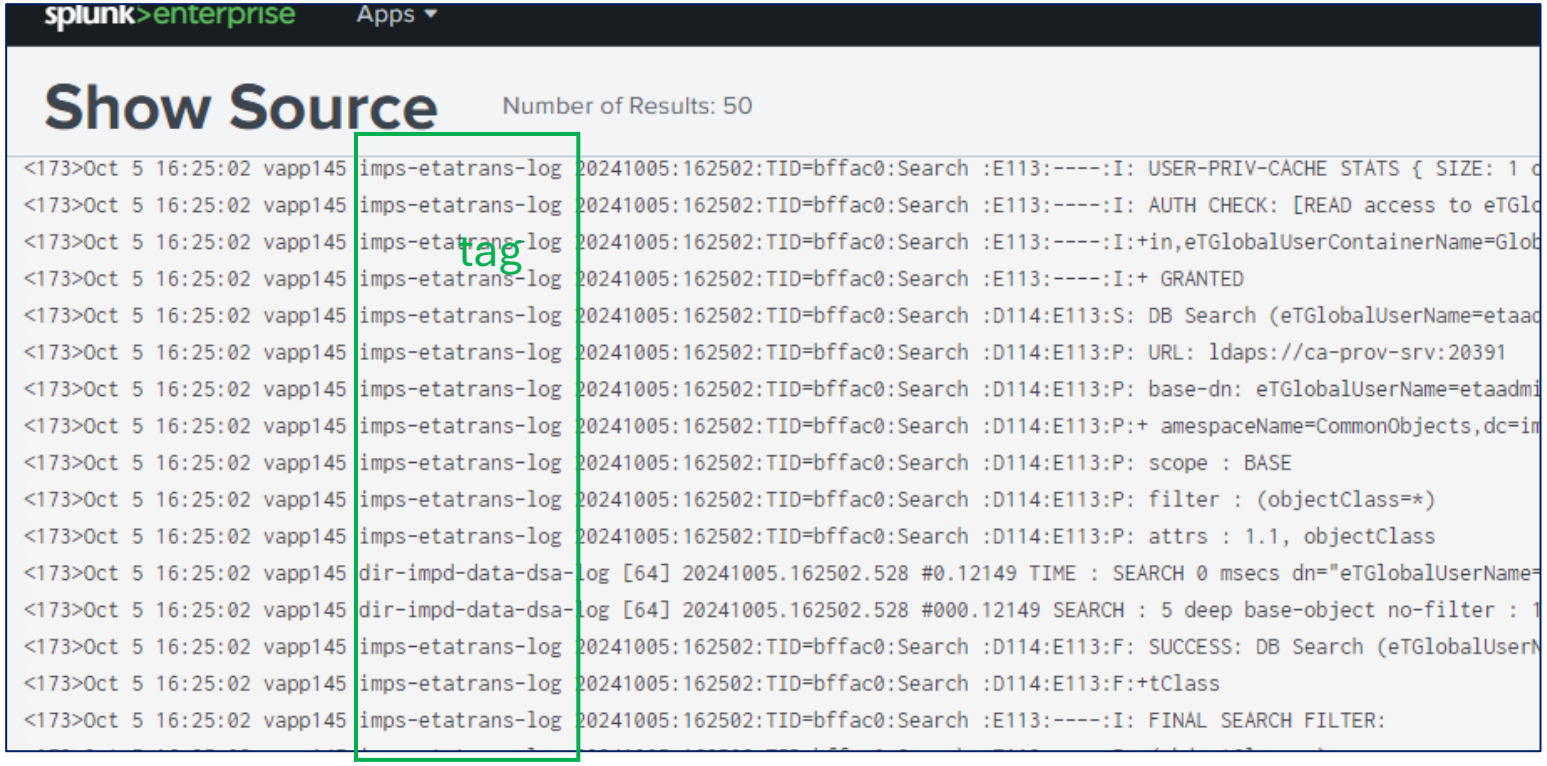
Syslog to Splunk for vApp

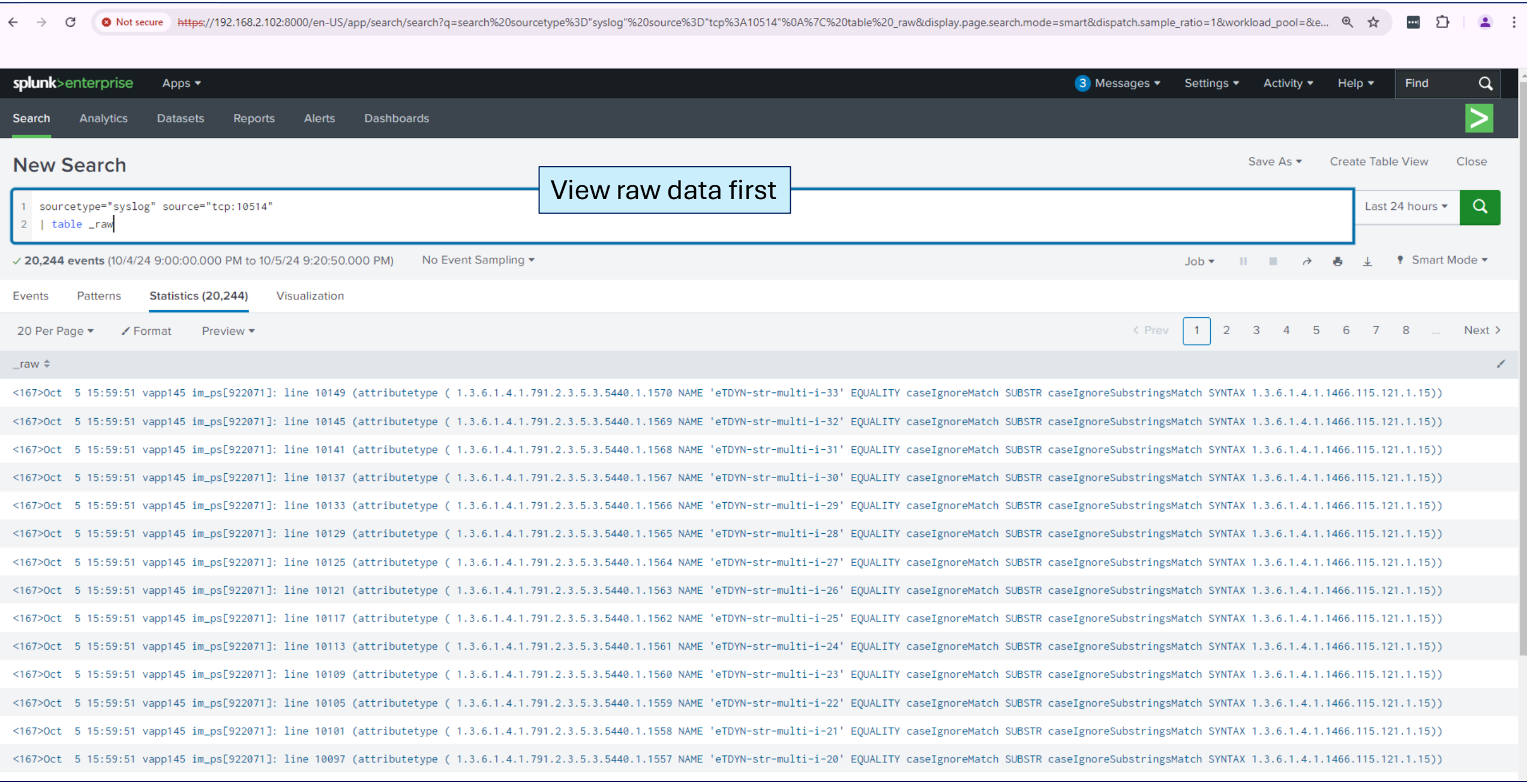
Update /etc/rsyslog.d/rsyslog-custom.conf & define "tag" strings (with hyphens) to be recognized within Splunk searches

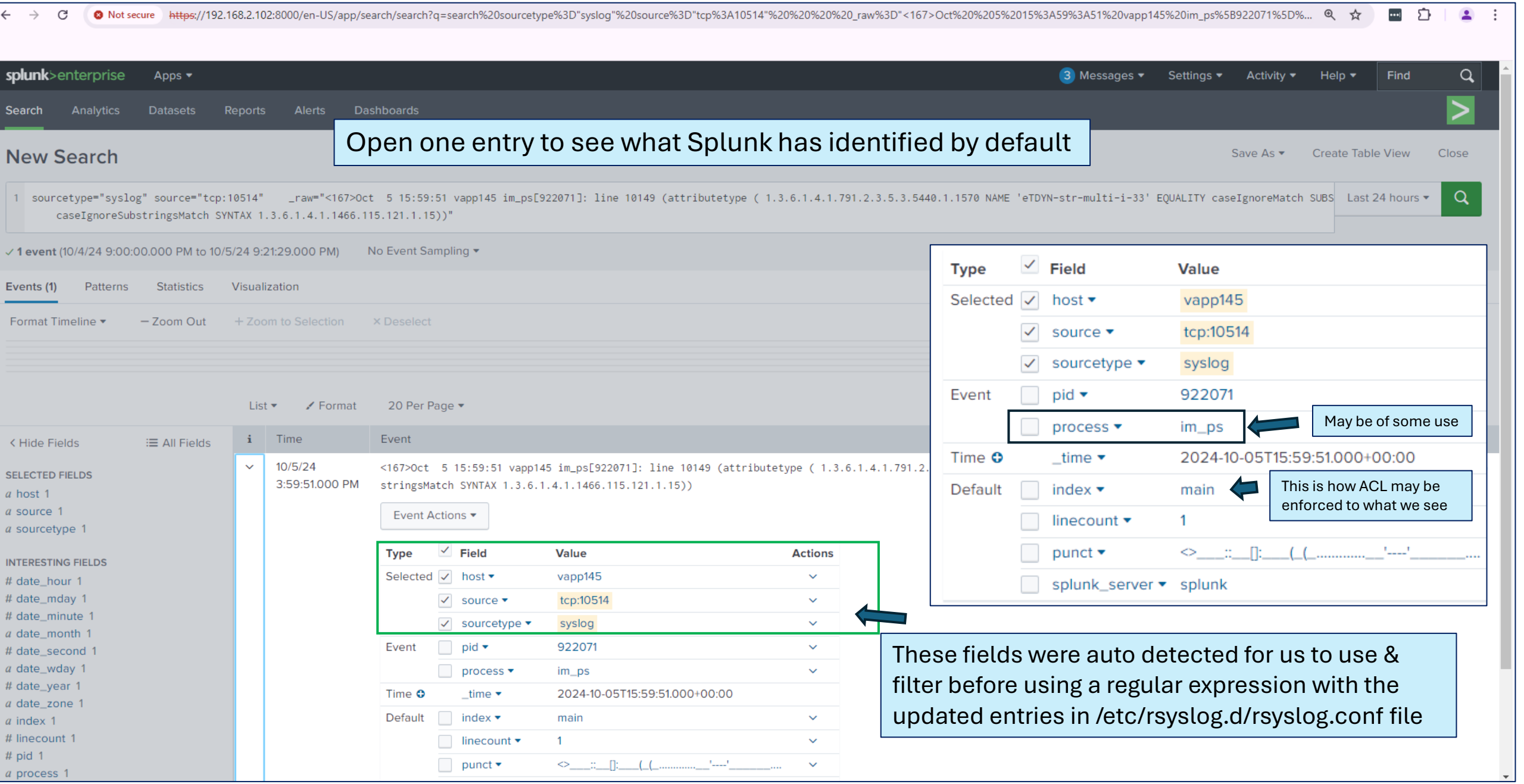
```
    Tag="vapp-main-log"
    Tag="vapp-deployment-log"
    Tag="im-wildfly-server-log"
    Tag="ip-wildfly-server-log"
#   Tag="ig-wildfly-server-log"
    Tag="jcs-daily-vapp-server-log"
    Tag="imps-etatrans-log"
    Tag="imps-im-ps-log"
    Tag="dir-idm-userstore-router-log"
    Tag="dir-idm-userstore-router-trace-log"
    Tag="dir-idm-userstore-log"
    Tag="dir-idm-userstore-trace-log"
    Tag="dir-imps-router-log"
    Tag="dir-imps-router-trace-log"
    Tag="dir-impd-data-dsa-log"
    Tag="dir-impd-data-dsa-trace-log"
```

