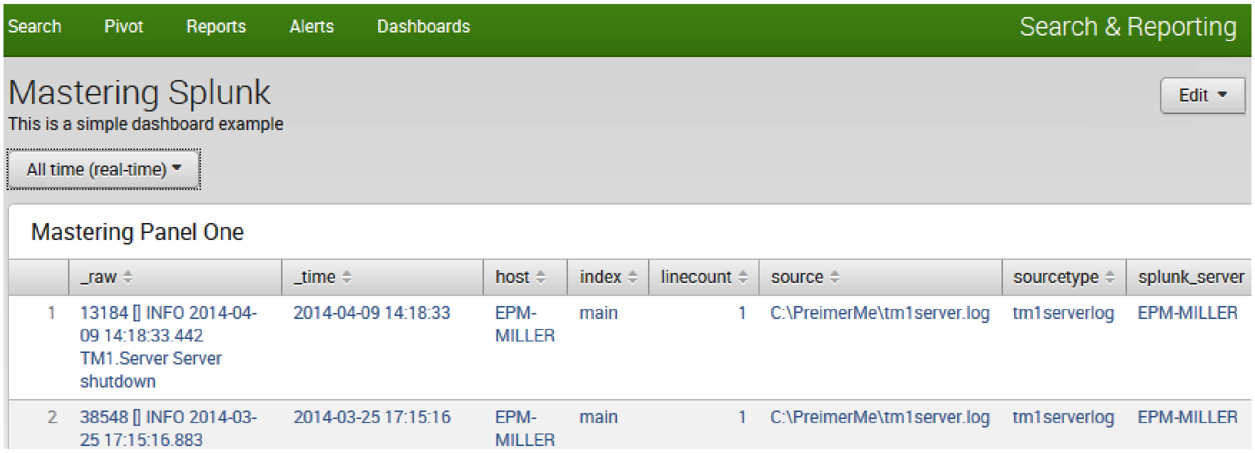
Time Range: All time



Mastering Splunk

This is a simple dashboard example



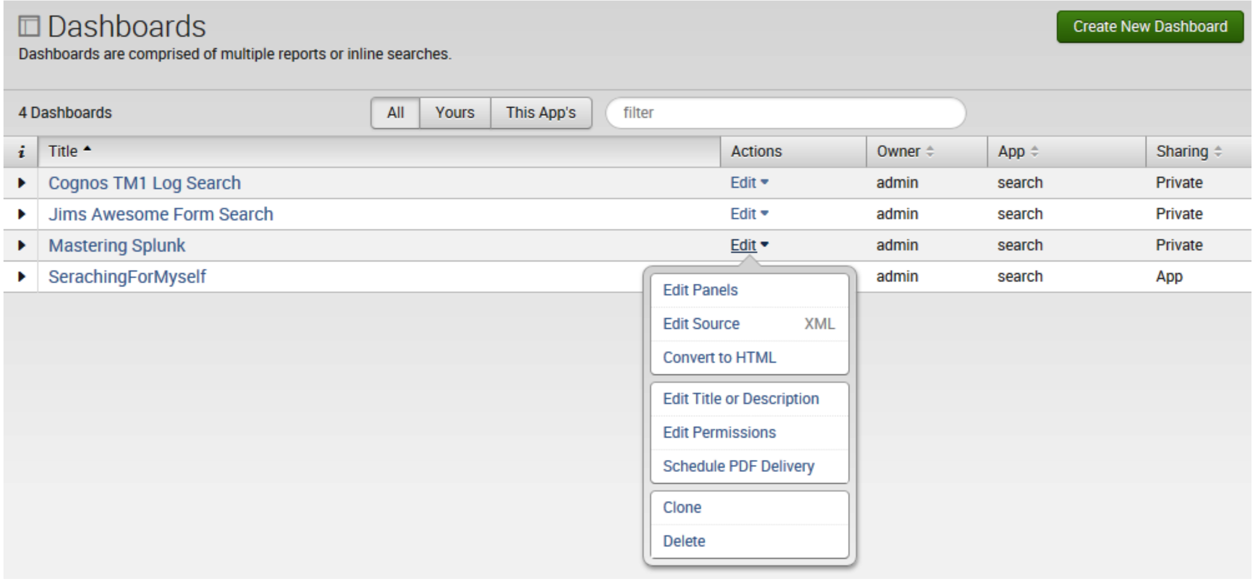


Mastering Splunk

This is a simple dashboard example

Mastering Panel One

	_raw	_time	host	index	linecount	source	sourcetype	splunk_server
1	13184 [] INFO 2014-04-09 14:18:33.442 TM1.Server Server shutdown	2014-04-09 14:18:33	EPM-MILLER	main	1	C:\PreimerMe\tm1server.log	tm1serverlog	EPM-MILLER
2	38548 [] INFO 2014-03-25 17:15:16.883	2014-03-25 17:15:16	EPM-MILLER	main	1	C:\PreimerMe\tm1server.log	tm1serverlog	EPM-MILLER

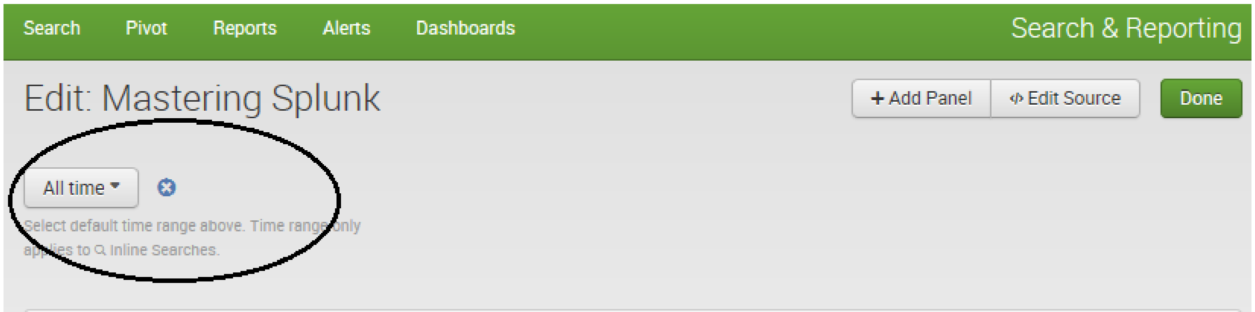


Dashboards

Dashboards are comprised of multiple reports or inline searches.

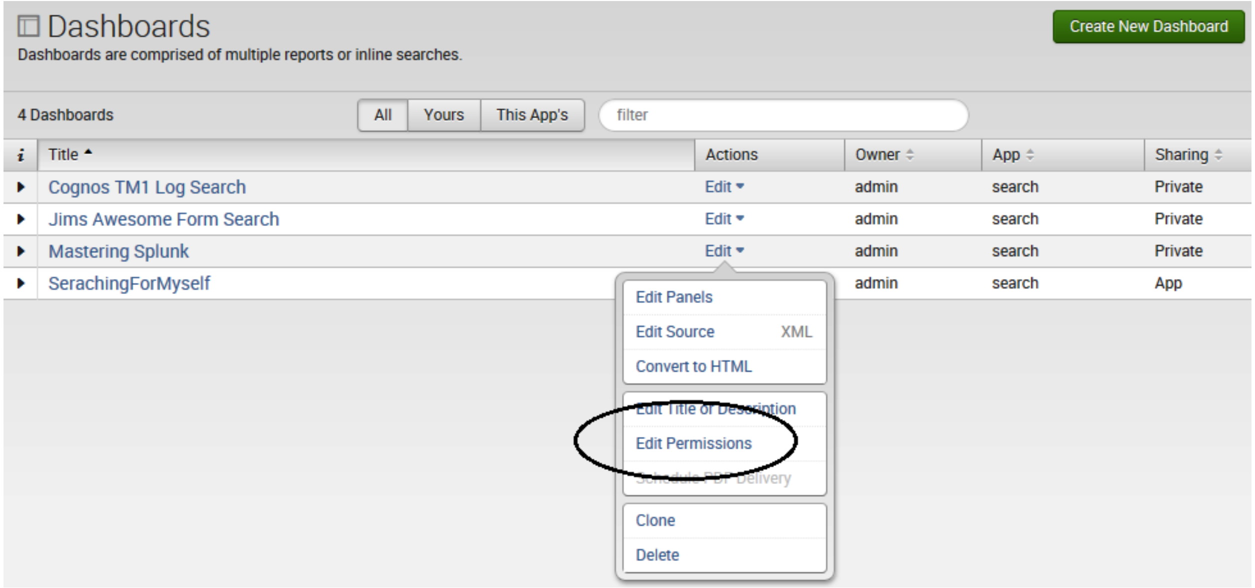
4 Dashboards

i	Title	Actions	Owner	App	Sharing
▸	Cognos TM1 Log Search	Edit	admin	search	Private
▸	Jims Awesome Form Search	Edit	admin	search	Private
▸	Mastering Splunk	Edit	admin	search	Private
▸	SerachingForMyself		admin	search	App



Edit: Mastering Splunk

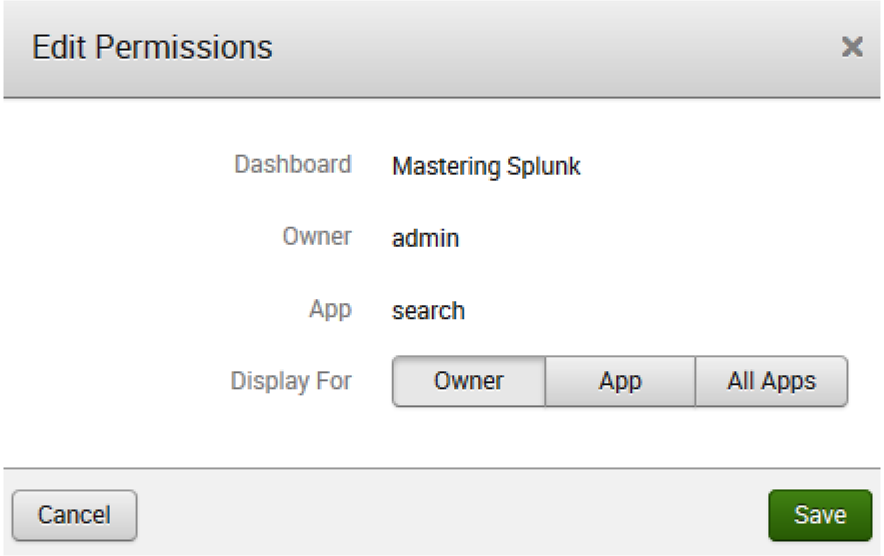
Select default time range above. Time range only applies to Inline Searches.



Dashboards

Dashboards are comprised of multiple reports or inline searches.

i	Title	Actions	Owner	App	Sharing
▸	Cognos TM1 Log Search	Edit ▾	admin	search	Private
▸	Jims Awesome Form Search	Edit ▾	admin	search	Private
▸	Mastering Splunk	Edit ▾	admin	search	Private
▸	SerachingForMyself		admin	search	App



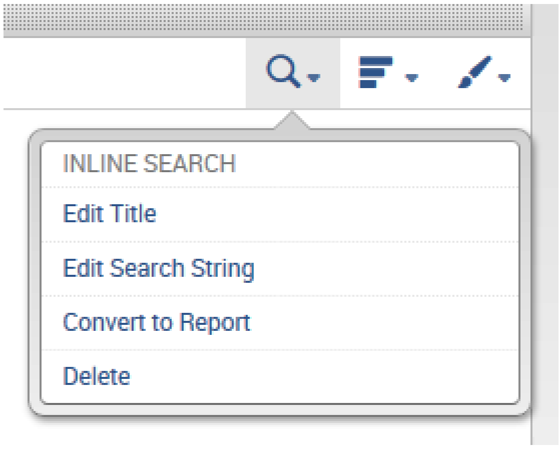
Edit Permissions

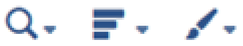
Dashboard: Mastering Splunk

Owner: admin

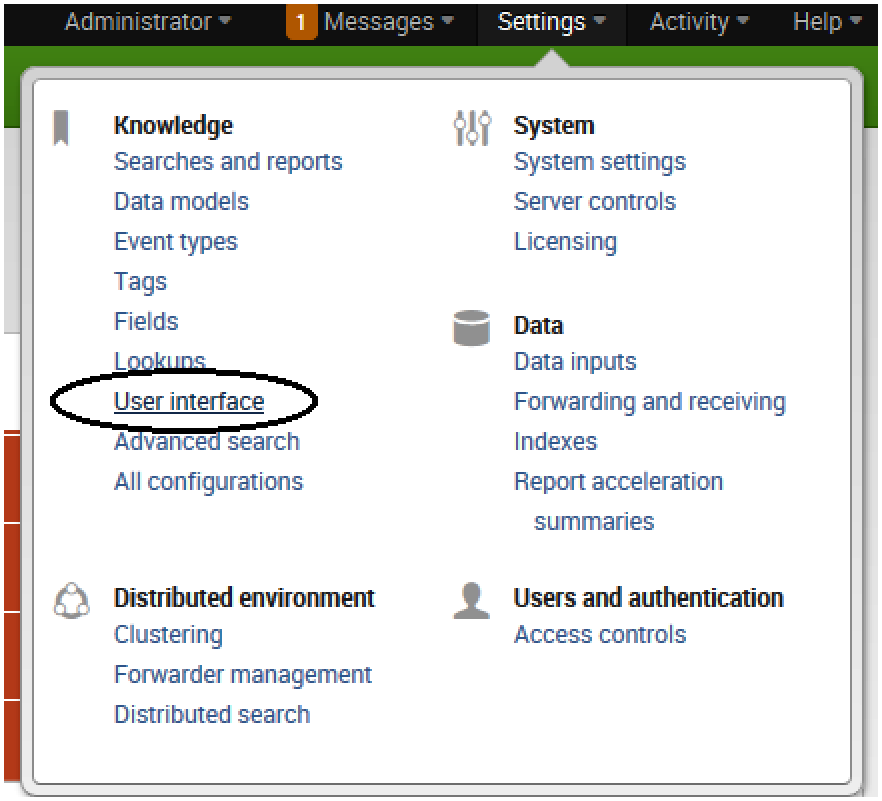
App: search

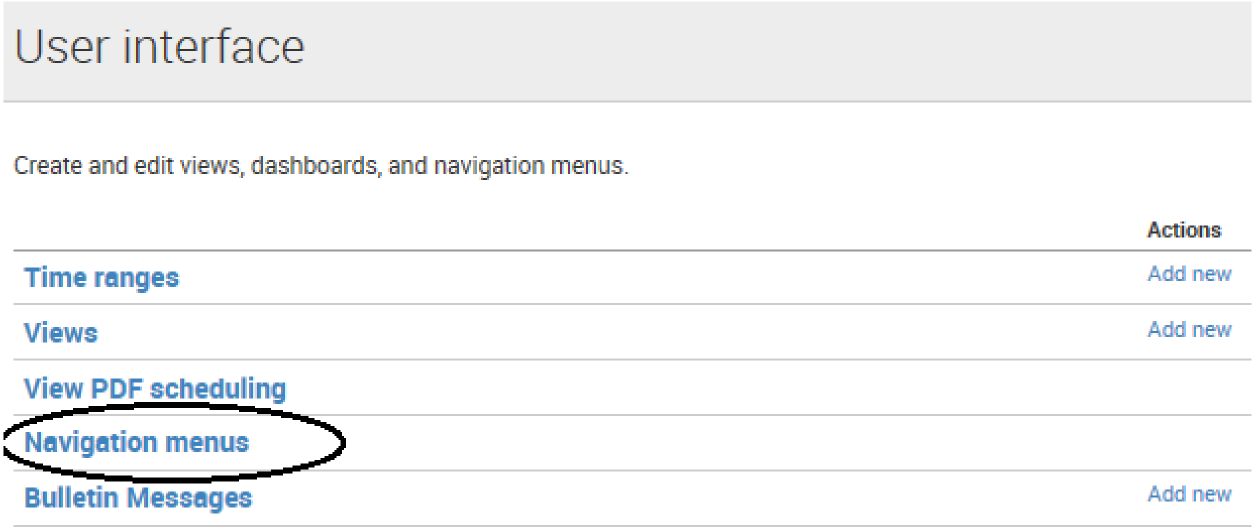
Display For: Owner | App | All Apps





(Panel Properties, Visualization Type, Visualization Format)

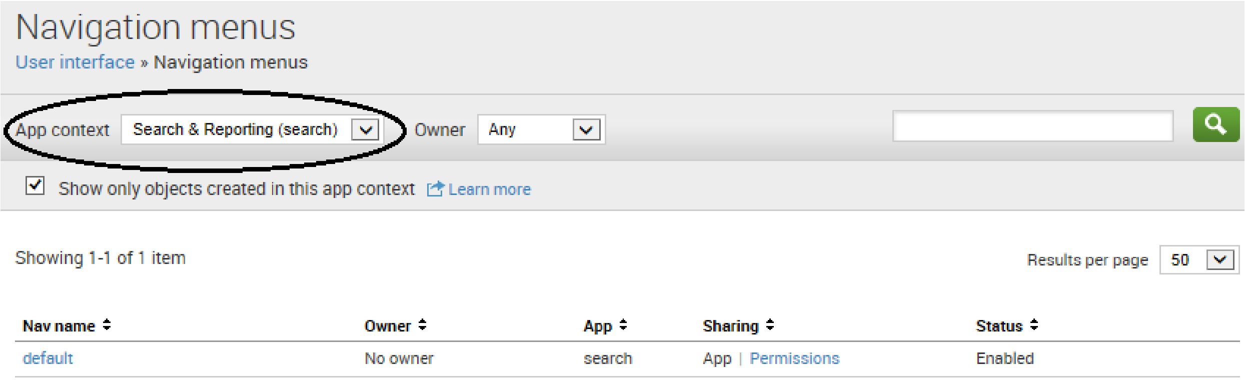




User interface

Create and edit views, dashboards, and navigation menus.

	Actions
Time ranges	Add new
Views	Add new
View PDF scheduling	
Navigation menus	
Bulletin Messages	Add new



Navigation menus

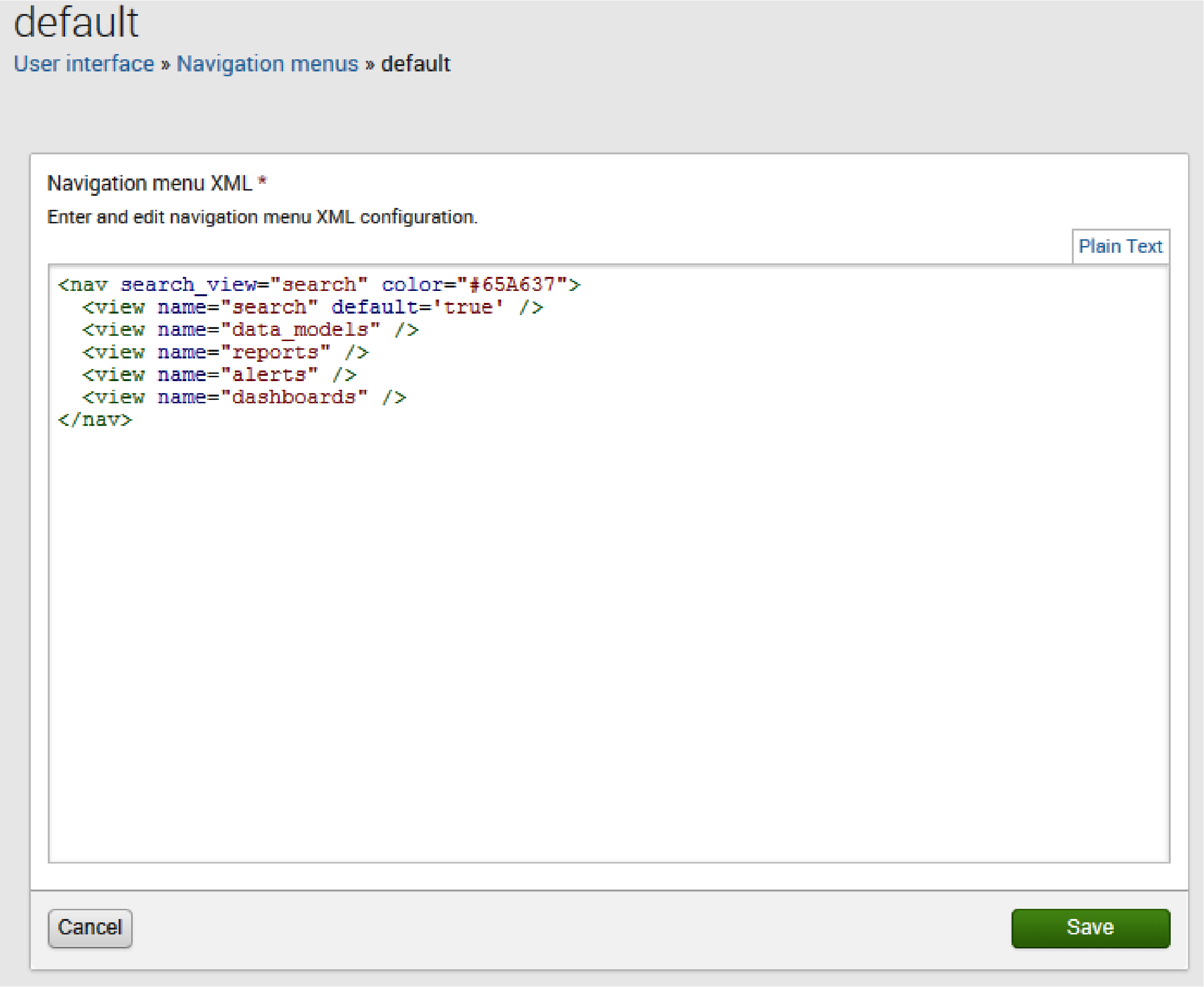
User interface » Navigation menus

☑ Show only objects created in this app context Learn more

Showing 1-1 of 1 item

Results per page 50

Nav name	Owner	App	Sharing	Status
default	No owner	search	App | Permissions	Enabled



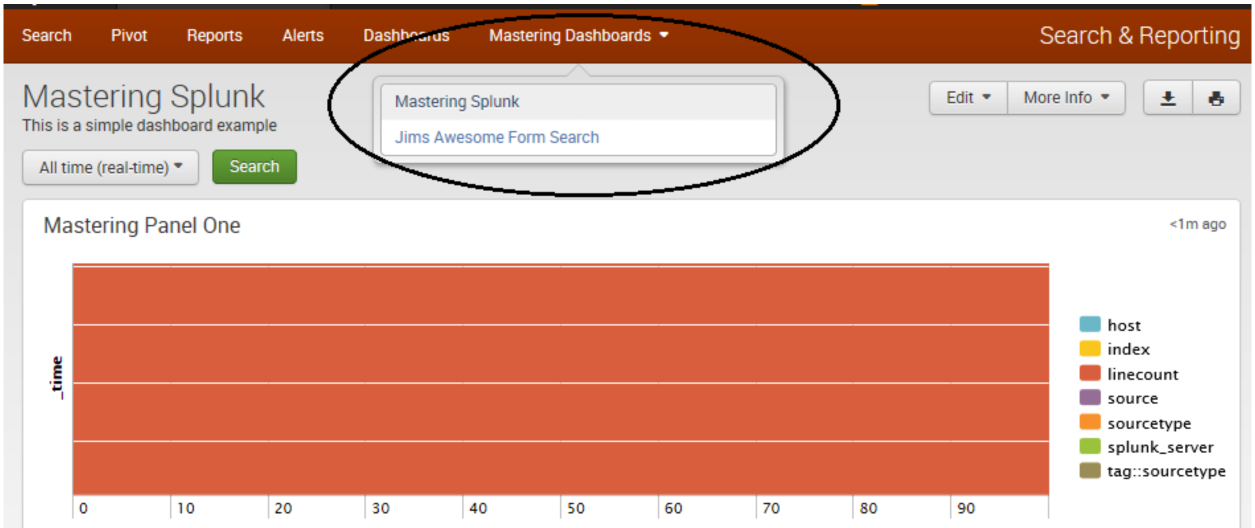
default

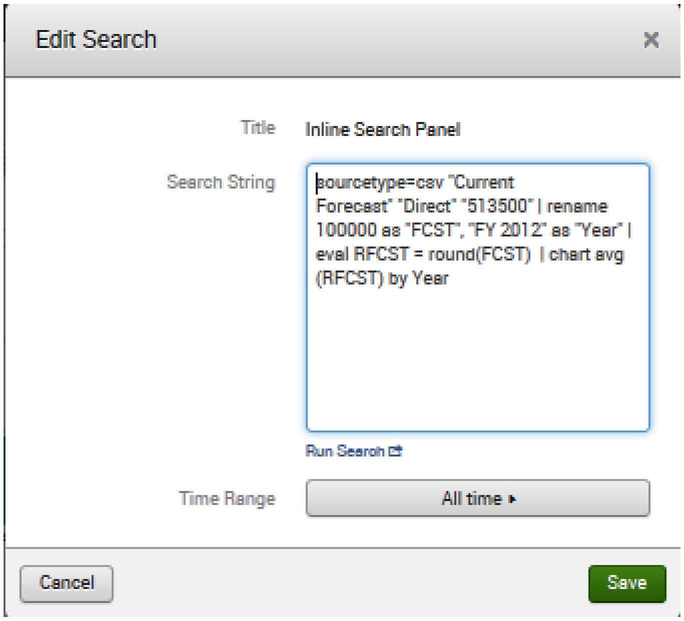
User interface » Navigation menus » default

Navigation menu XML *

Enter and edit navigation menu XML configuration.

```
<nav search_view="search" color="#65A637">
  <view name="search" default='true' />
  <view name="data_models" />
  <view name="reports" />
  <view name="alerts" />
  <view name="dashboards" />
</nav>
```





Edit Search

Title: Inline Search Panel

Search String:

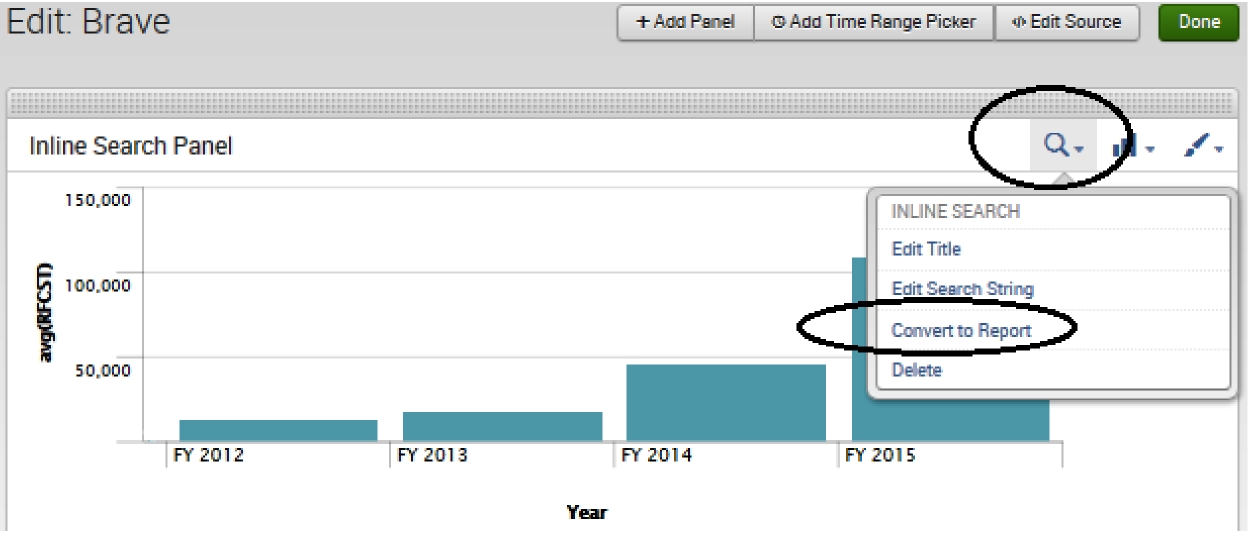
```
sourcetype=csv "Current Forecast" "Direct" "513500" | rename 100000 as "FCST", "FY 2012" as "Year" | eval RFCST = round(FCST)  | chart avg(RFCST) by Year
```

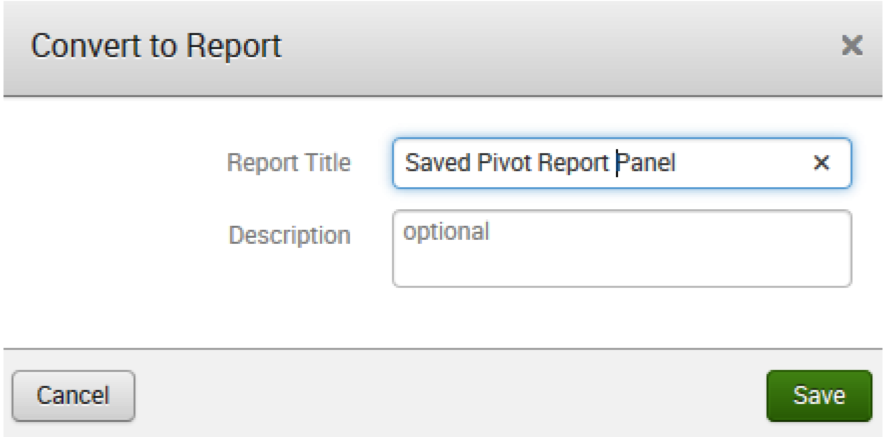
Run Search

Time Range: All time

Cancel

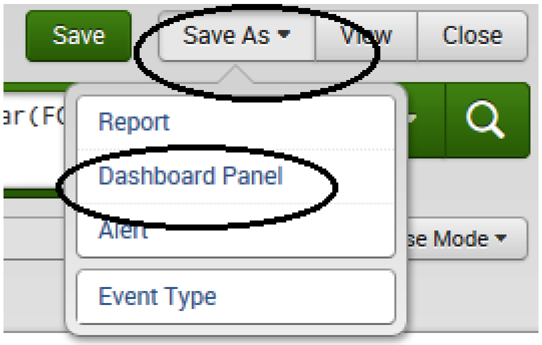
Save

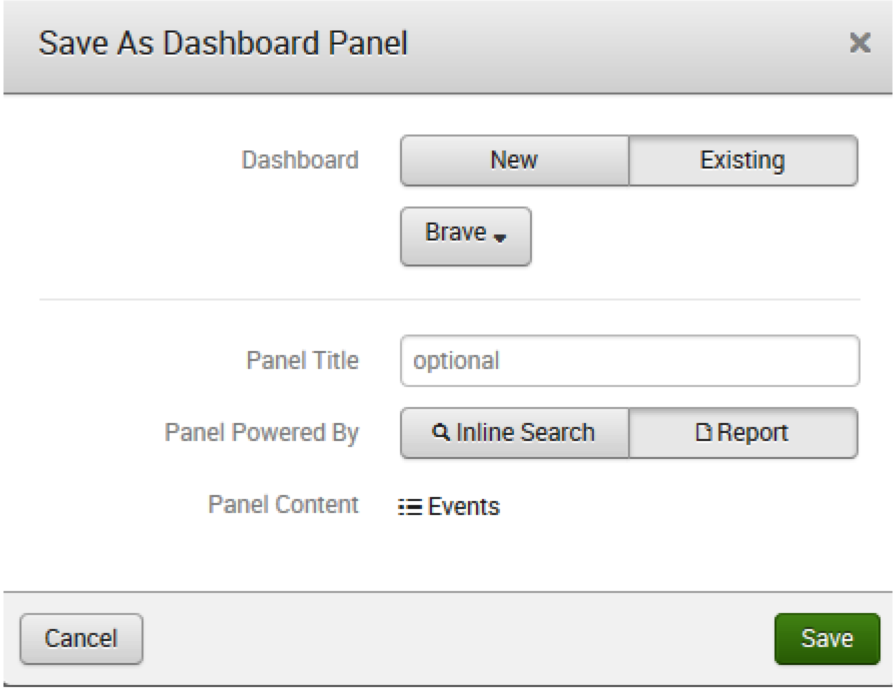




Report Title: Saved Pivot Report Panel

Description: optional





Save As Dashboard Panel

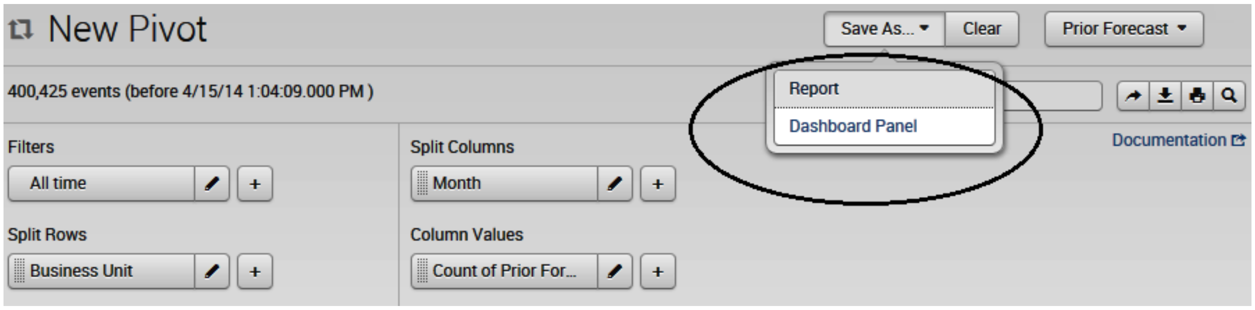
Dashboard: New | Existing

Brave

Panel Title: optional

Panel Powered By: Inline Search | Report

Panel Content: ☰ Events



New Pivot

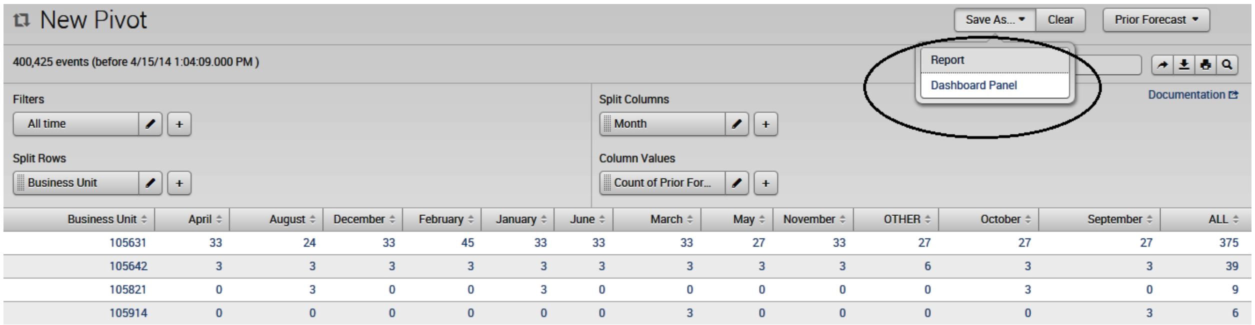
400,425 events (before 4/15/14 1:04:09.000 PM)

Filters: All time

Split Rows: Business Unit

Split Columns: Month

Column Values: Count of Prior For...



New Pivot

400,425 events (before 4/15/14 1:04:09.000 PM)

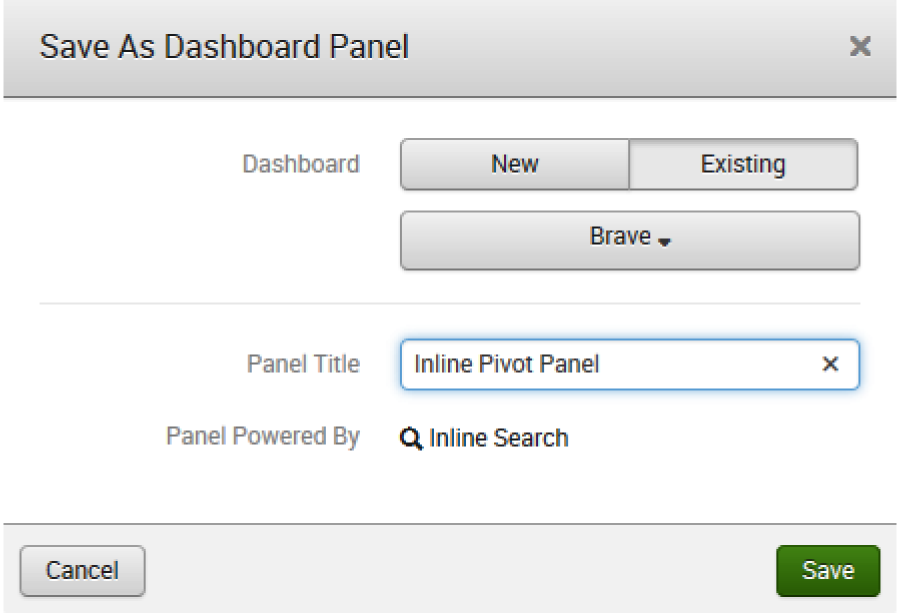
Filters: All time

Split Rows: Business Unit

Split Columns: Month

Column Values: Count of Prior For...