tag



To assist with Splunk Queries, we may wish to add more tags to exclude noise


Not secure
https://192.168.2.102:8000/en-US/app/search/search?q=search%20sourcetype%3D"syslog"%20source%3D"tcp%3A10514"%0A%7C%20table%20_raw&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&e...
splunk>enterprise
Apps
3 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table View
Close
View raw data first
1 sourcetype="syslog" source="tcp:10514"
2 | table _raw
Last 24 hours
✓ 20,244 events (10/4/24 9:00:00.000 PM to 10/5/24 9:20:50.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (20,244)
Visualization
20 Per Page
Format
Preview
Prev
1
2
3
4
5
6
7
8
Next
_raw
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10149 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1570 NAME 'eTDYN-str-multi-i-33' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10145 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1569 NAME 'eTDYN-str-multi-i-32' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10141 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1568 NAME 'eTDYN-str-multi-i-31' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10137 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1567 NAME 'eTDYN-str-multi-i-30' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10133 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1566 NAME 'eTDYN-str-multi-i-29' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10129 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1565 NAME 'eTDYN-str-multi-i-28' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10125 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1564 NAME 'eTDYN-str-multi-i-27' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10121 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1563 NAME 'eTDYN-str-multi-i-26' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10117 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1562 NAME 'eTDYN-str-multi-i-25' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10113 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1561 NAME 'eTDYN-str-multi-i-24' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10109 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1560 NAME 'eTDYN-str-multi-i-23' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10105 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1559 NAME 'eTDYN-str-multi-i-22' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10101 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1558 NAME 'eTDYN-str-multi-i-21' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10097 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1557 NAME 'eTDYN-str-multi-i-20' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))


Not secure https://192.168.2.102:8000/en-US/app/search/search?q=search%20sourcetype%3D"syslog"%20source%3D"tcp%3A10514"%20%20%20%20_raw%3D"<167>Oct%20%205%2015%3A59%3A51%20vapp145%20im_ps%5B922071%5D%...
splunk>enterprise
Apps
3 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Open one entry to see what Splunk has identified by default
New Search
Save As
Create Table View
Close
1 sourcetype="syslog" source="tcp:10514" _raw="<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10149 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1570 NAME 'eTDYN-str-multi-i-33' EQUALITY caseIgnoreMatch SUBS
caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))"
Last 24 hours
✓ 1 event (10/4/24 9:00:00.000 PM to 10/5/24 9:21:29.000 PM)
No Event Sampling
Events (1)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
a date_month 1
date_second 1
a date_wday 1
date_year 1
a date_zone 1
a index 1
linecount 1
pid 1
a process 1
Time
Event
10/5/24
3:59:51.000 PM
<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10149 (attributetype (1.3.6.1.4.1.791.2.
stringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))
Event Actions
Type Field Value Actions
Selected host vapp145
source tcp:10514
sourcetype syslog
Event pid 922071
process im_ps
Time _time 2024-10-05T15:59:51.000+00:00
Default index main
linecount 1
punct
Type Field Value
Selected host vapp145
source tcp:10514
sourcetype syslog
Event pid 922071
process im_ps
May be of some use
Time _time 2024-10-05T15:59:51.000+00:00
Default index main
This is how ACL may be enforced to what we see
linecount 1
punct
splunk_server splunk
These fields were auto detected for us to use & filter before using a regular expression with the updated entries in /etc/rsyslog.d/rsyslog.conf file

Not secure https://192.168.2.102:8000/en-US/app/search/search?q=search%20sourcetype%3D"syslog"%20source%3D"tcp%3A10514"%20host%3D"vapp145"%20%20%0A%7C%20table%20_raw&display.page.search.mode=smart&dispatch.sam...

splunk>enterprise Apps ▾ 3 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards

New Search

```
1 sourcetype="syslog" source="tcp:10514" host="vapp145"
2 | table _raw
```

Save As ▾ Create Table View Close

Last 24 hours ▾

✓ **20,376 events** (10/4/24 9:00:00.000 PM to 10/5/24 9:22:24.000 PM) No Event Sampling ▾

Job ▾ Smart Mode ▾

View raw data first with host entry
- Note that the Statistic number is lower.

Events Patterns **Statistics (20,376)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

_raw

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10149 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1570 NAME 'eTDYN-str-multi-i-33' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10145 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1569 NAME 'eTDYN-str-multi-i-32' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10141 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1568 NAME 'eTDYN-str-multi-i-31' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10137 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1567 NAME 'eTDYN-str-multi-i-30' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10133 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1566 NAME 'eTDYN-str-multi-i-29' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10129 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1565 NAME 'eTDYN-str-multi-i-28' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10125 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1564 NAME 'eTDYN-str-multi-i-27' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10121 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1563 NAME 'eTDYN-str-multi-i-26' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10117 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1562 NAME 'eTDYN-str-multi-i-25' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10113 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1561 NAME 'eTDYN-str-multi-i-24' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10109 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1560 NAME 'eTDYN-str-multi-i-23' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10105 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1559 NAME 'eTDYN-str-multi-i-22' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10101 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1558 NAME 'eTDYN-str-multi-i-21' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10097 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1557 NAME 'eTDYN-str-multi-i-20' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

<167>Oct 5 15:59:51 vapp145 im_ps[922071]: line 10093 (attributetype (1.3.6.1.4.1.791.2.3.5.3.5440.1.1556 NAME 'eTDYN-str-multi-i-19' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15))

Not secure https://192.168.2.102:8000/en-US/app/search/search?q=search%20index%3Dmain%20sourcetype%3D"syslog"%20source%3D"tcp%3A10514"%20host%3D"vapp145"%20imps_etatrans_log%0A%7C%20rex%20field%3D_raw%20"%5E(...

```
index=main sourcetype="syslog" source="tcp:10514" host="vapp145" imps_etatrans_log
| rex field=_raw
"^(<(?<priority>\d+)>)?\s*(?<timestamp>\w{3}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+(?<host>\S+)\s+(?<syslogtag>\S+)\s+(?<imps_time>\d{8}:\d{6}):TID=(?<tid>\w+):(?<action>\S+)\s+:(?<status>[^\[]+)"
| transaction tid maxspan=5m
| table timestamp host syslogtag imps_time tid action status duration eventcount
```

splunk>enterprise Apps ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports

New Search

Save As ▾ Create Table View Close

```
1 index=main sourcetype="syslog" source="tcp:10514" host="vapp145" imps_etatrans_log
2 | rex field=_raw "^(<(?<priority>\d+)>)?\s*(?<timestamp>\w{3}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+(?<host>\S+)\s+(?<syslogtag>\S+)\s+(?<imps_time>\d{8}:\d{6}):TID=(?<tid>\w+):(?<action>\S+)\s+:(?<status>[^\[]+)"
3 | transaction tid maxspan=5m
4 | table timestamp host syslogtag imps_time tid action status duration eventcount
```

All time ▾

✓ **67 events** (before 10/5/24 9:46:00.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (67)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 Next >

timestamp	host	syslogtag	imps_time	tid	action	status	duration	eventcount
Oct 5 15:53:03 Oct 5 15:54:06	vapp145	imps_etatrans_log	20241005:155303 20241005:155406	e14ac0	LDAP	----:----:*: IDLE ----:----:*: CONPOOL 0x24f55750 ----:----:*: CONPOOL 0x251d27e0 ----:----:*: ldaps://192.168.2.251:20411. Connecting (busy=0, waiters=0, connecting=1) ----:----:*: ldaps://192.168.2.251:20411. Failed to connect: RC=LDAP_TIMEOUT (0x55) Retry=0 ----:----:*:+ ----:----:*:+ldaps://ca-prov-srv:20391;eTDSAContainerName=DSAs]	63	9
Oct 5 15:50:18	vapp145	imps_etatrans_log	20241005:155018	9ffac0	Unbind	E636:----:F: SUCCESS: External Unbind (eTGlobalUserName=etaadmin) E636:----:P: dn: eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamesp E636:----:P:+ aceName=CommonObjects,dc=im E636:----:S: ========== E636:----:S: External Unbind (eTGlobalUserName=etaadmin) Requested by User etaadmin - TenantNo E636:----:S:+tSet	0	6
Oct 5 15:50:18	vapp145	imps_etatrans_log	20241005:155018	5ffac0	Unbind	E635:----:F: SUCCESS: External Unbind (eTGlobalUserName=etaadmin) E635:----:P: dn: eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamesp E635:----:P:+ aceName=CommonObjects,dc=im E635:----:S: ========== E635:----:S: External Unbind (eTGlobalUserName=etaadmin) Requested by User etaadmin - TenantNo E635:----:S:+tSet	0	6
Oct 5 15:50:02	vapp145	imps_etatrans_log	20241005:155002	1faac0	Search	D634:E633:F: SUCCESS: DB Search (eTGlobalUserName=etaadmin), entry-count: 1, attributes: objec	300	56

Dashboards | Splunk 9.3.1

Not secure https://192.168.2.102:8000/en-US/app/search/dashboards

splunk>enterprise Apps

3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Dashboards

Dashboards include searches, visualizations, and input controls that capture and present avail

Create New Dashboard

Latest Resources

Examples for Dashboard Studio
Browse examples of dashboards & visualizations. Visit Example Hub

Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

13 Dashboards

Title	Owner	App	Sharing	Type
ANA Directory Metrics	admin	search	Private	Dashboard Studio
ANA Directory Stats	admin	search	App	Dashboard Studio
ANA Directory Time Metrics	admin	search	App	Dashboard Studio
ANA IM Wildfly Errors	admin	search	App	Dashboard Studio
ANA IMPS Event Count	admin	search	App	Dashboard Studio
ANA JCS & Directory Load Balance	admin	search	App	Dashboard Studio
ANA Provisioning Actions	admin	search	Private	Dashboard Studio
ANA Wildfly Log All	admin	search	App	Dashboard Studio
Integrity Check of Installed Files	nobody	search	App	Dashboard Studio
Job Details Dashboard	nobody	search	App	Dashboard Studio
jQuery Upgrade	nobody	search	App	Classic
Orphaned Scheduled Searches, Reports, and Alerts	nobody	search	App	Dashboard Studio
Scheduled export is now available for Dashboard Studio	nobody	search	Global	Dashboard Studio