Business Unit	April	August	December	February	January	June	March	May	November	OTHER	October	September	ALL
105631	33	24	33	45	33	33	33	27	33	27	27	27	375
105642	3	3	3	3	3	3	3	3	3	6	3	3	39
105821	0	3	0	0	3	0	0	0	0	0	3	0	9
105914	0	0	0	0	0	0	3	0	0	0	0	3	6



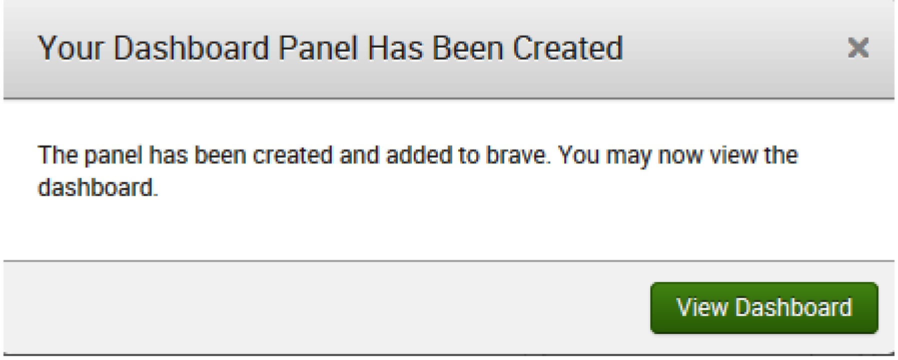
Save As Dashboard Panel

Dashboard: New | Existing

Brave

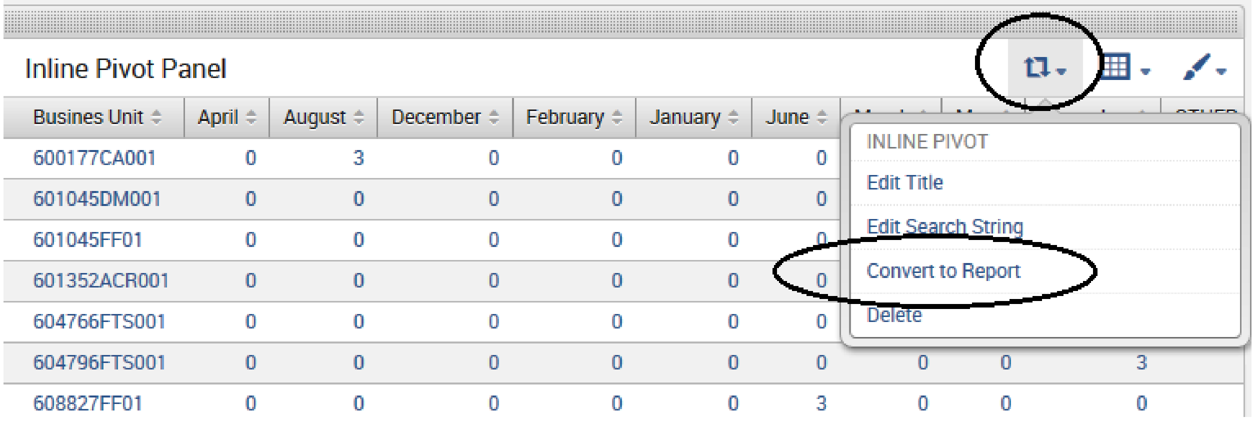
Panel Title: Inline Pivot Panel

Panel Powered By: Inline Search



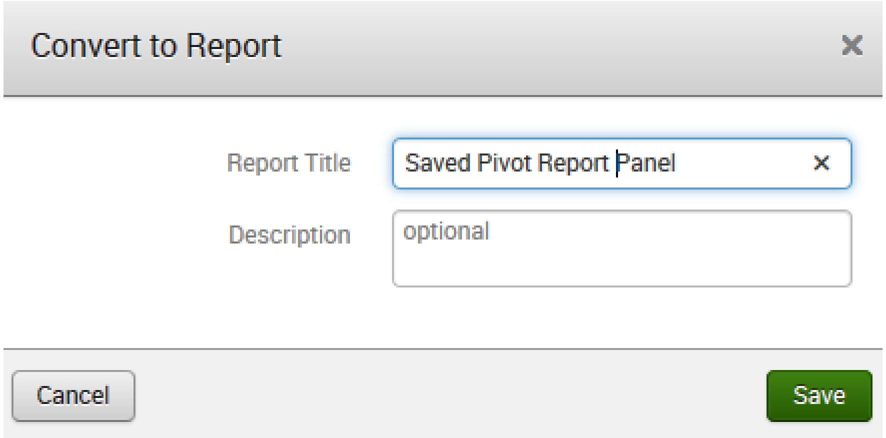
Your Dashboard Panel Has Been Created

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



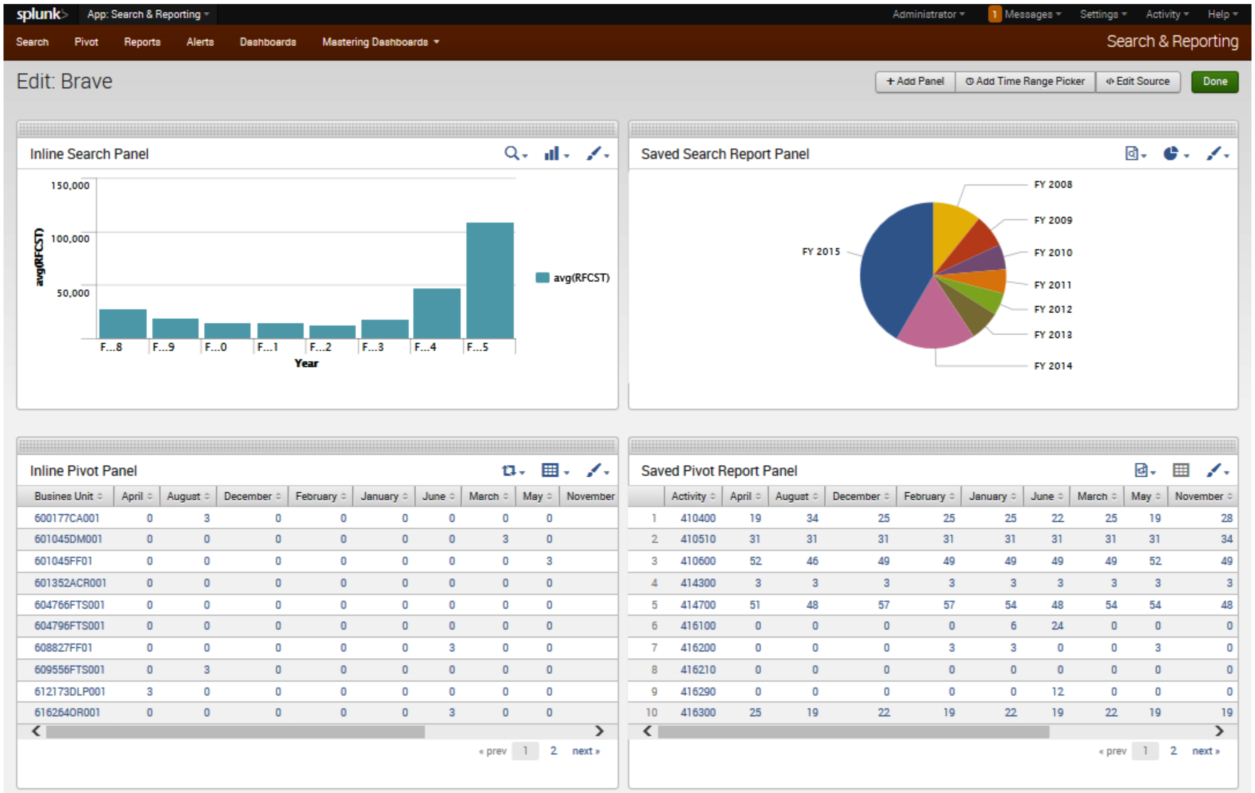
Inline Pivot Panel

Busines Unit	April	August	December	February	January	June	[illegible]	[illegible]	[illegible]	OTHER
600177CA001	0	3	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]
601045DM001	0	0	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]
601045FF01	0	0	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]
601352ACR001	0	0	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]
604766FTS001	0	0	0	0	0	0	[illegible]	[illegible]	[illegible]	[illegible]
604796FTS001	0	0	0	0	0	0	0	0	3	
608827FF01	0	0	0	0	0	3	0	0	0	



Report Title: Saved Pivot Report Panel

Description: optional



Edit: Brave

Inline Search Panel

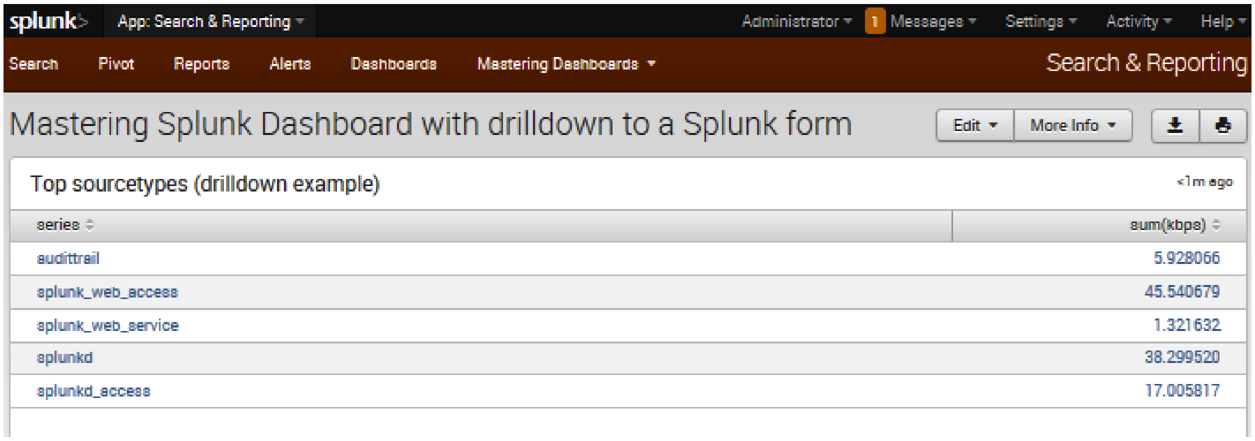
Saved Search Report Panel

Inline Pivot Panel

Busines Unit	April	August	December	February	January	June	March	May	November
600177CA001	0	3	0	0	0	0	0	0	
601045DM001	0	0	0	0	0	0	3	0	
601045FF01	0	0	0	0	0	0	0	3	
601352ACR001	0	0	0	0	0	0	0	0	
604766FTS001	0	0	0	0	0	0	0	0	
604796FTS001	0	0	0	0	0	0	0	0	
608827FF01	0	0	0	0	0	3	0	0	
609556FTS001	0	3	0	0	0	0	0	0	
612173DLP001	3	0	0	0	0	0	0	0	
616264OR001	0	0	0	0	0	3	0	0	

Saved Pivot Report Panel

	Activity	April	August	December	February	January	June	March	May	November
1	410400	19	34	25	25	25	22	25	19	28
2	410510	31	31	31	31	31	31	31	31	34
3	410600	52	46	49	49	49	49	49	52	49
4	414300	3	3	3	3	3	3	3	3	3
5	414700	51	48	57	57	54	48	54	54	48
6	416100	0	0	0	0	6	24	0	0	0
7	416200	0	0	0	3	3	0	0	3	0
8	416210	0	0	0	0	0	0	0	0	0
9	416290	0	0	0	0	0	12	0	0	0
10	416300	25	19	22	19	22	19	22	19	19

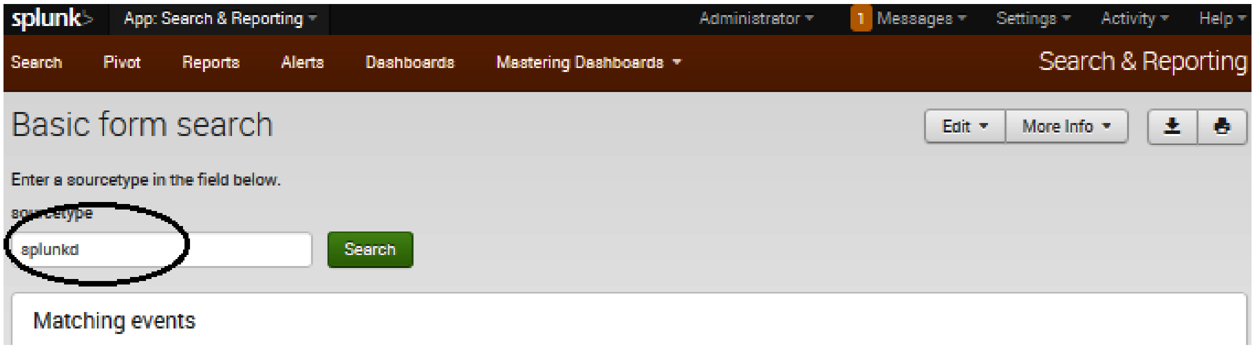


Mastering Splunk Dashboard with drilldown to a Splunk form

Top sourcetypes (drilldown example)

<1m ago

series	sum(kbps)
audittrail	5.928066
splunk_web_access	45.540679
splunk_web_service	1.321632
splunkd	38.299520
splunkd_access	17.005817



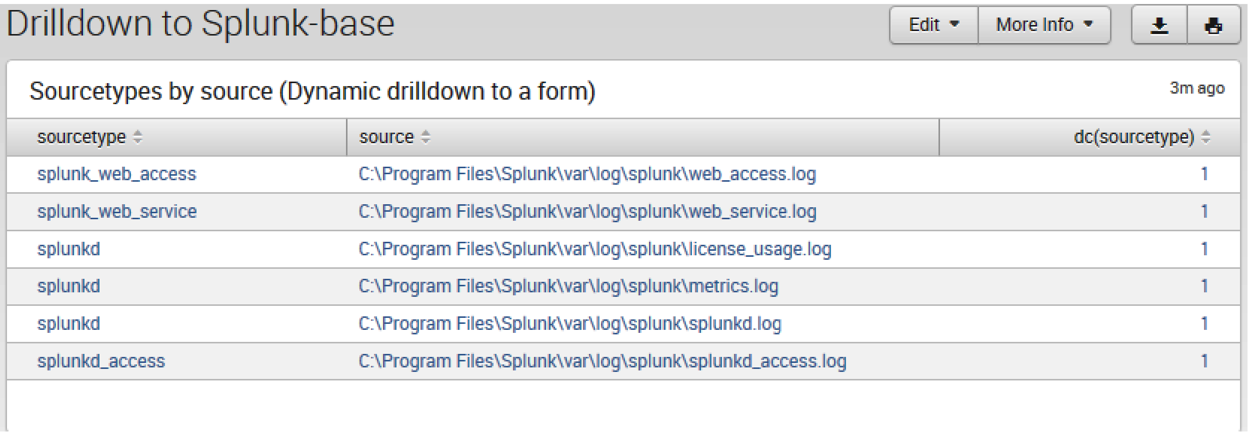
Basic form search

Enter a sourcetype in the field below.

sourcetype

splunkd

Matching events

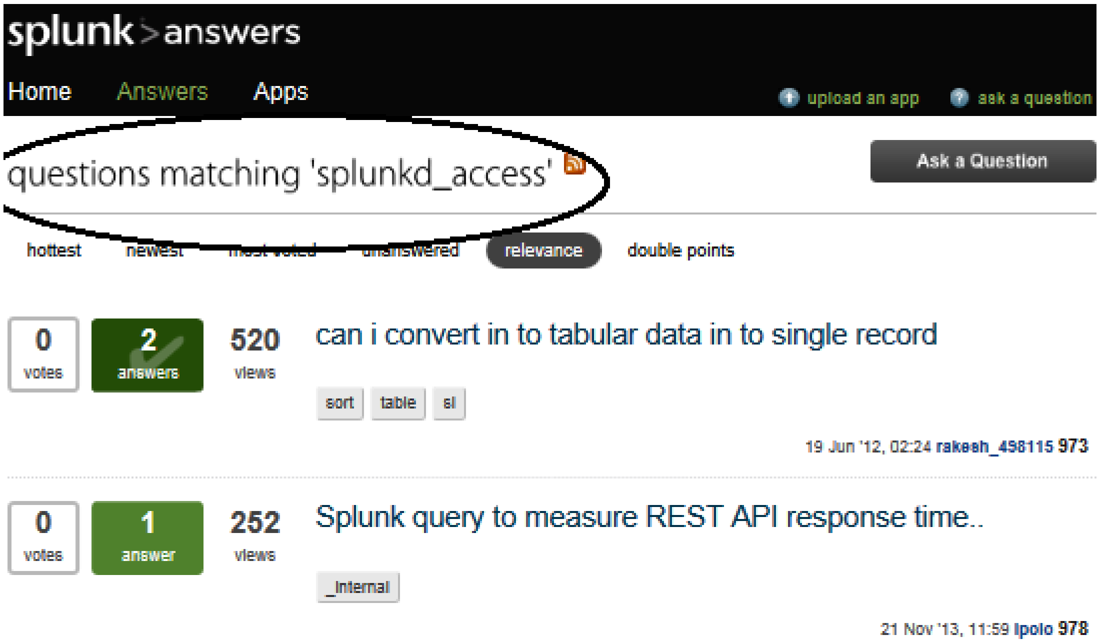


Drilldown to Splunk-base

Sourcetypes by source (Dynamic drilldown to a form)

3m ago

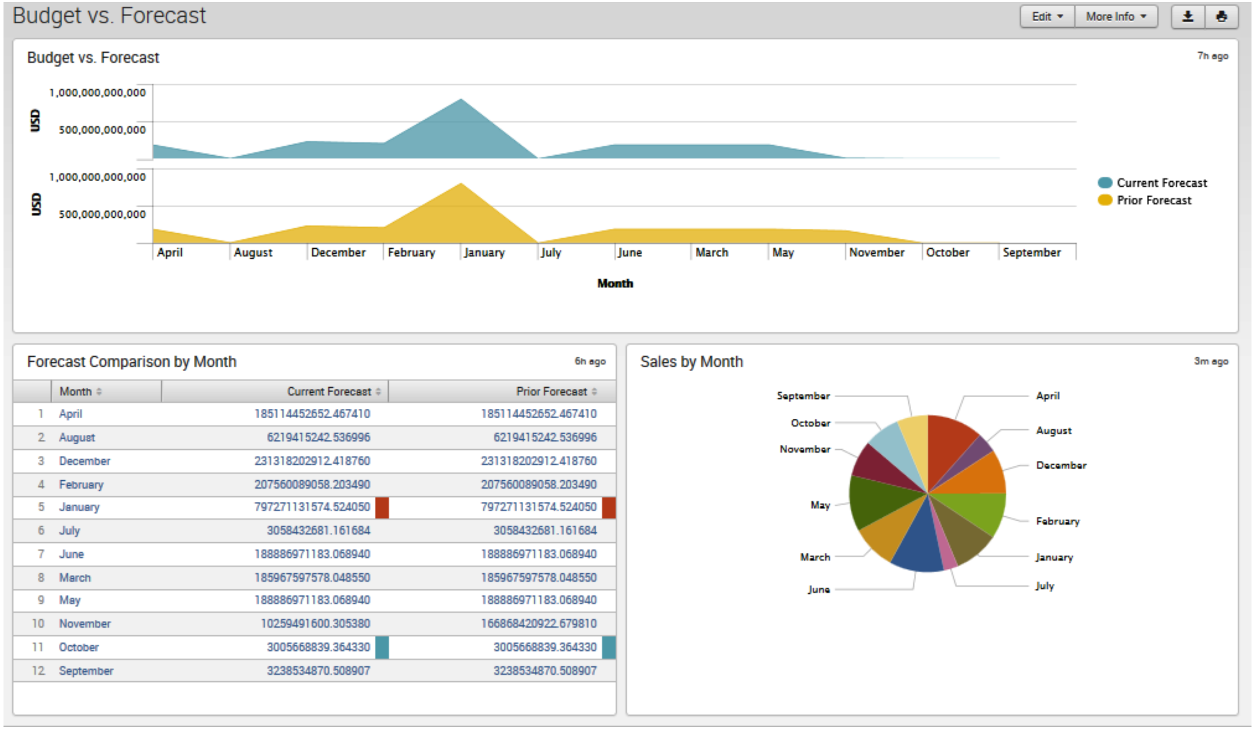
sourcetype	source	dc(sourcetype)
splunk_web_access	C:\Program Files\Splunk\var\log\splunk\web_access.log	1
splunk_web_service	C:\Program Files\Splunk\var\log\splunk\web_service.log	1
splunkd	C:\Program Files\Splunk\var\log\splunk\license_usage.log	1
splunkd	C:\Program Files\Splunk\var\log\splunk\metrics.log	1
splunkd	C:\Program Files\Splunk\var\log\splunk\splunkd.log	1
splunkd_access	C:\Program Files\Splunk\var\log\splunk\splunkd_access.log	1



questions matching 'splunkd_access'

0 votes | 2 answers | 520 views
can i convert in to tabular data in to single record
sort table sl
19 Jun '12, 02:24 rakesh_498115 973

0 votes | 1 answer | 252 views
Splunk query to measure REST API response time..
_internal
21 Nov '13, 11:59 lpolo 978

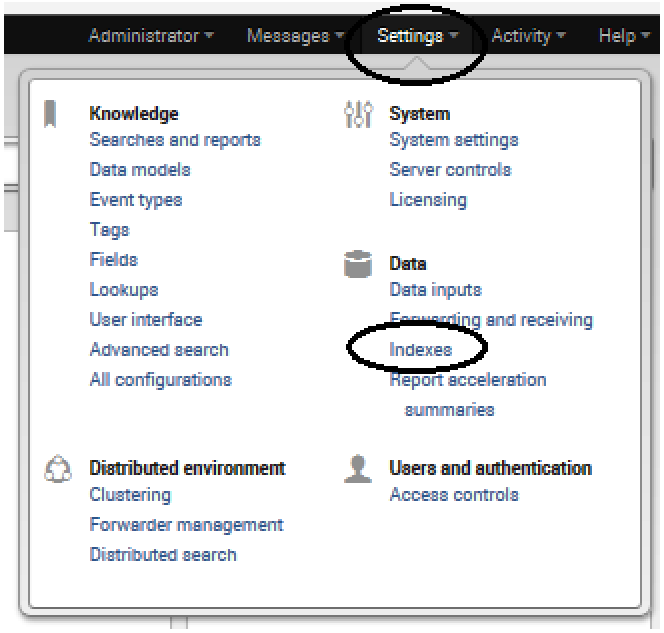


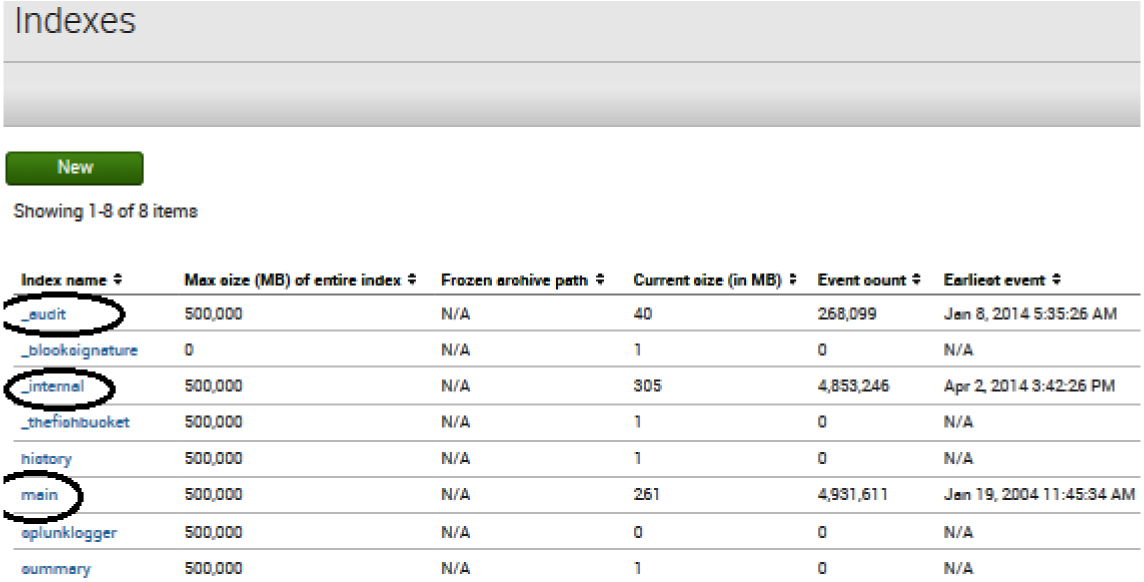
Forecast Comparison by Month

6h ago

	Month	Current Forecast	Prior Forecast
1	April	185114452652.467410	185114452652.467410
2	August	6219415242.536996	6219415242.536996
3	December	231318202912.418760	231318202912.418760
4	February	207560089058.203490	207560089058.203490
5	January	797271131574.524050	797271131574.524050
6	July	3058432681.161684	3058432681.161684
7	June	188886971183.068940	188886971183.068940
8	March	185967597578.048550	185967597578.048550
9	May	188886971183.068940	188886971183.068940
10	November	10259491600.305380	166868420922.679810
11	October	3005668839.364330	3005668839.364330
12	September	3238534870.508907	3238534870.508907

Chapter 6, *Indexes and Indexing*

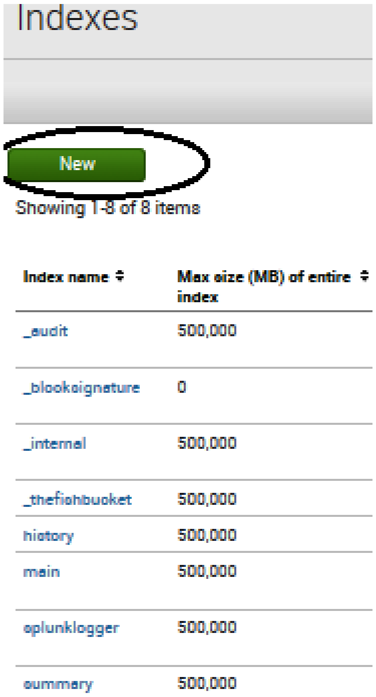




Indexes

Showing 1-8 of 8 items

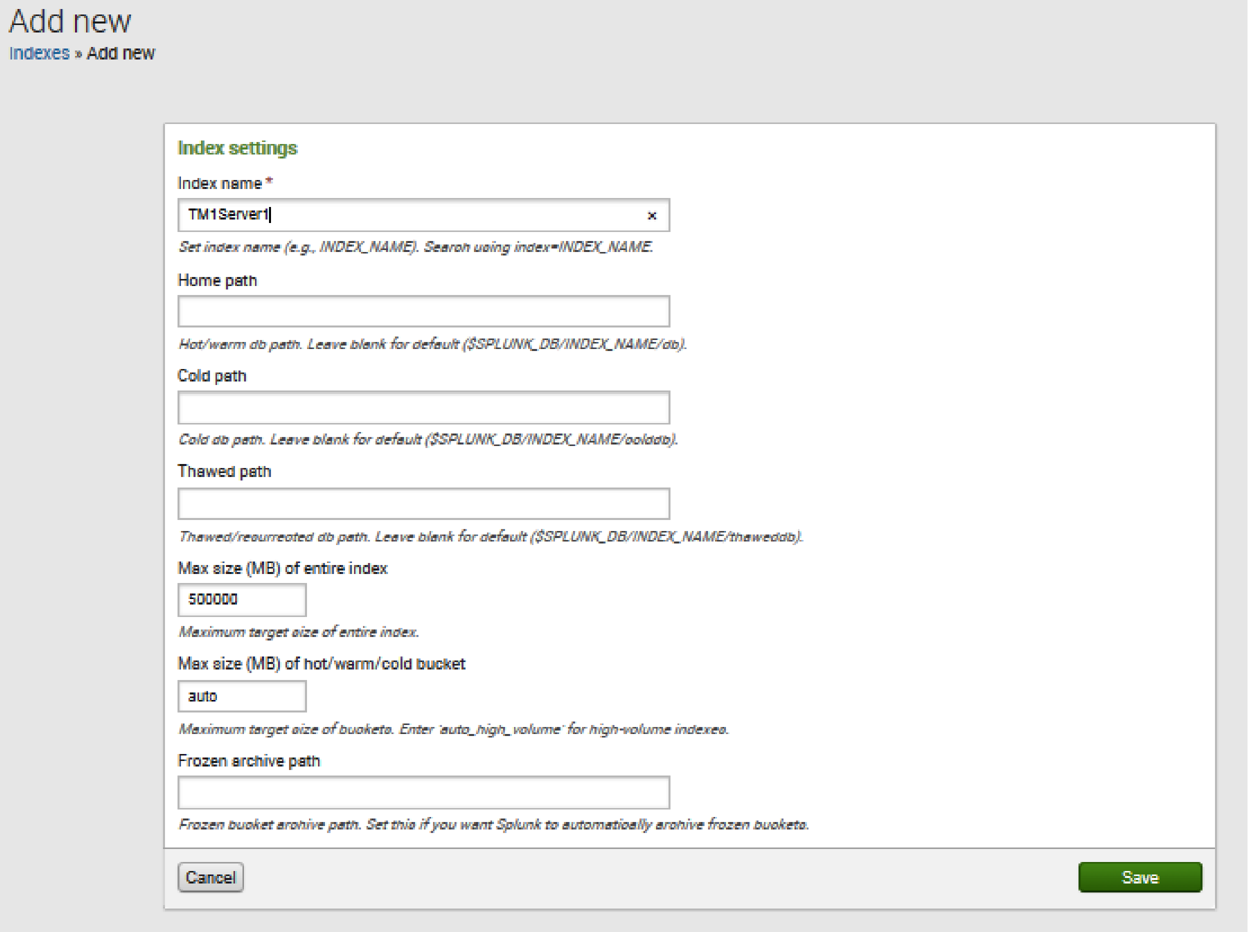
Index name ⇕	Max size (MB) of entire index ⇕	Frozen archive path ⇕	Current size (in MB) ⇕	Event count ⇕	Earliest event ⇕
_audit	500,000	N/A	40	268,099	Jan 8, 2014 5:35:26 AM
_blocksignature	0	N/A	1	0	N/A
_internal	500,000	N/A	305	4,853,246	Apr 2, 2014 3:42:26 PM
_thefishbucket	500,000	N/A	1	0	N/A
history	500,000	N/A	1	0	N/A
main	500,000	N/A	261	4,931,611	Jan 19, 2004 11:45:34 AM
splunklogger	500,000	N/A	0	0	N/A
summary	500,000	N/A	1	0	N/A



Indexes

Showing 1-8 of 8 items

Index name ⇕	Max size (MB) of entire index ⇕
_audit	500,000
_blocksignature	0
_internal	500,000
_thefishbucket	500,000
history	500,000
main	500,000
splunklogger	500,000
summary	500,000



Add new

Indexes » Add new

Index settings

Index name *

TM1Server1

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Home path

Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold path

Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed path

Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Max size (MB) of entire index

500000

Maximum target size of entire index.

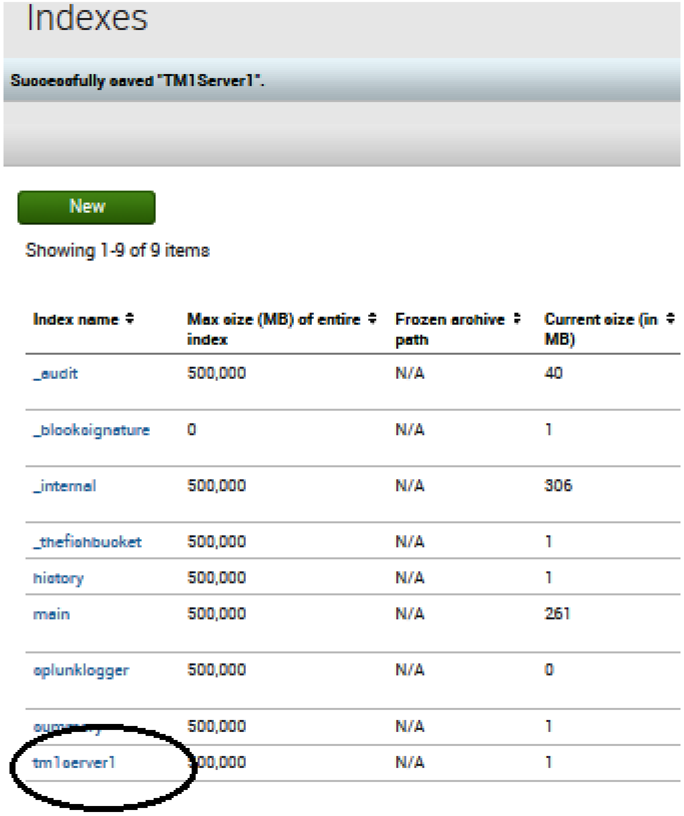
Max size (MB) of hot/warm/cold bucket

auto

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen archive path

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.



Indexes

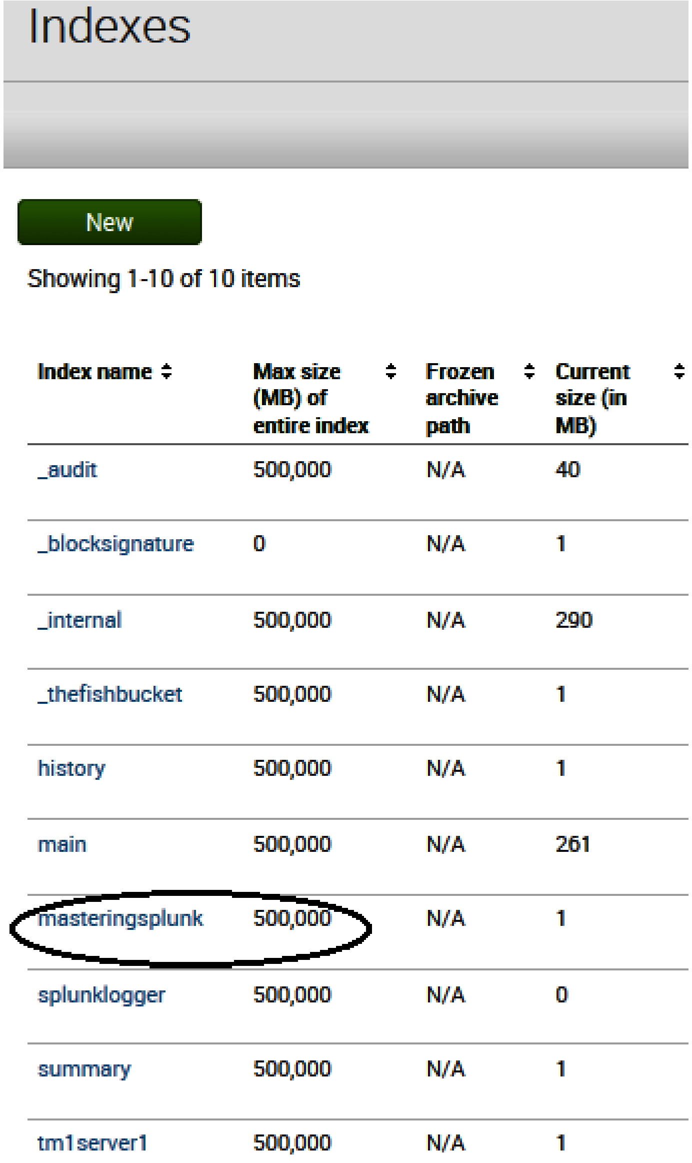
Successfully saved "TM1Server1".