Create New Dashboard

Dashboard Title: ANA IMPS ETATRANS

ana_imps_etatrans Edit ID

Description: Optional

Permissions: Shared in App

How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

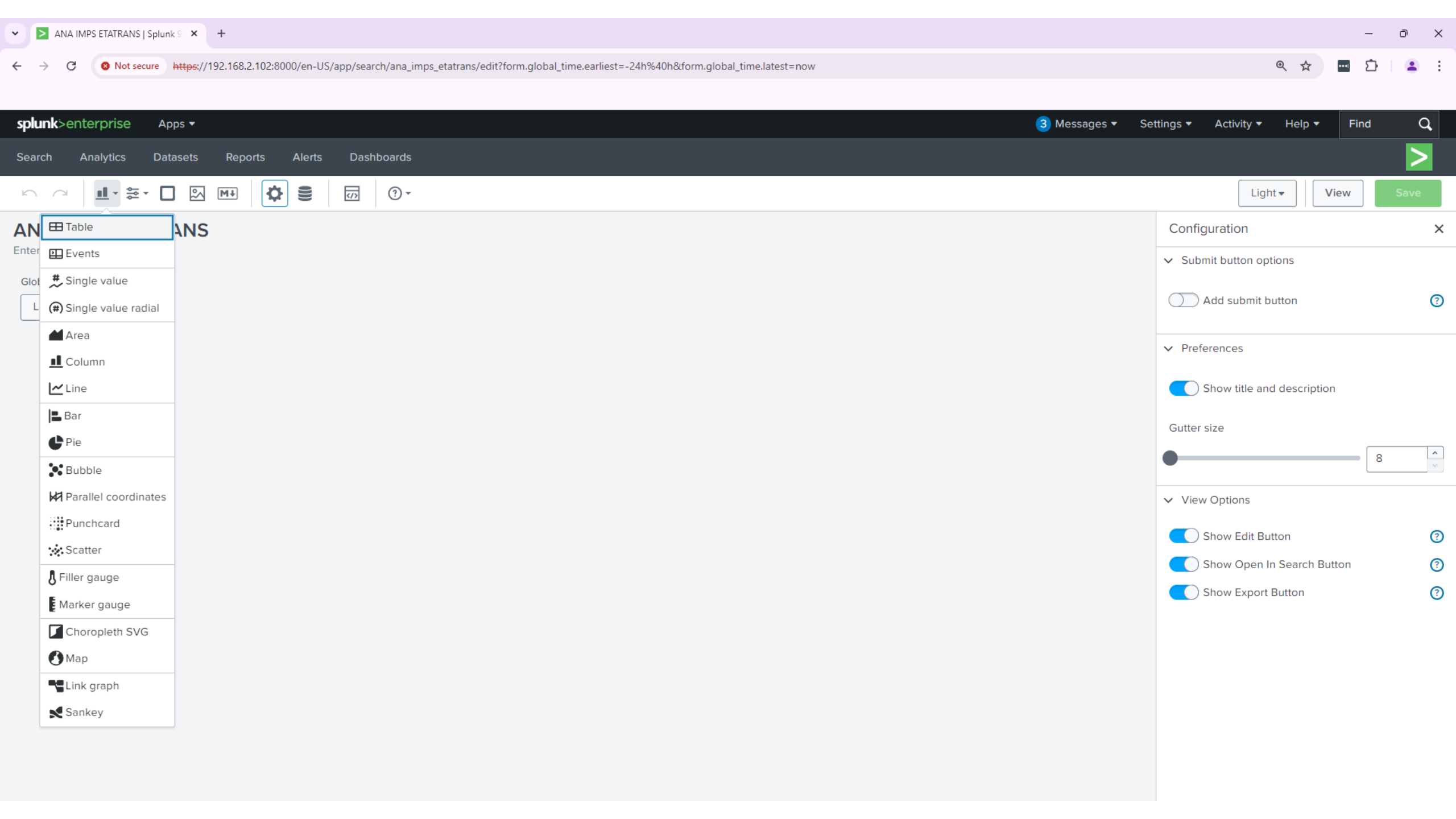
Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Select layout mode

Absolute
Full layout control

Grid
Quick organization

Cancel Create


ANA IMPS ETATRANS | Splunk
Not secure
https://192.168.2.102:8000/en-US/app/search/ana_imps_etatrans/edit?form.global_time.earliest=-24h%40h&form.global_time.latest=now
splunk>enterprise
Apps
3 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Light
View
Save
Table
Events
Single value
Single value radial
Area
Column
Line
Bar
Pie
Bubble
Parallel coordinates
Punchcard
Scatter
Filler gauge
Marker gauge
Choropleth SVG
Map
Link graph
Sankey
Configuration
Submit button options
Add submit button
Preferences
Show title and description
Gutter size
8
View Options
Show Edit Button
Show Open In Search Button
Show Export Button

ANA IMPS ETATRANS | Splunk

Not secure https://192.168.2.102:8000/en-US/app/search/ana_imps_etatrans/edit?form.global_time.earliest=-24h%40h&form.global_time.latest=now

splunk>enterprise Apps 3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Light View Save

ANA IMPS ETATRANS

Enter dashboard description.

Global Time Range

Last 24 hours

New data source

Data source name

imps_etatrans

Access search results or metadata

SPL query Open in search

```
index=main sourcetype="syslog" source="tcp:10514"
    host="vapp145" imps_etatrans_log
| rex field=_raw "^(<(?<priority>\d+)>)?\s
    *(?<timestamp>\w{3}\s+\d{1,2}\s+\d{2}:\d{2}
    :\d{2})\s+(?<host>\S+)\s+(?<syslogtag>\S+)\s
    +(?<imps_time>\d{8}:\d{6}):TID=(?<tid>\w
    +):(?<action>\S+)\s+:(?<status>[^\[]+)"
| transaction tid maxspan=5m
| table timestamp host syslogtag imps_time tid
    action status duration eventcount
```

Time range

Input Static Default

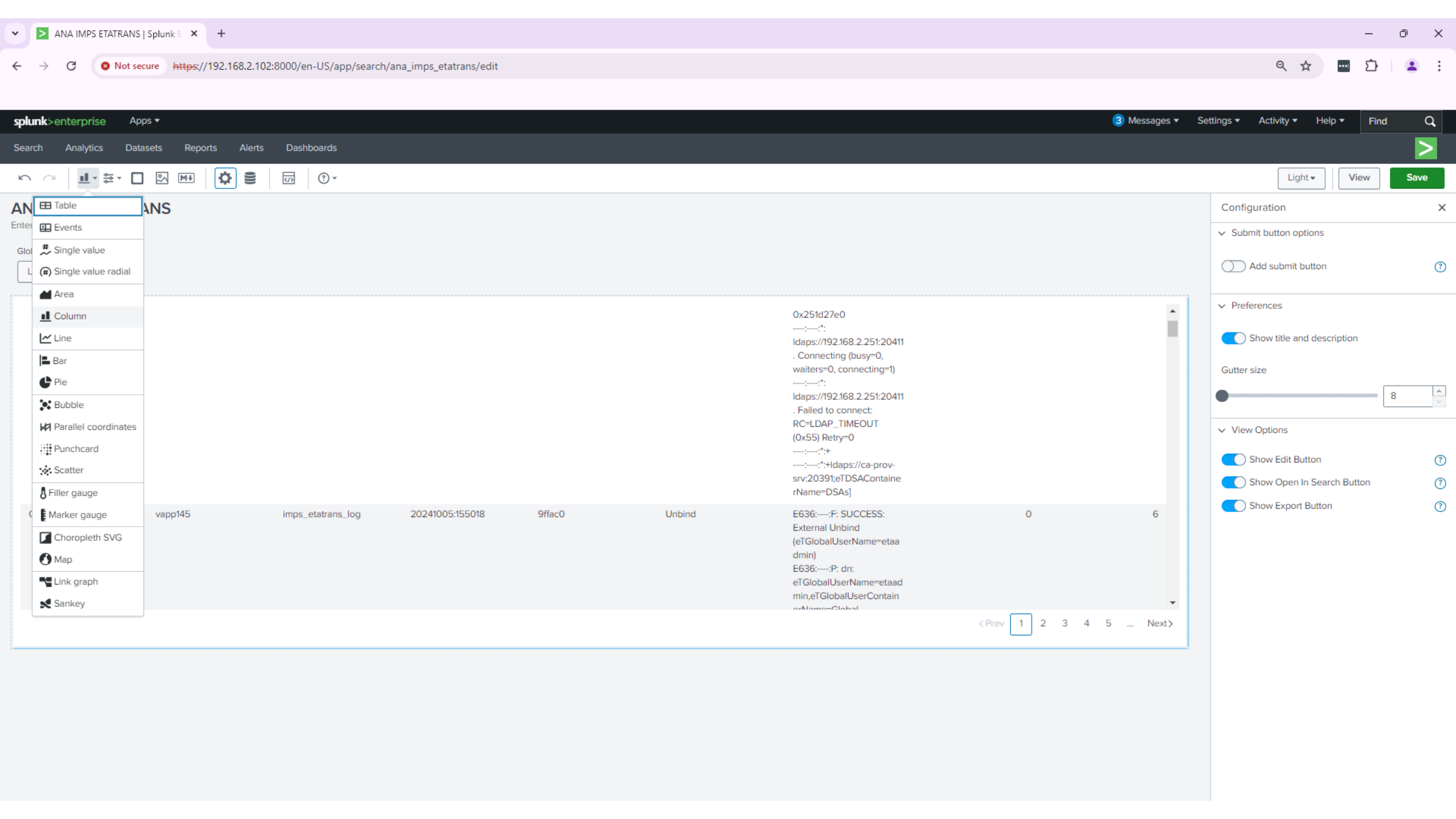
Time range set by dashboard source default value

$global_time.earliest$ - $global_time.latest$

Configure in source editor

1 visualization will be updated

Cancel Apply and close


ANA IMPS ETATRANS | Splunk
Not secure
https://192.168.2.102:8000/en-US/app/search/ana_imps_etatrans/edit
splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Light
View
Save
Table
Events
Single value
Single value radial
Area
Column
Line
Bar
Pie
Bubble
Parallel coordinates
Punchcard
Scatter
Filler gauge
Marker gauge
Choropleth SVG
Map
Link graph
Sankey
0x251d27e0
----:----:*:
ldaps://192.168.2.251:20411
. Connecting (busy=0,
waiters=0, connecting=1)
----:----:*:
ldaps://192.168.2.251:20411
. Failed to connect:
RC=LDAP_TIMEOUT
(0x55) Retry=0
----:----:*:+
----:----:*:+ldaps://ca-prov-
srv:20391;eTDSAContaine
rName=DSAs]
vapp145
imps_etatrans_log
20241005:155018
9ffac0
Unbind
E636:----:F: SUCCESS:
External Unbind
(eTGlobalUserName=etaa
dmin)
E636:----:P: dn:
eTGlobalUserName=etaad
min,eTGlobalUserContain
0
6
Prev
1
2
3
4
5
...
Next
Configuration
Submit button options
Add submit button
Preferences
Show title and description
Gutter size
8
View Options
Show Edit Button
Show Open In Search Button
Show Export Button

ANA IMPS ETATRANS | Splunk

Not secure https://192.168.2.102:8000/en-US/app/search/ana_imps_etatrans/edit

splunk>enterprise Apps

Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Success! Dashboard saved.