New

Showing 1-9 of 9 items

Index name	Max size (MB) of entire index	Frozen archive path	Current size (in MB)
_audit	500,000	N/A	40
_blocksignature	0	N/A	1
_internal	500,000	N/A	306
_thefishbucket	500,000	N/A	1
history	500,000	N/A	1
main	500,000	N/A	261
splunklogger	500,000	N/A	0
summary	500,000	N/A	1
tm1server1	500,000	N/A	1

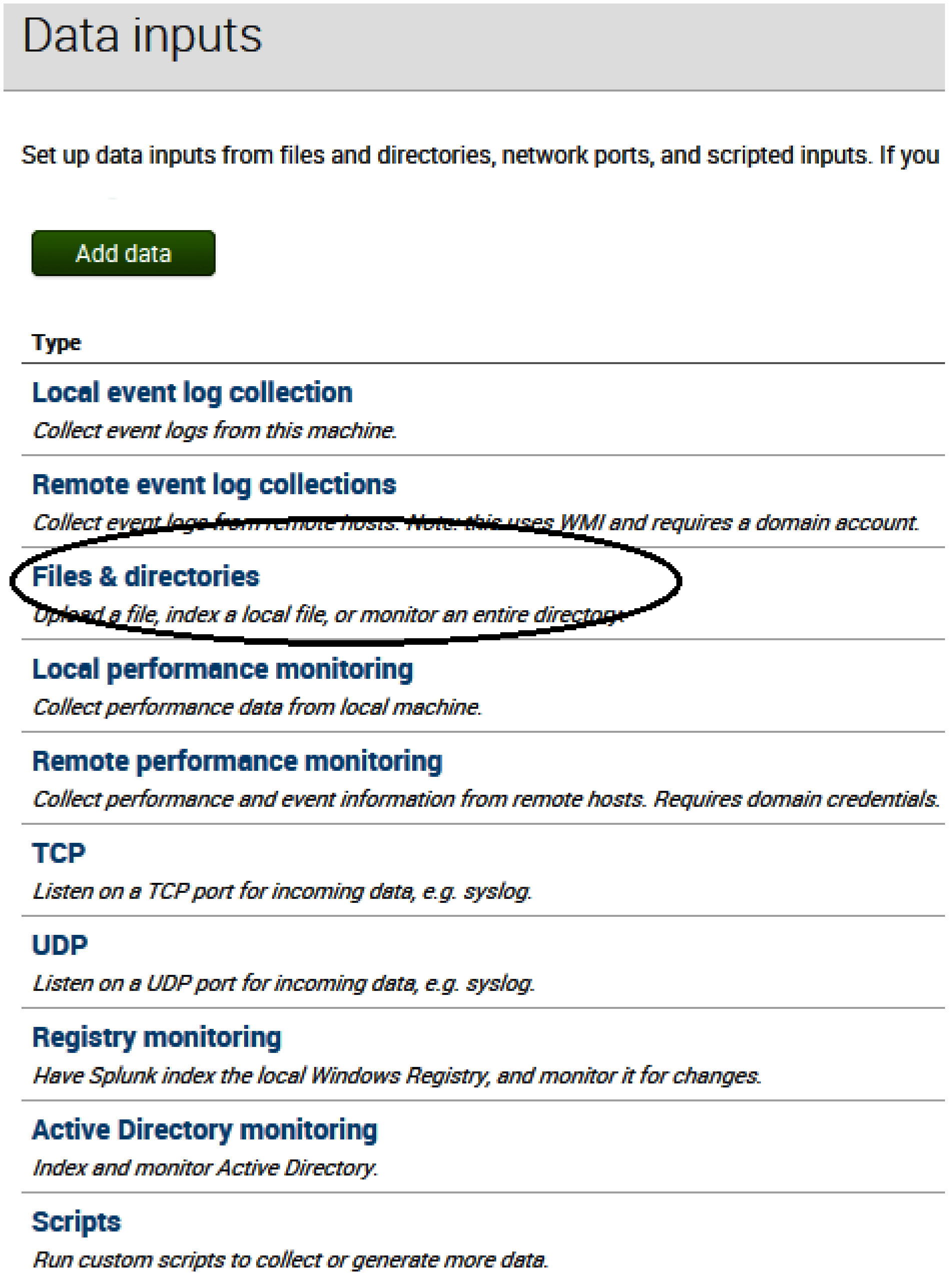
```
# new index exmple for the future splunk masters
[masteringsplunk]
homePath   = $SPLUNK_DB\masteringsplunk\db
coldPath   = $SPLUNK_DB\masteringsplunk\colddb
thawedPath = $SPLUNK_DB\masteringsplunk\thaweddb
```



Indexes

Showing 1-10 of 10 items

Index name	Max size (MB) of entire index	Frozen archive path	Current size (in MB)
_audit	500,000	N/A	40
_blocksignature	0	N/A	1
_internal	500,000	N/A	290
_thefishbucket	500,000	N/A	1
history	500,000	N/A	1
main	500,000	N/A	261
masteringsplunk	500,000	N/A	1
splunklogger	500,000	N/A	0
summary	500,000	N/A	1
tm1server1	500,000	N/A	1



Data inputs

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

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.

[✓ **Files & directories**]
Upload a file, index a local file, or monitor an entire directory.

Local performance monitoring
Collect performance data from local machine.

Remote performance monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

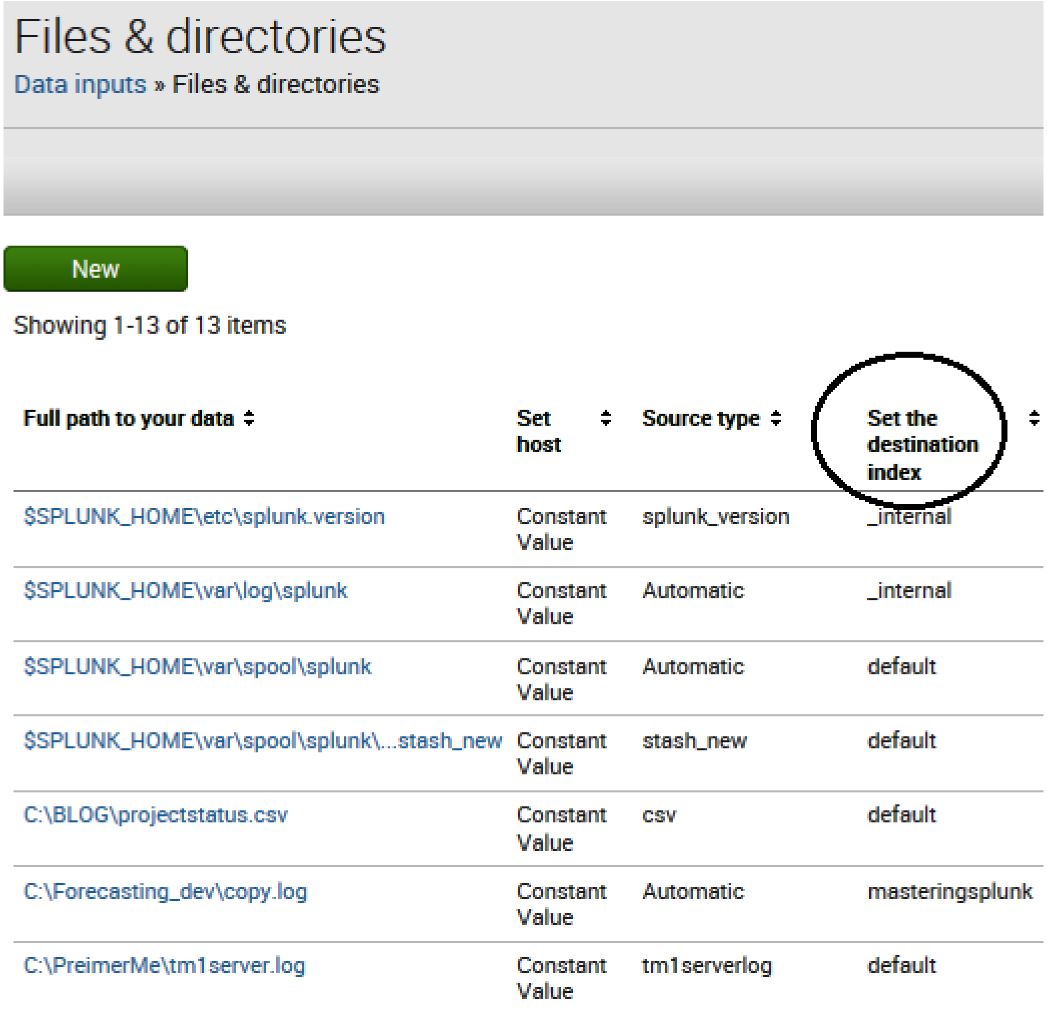
TCP
Listen on a TCP port for incoming data, e.g. syslog.

UDP
Listen on a UDP port for incoming data, e.g. syslog.

Registry monitoring
Have Splunk index the local Windows Registry, and monitor it for changes.

Active Directory monitoring
Index and monitor Active Directory.

Scripts
Run custom scripts to collect or generate more data.

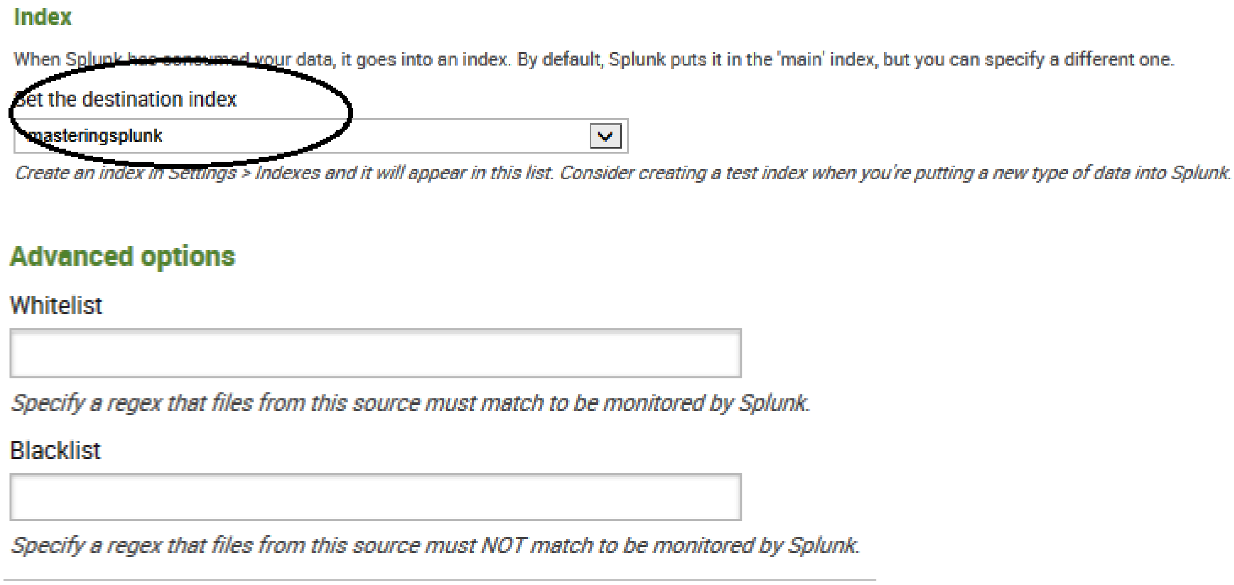


Files & directories

Data inputs » Files & directories

Showing 1-13 of 13 items

Full path to your data	Set host	Source type	Set the destination index
$SPLUNK_HOME\etc\splunk.version	Constant Value	splunk_version	_internal
$SPLUNK_HOME\var\log\splunk	Constant Value	Automatic	_internal
$SPLUNK_HOME\var\spool\splunk	Constant Value	Automatic	default
$SPLUNK_HOME\var\spool\splunk\...stash_new	Constant Value	stash_new	default
C:\BLOG\projectstatus.csv	Constant Value	csv	default
C:\Forecasting_dev\copy.log	Constant Value	Automatic	masteringsplunk
C:\PreimerMe\tm1server.log	Constant Value	tm1serverlog	default



Index

When Splunk has consumed your data, it goes into an index. By default, Splunk puts it in the 'main' index, but you can specify a different one.

Set the destination index: masteringsplunk

Create an index in Settings > Indexes and it will appear in this list. Consider creating a test index when you're putting a new type of data into Splunk.

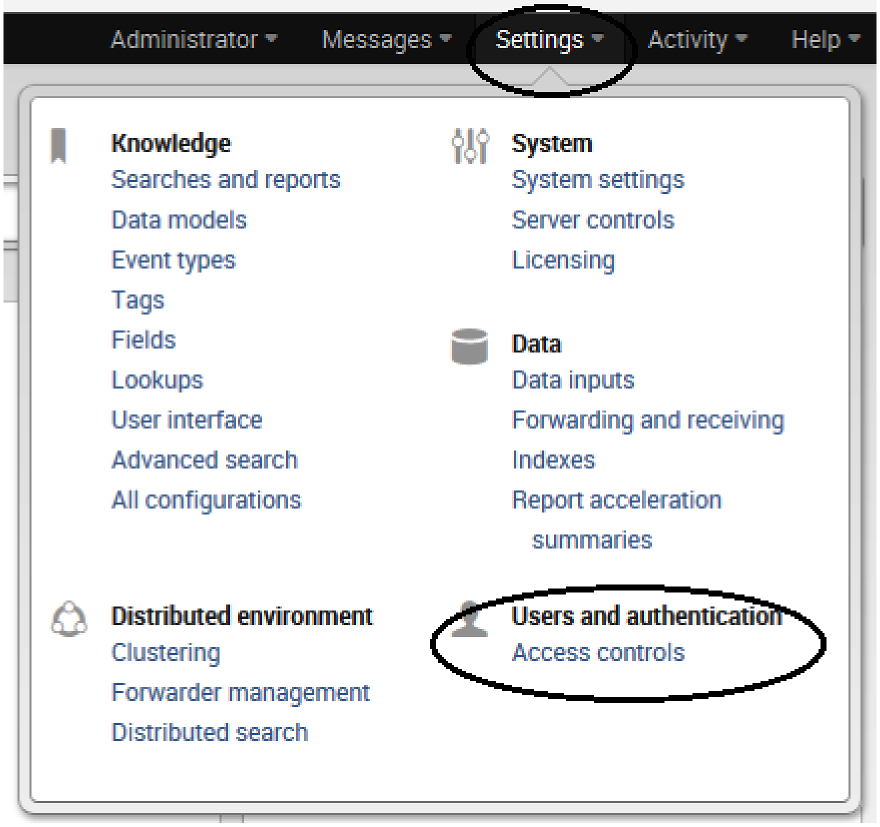
Advanced options

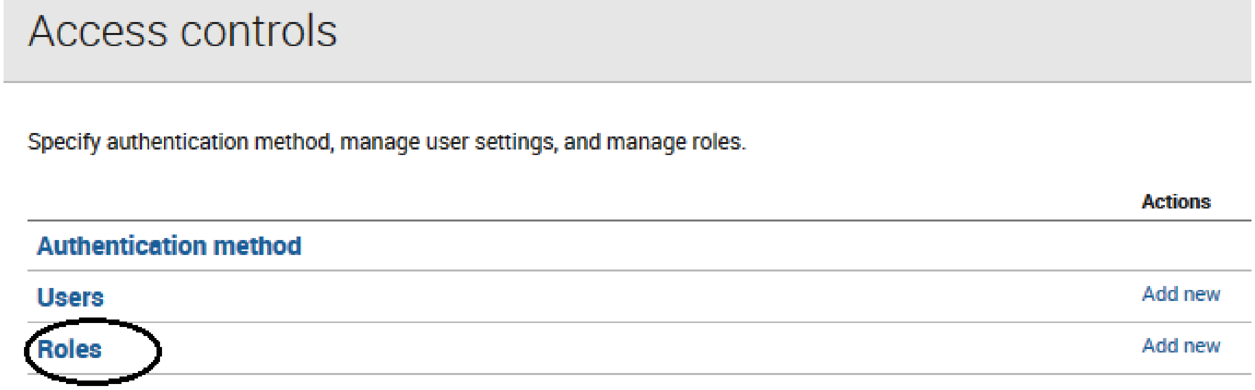
Whitelist

Specify a regex that files from this source must match to be monitored by Splunk.

Blacklist

Specify a regex that files from this source must NOT match to be monitored by Splunk.

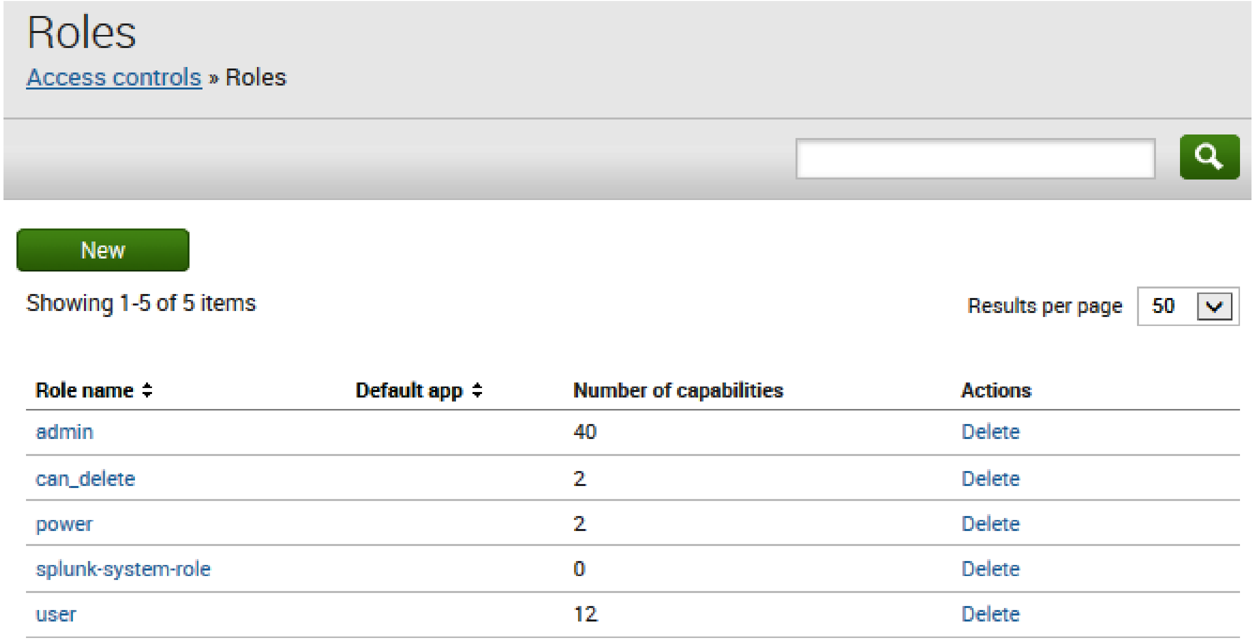




Access controls

Specify authentication method, manage user settings, and manage roles.

	Actions
Authentication method	
Users	Add new
Roles	Add new



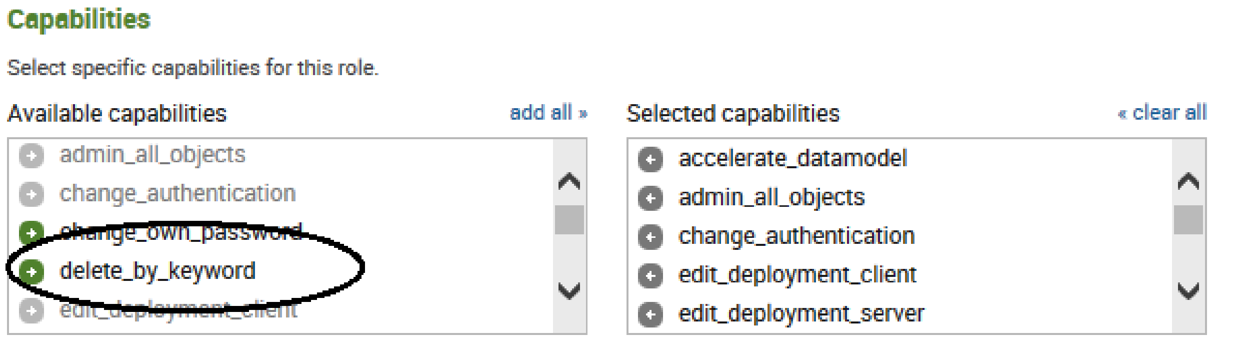
Roles

Access controls » Roles

Showing 1-5 of 5 items

Results per page 50

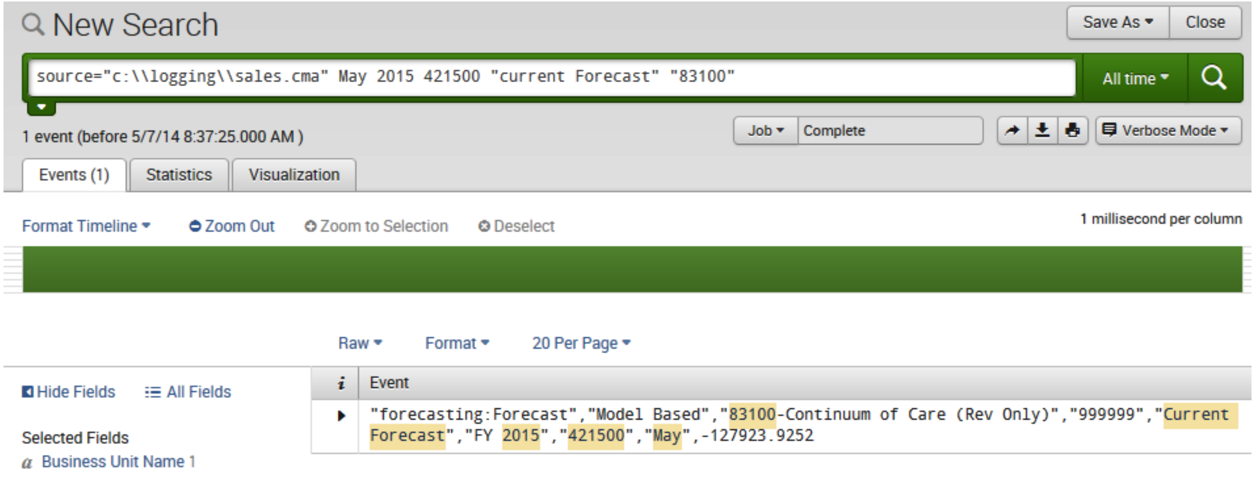
Role name	Default app	Number of capabilities	Actions
admin		40	Delete
can_delete		2	Delete
power		2	Delete
splunk-system-role		0	Delete
user		12	Delete



Capabilities

Select specific capabilities for this role.

Available capabilities	Selected capabilities
admin_all_objects	accelerate_datamodel
change_authentication	admin_all_objects
change_own_password	change_authentication
delete_by_keyword	edit_deployment_client
edit_deployment_client	edit_deployment_server



New Search

```
source="c:\\logging\\sales.cma" May 2015 421500 "current Forecast" "83100"
```

1 event (before 5/7/14 8:37:25.000 AM)

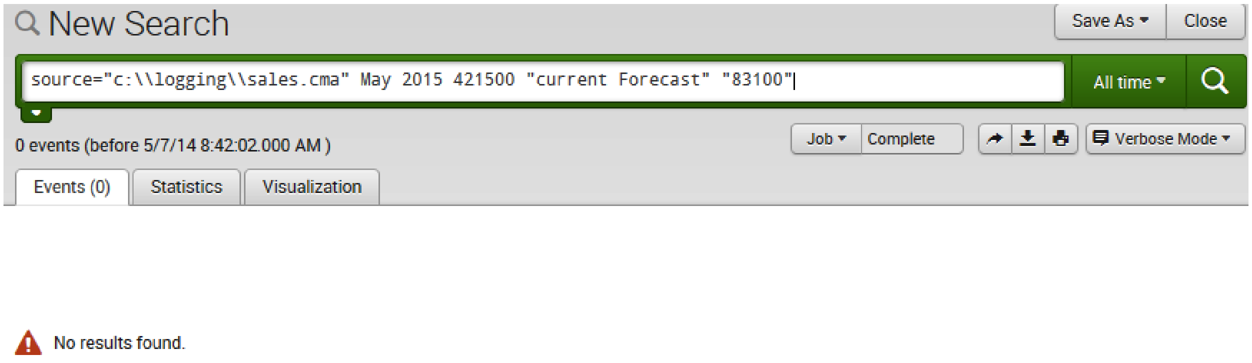
Job: Complete

1 millisecond per column

Selected Fields

a Business Unit Name 1

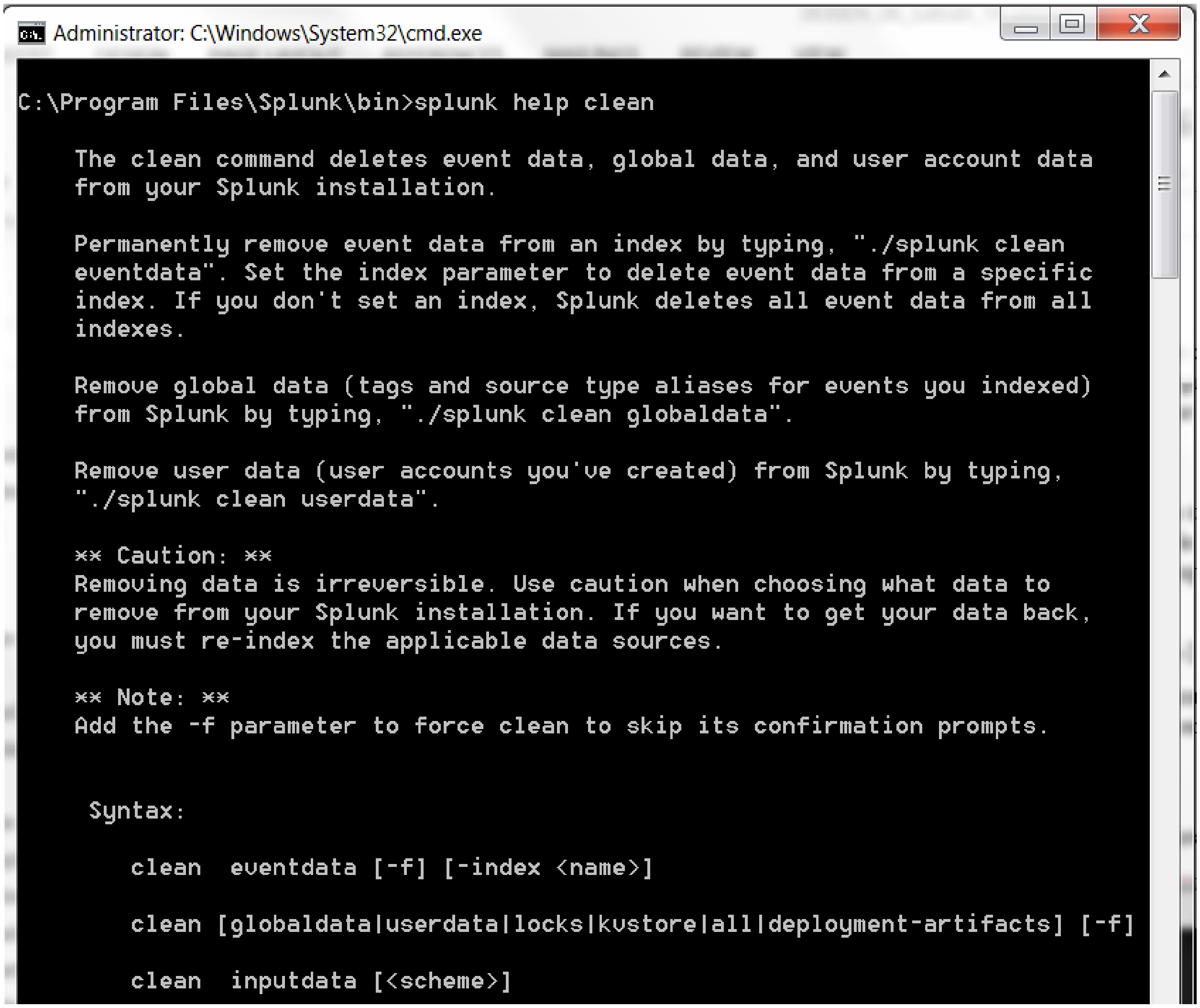
i	Event
▶	"forecasting:Forecast","Model Based","83100-Continuum of Care (Rev Only)","999999","Current Forecast","FY 2015","421500","May",-127923.9252



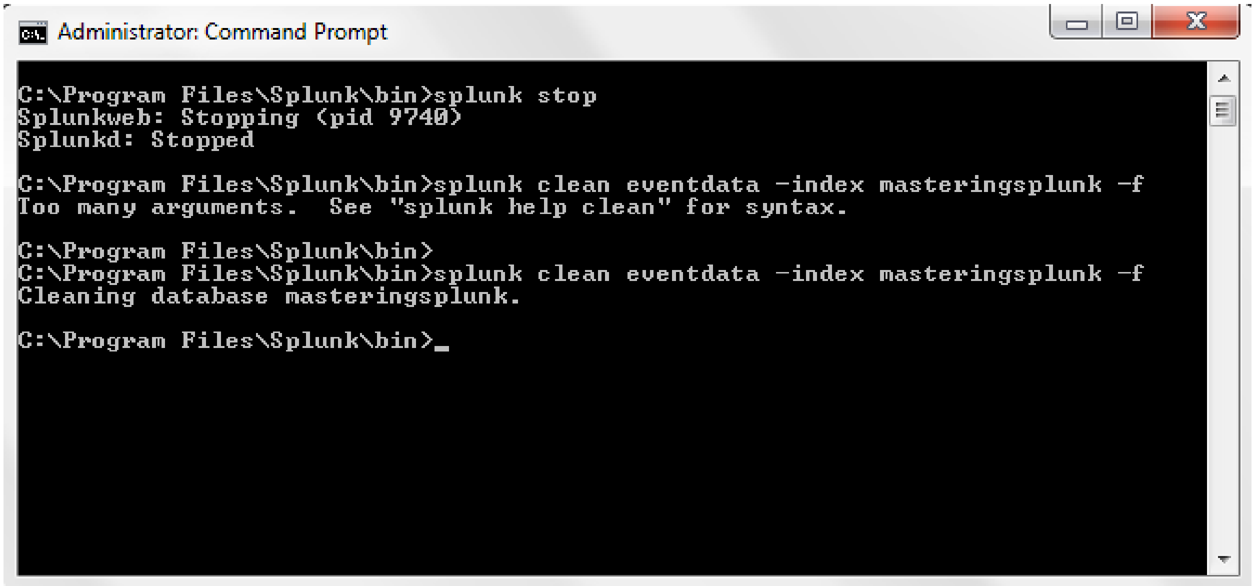
```
source="c:\\logging\\sales.cma" May 2015 421500 "current Forecast" "83100"
```

0 events (before 5/7/14 8:42:02.000 AM)

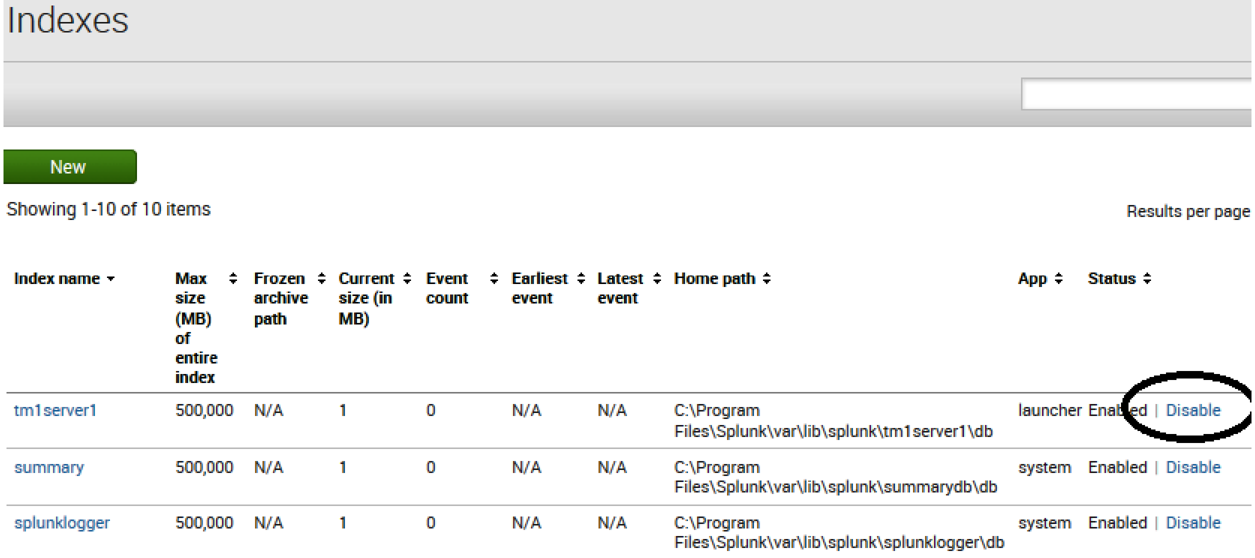
No results found.



```
C:\Program Files\Splunk\bin>splunk help clean

    The clean command deletes event data, global data, and user account data
    from your Splunk installation.

    Permanently remove event data from an index by typing, "./splunk clean
    eventdata". Set the index parameter to delete event data from a specific
    index. If you don't set an index, Splunk deletes all event data from all
    indexes.

    Remove global data (tags and source type aliases for events you indexed)
    from Splunk by typing, "./splunk clean globaldata".

    Remove user data (user accounts you've created) from Splunk by typing,
    "./splunk clean userdata".

    ** Caution: **
    Removing data is irreversible. Use caution when choosing what data to
    remove from your Splunk installation. If you want to get your data back,
    you must re-index the applicable data sources.

    ** Note: **
    Add the -f parameter to force clean to skip its confirmation prompts.


     Syntax:

        clean  eventdata [-f] [-index <name>]

        clean [globaldata|userdata|locks|kvstore|all|deployment-artifacts] [-f]

        clean  inputdata [<scheme>]
```



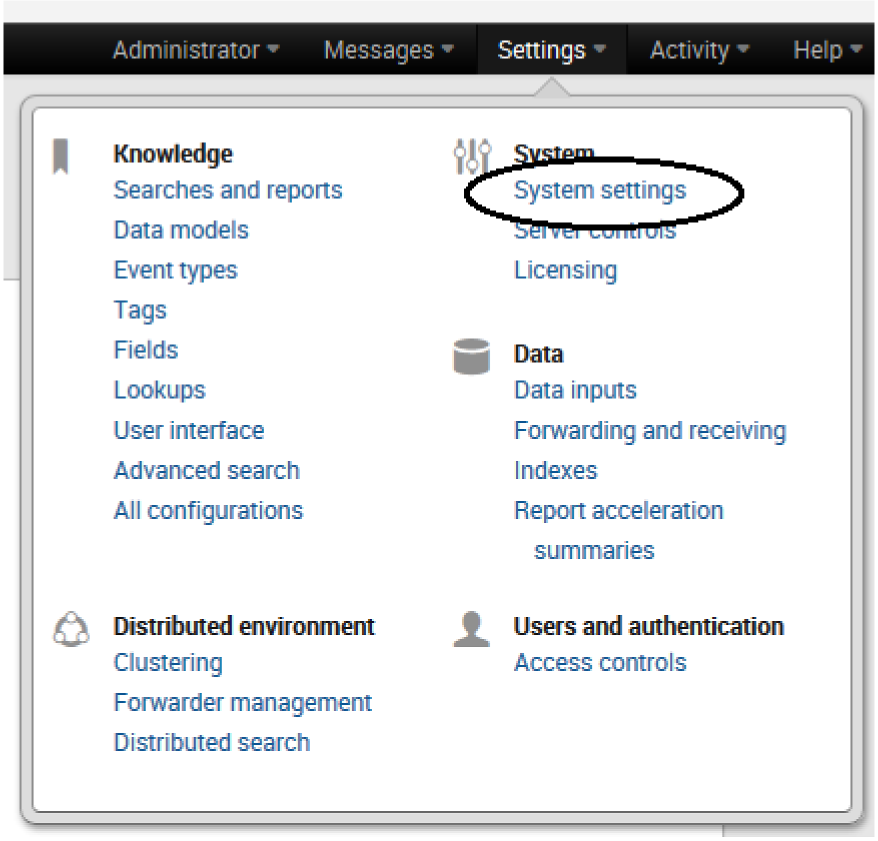
```
C:\Program Files\Splunk\bin>splunk stop
Splunkweb: Stopping (pid 9740)
Splunkd: Stopped

C:\Program Files\Splunk\bin>splunk clean eventdata -index masteringsplunk -f
Too many arguments.  See "splunk help clean" for syntax.

C:\Program Files\Splunk\bin>
C:\Program Files\Splunk\bin>splunk clean eventdata -index masteringsplunk -f
Cleaning database masteringsplunk.

C:\Program Files\Splunk\bin>_
```

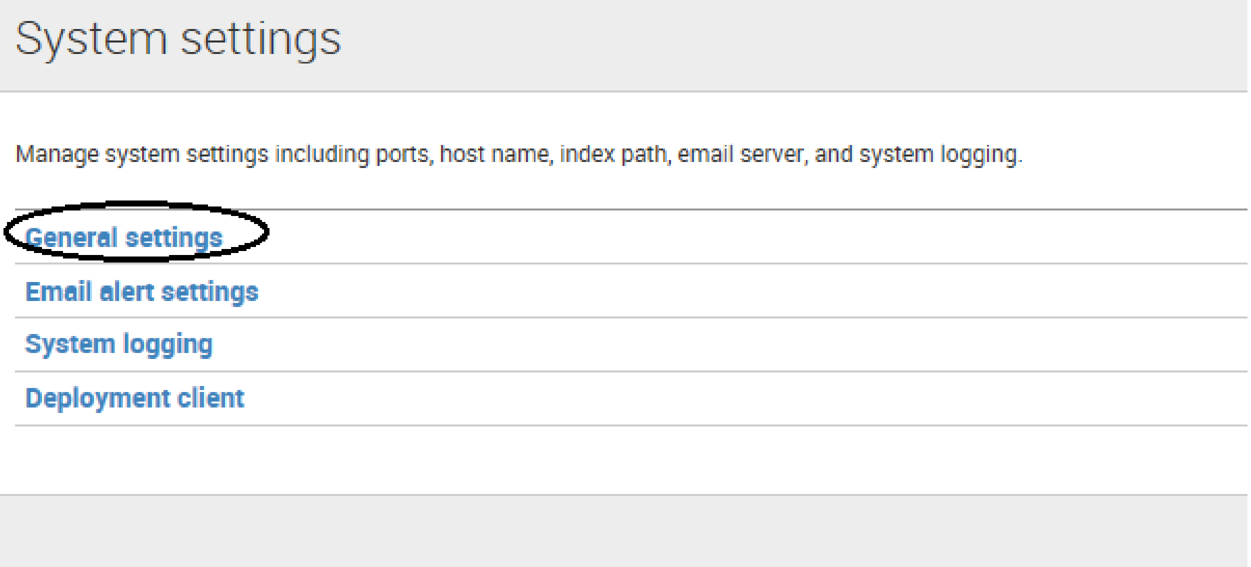


Showing 1-10 of 10 items

Results per page

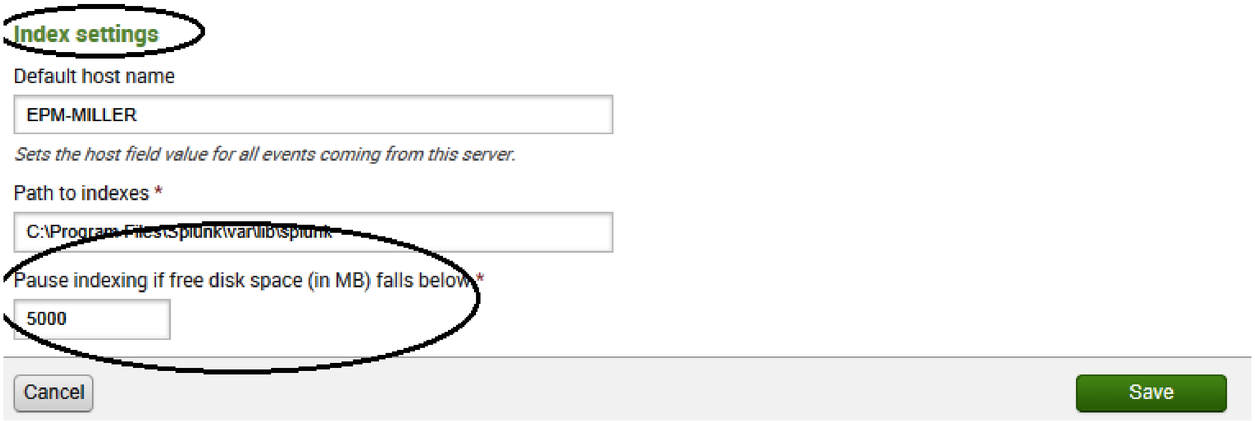
Index name	Max size (MB) of entire index	Frozen archive path	Current size (in MB)	Event count	Earliest event	Latest event	Home path	App	Status
tm1server1	500,000	N/A	1	0	N/A	N/A	C:\Program Files\Splunk\var\lib\splunk\tm1server1\db	launcher	Enabled | Disable
summary	500,000	N/A	1	0	N/A	N/A	C:\Program Files\Splunk\var\lib\splunk\summarydb\db	system	Enabled | Disable
splunklogger	500,000	N/A	1	0	N/A	N/A	C:\Program Files\Splunk\var\lib\splunk\splunklogger\db	system	Enabled | Disable





System settings

Manage system settings including ports, host name, index path, email server, and system logging.



Index settings

Default host name

EPM-MILLER

Sets the host field value for all events coming from this server.

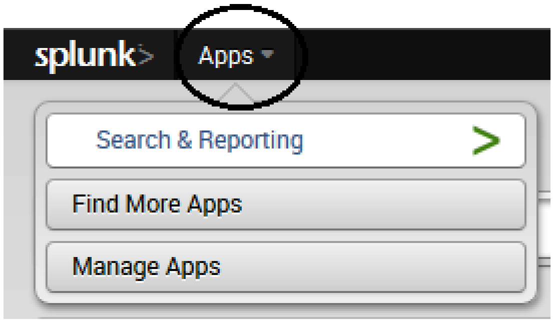
Path to indexes *

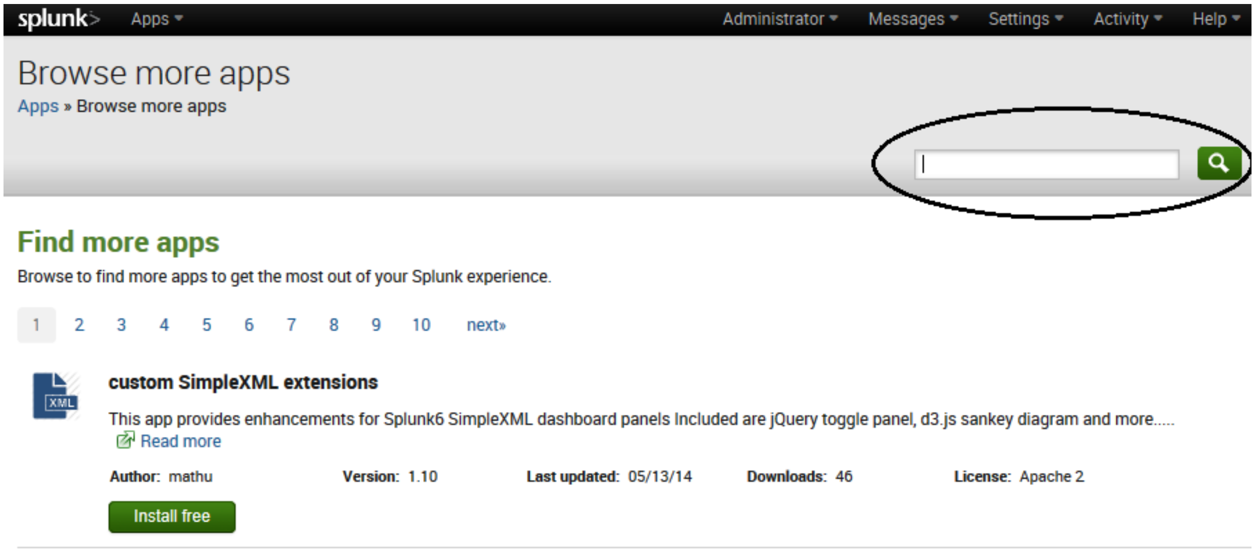
C:\Program Files\Splunk\var\lib\splunk

Pause indexing if free disk space (in MB) falls below *

5000

Chapter 7, *Evolving your Apps*





Browse more apps

Apps » Browse more apps

Find more apps

Browse to find more apps to get the most out of your Splunk experience.

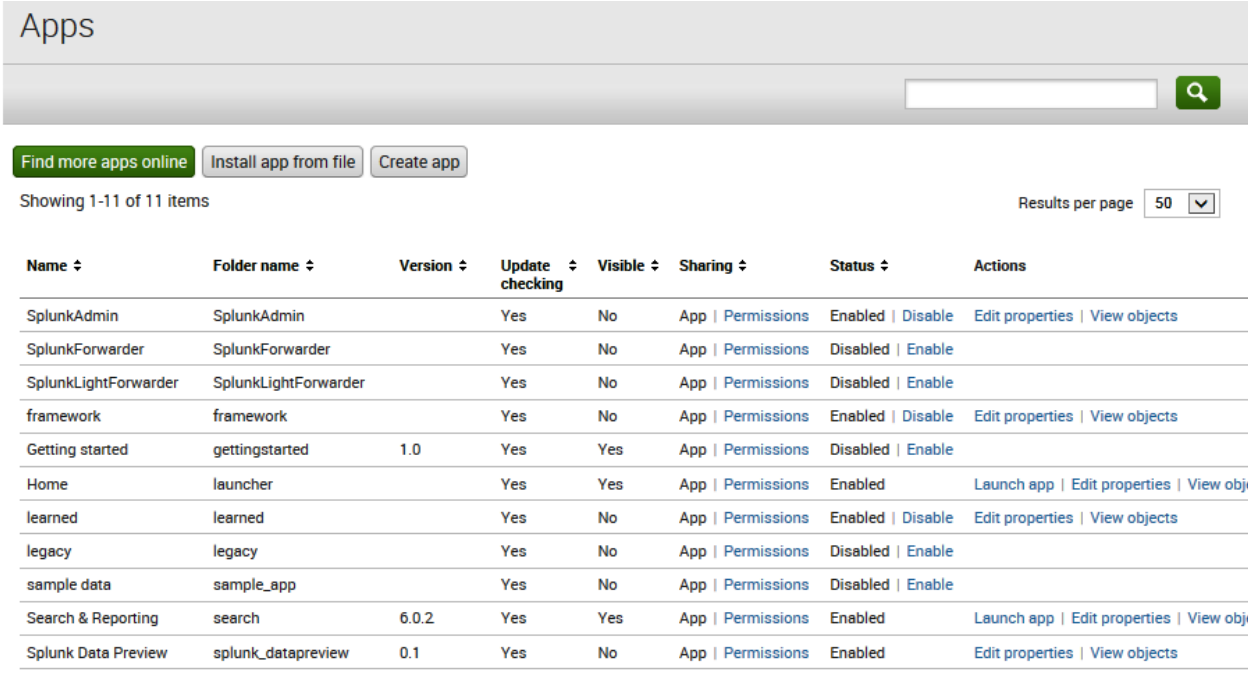
1 2 3 4 5 6 7 8 9 10 next»

custom SimpleXML extensions

This app provides enhancements for Splunk6 SimpleXML dashboard panels Included are jQuery toggle panel, d3.js sankey diagram and more.....

Read more

Author: mathu **Version:** 1.10 **Last updated:** 05/13/14 **Downloads:** 46 **License:** Apache 2



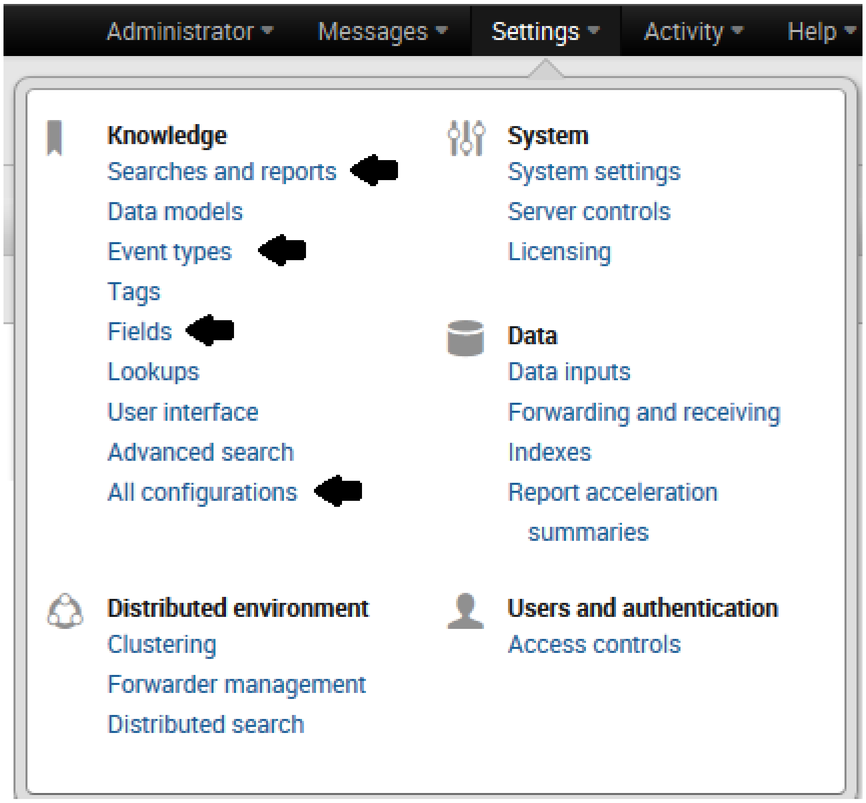
Apps

Find more apps online | Install app from file | Create app

Showing 1-11 of 11 items

Results per page 50

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkAdmin	SplunkAdmin		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
framework	framework		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Getting started	gettingstarted	1.0	Yes	Yes	App | Permissions	Disabled | Enable	
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View obj
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable	
sample data	sample_app		Yes	No	App | Permissions	Disabled | Enable	
Search & Reporting	search	6.0.2	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View obj
Splunk Data Preview	splunk_datapreview	0.1	Yes	No	App | Permissions	Enabled	Edit properties | View objects



Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

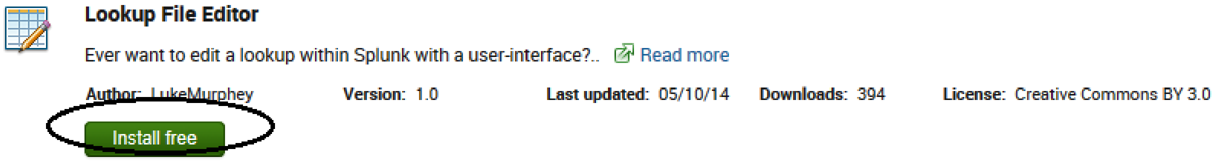
Knowledge
Searches and reports
Data models
Event types
Tags
Fields
Lookups
User interface
Advanced search
All configurations

System
System settings
Server controls
Licensing

Data
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries

Distributed environment
Clustering
Forwarder management
Distributed search

Users and authentication
Access controls

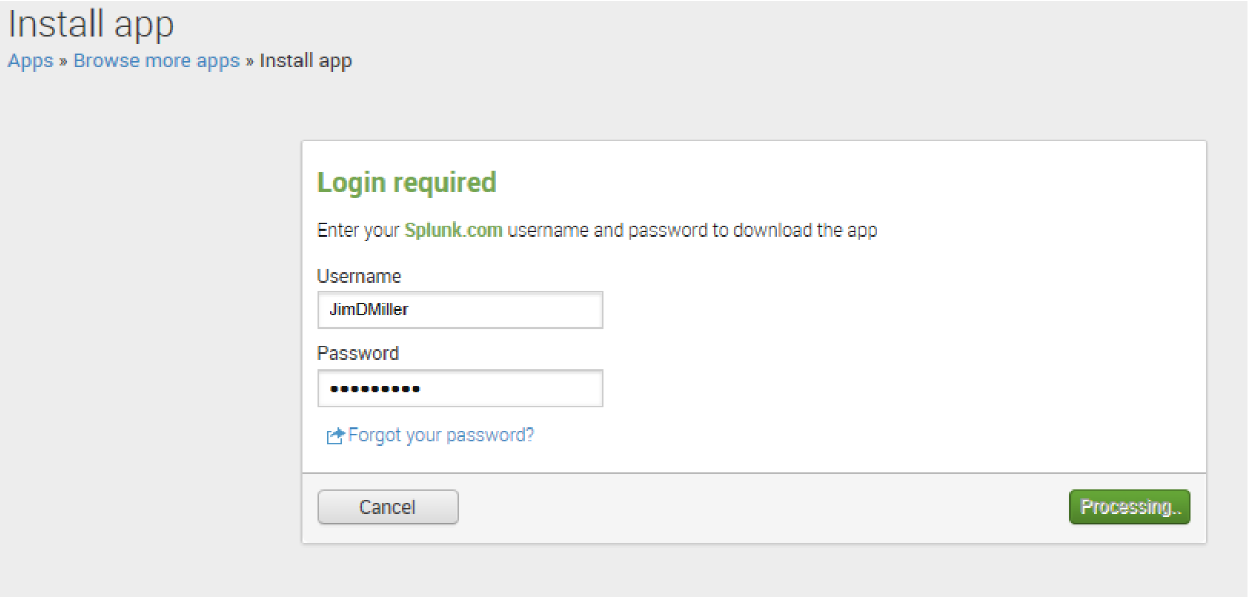


Lookup File Editor

Ever want to edit a lookup within Splunk with a user-interface?.. Read more

Author: LukeMurphey **Version:** 1.0 **Last updated:** 05/10/14 **Downloads:** 394 **License:** Creative Commons BY 3.0

Install free



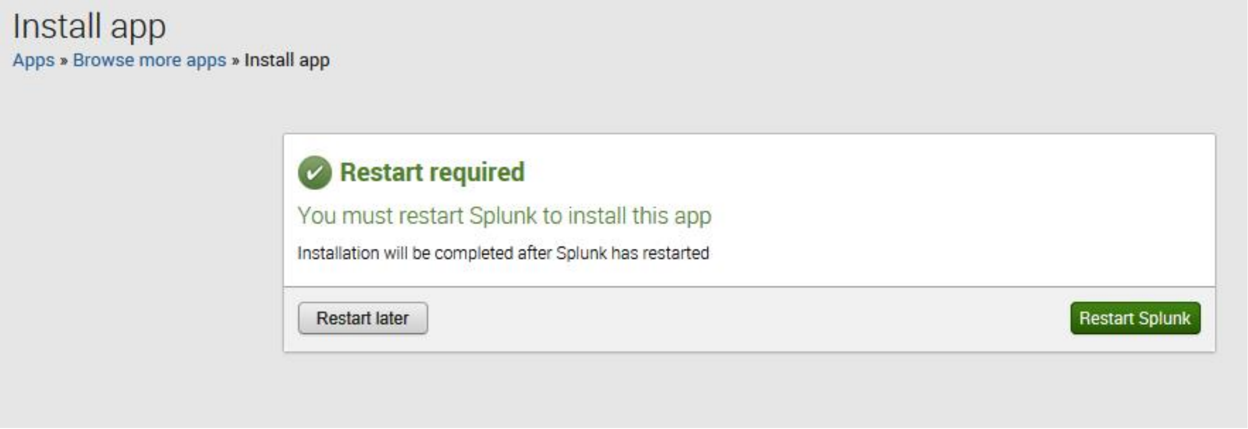
Install app

Login required

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

Username: JimDMiller

Password: ●●●●●●●●●

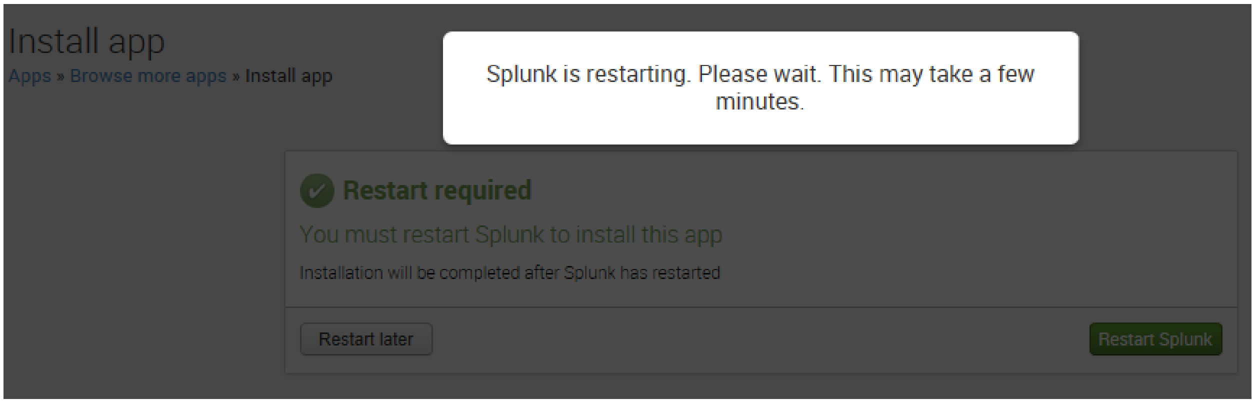


Install app

Restart required

You must restart Splunk to install this app

Installation will be completed after Splunk has restarted



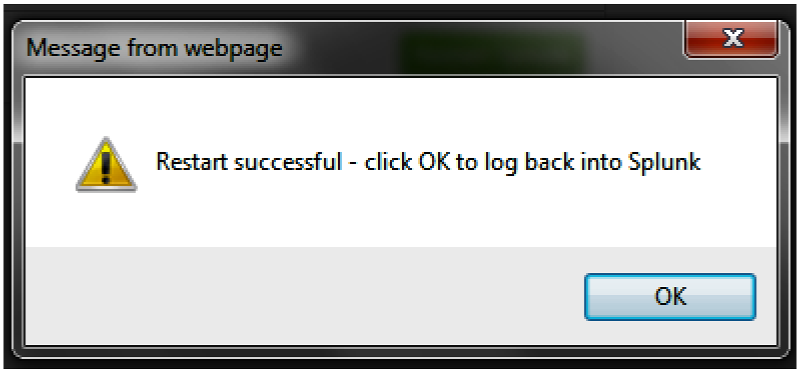
Splunk is restarting. Please wait. This may take a few minutes.

Install app

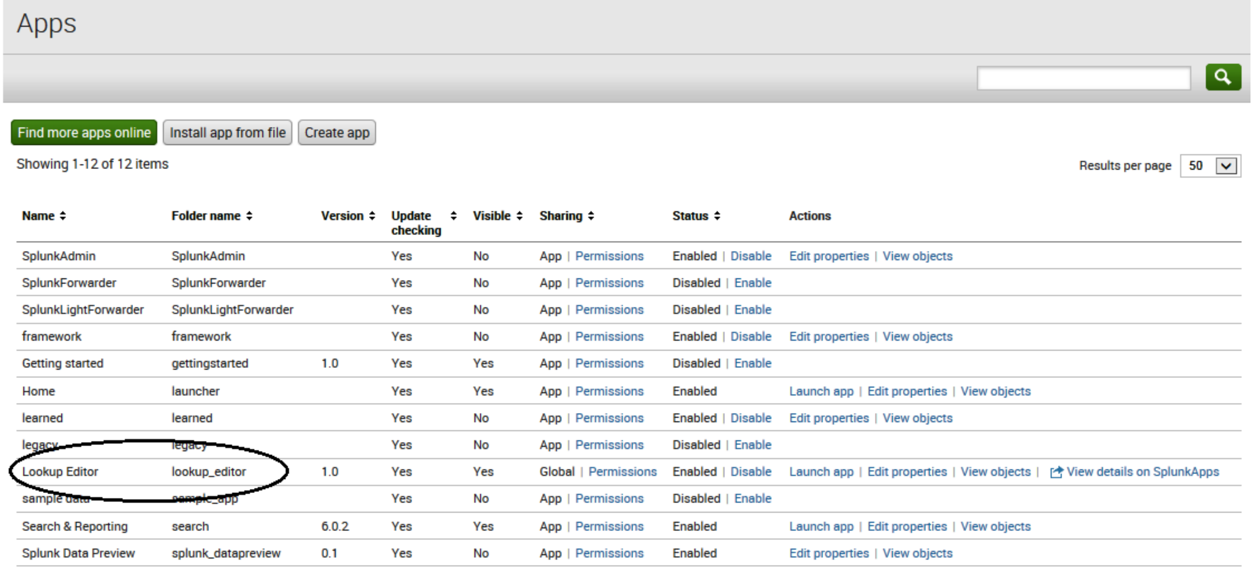
Restart required

You must restart Splunk to install this app

Installation will be completed after Splunk has restarted



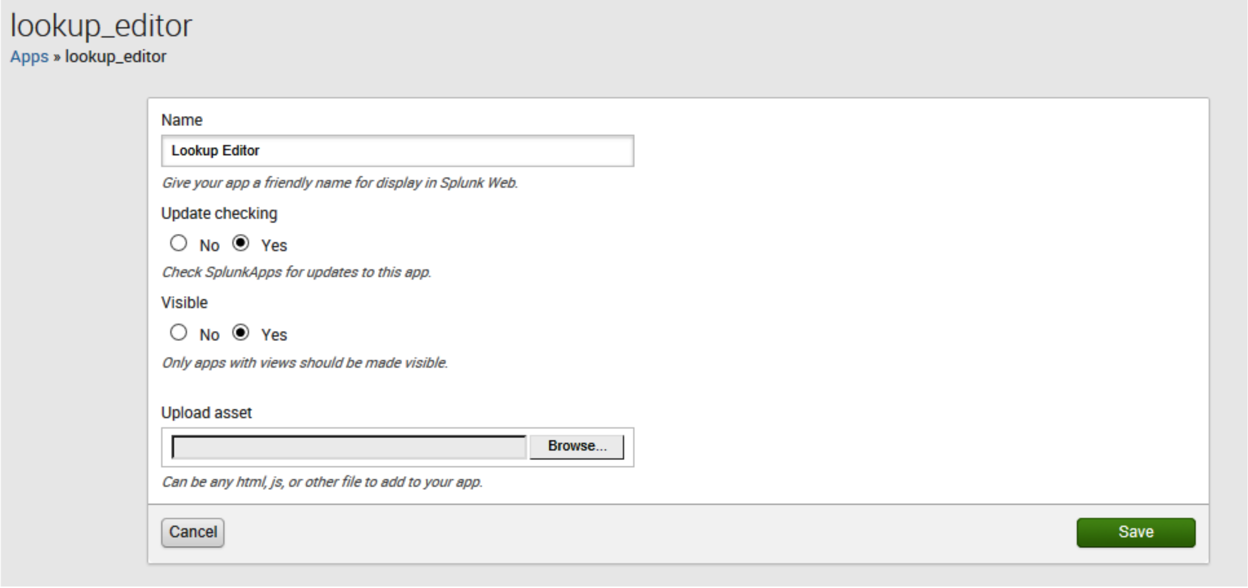
Restart successful - click OK to log back into Splunk



Showing 1-12 of 12 items

Results per page 50

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkAdmin	SplunkAdmin		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
framework	framework		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Getting started	gettingstarted	1.0	Yes	Yes	App | Permissions	Disabled | Enable	
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable	
Lookup Editor	lookup_editor	1.0	Yes	Yes	Global | Permissions	Enabled | Disable	Launch app | Edit properties | View objects | View details on SplunkApps
sample data	sample_app		Yes	No	App | Permissions	Disabled | Enable	
Search & Reporting	search	6.0.2	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
Splunk Data Preview	splunk_datapreview	0.1	Yes	No	App | Permissions	Enabled	Edit properties | View objects



lookup_editor

Apps » lookup_editor

Name

Lookup Editor

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

Update checking

○ No ● Yes

Check SplunkApps for updates to this app.

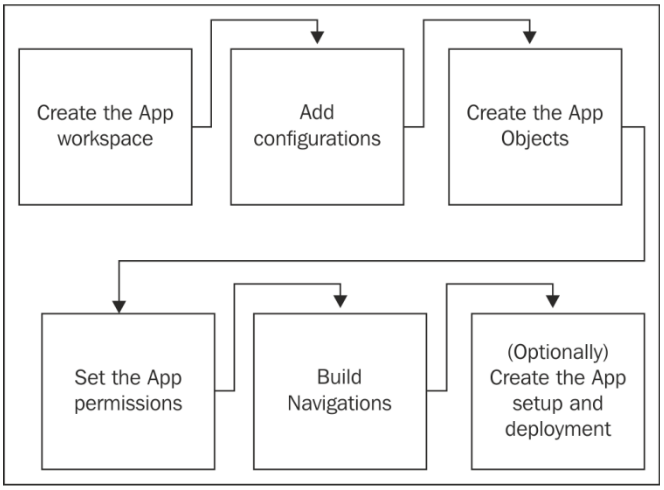
Visible

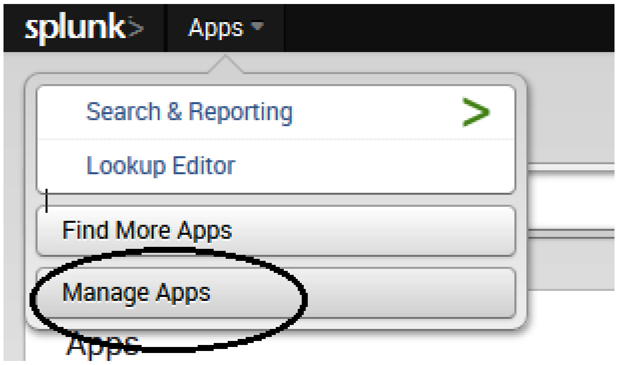
○ No ● Yes

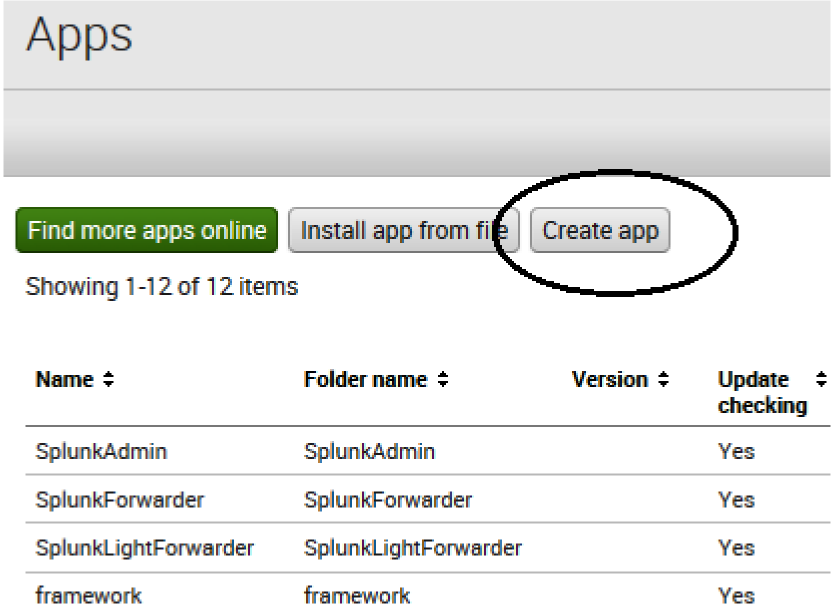
Only apps with views should be made visible.

Upload asset

Can be any html, js, or other file to add to your app.

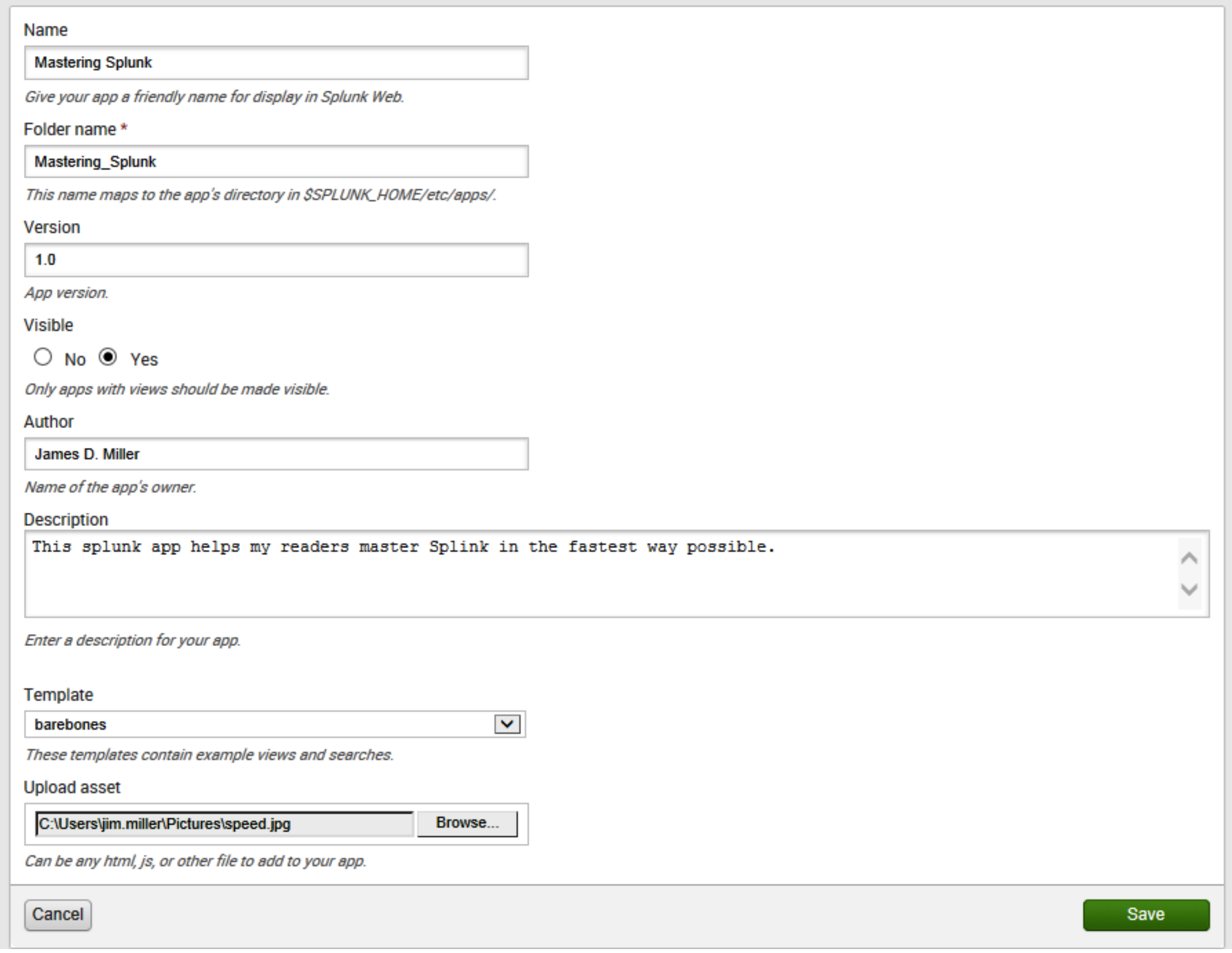






Showing 1-12 of 12 items

Name	Folder name	Version	Update checking
SplunkAdmin	SplunkAdmin		Yes
SplunkForwarder	SplunkForwarder		Yes
SplunkLightForwarder	SplunkLightForwarder		Yes
framework	framework		Yes



Name

Mastering Splunk

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

Folder name *

Mastering_Splunk

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

Version

1.0

App version.

Visible

○ No ● Yes

Only apps with views should be made visible.

Author

James D. Miller

Name of the app's owner.

Description

```
This splunk app helps my readers master Splink in the fastest way possible.
```

Enter a description for your app.