Light View Save

ANA IMPS ETATRANS

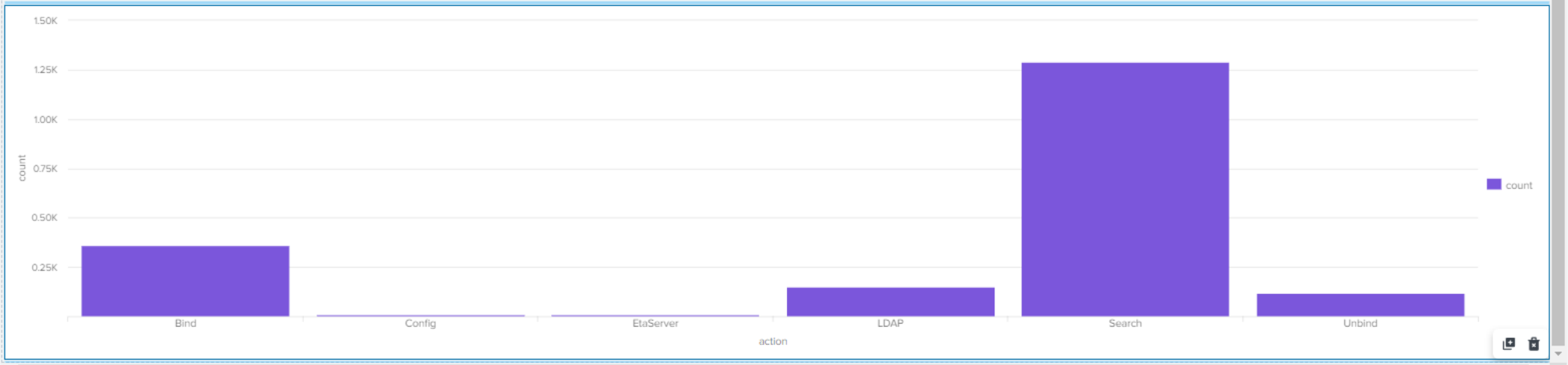
Enter dashboard description.

Global Time Range

Last 24 hours

E638:----:I: FOUND EXISTING CACHED ITEM
E638:----:I: USER-PRIV-CACHE STATS { SIZE: 1 of 20, USED 1 for 1, CAN 0 UNINIT 0 }
E638:----:I: eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=
E638:----:I:+ GRANTED

Prev 1 2 3 4 5 ... Next



Edit data source

Data source name

imps_action_count

Access search results or metadata

SPL query Open in search

```
index=main sourcetype="syslog" source="tcp:10514"
    host="vapp145" imps_etatrans_log
| rex field=_raw "^(<(?<priority>\d+)>)?\s
    *(?<timestamp>\w{3}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2}
    )\s+(?<host>\S+)\s+(?<syslogtag>\S+)\s
    +(?<imps_time>\d{8}:\d{6}):TID=(?<tid>\w
    +):(?<action>\S+)\s+:(?<status>[^\[]+)"
| stats count by action
| table action count
```

Time range

Input Static Default

Time range set by dashboard source default value

$global_time.earliest$ - $global_time.latest$

Configure in source editor

Usage

1 visualization
0 inputs
0 chain searches

Source code

Cancel Apply and close

```
config@vapp145 VAPP-14.5.1 (192.168.2.102):/etc/rsyslog.d > cat rsyslog-custom.conf
# Stop imjournal module from flooding imfile module
# Prevent forwarding logs from imjournal to imfile
if $programname == 'imjournal' then {
   stop
}

# Enable debug as needed
# $DebugFile /var/log/rsyslog-debug.log
# $DebugLevel 2
# Use: cat /var/log/rsyslog-debug.log

# Global Settings
# Increase maxMessageSize from default of 8k to 64k
global(maxMessageSize="64k")


# 2024-10-03: Use imfile module to monitor logs efficiently with inotify
module(load="imfile" mode="inotify")

# vApp Main log
input(type="imfile"
    addMetadata="on"
    File="/opt/CA/VirtualAppliance/logs/ca_vapp_main.log"
    Tag="vapp-main-log"
    Facility="local5")

# vApp Deployment log
input(type="imfile"
    addMetadata="on"
    File="/opt/CA/VirtualAppliance/logs/ca_vapp_deployment.log"
    Tag="vapp-deployment-log"
    Facility="local5")

# IM Wildfly Server log: server.log
input(type="imfile"
    addMetadata="on"
    File="/opt/CA/VirtualAppliance/logs/IDM_logs/server.log"
    Tag="im-wildfly-server-log"
    Facility="local5")

# IP Wildfly Server log: server.log
input(type="imfile"
    addMetadata="on"
    File="/opt/CA/VirtualAppliance/logs/IP_logs/server.log"
    Tag="ip-wildfly-server-log"
    Facility="local5")

# JCS Server log: jcs_daily.log
input(type="imfile"
    addMetadata="on"
    File="/opt/CA/VirtualAppliance/logs/ConnectorServer_logs/jcs_daily.log"
    Tag="jcs-daily-vapp-server-log"
    Facility="local5")
```

```
# IM Prov Server logs: etatrans*.log
input(type="imfile"
    addMetadata="on"
    File="/opt/CA/VirtualAppliance/logs/ProvisioningServer_logs/etatrans*.log"
    Tag="imps-etatrans-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*-idm-userstore-router-caim-srv-*_*_*.log"
    Tag="dir-idm-userstore-router-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*-idm-userstore-router-caim-srv-*_trace.log"
    Tag="dir-idm-userstore-router-trace-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*UserStore_userstore-*_*_*.log"
    Tag="dir-idm-userstore-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*UserStore_userstore-*_trace.log"
    Tag="dir-idm-userstore-trace-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*ca-prov-srv-*-imps_*.log"
    Tag="dir-imps-router-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*ca-prov-srv-*-imps_trace.log"
    Tag="dir-imps-router-trace-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*ca-prov-srv-*-impd-*_*_*.log"
    Tag="dir-impd-data-dsa-log"
    Facility="local5")

input(type="imfile"
    addMetadata="on"
    File="/opt/CA/Directory/dxserver/logs/*ca-prov-srv-*-impd-*_trace.log"
    Tag="dir-impd-data-dsa-trace-log"
    Facility="local5")
```

```
# Send logs to remote syslog server using TCP (reliable transmission)
# Adding an action queue for better reliability and buffering in case of connection issues with TCP
# Larger queue configuration with disk-based queue if needed
# Only allow logs with Facility local5 to be forwarded
if ($syslogfacility-text == "local5") then {
   action(
     type="omfwd"
     target="log-srv"
     port="10514"
     protocol="tcp"
     action.resumeRetryCount="-1"      # Retry indefinitely if the connection is lost
     queue.type="LinkedList"          # Use a linked list for the queue
     queue.size="50000"              # Buffer up to 50,000 log messages in memory
     queue.dequeueBatchSize="100"      # Process 100 messages at a time when the queue is being flushed
     queue.highWatermark="40000"      # Start applying flow control when the queue size reaches 40,000
     queue.lowWatermark="10000"       # Resume normal operations when the queue size drops to 10,000
     queue.timeoutEnqueue="0"         # Do not drop messages, wait indefinitely if the queue is full
     queue.workerThreads="4"          # Use multiple worker threads to improve message throughput

     # Disk-based queue settings to handle overflow when memory queue fills up
     queue.spoolDirectory="/var/log/rsyslog-queue"   # Directory for disk-backed queue
     queue.maxDiskSpace="10g"                 # Maximum disk space for the queue
     queue.fileName="largequeue"               # Name for disk queue files
     queue.saveOnShutdown="on"                # Save queue to disk on shutdown to prevent data loss
   )
   stop  # Prevent further processing of local5 logs
}


# The '@@' indicates TCP; '@' would indicate UDP
# # Use override here to define where the facility will be redirected to a remote syslog collector
# local5.* @log-srv:10514
#
# Restart rsyslog:   sudo systemctl restart rsyslog
# Note: Check /var/log/messages for any typo errors via
#   sudo systemctl restart rsyslog ; tail -n 100 -F /var/log/messages | grep -i syslog
#
# Optional: You may redirect additional facility levels as needed
# local5.* /var/log/local5.log
#
# Within Splunk UI - Use sourcetype="syslog"  and the tag strings
```