Template

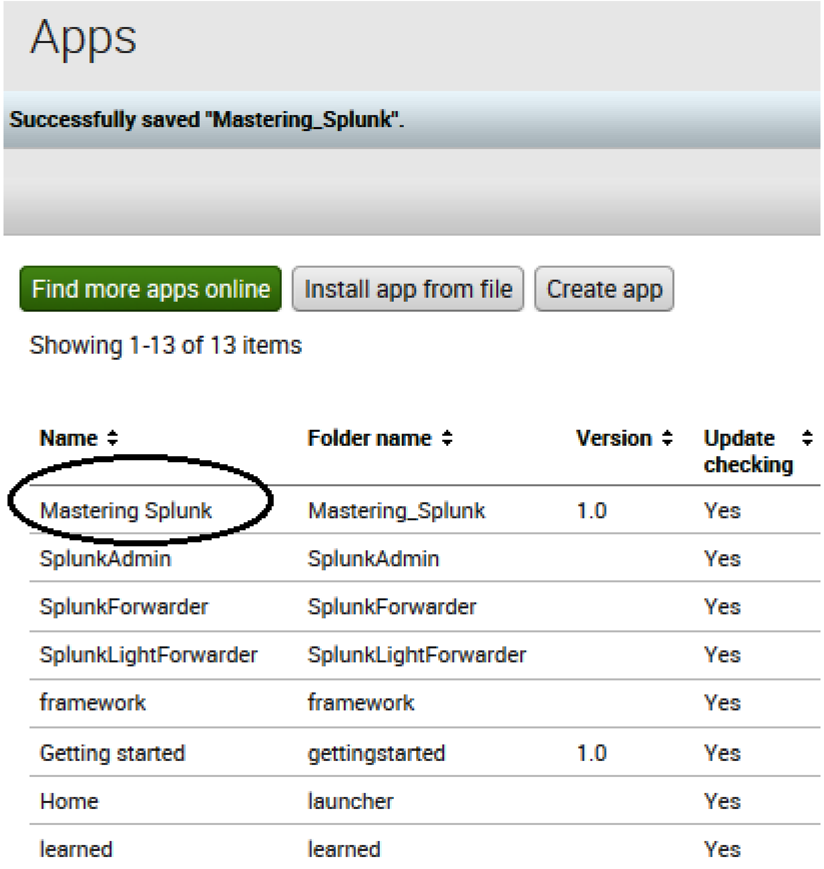
barebones

These templates contain example views and searches.

Upload asset

C:\Users\jim.miller\Pictures\speed.jpg

Can be any html, js, or other file to add to your app.

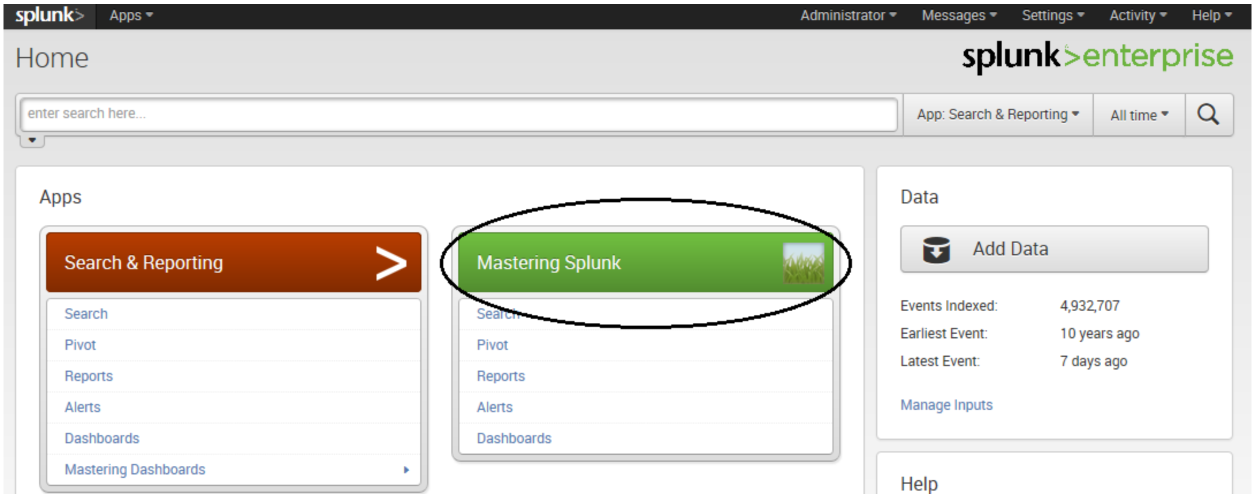


Successfully saved "Mastering_Splunk".

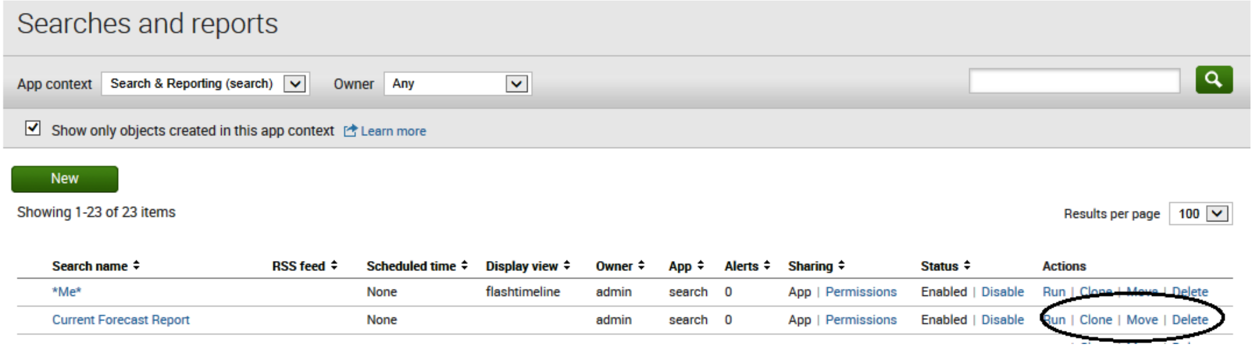
Showing 1-13 of 13 items

Name	Folder name	Version	Update checking
Mastering Splunk	Mastering_Splunk	1.0	Yes
SplunkAdmin	SplunkAdmin		Yes
SplunkForwarder	SplunkForwarder		Yes
SplunkLightForwarder	SplunkLightForwarder		Yes
framework	framework		Yes
Getting started	gettingstarted	1.0	Yes
Home	launcher		Yes
learned	learned		Yes

```
#
# Splunk app configuration file
#

[install]
is_configured = 0

[ui]
is_visible = 1
label = Mastering Splunk

[launcher]
author = James D. Miller
description = This splunk app helps my readers master Splink in the fastest way possible.
version = 1.0
```



Events Indexed: 4,932,707
Earliest Event: 10 years ago
Latest Event: 7 days ago

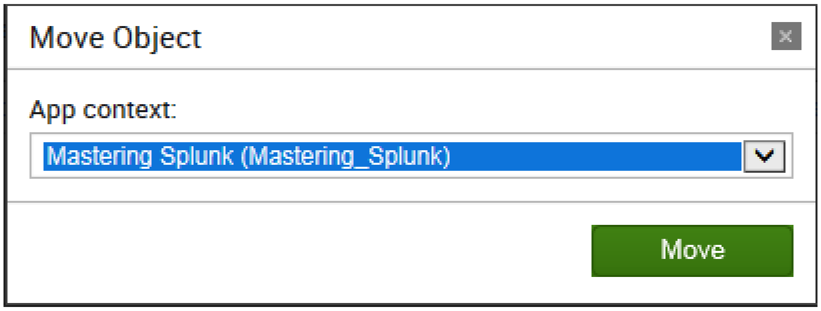


App context: Search & Reporting (search)   Owner: Any

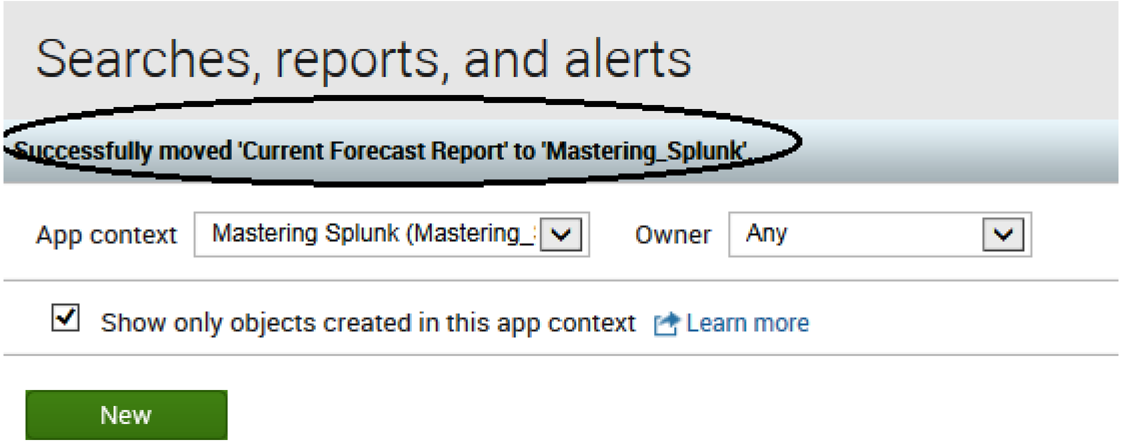
☑ Show only objects created in this app context Learn more

Showing 1-23 of 23 items

Search name	RSS feed	Scheduled time	Display view	Owner	App	Alerts	Sharing	Status	Actions
Me		None	flashtimeline	admin	search	0	App | Permissions	Enabled | Disable	Run | Clone | Move | Delete
Current Forecast Report		None		admin	search	0	App | Permissions	Enabled | Disable	Run | Clone | Move | Delete



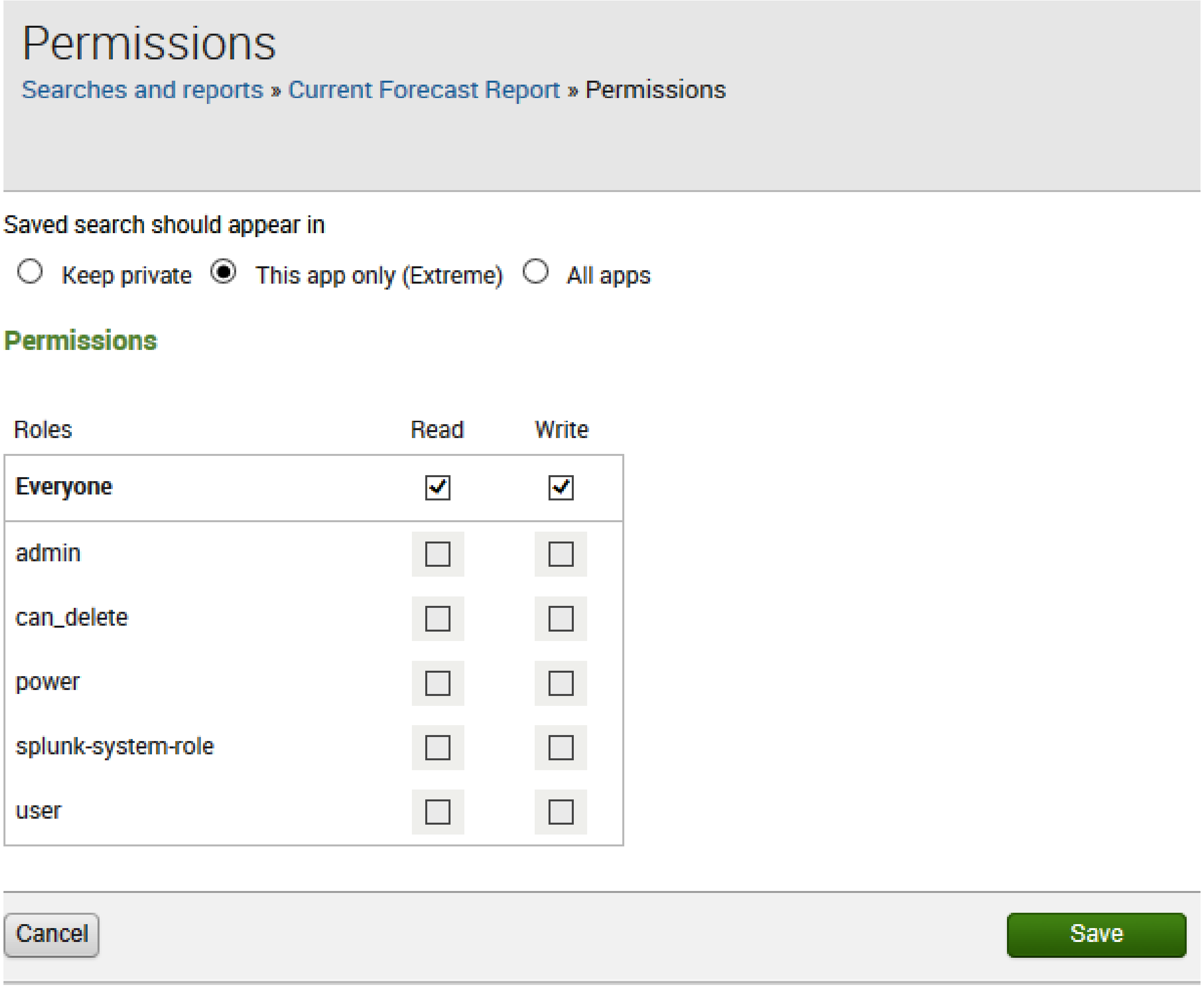
App context: Mastering Splunk (Mastering_Splunk)



Successfully moved 'Current Forecast Report' to 'Mastering_Splunk'

App context: Mastering Splunk (Mastering_   Owner: Any

☑ Show only objects created in this app context Learn more



Permissions

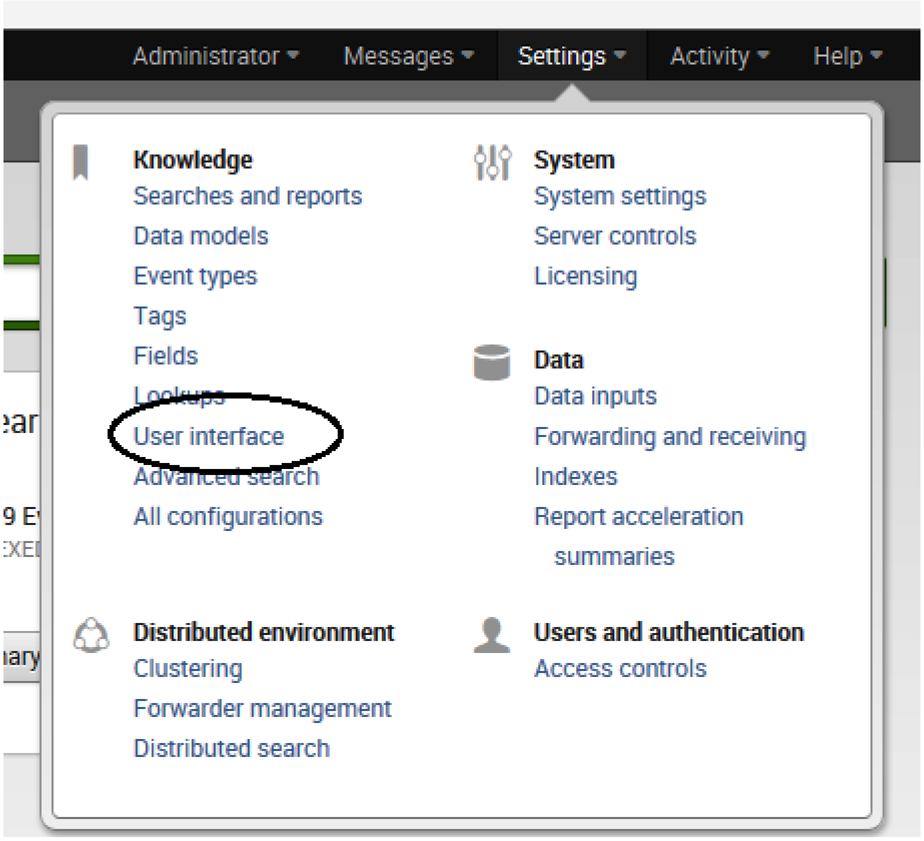
Searches and reports » Current Forecast Report » Permissions

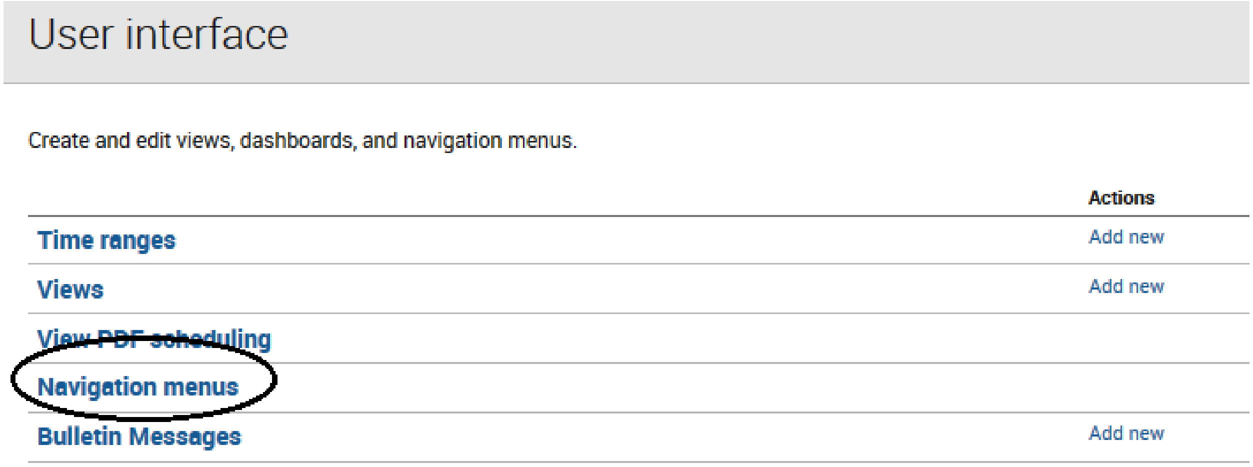
Saved search should appear in

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

Permissions

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

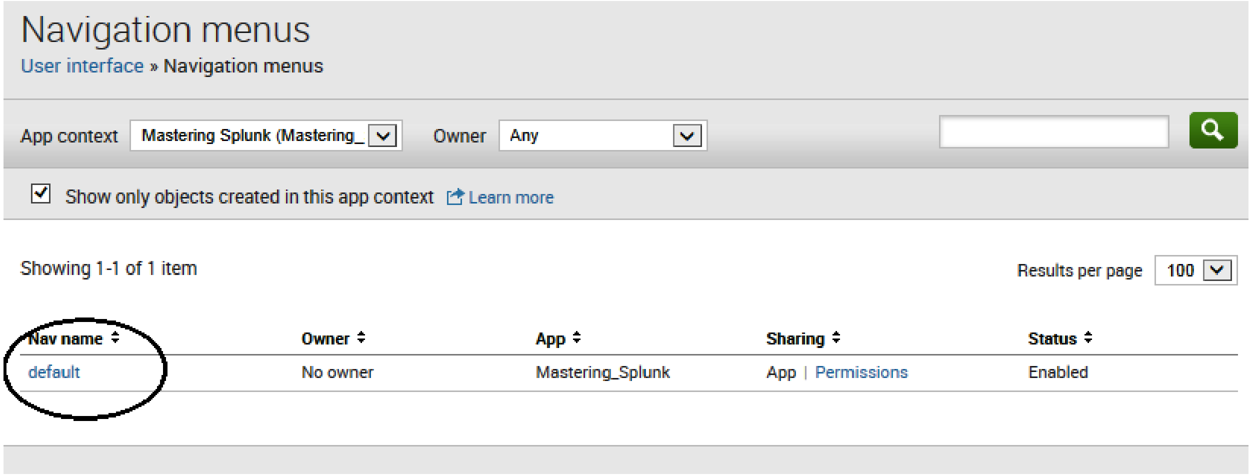




User interface

Create and edit views, dashboards, and navigation menus.

	Actions
Time ranges	Add new
Views	Add new
View PDF scheduling	
Navigation menus	
Bulletin Messages	Add new



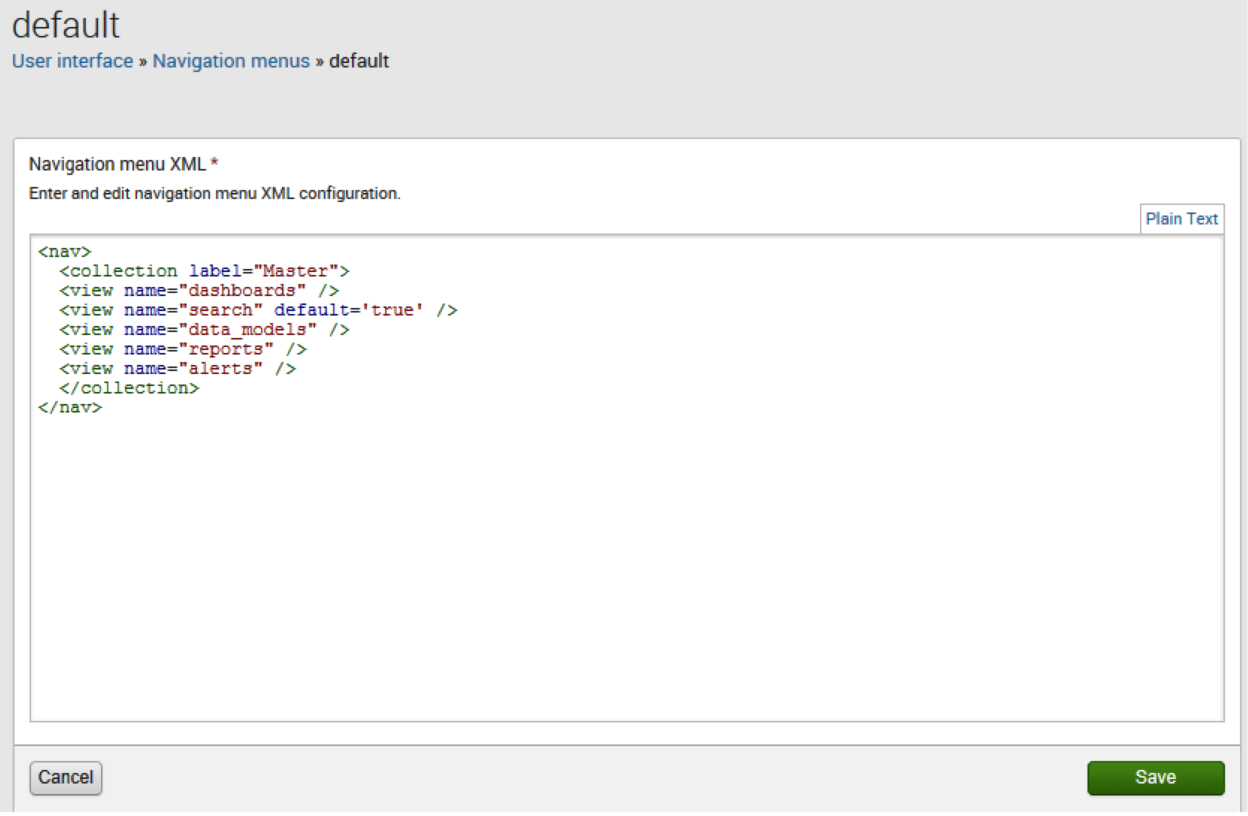
Navigation menus

User interface » Navigation menus

☑ Show only objects created in this app context

Showing 1-1 of 1 item

Nav name	Owner	App	Sharing	Status
default	No owner	Mastering_Splunk	App | Permissions	Enabled



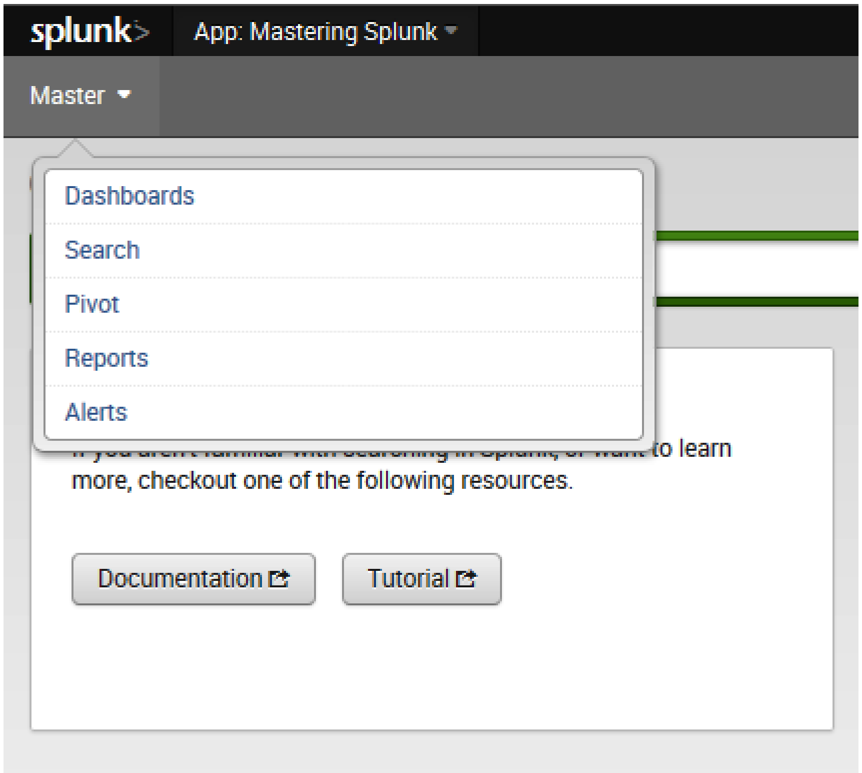
default

User interface » Navigation menus » default

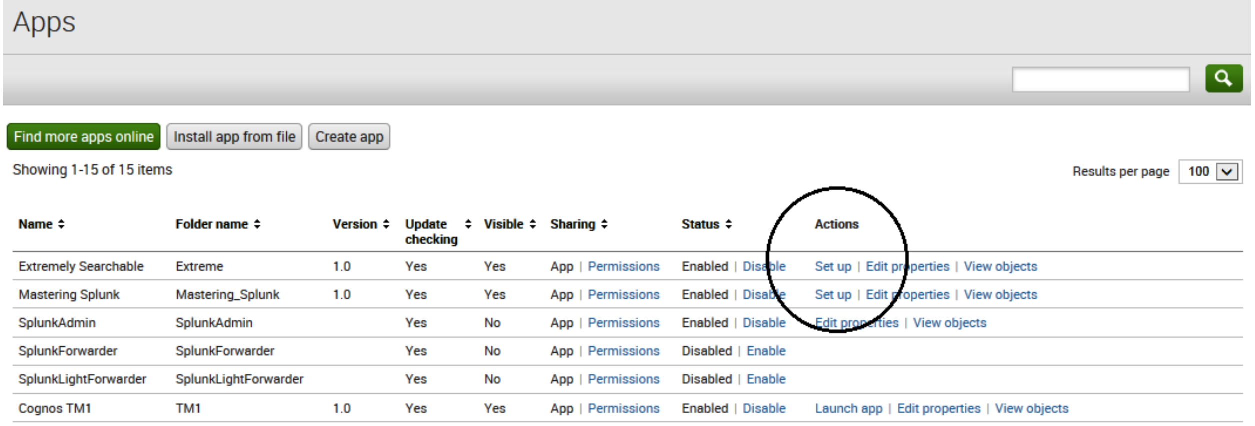
Navigation menu XML *

Enter and edit navigation menu XML configuration.

```
<nav>
  <collection label="Master">
  <view name="dashboards" />
  <view name="search" default='true' />
  <view name="data_models" />
  <view name="reports" />
  <view name="alerts" />
  </collection>
</nav>
```



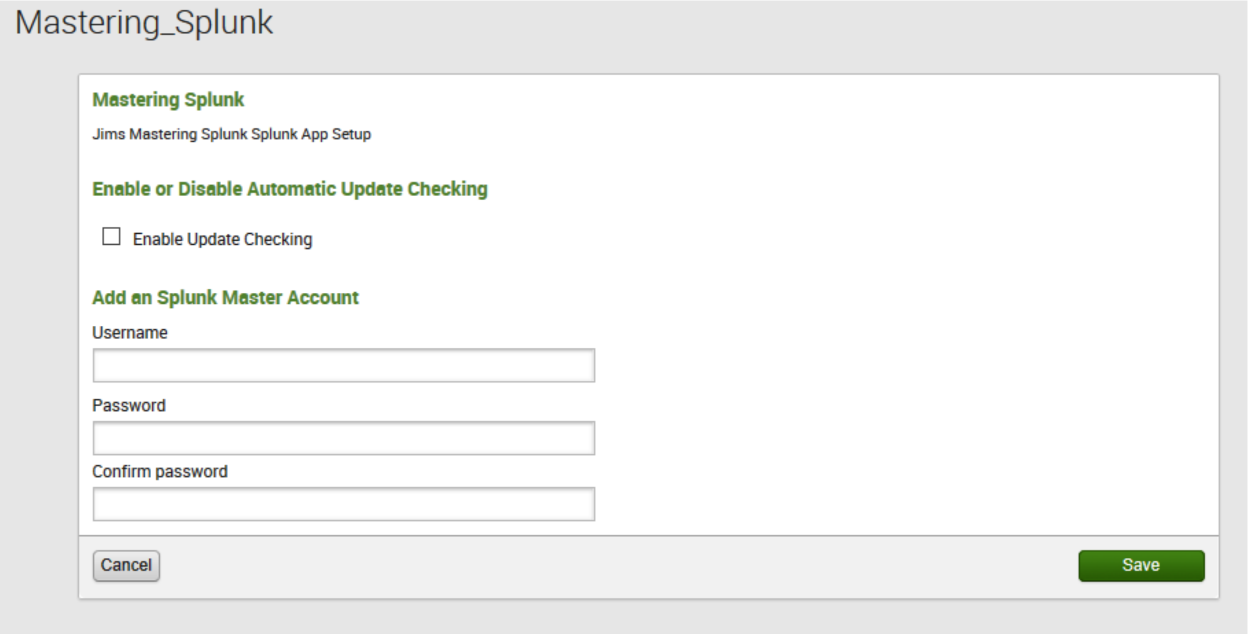
to learn more, checkout one of the following resources.



Showing 1-15 of 15 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Extremely Searchable	Extreme	1.0	Yes	Yes	App | Permissions	Enabled | Disable	Set up | Edit properties | View objects
Mastering Splunk	Mastering_Splunk	1.0	Yes	Yes	App | Permissions	Enabled | Disable	Set up | Edit properties | View objects
SplunkAdmin	SplunkAdmin		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Cognos TM1	TM1	1.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects

```
<setup>
 <block title="Mastering Splunk" endpoint="saved/searches/" entity="foobar">
    <text> Jims Mastering Splunk Splunk App Setup </text>
    </block>
    <block title="Enable or Disable Automatic Update Checking" endpoint="storage/passwords" entity="_new">
        <input field="check_for_updates">
      <label>Enable Update Checking</label>
      <type>bool</type>
    </input>
  </block> |
  <block title="Add an Splunk Master Account" endpoint="storage/passwords" entity="_new">
    <input field="name">
      <label>Username</label>
      <type>text</type>
    </input>
    <input field="password">
      <label>Password</label>
      <type>password</type>
    </input>
  </block>
```



Mastering_Splunk

Mastering Splunk

Jims Mastering Splunk Splunk App Setup

Enable or Disable Automatic Update Checking

☐ Enable Update Checking

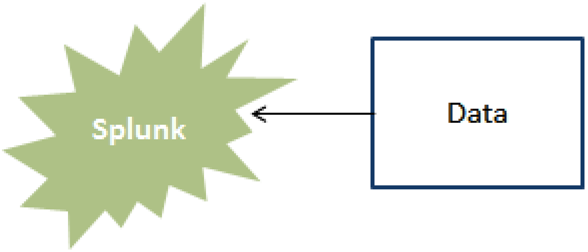
Add an Splunk Master Account

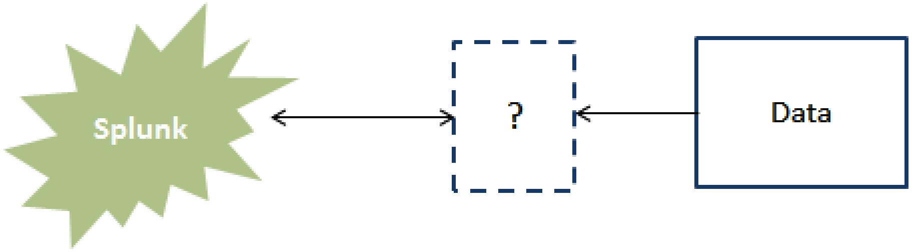
Username

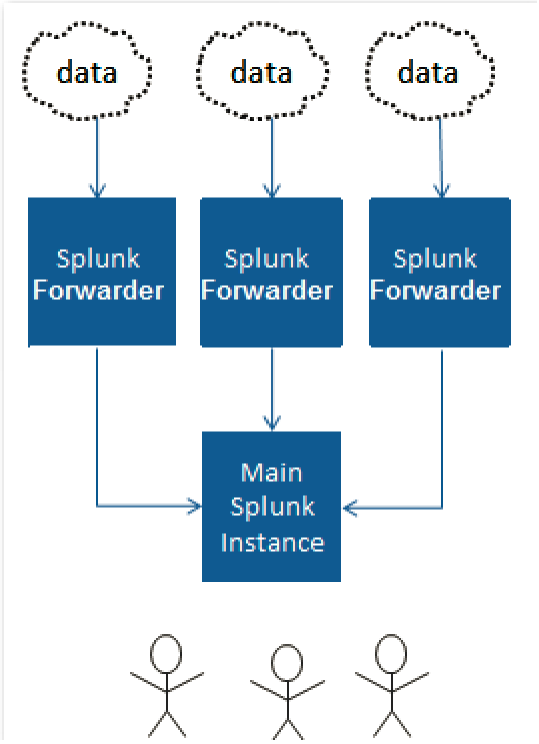
Password

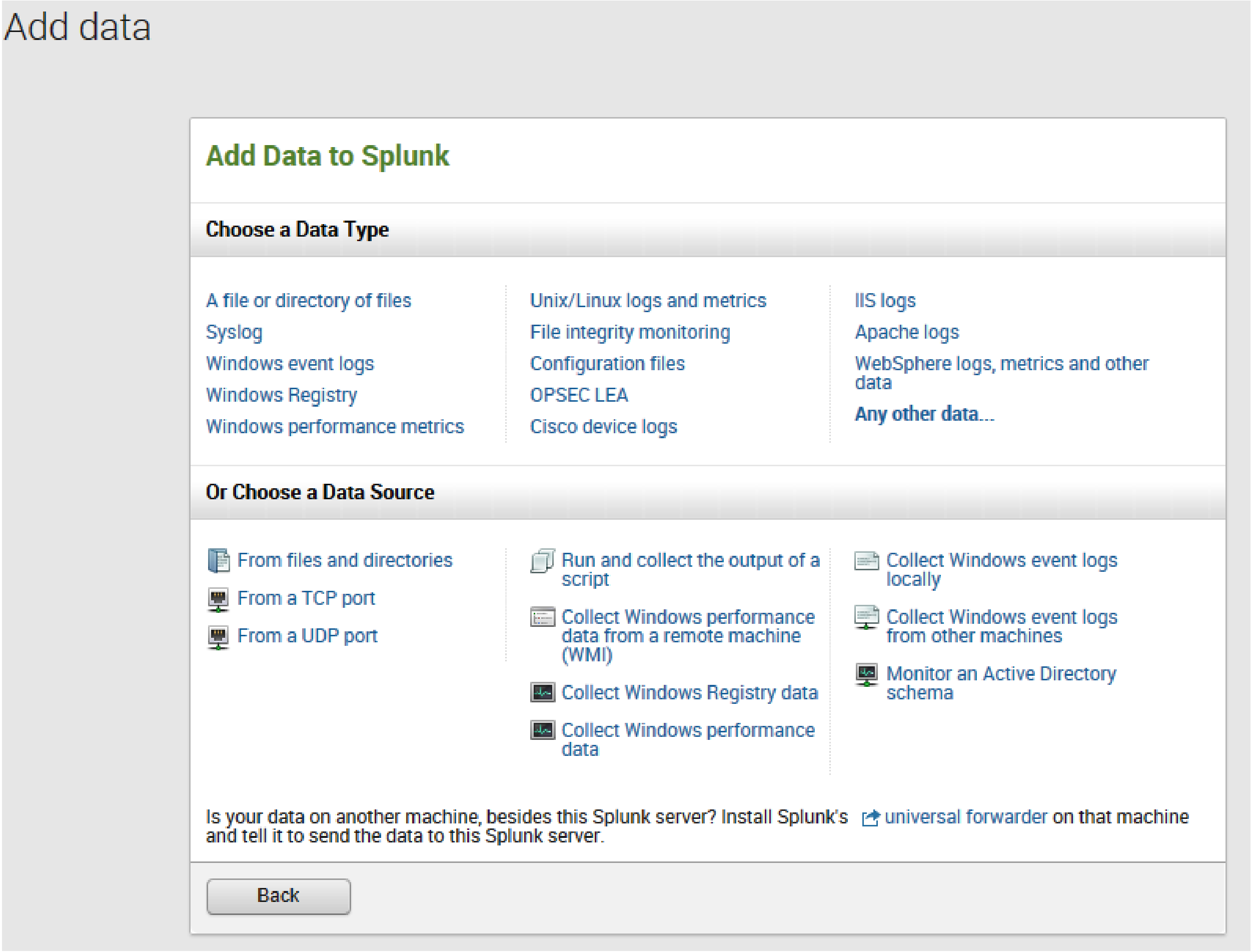
Confirm password

Chapter 8, *Monitoring and Alerting*









Add data

Add Data to Splunk

Choose a Data Type

A file or directory of files
Syslog
Windows event logs
Windows Registry
Windows performance metrics

Unix/Linux logs and metrics
File integrity monitoring
Configuration files
OPSEC LEA
Cisco device logs

IIS logs
Apache logs
WebSphere logs, metrics and other data
Any other data...

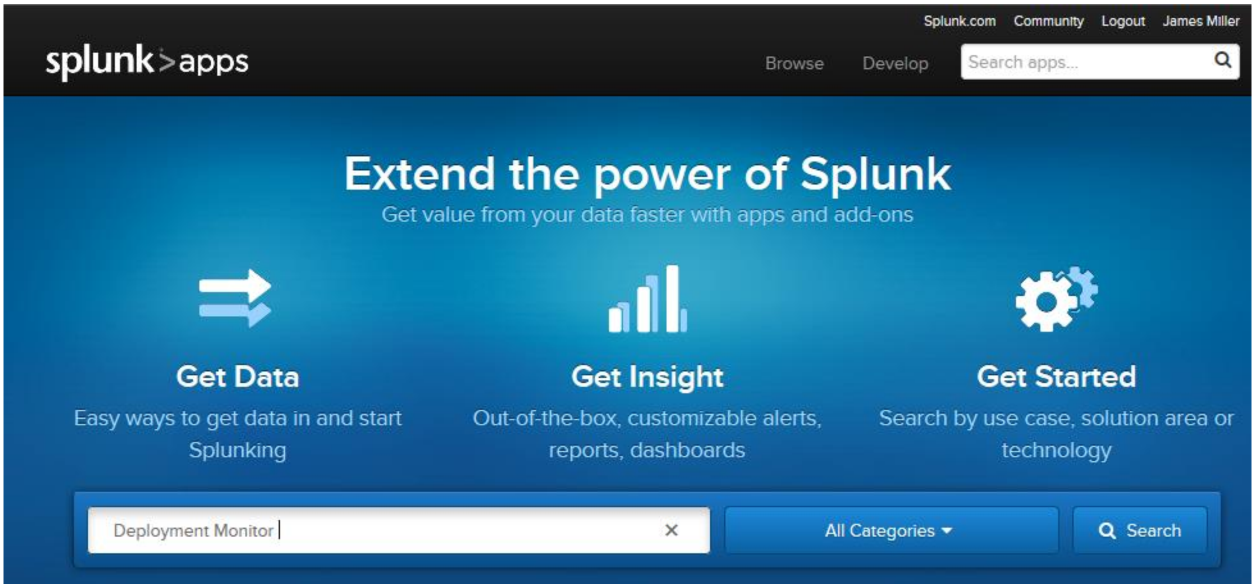
Or Choose a Data Source

From files and directories
From a TCP port
From a UDP port

Run and collect the output of a script
Collect Windows performance data from a remote machine (WMI)
Collect Windows Registry data
Collect Windows performance data

Collect Windows event logs locally
Collect Windows event logs from other machines
Monitor an Active Directory schema

Is your data on another machine, besides this Splunk server? Install Splunk's universal forwarder on that machine and tell it to send the data to this Splunk server.



Extend the power of Splunk

Get value from your data faster with apps and add-ons

Get Data

Easy ways to get data in and start Splunking

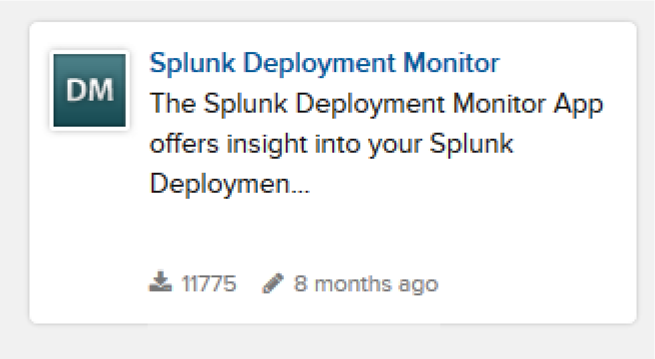
Get Insight

Out-of-the-box, customizable alerts, reports, dashboards

Get Started

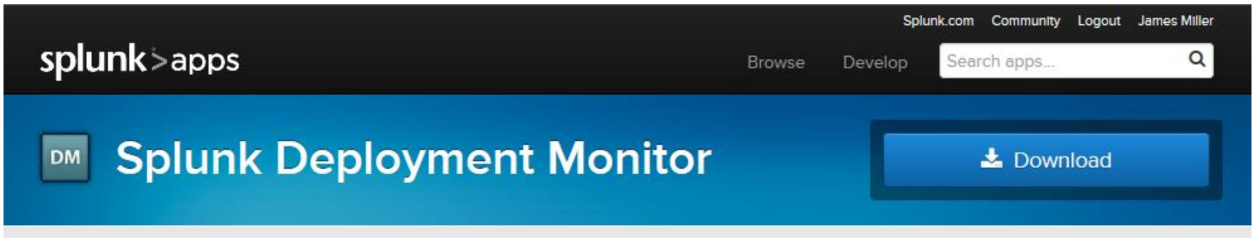
Search by use case, solution area or technology

Deployment Monitor

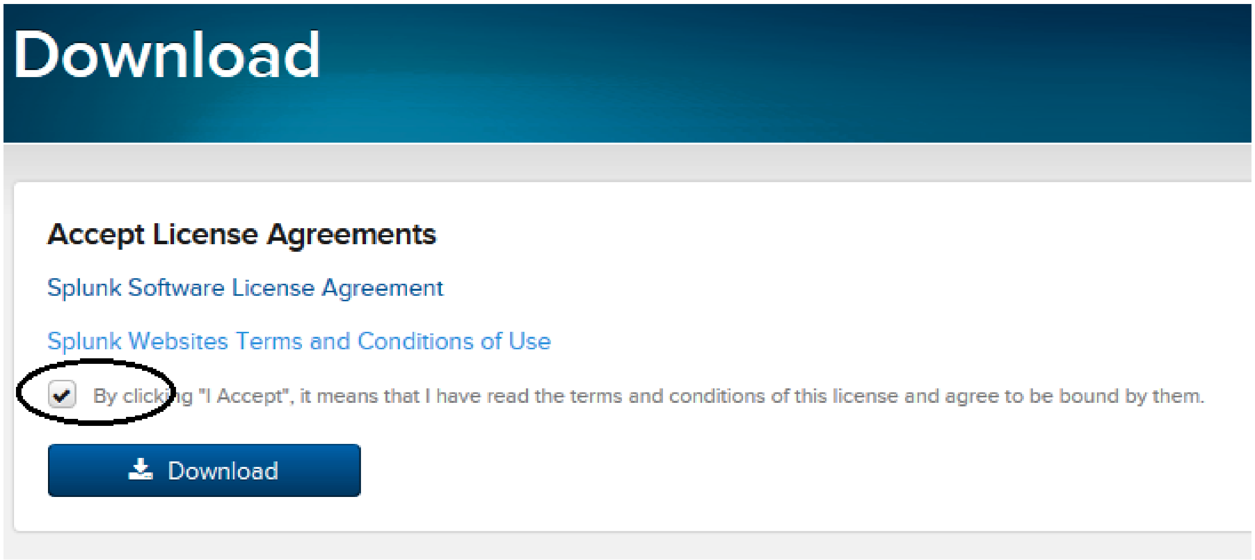


Splunk Deployment Monitor

The Splunk Deployment Monitor App offers insight into your Splunk Deploymen...



Splunk Deployment Monitor



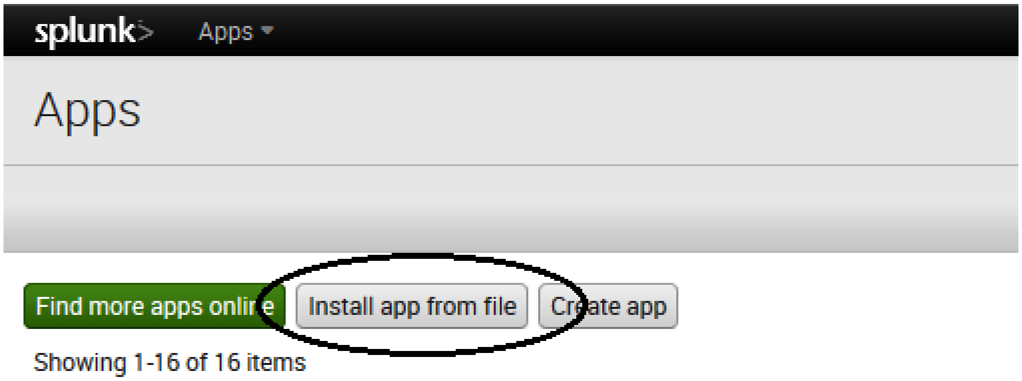
Download

Accept License Agreements

Splunk Software License Agreement

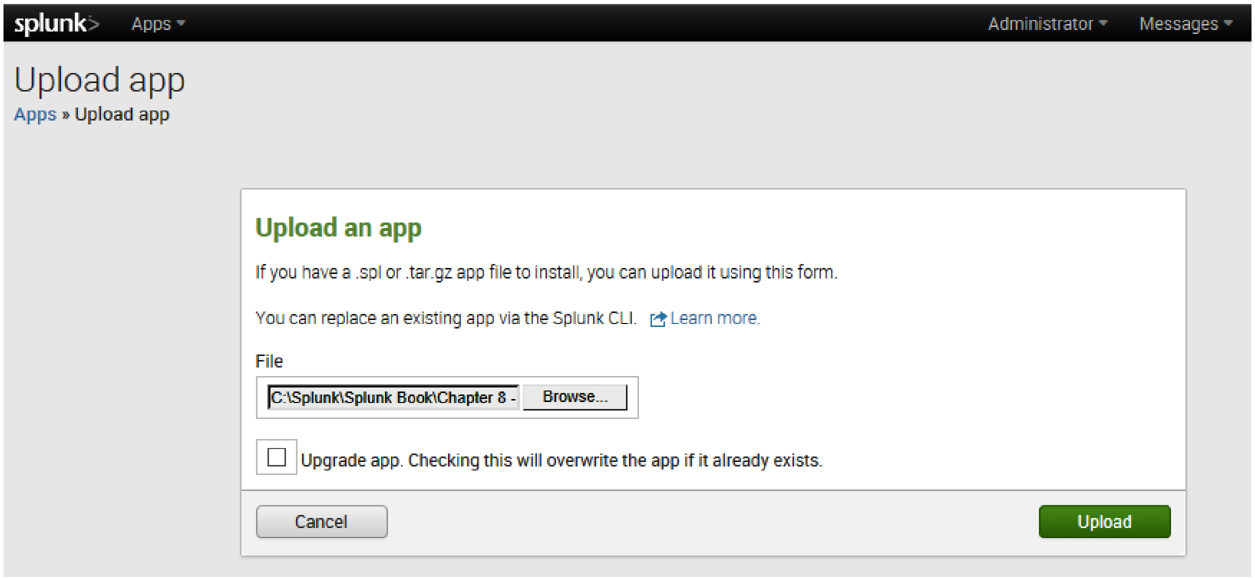
Splunk Websites Terms and Conditions of Use

☑ By clicking "I Accept", it means that I have read the terms and conditions of this license and agree to be bound by them.



Apps

Showing 1-16 of 16 items



Upload app

Apps » Upload app

Upload an app

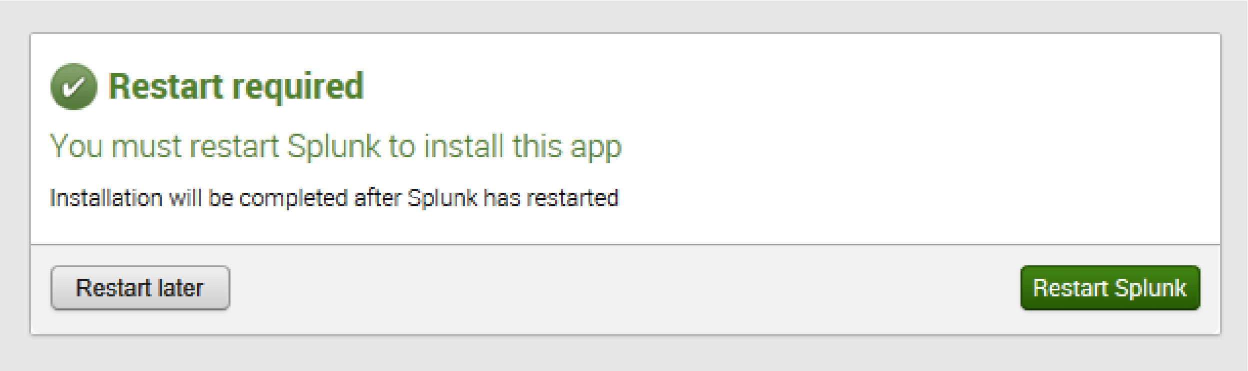
If you have a .spl or .tar.gz app file to install, you can upload it using this form.

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

File

C:\Splunk\Splunk Book\Chapter 8 -

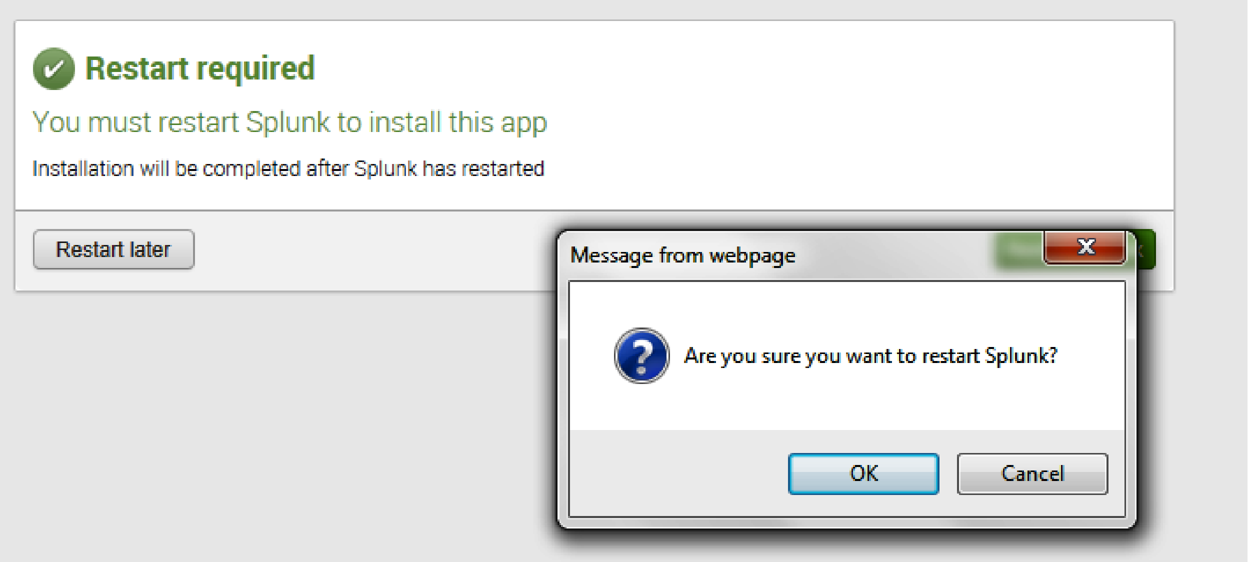
☐ Upgrade app. Checking this will overwrite the app if it already exists.



Restart required

You must restart Splunk to install this app

Installation will be completed after Splunk has restarted



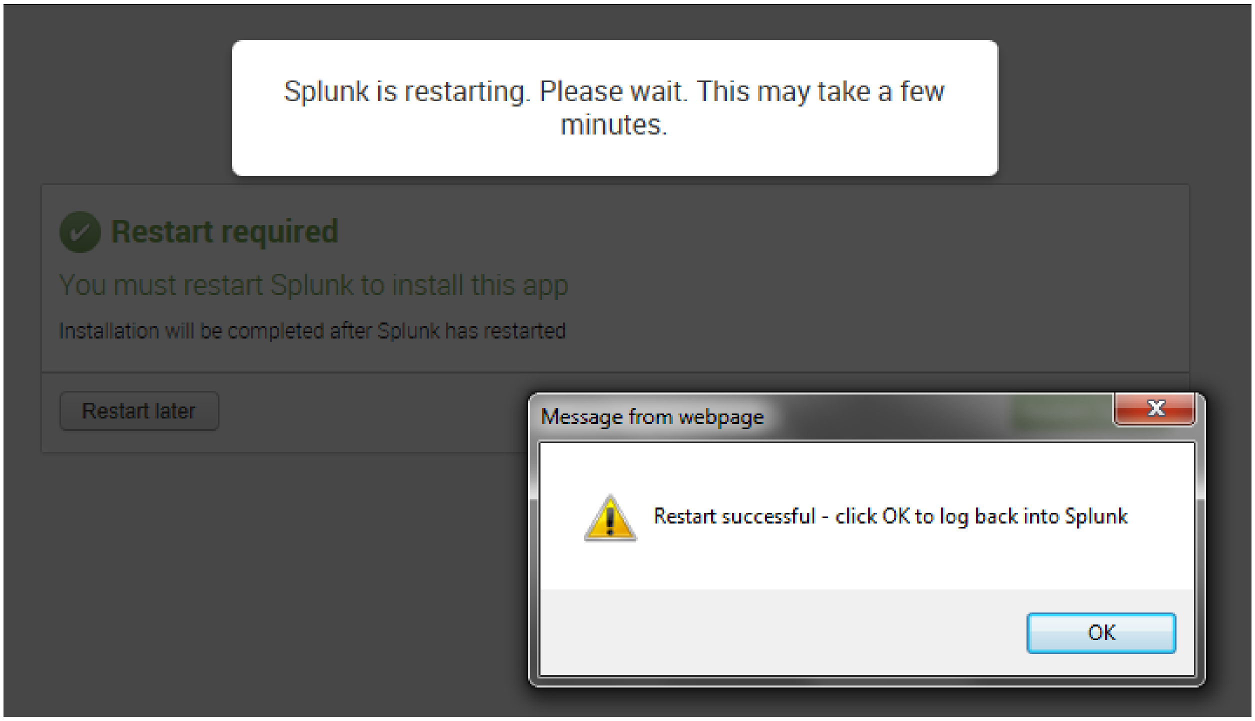
Restart required

You must restart Splunk to install this app

Installation will be completed after Splunk has restarted

Message from webpage

Are you sure you want to restart Splunk?



Splunk is restarting. Please wait. This may take a few minutes.

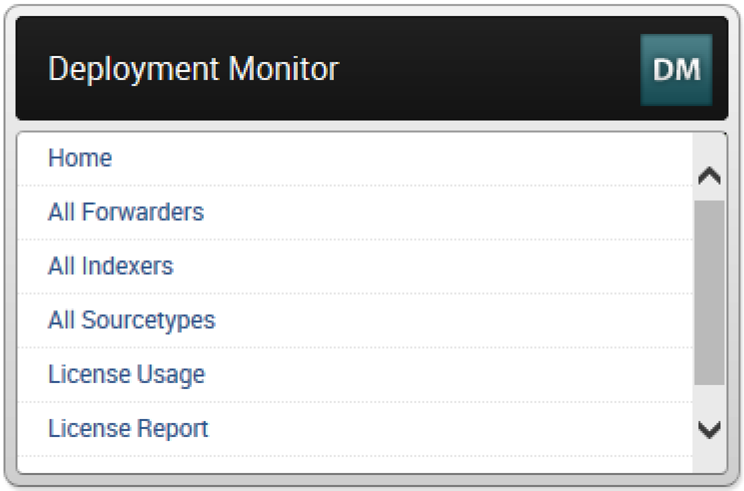
Restart required

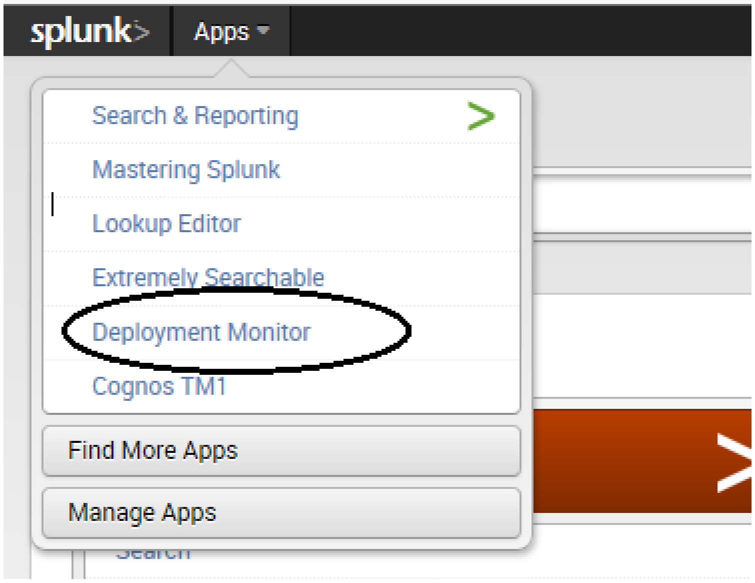
You must restart Splunk to install this app

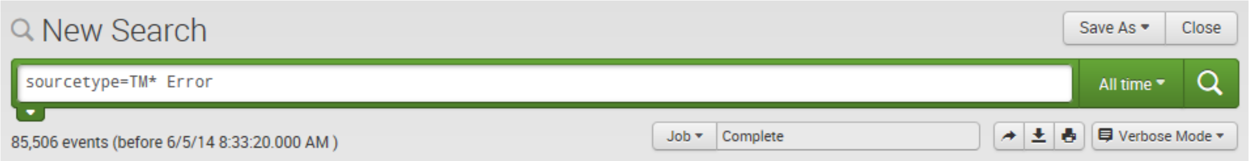
Installation will be completed after Splunk has restarted

Message from webpage

Restart successful - click OK to log back into Splunk

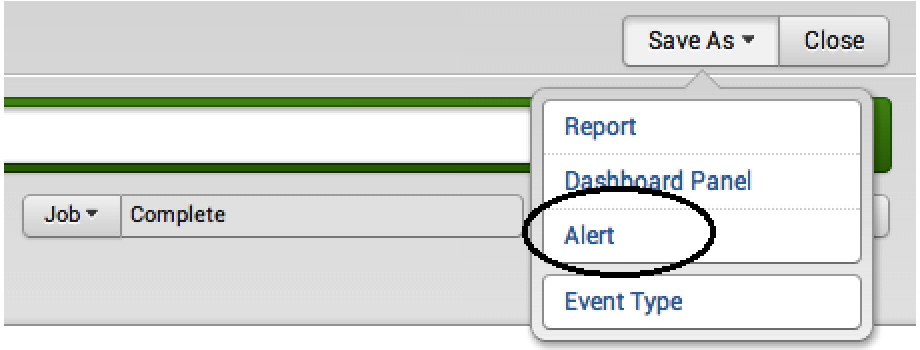


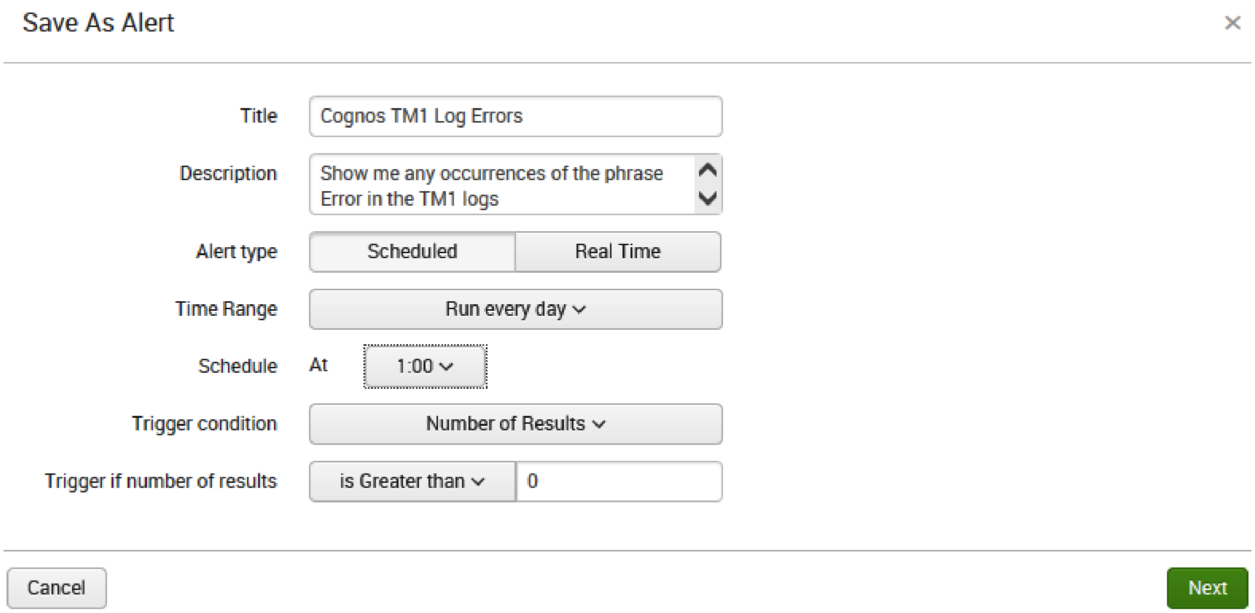




```
sourcetype=TM* Error
```

85,506 events (before 6/5/14 8:33:20.000 AM)





Title: Cognos TM1 Log Errors

Description: Show me any occurrences of the phrase Error in the TM1 logs

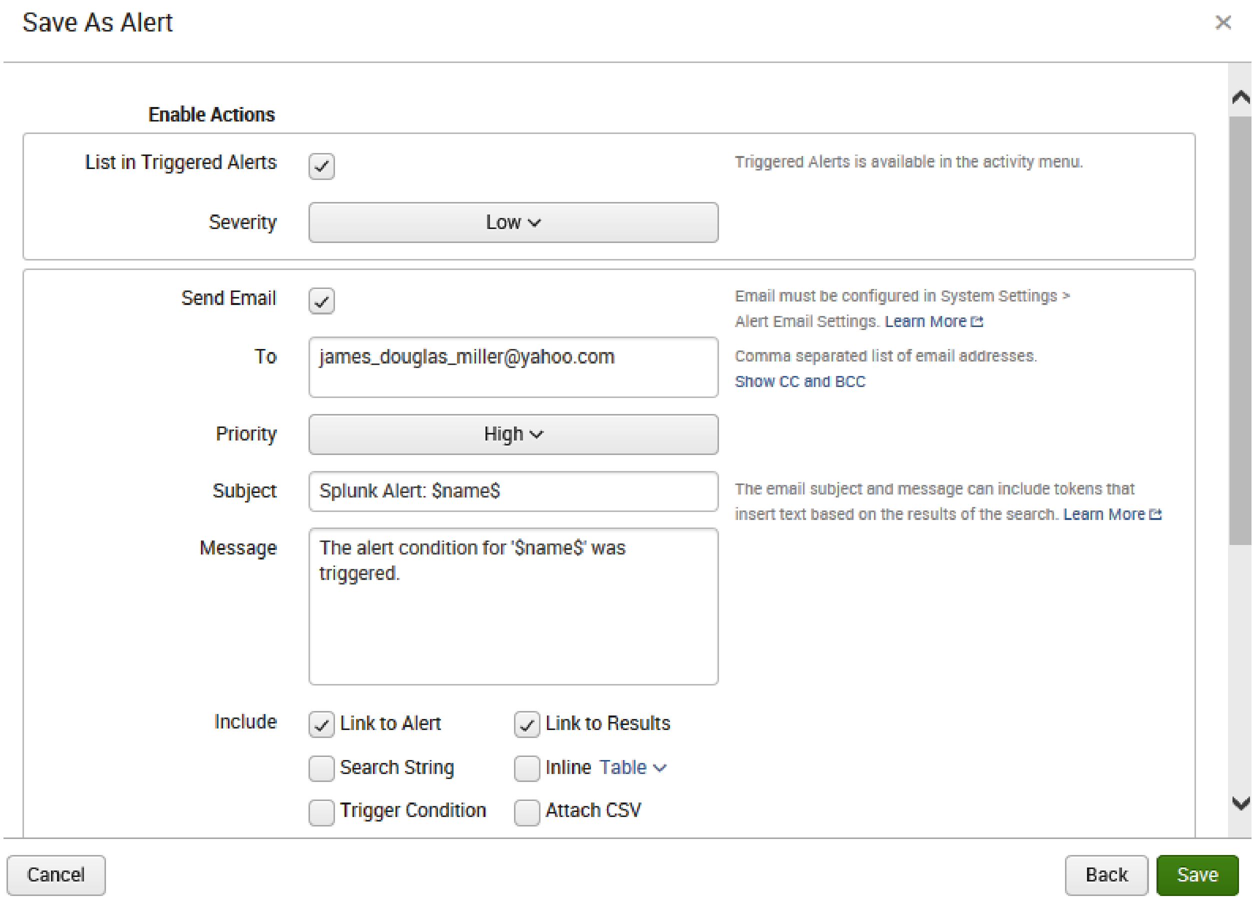
Alert type: Scheduled | Real Time

Time Range: Run every day

Schedule: At 1:00

Trigger condition: Number of Results

Trigger if number of results: is Greater than 0



Enable Actions

List in Triggered Alerts: ☑ — Triggered Alerts is available in the activity menu.

Severity: Low

Send Email: ☑ — Email must be configured in System Settings > Alert Email Settings. Learn More

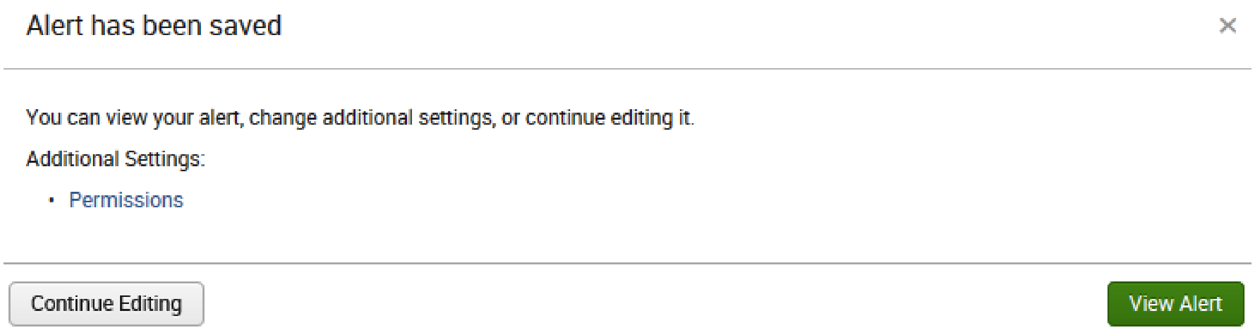
To: james_douglas_miller@yahoo.com — Comma separated list of email addresses. Show CC and BCC

Priority: High

Subject: Splunk Alert: $name$ — The email subject and message can include tokens that insert text based on the results of the search. Learn More

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

Include:
☑ Link to Alert ☑ Link to Results
□ Search String □ Inline Table
□ Trigger Condition □ Attach CSV

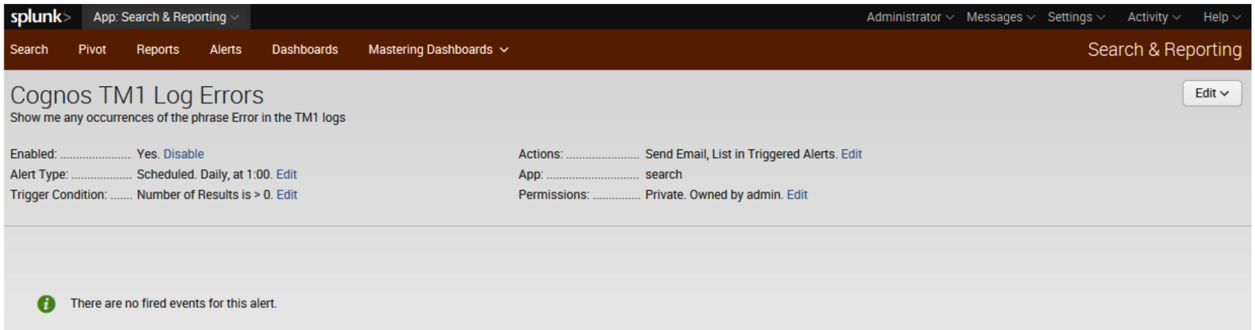


Alert has been saved

You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- Permissions



splunk> App: Search & Reporting
Administrator Messages Settings Activity Help
Search Pivot Reports Alerts Dashboards Mastering Dashboards
Search & Reporting
Edit

Cognos TM1 Log Errors

Show me any occurrences of the phrase Error in the TM1 logs

Enabled: Yes. Disable

Alert Type: Scheduled. Daily, at 1:00. Edit

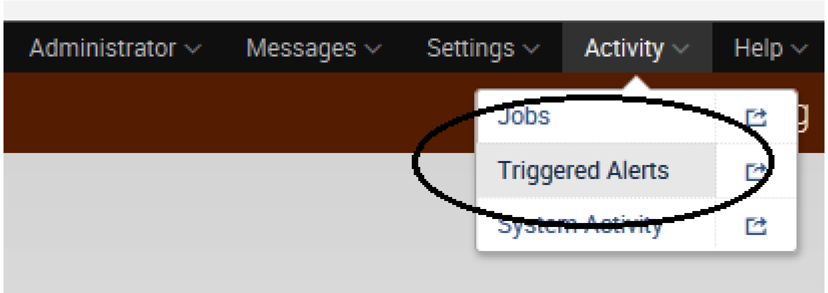
Trigger Condition: Number of Results is > 0. Edit

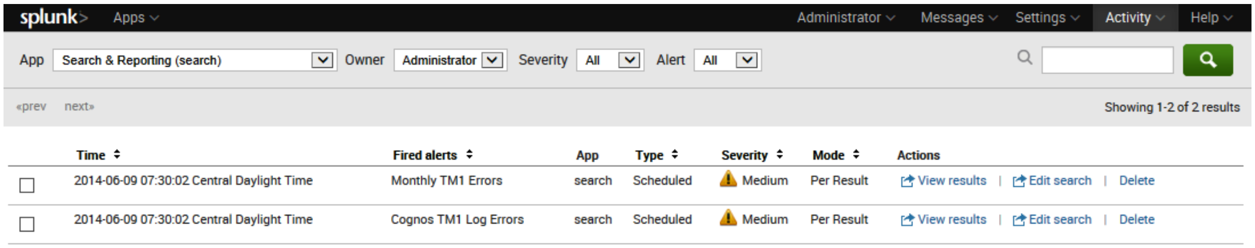
Actions: Send Email, List in Triggered Alerts. Edit

App: search

Permissions: Private. Owned by admin. Edit

There are no fired events for this alert.



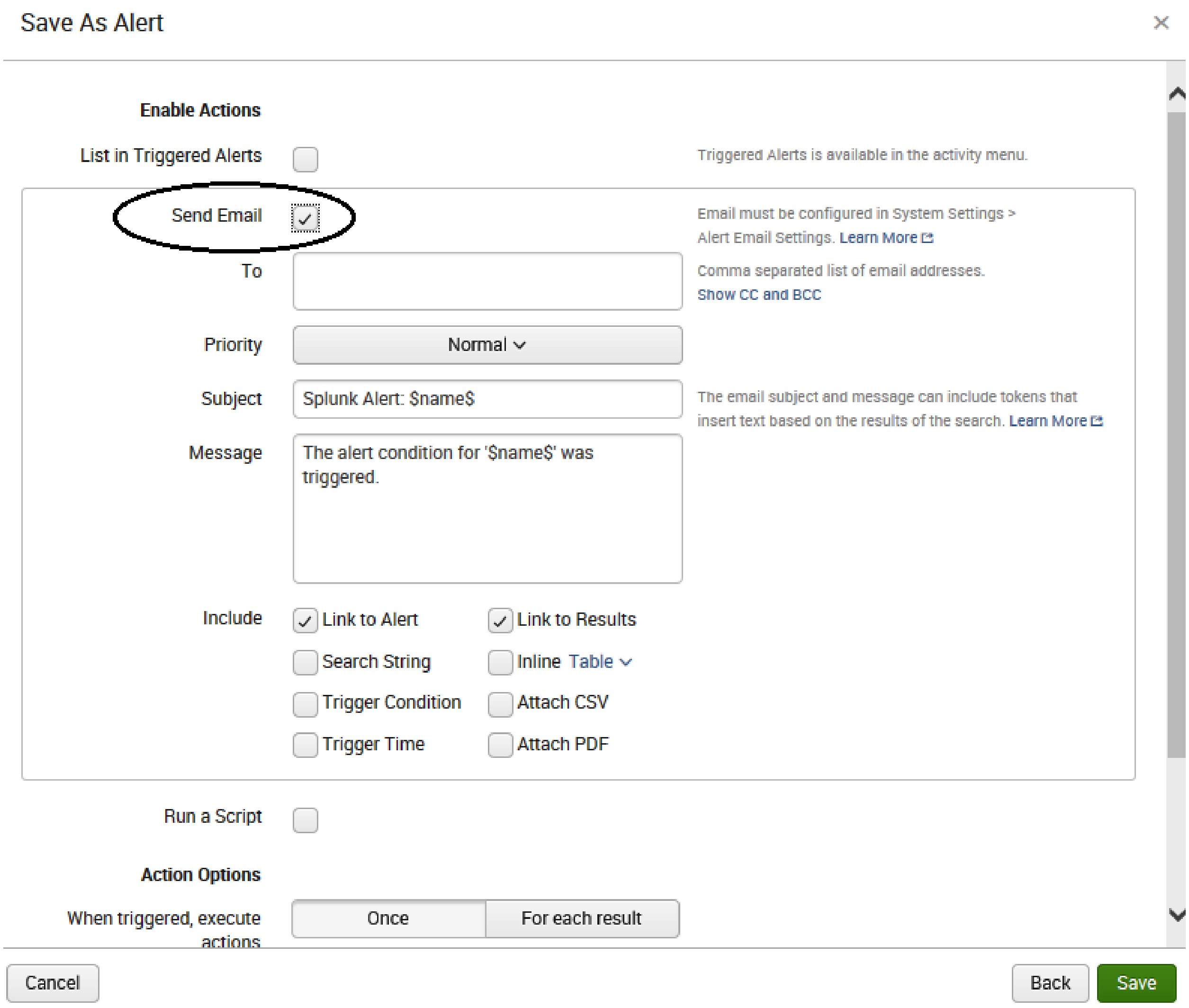


App: Search & Reporting (search) Owner: Administrator Severity: All Alert: All

«prev next»

Showing 1-2 of 2 results

	Time	Fired alerts	App	Type	Severity	Mode	Actions
□	2014-06-09 07:30:02 Central Daylight Time	Monthly TM1 Errors	search	Scheduled	⚠ Medium	Per Result	View results | Edit search | Delete
□	2014-06-09 07:30:02 Central Daylight Time	Cognos TM1 Log Errors	search	Scheduled	⚠ Medium	Per Result	View results | Edit search | Delete



Save As Alert

Enable Actions

List in Triggered Alerts □ — Triggered Alerts is available in the activity menu.

Send Email ☑ — Email must be configured in System Settings > Alert Email Settings. Learn More

To: — Comma separated list of email addresses. Show CC and BCC

Priority: Normal

Subject: Splunk Alert: $name$ — The email subject and message can include tokens that insert text based on the results of the search. Learn More

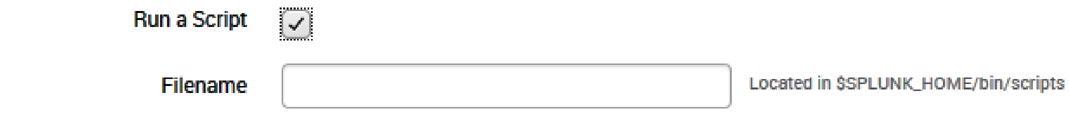
Message: The alert condition for '$name$' was triggered.

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

Run a Script □

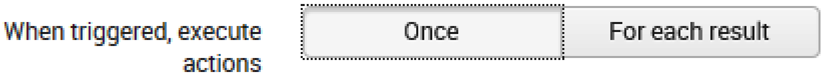
Action Options

When triggered, execute actions: Once | For each result

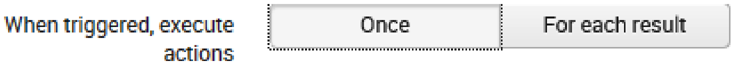


Run a Script ☑

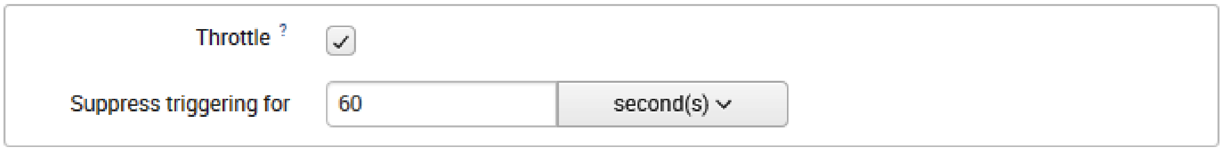
Filename: — Located in $SPLUNK_HOME/bin/scripts



When triggered, execute actions: Once | For each result

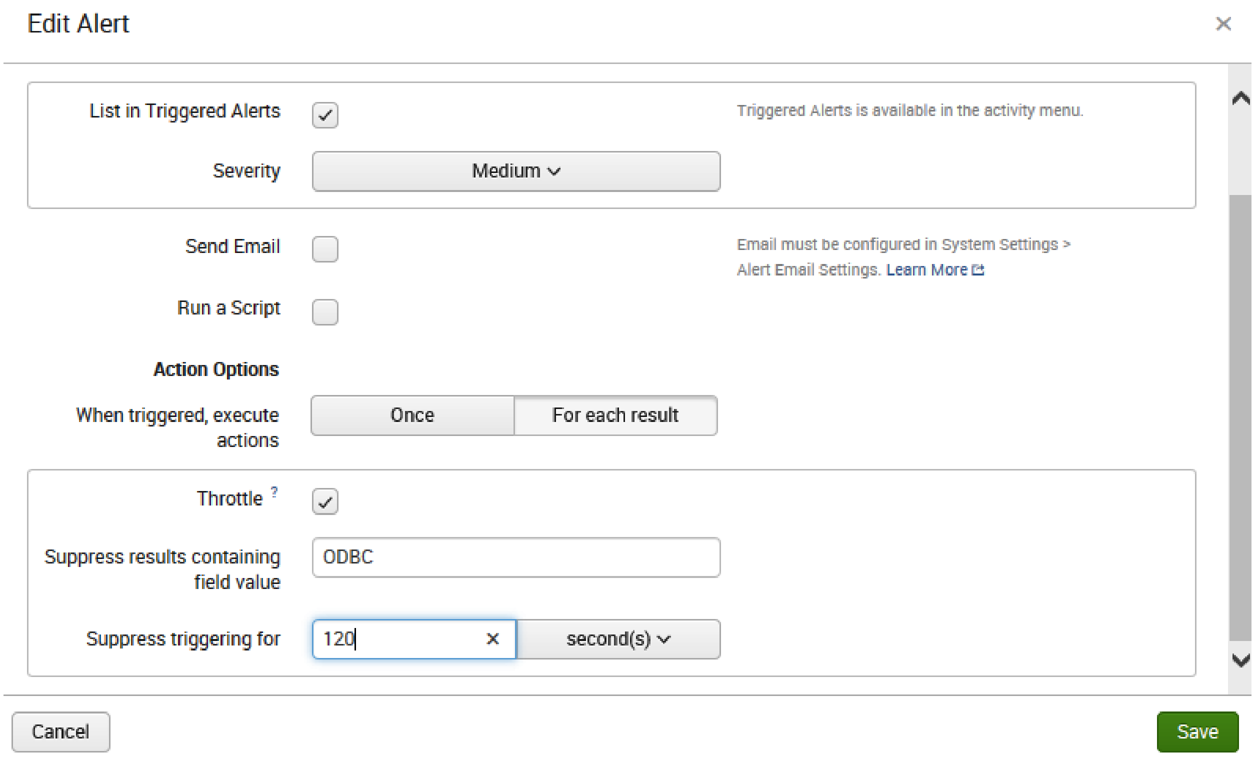


When triggered, execute actions: Once | For each result



Throttle ? ☑

Suppress triggering for: 60 second(s)



Edit Alert

List in Triggered Alerts ☑ Triggered Alerts is available in the activity menu.

Severity: Medium

Send Email □ Email must be configured in System Settings > Alert Email Settings. Learn More

Run a Script □

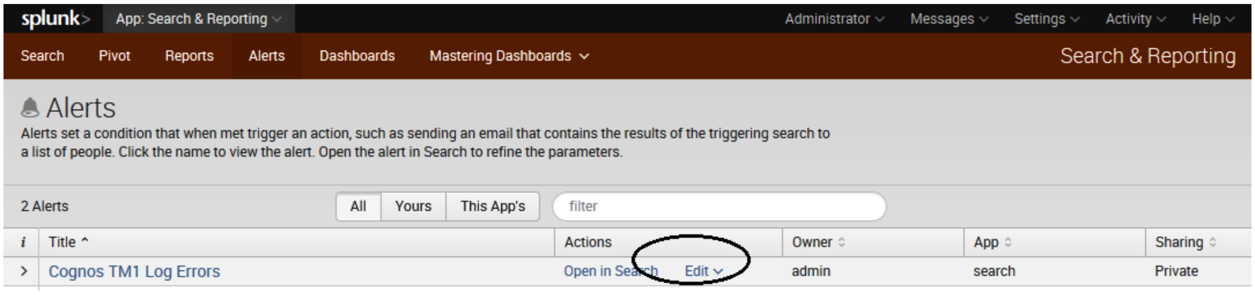
Action Options

When triggered, execute actions: Once | For each result

Throttle ? ☑

Suppress results containing field value: ODBC

Suppress triggering for: 120 second(s)

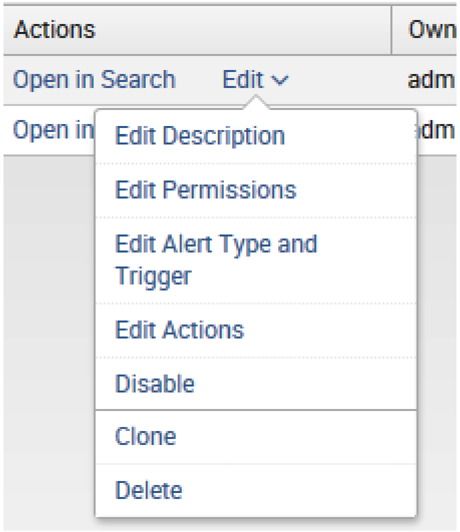


Alerts

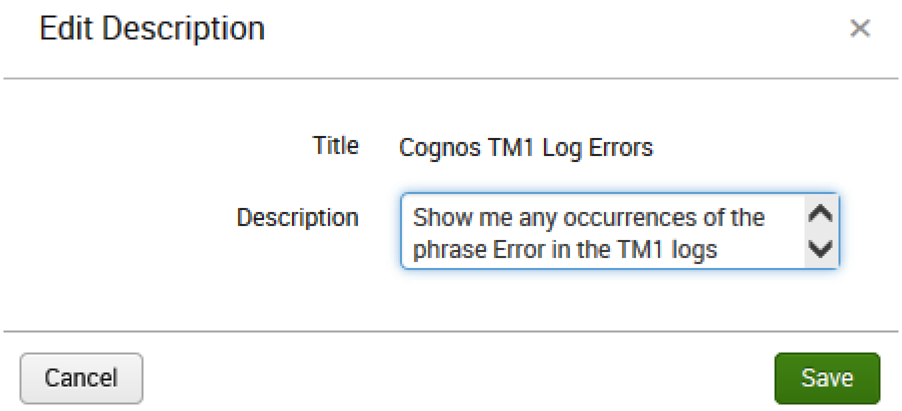
Alerts set a condition that when met trigger an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

2 Alerts

i	Title ^	Actions	Owner	App	Sharing
>	Cognos TM1 Log Errors	Open in Search Edit	admin	search	Private



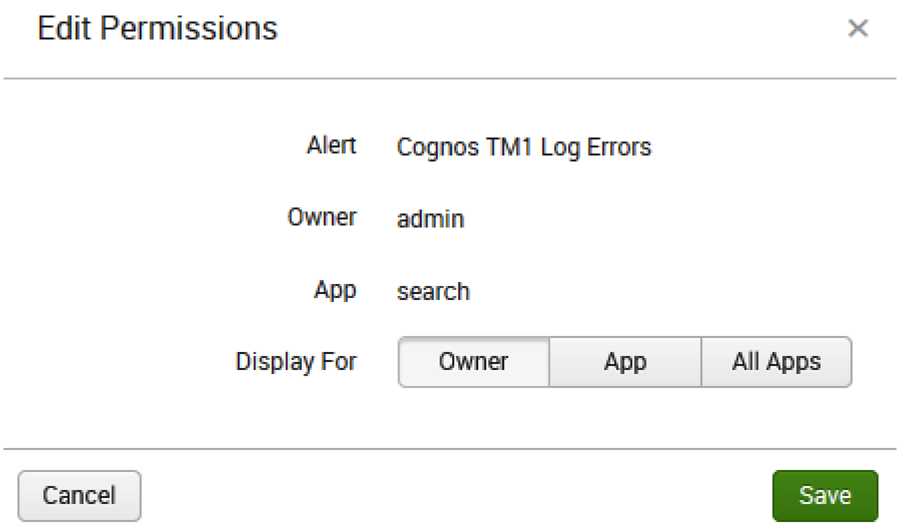
Actions	Own
Open in Search Edit	adm
Open in	adm



Edit Description

Title: Cognos TM1 Log Errors

Description: Show me any occurrences of the phrase Error in the TM1 logs



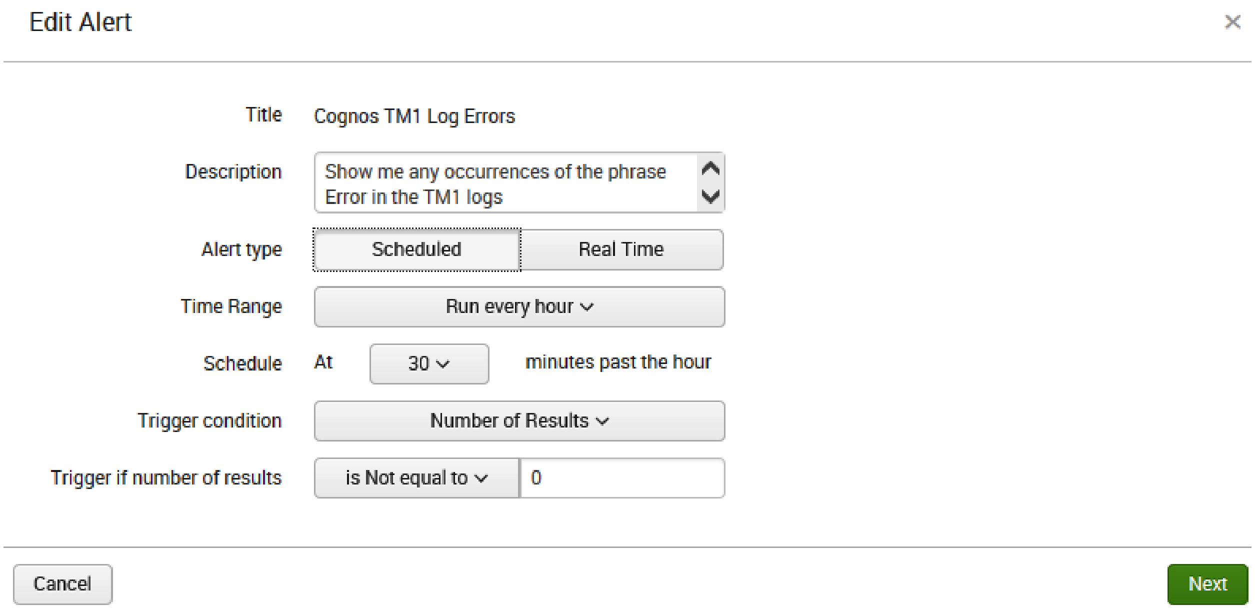
Edit Permissions

Alert: Cognos TM1 Log Errors

Owner: admin

App: search

Display For: Owner | App | All Apps



Edit Alert

Title: Cognos TM1 Log Errors

Description: Show me any occurrences of the phrase Error in the TM1 logs

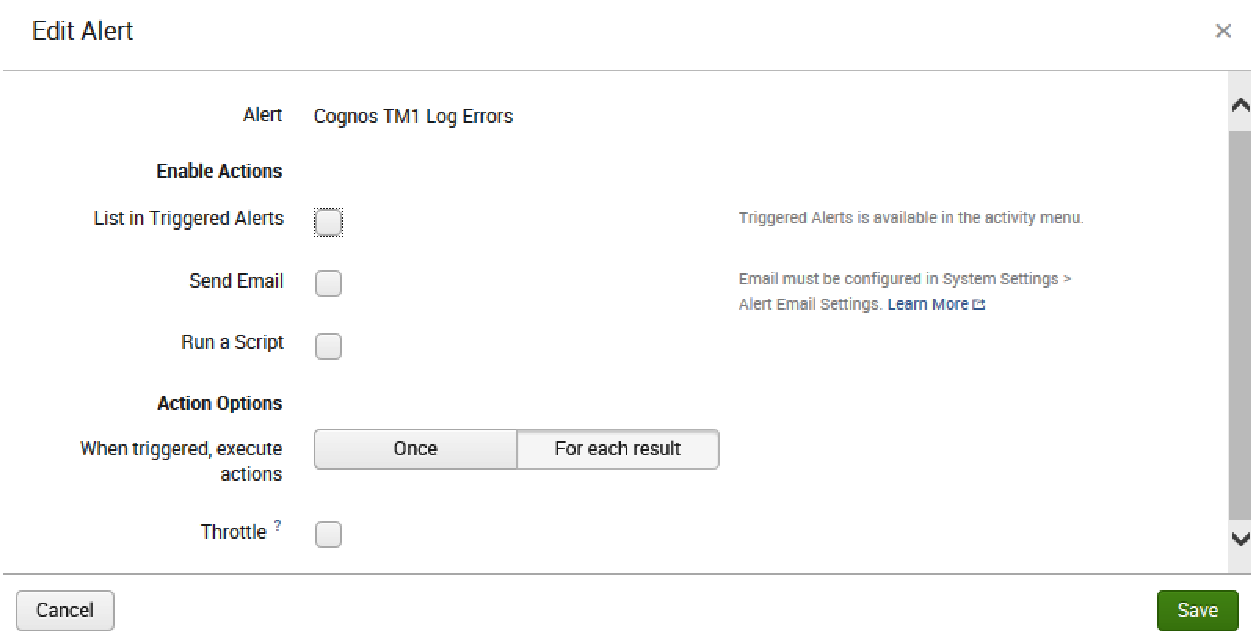
Alert type: Scheduled | Real Time

Time Range: Run every hour

Schedule: At 30 minutes past the hour

Trigger condition: Number of Results

Trigger if number of results: is Not equal to 0



Edit Alert

Alert Cognos TM1 Log Errors

Enable Actions

List in Triggered Alerts □ Triggered Alerts is available in the activity menu.

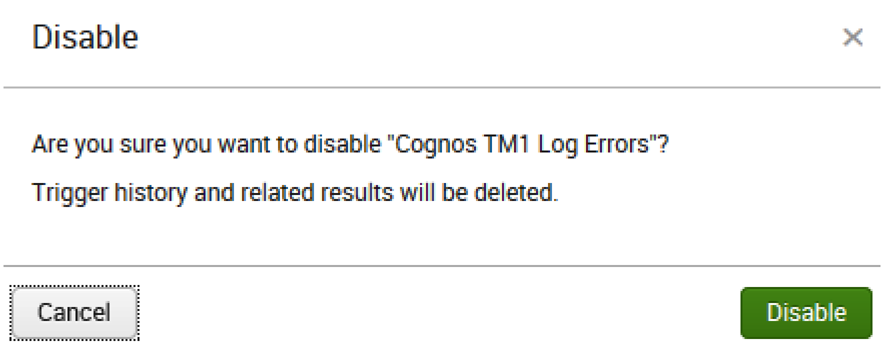
Send Email □ Email must be configured in System Settings > Alert Email Settings. Learn More

Run a Script □

Action Options

When triggered, execute actions: Once | For each result

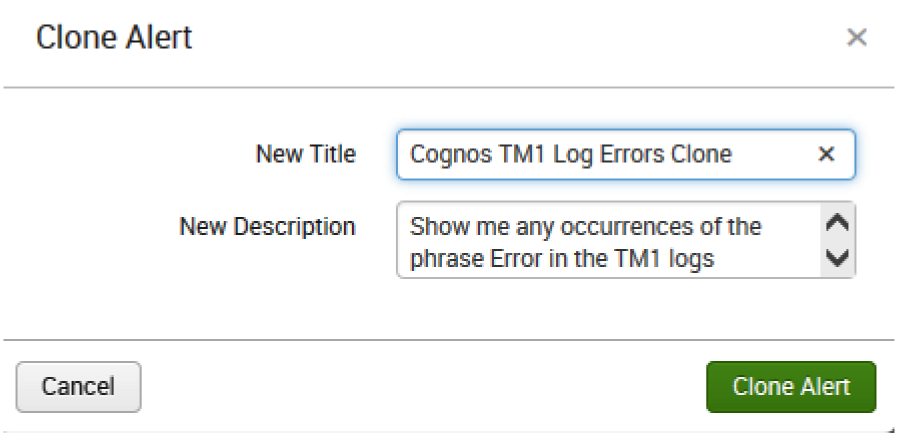
Throttle ? □



Disable

Are you sure you want to disable "Cognos TM1 Log Errors"?

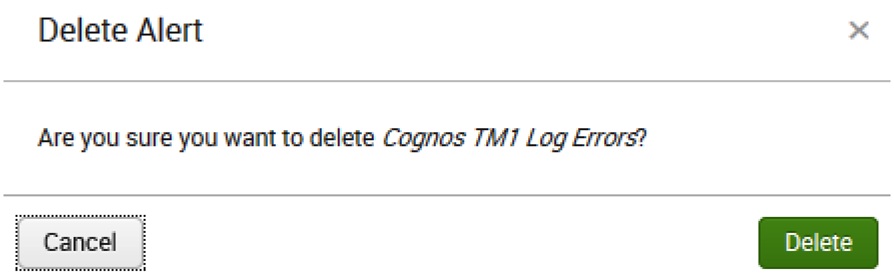
Trigger history and related results will be deleted.



Clone Alert

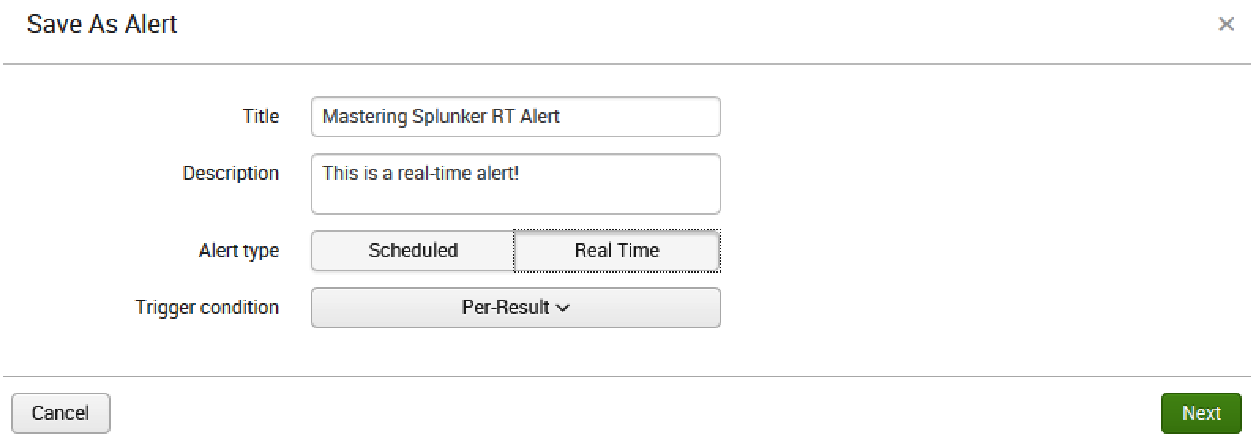
New Title: Cognos TM1 Log Errors Clone

New Description: Show me any occurrences of the phrase Error in the TM1 logs



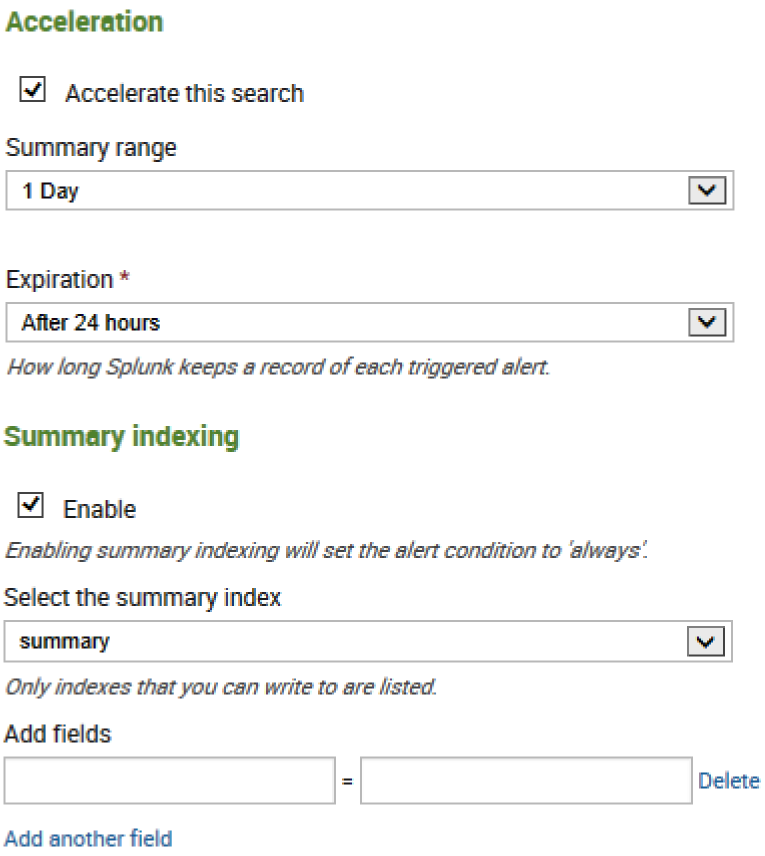
Delete Alert

Are you sure you want to delete *Cognos TM1 Log Errors*?



Save As Alert

Title	Mastering Splunker RT Alert
Description	This is a real-time alert!
Alert type	Scheduled / [✓ Real Time]
Trigger condition	Per-Result



Acceleration

☑ Accelerate this search

Summary range: 1 Day

Expiration *: After 24 hours

How long Splunk keeps a record of each triggered alert.

Summary indexing

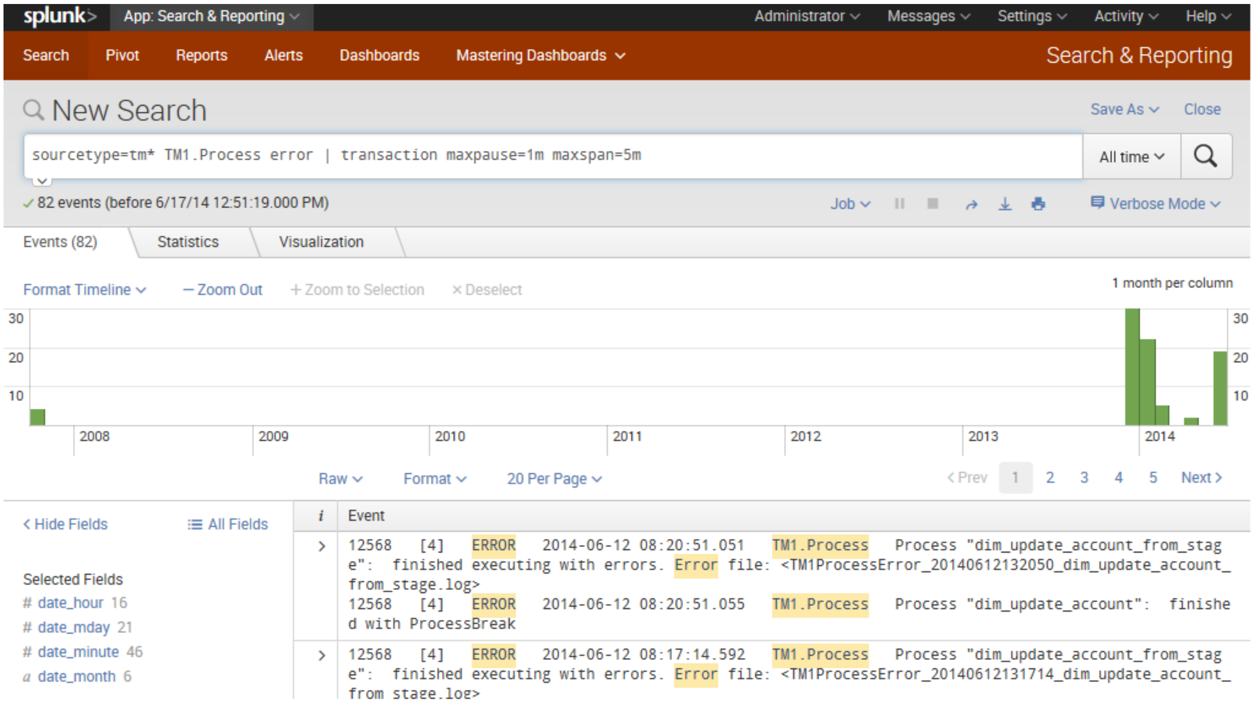
☑ Enable

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

Select the summary index: summary

Only indexes that you can write to are listed.

Add fields

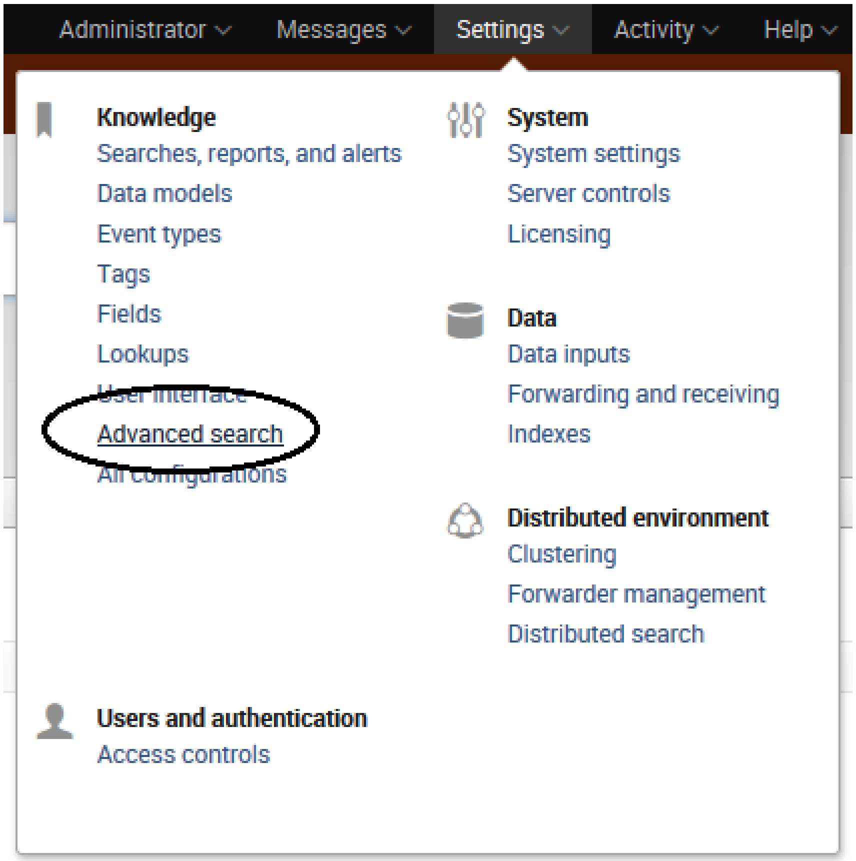


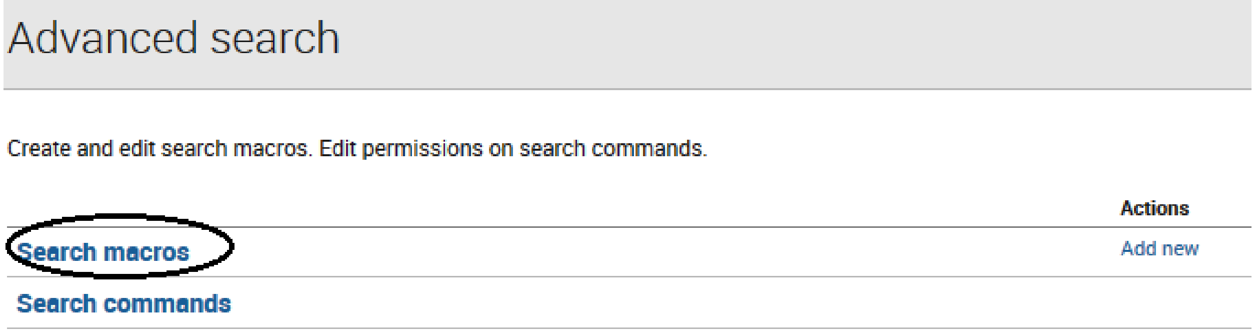
```
sourcetype=tm* TM1.Process error | transaction maxpause=1m maxspan=5m
```

✓ 82 events (before 6/17/14 12:51:19.000 PM)

Selected Fields
- # date_hour 16
- # date_mday 21
- # date_minute 46
- a date_month 6

```
12568   [4]   ERROR   2014-06-12 08:20:51.051   TM1.Process   Process "dim_update_account_from_stag
e":  finished executing with errors. Error file: <TM1ProcessError_20140612132050_dim_update_account_
from_stage.log>
12568   [4]   ERROR   2014-06-12 08:20:51.055   TM1.Process   Process "dim_update_account":  finishe
d with ProcessBreak

12568   [4]   ERROR   2014-06-12 08:17:14.592   TM1.Process   Process "dim_update_account_from_stag
e":  finished executing with errors. Error file: <TM1ProcessError_20140612131714_dim_update_account_
from_stage.log>
```

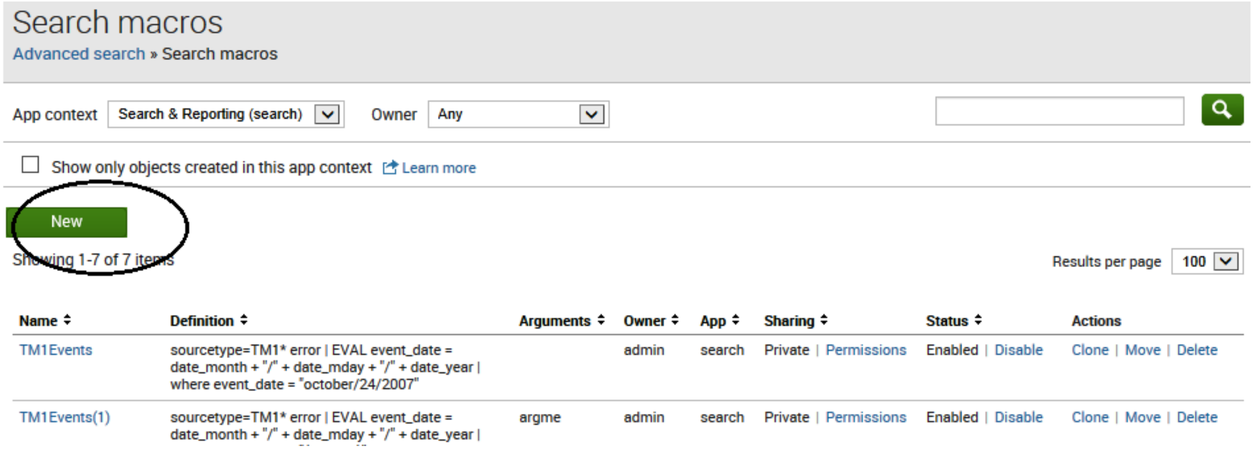




Advanced search

Create and edit search macros. Edit permissions on search commands.

	Actions
Search macros	Add new
Search commands	



Search macros

Advanced search » Search macros

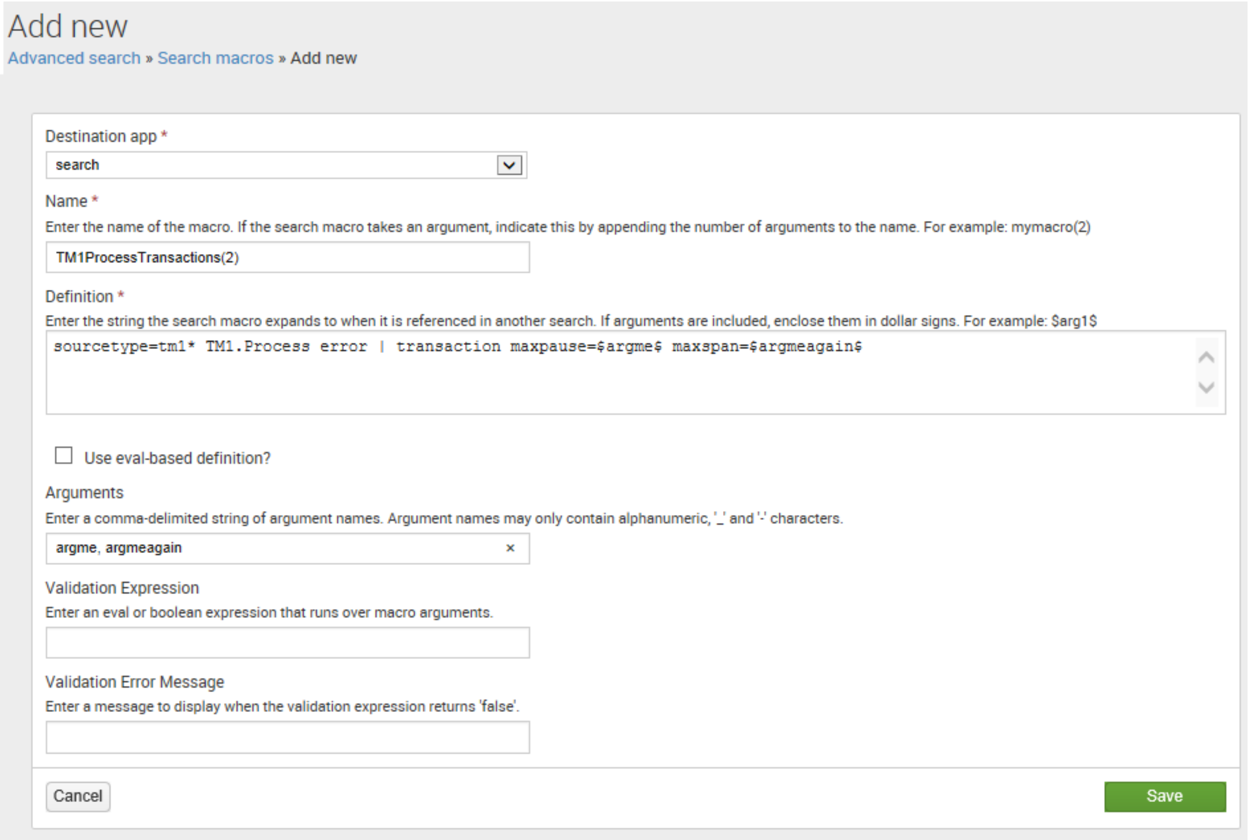
App context: Search & Reporting (search)   Owner: Any

□ Show only objects created in this app context   Learn more

Showing 1-7 of 7 items

Results per page: 100

Name	Definition	Arguments	Owner	App	Sharing	Status	Actions
TM1Events	sourcetype=TM1* error | EVAL event_date = date_month + "/" + date_mday + "/" + date_year | where event_date = "october/24/2007"		admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete
TM1Events(1)	sourcetype=TM1* error | EVAL event_date = date_month + "/" + date_mday + "/" + date_year |	argme	admin	search	Private | Permissions	Enabled | Disable	Clone | Move | Delete



Add new

Advanced search » Search macros » Add new

Destination app *

search

Name *

Enter the name of the macro. If the search macro takes an argument, indicate this by appending the number of arguments to the name. For example: mymacro(2)

TM1ProcessTransactions(2)

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
sourcetype=tm1* TM1.Process error | transaction maxpause=$argme$ maxspan=$argmeagain$
```

□ Use eval-based definition?

Arguments

Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

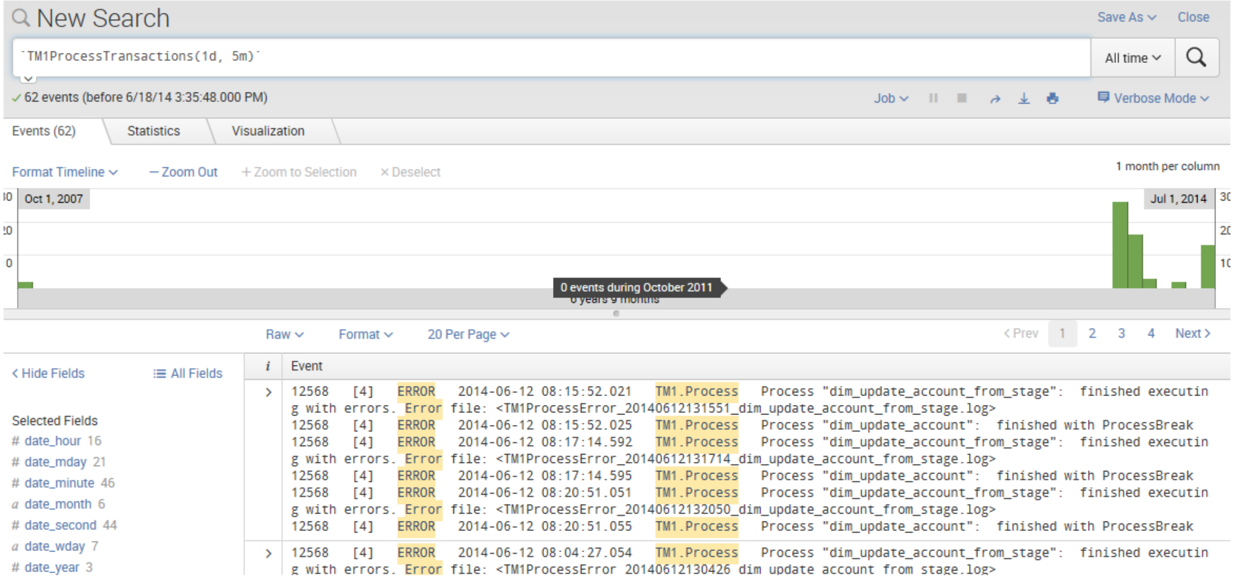
argme, argmeagain

Validation Expression

Enter an eval or boolean expression that runs over macro arguments.

Validation Error Message

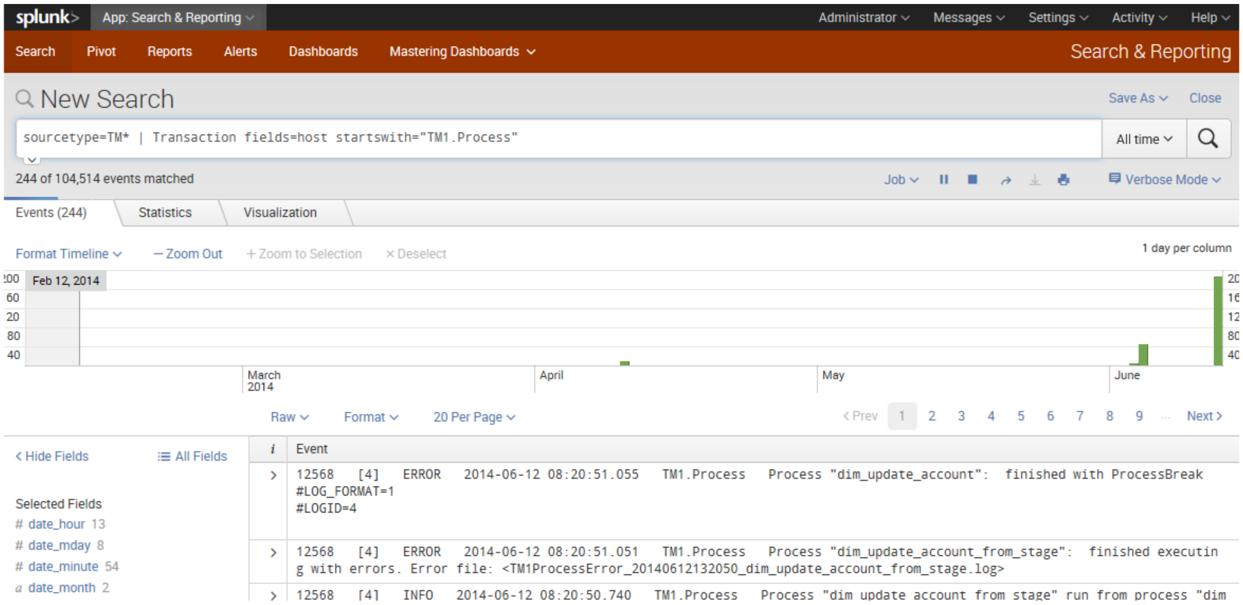
Enter a message to display when the validation expression returns 'false'.



```
`TM1ProcessTransactions(1d, 5m)`
```

✓ 62 events (before 6/18/14 3:35:48.000 PM)

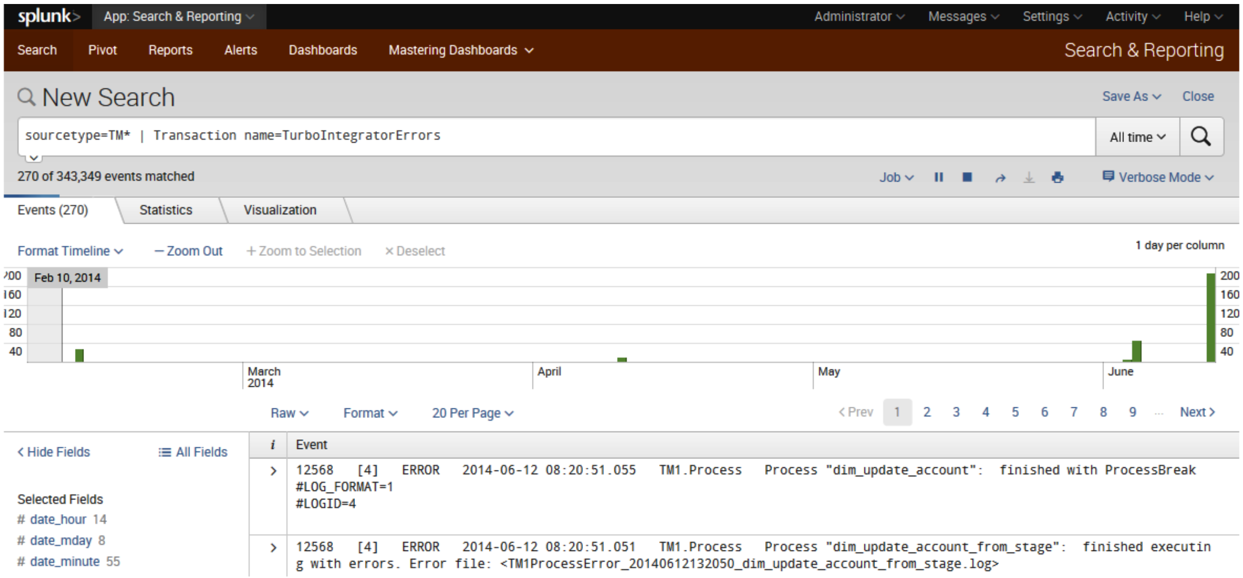
```
12568   [4]   ERROR   2014-06-12 08:15:52.021   TM1.Process   Process "dim_update_account_from_stage":  finished executin
g with errors. Error file: <TM1ProcessError_20140612131551_dim_update_account_from_stage.log>
12568   [4]   ERROR   2014-06-12 08:15:52.025   TM1.Process   Process "dim_update_account":  finished with ProcessBreak
12568   [4]   ERROR   2014-06-12 08:17:14.592   TM1.Process   Process "dim_update_account_from_stage":  finished executin
g with errors. Error file: <TM1ProcessError_20140612131714_dim_update_account_from_stage.log>
12568   [4]   ERROR   2014-06-12 08:17:14.595   TM1.Process   Process "dim_update_account":  finished with ProcessBreak
12568   [4]   ERROR   2014-06-12 08:20:51.051   TM1.Process   Process "dim_update_account_from_stage":  finished executin
g with errors. Error file: <TM1ProcessError_20140612132050_dim_update_account_from_stage.log>
12568   [4]   ERROR   2014-06-12 08:20:51.055   TM1.Process   Process "dim_update_account":  finished with ProcessBreak

12568   [4]   ERROR   2014-06-12 08:04:27.054   TM1.Process   Process "dim_update_account_from_stage":  finished executin
g with errors. Error file: <TM1ProcessError 20140612130426 dim update account from stage.log>
```



```
sourcetype=TM* | Transaction fields=host startswith="TM1.Process"
```

244 of 104,514 events matched

```
12568   [4]   ERROR   2014-06-12 08:20:51.055   TM1.Process   Process "dim_update_account":  finished with ProcessBreak
#LOG_FORMAT=1
#LOGID=4

12568   [4]   ERROR   2014-06-12 08:20:51.051   TM1.Process   Process "dim_update_account_from_stage":  finished executin
g with errors. Error file: <TM1ProcessError_20140612132050_dim_update_account_from_stage.log>

12568   [4]   INFO   2014-06-12 08:20:50.740   TM1.Process   Process "dim update account from stage" run from process "dim
```

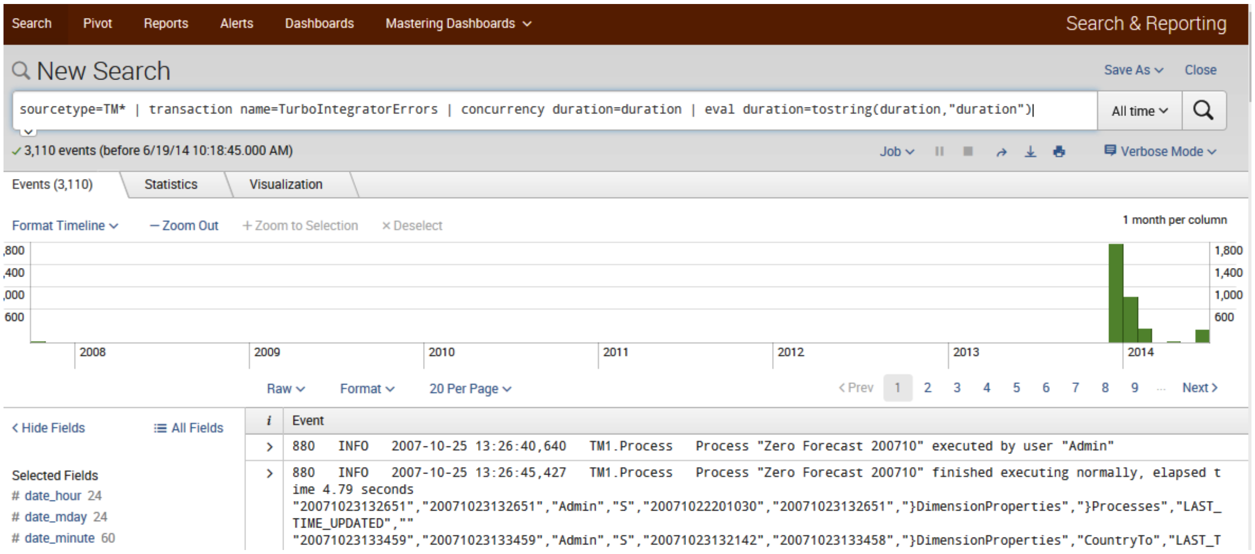


```
sourcetype=TM* | Transaction name=TurboIntegratorErrors
```

270 of 343,349 events matched

Selected Fields
- # date_hour 14
- # date_mday 8
- # date_minute 55

```
12568   [4]   ERROR   2014-06-12 08:20:51.055   TM1.Process   Process "dim_update_account":  finished with ProcessBreak
#LOG_FORMAT=1
#LOGID=4

12568   [4]   ERROR   2014-06-12 08:20:51.051   TM1.Process   Process "dim_update_account_from_stage":  finished executin
g with errors. Error file: <TM1ProcessError_20140612132050_dim_update_account_from_stage.log>
```

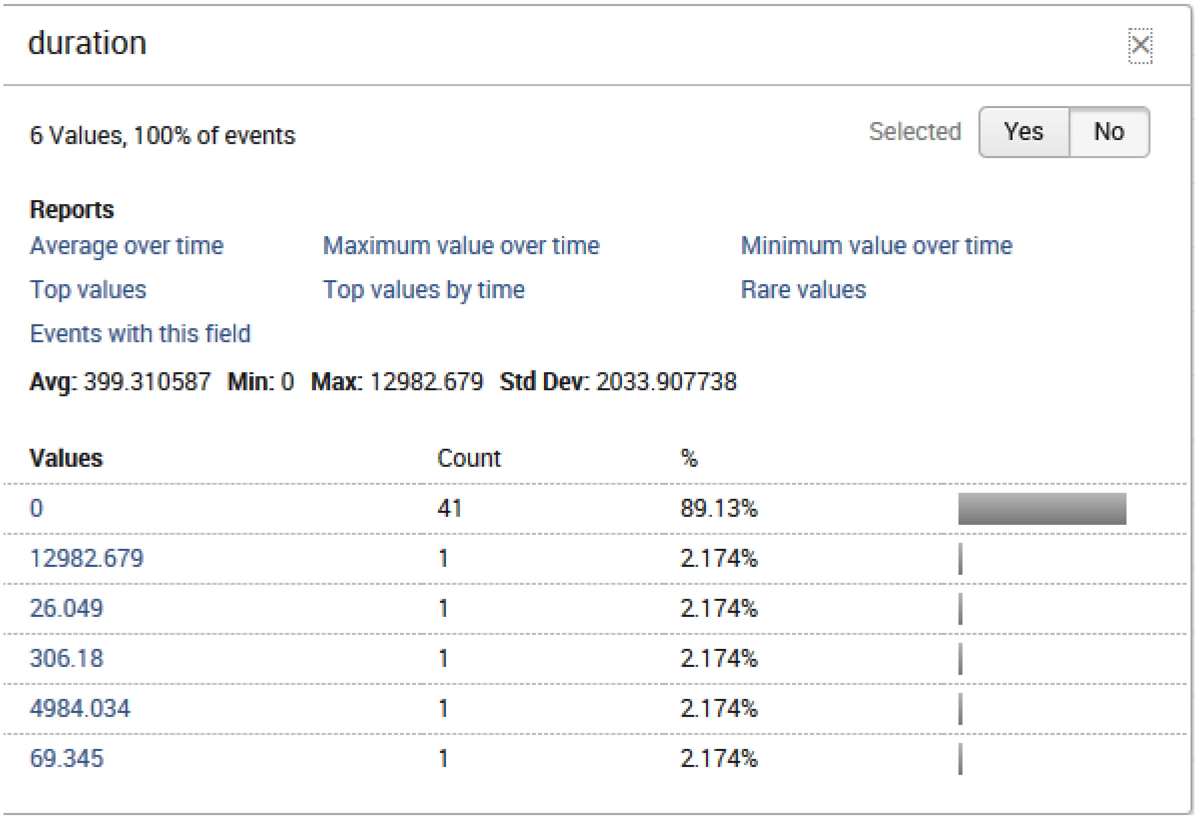


```
sourcetype=TM* | transaction name=TurboIntegratorErrors | concurrency duration=duration | eval duration=tostring(duration,"duration")
```

✓ 3,110 events (before 6/19/14 10:18:45.000 AM)

Selected Fields
- # date_hour 24
- # date_mday 24
- # date_minute 60

```
880   INFO   2007-10-25 13:26:40,640   TM1.Process   Process "Zero Forecast 200710" executed by user "Admin"

880   INFO   2007-10-25 13:26:45,427   TM1.Process   Process "Zero Forecast 200710" finished executing normally, elapsed t
ime 4.79 seconds
"20071023132651","20071023132651","Admin","S","20071022201030","20071023132651","}DimensionProperties","}Processes","LAST_
TIME_UPDATED",""
"20071023133459","20071023133459","Admin","S","20071023132142","20071023133458","}DimensionProperties","CountryTo","LAST_T
```



duration

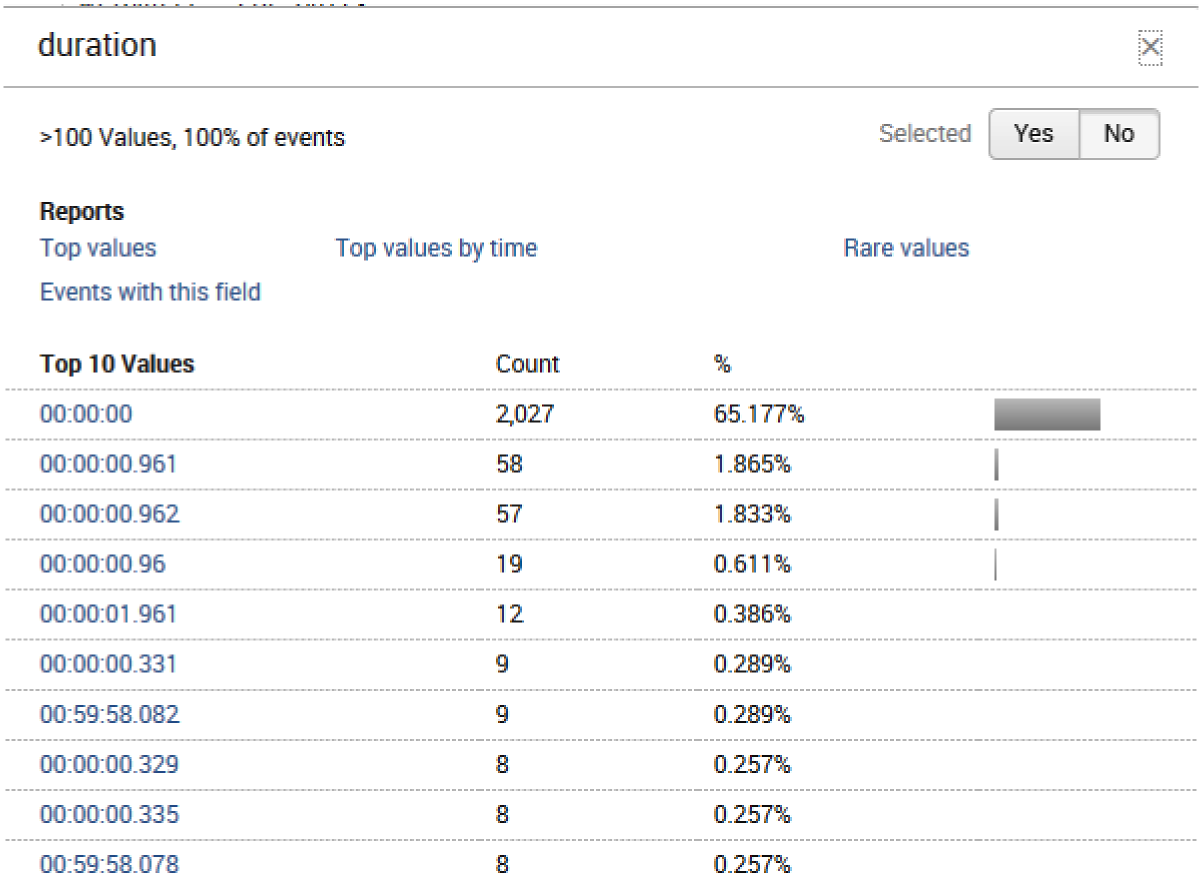
6 Values, 100% of events

Reports

Average over time
Maximum value over time
Minimum value over time
Top values
Top values by time
Rare values
Events with this field

Avg: 399.310587 **Min:** 0 **Max:** 12982.679 **Std Dev:** 2033.907738

Values	Count	%
0	41	89.13%
12982.679	1	2.174%
26.049	1	2.174%
306.18	1	2.174%
4984.034	1	2.174%
69.345	1	2.174%



duration

>100 Values, 100% of events

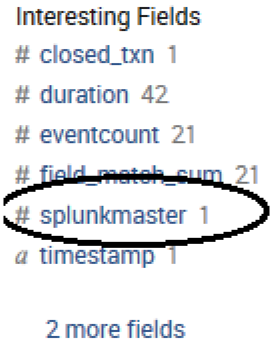
Selected [✓ Yes] No

Reports

Top values   Top values by time   Rare values

Events with this field

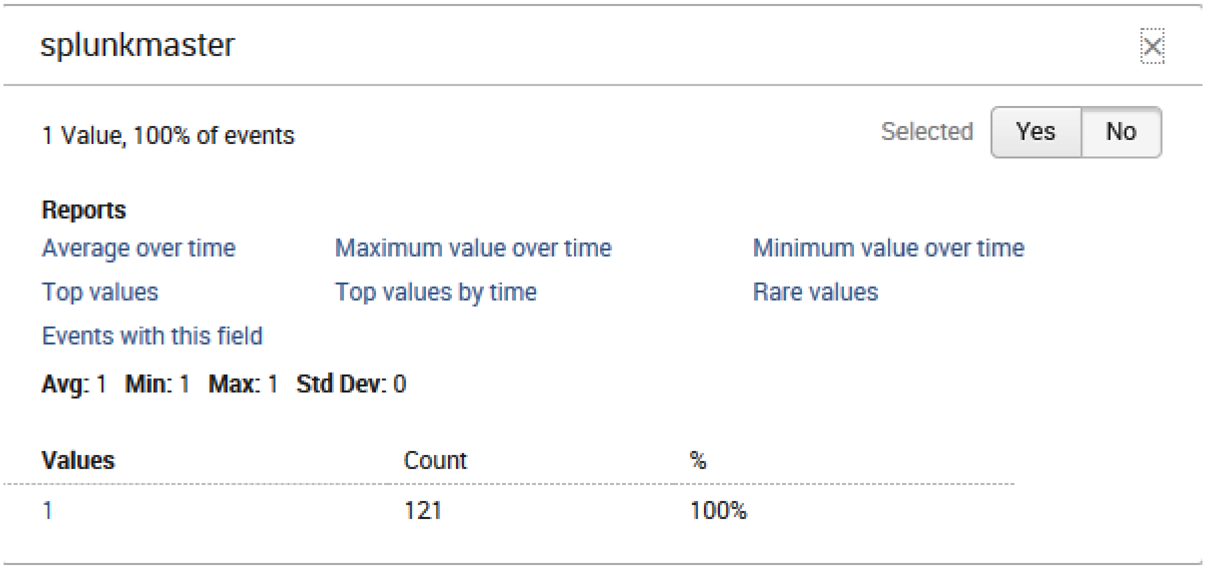
Top 10 Values	Count	%
00:00:00	2,027	65.177%
00:00:00.961	58	1.865%
00:00:00.962	57	1.833%
00:00:00.96	19	0.611%
00:00:01.961	12	0.386%
00:00:00.331	9	0.289%
00:59:58.082	9	0.289%
00:00:00.329	8	0.257%
00:00:00.335	8	0.257%
00:59:58.078	8	0.257%



Interesting Fields

#	closed_txn	1
#	duration	42
#	eventcount	21
#	field_match_sum	21
#	splunkmaster	1
a	timestamp	1

2 more fields



splunkmaster

1 Value, 100% of events

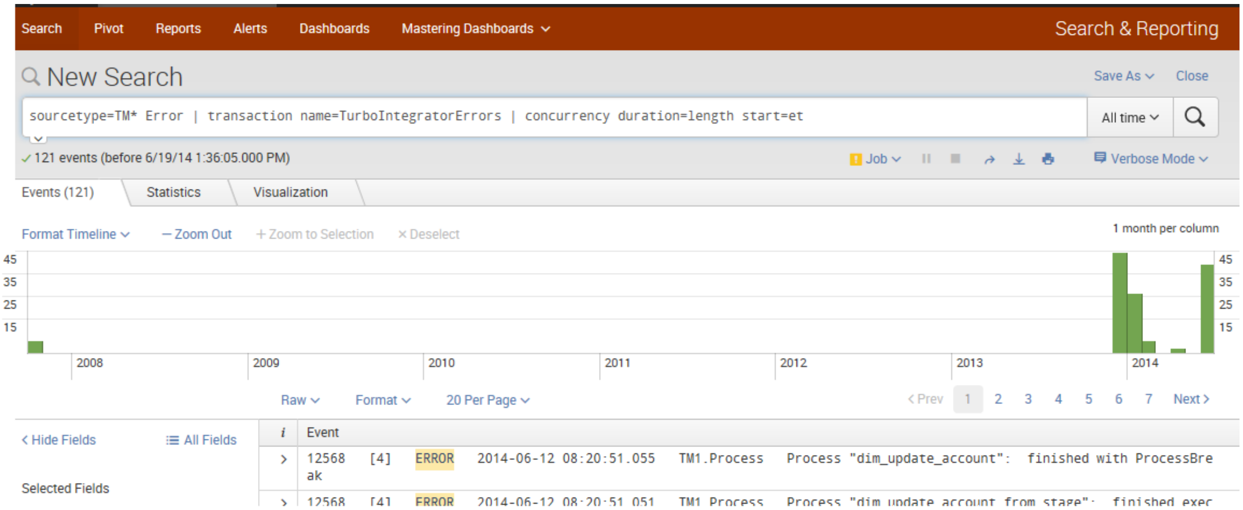
Selected Yes No

Reports

Average over time | Maximum value over time | Minimum value over time
Top values | Top values by time | Rare values
Events with this field

Avg: 1 **Min:** 1 **Max:** 1 **Std Dev:** 0

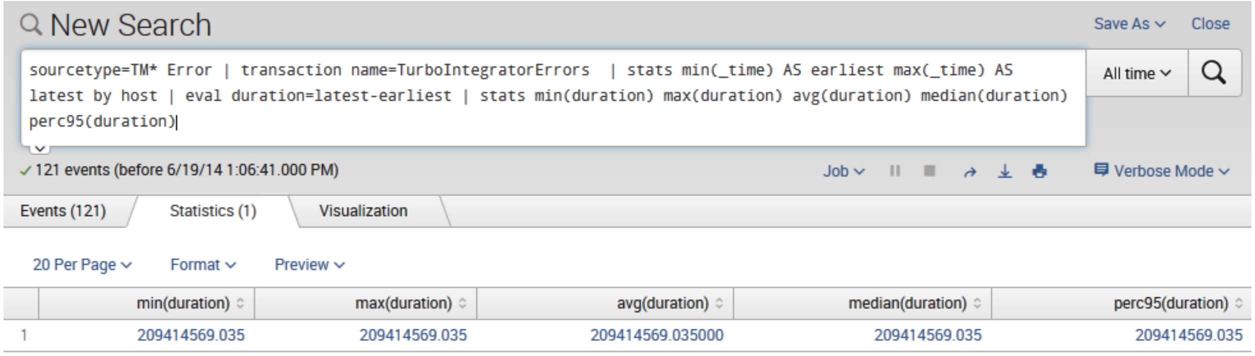
Values	Count	%
1	121	100%



```
sourcetype=TM* Error | transaction name=TurboIntegratorErrors | concurrency duration=length start=et
```

✓ 121 events (before 6/19/14 1:36:05.000 PM)

```
12568   [4]   ERROR   2014-06-12 08:20:51.055   TM1.Process   Process "dim_update_account":  finished with ProcessBre
ak
12568   [4]   ERROR   2014-06-12 08:20:51.051   TM1.Process   Process "dim_update_account_from_stage":  finished exec
```

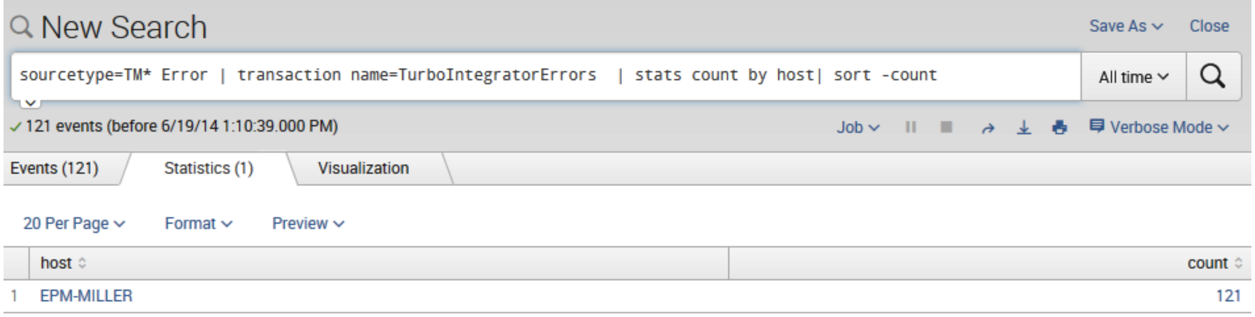


New Search

```
sourcetype=TM* Error | transaction name=TurboIntegratorErrors  | stats min(_time) AS earliest max(_time) AS
latest by host | eval duration=latest-earliest | stats min(duration) max(duration) avg(duration) median(duration)
perc95(duration)
```

✓ 121 events (before 6/19/14 1:06:41.000 PM)

	min(duration)	max(duration)	avg(duration)	median(duration)	perc95(duration)
1	209414569.035	209414569.035	209414569.035000	209414569.035	209414569.035



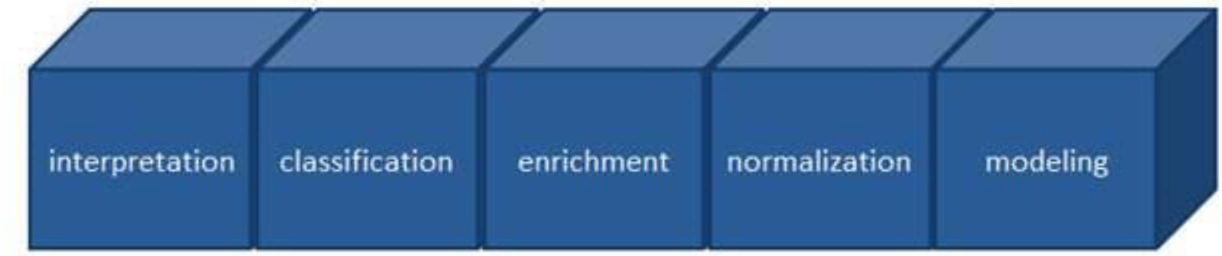
New Search

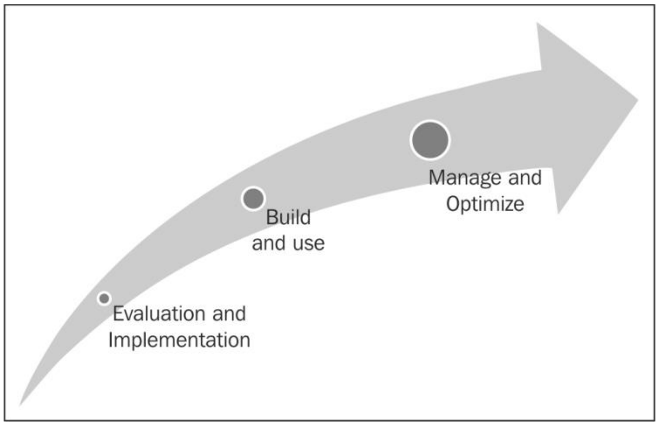
```
sourcetype=TM* Error | transaction name=TurboIntegratorErrors  | stats count by host| sort -count
```

✓ 121 events (before 6/19/14 1:10:39.000 PM)

	host	count
1	EPM-MILLER	121

Chapter 10, *Splunk – Meet the Enterprise*


interpretation
classification
enrichment
normalization
modeling


Manage and Optimize
Build and use
Evaluation and Implementation