Updated /etc/rsyslog.d/rsyslog-custom.conf to use imfile and exclude any noise from imjournal

1) Noise from imjournal and IP6 via Network Manager impacted queries

```
config@vapp145 VAPP-14.5.1 (192.168.2.102):/etc/rsyslog.d > tail -n 100 -F /var/log/messages
Oct  5 17:27:00 vapp145 dir-impd-data-dsa-log [128] 20241005.172700.833 STATS : Assocs 0 NilCredit 0 Queue 0+0 MWQ 0/0 Active 0 Ops 0 Entries 0 Mem 21/13 CPU Seconds 60/60 CPU kTicks 1
Oct  5 17:27:02 vapp145 NetworkManager[793]: <warn>  [1728167222.6048] platform-linux: do-add-ip6-address[2: fe80::8429:f9e3:3058:be00]: failure 13 (Permission denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:04 vapp145 NetworkManager[793]: <warn>  [1728167224.6076] platform-linux: do-add-ip6                                                    ion denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:06 vapp145 NetworkManager[793]: <warn>  [1728167226.6108] platform-linux: do-add-ip6                                                    ion denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:08 vapp145 NetworkManager[793]: <warn>  [1728167228.6125] platform-linux: do-add-ip6                                                    ion denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:10 vapp145 NetworkManager[793]: <warn>  [1728167230.6144] ipv6ll[1ad01a420750ae45,if                                                    er Duplicate Address Detection failures (back off)
Oct  5 17:27:20 vapp145 NetworkManager[793]: <warn>  [1728167240.6157] platform-linux: do-add-ip6-address[2: fe80::290a:17e6:ea50:c07]: failure 13 (Permission denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:20 vapp145 NetworkManager[793]: <warn>  [1728167240.6158] l3cfg[e72522d0d139da92,ifindex=2]: unable to configure IPv6 route: type unicast fe80::/64 dev 2 metric 1024 mss 0 rt-src ipv6ll
Oct  5 17:27:22 vapp145 NetworkManager[793]: <warn>  [1728167242.6184] platform-linux: do-add-ip6-address[2: fe80::f262:f3c1:cf89:f75c]: failure 13 (Permission denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:24 vapp145 NetworkManager[793]: <warn>  [1728167244.6195] platform-linux: do-add-ip6-address[2: fe80::8429:f9e3:3058:be00]: failure 13 (Permission denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:26 vapp145 NetworkManager[793]: <warn>  [1728167246.6220] platform-linux: do-add-ip6-address[2: fe80::c567:d572:15ca:c716]: failure 13 (Permission denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:28 vapp145 NetworkManager[793]: <warn>  [1728167248.6239] platform-linux: do-add-ip6-address[2: fe80::5307:1173:a17a:490]: failure 13 (Permission denied - ipv6: IPv6 is disabled on this device)
Oct  5 17:27:30 vapp145 NetworkManager[793]: <warn>  [1728167250.6269] platform-linux: do-add-ip6-address[2:                                                                                                    e)
Oct  5 17:27:32 vapp145 NetworkManager[793]: <warn>  [1728167252.6294] ipv6ll[1ad01a420750ae45,ifindex=2]: cha                                                                                                    )
Oct  5 17:27:42 vapp145 NetworkManager[793]: <warn>  [1728167262.6342] platform-linux: do-add-ip6-address[2:                                                                                                    e)
Oct  5 17:27:42 vapp145 NetworkManager[793]: <warn>  [1728167262.6343] l3cfg[e72522d0d139da92,ifindex=2]: unal
Oct  5 17:27:44 vapp145 NetworkManager[793]: <warn>  [1728167264.6369] platform-linux: do-add-ip6-address[2:                                                                                                    ce)
Oct  5 17:27:46 vapp145 NetworkManager[793]: <warn>  [1728167266.6400] platform-linux: do-add-ip6-address[2:                                                                                                    ce)
Oct  5 17:27:48 vapp145 NetworkManager[793]: <warn>  [1728167268.6426] platform-linux: do-add-ip6-address[2:                                                                                                    ce)
```

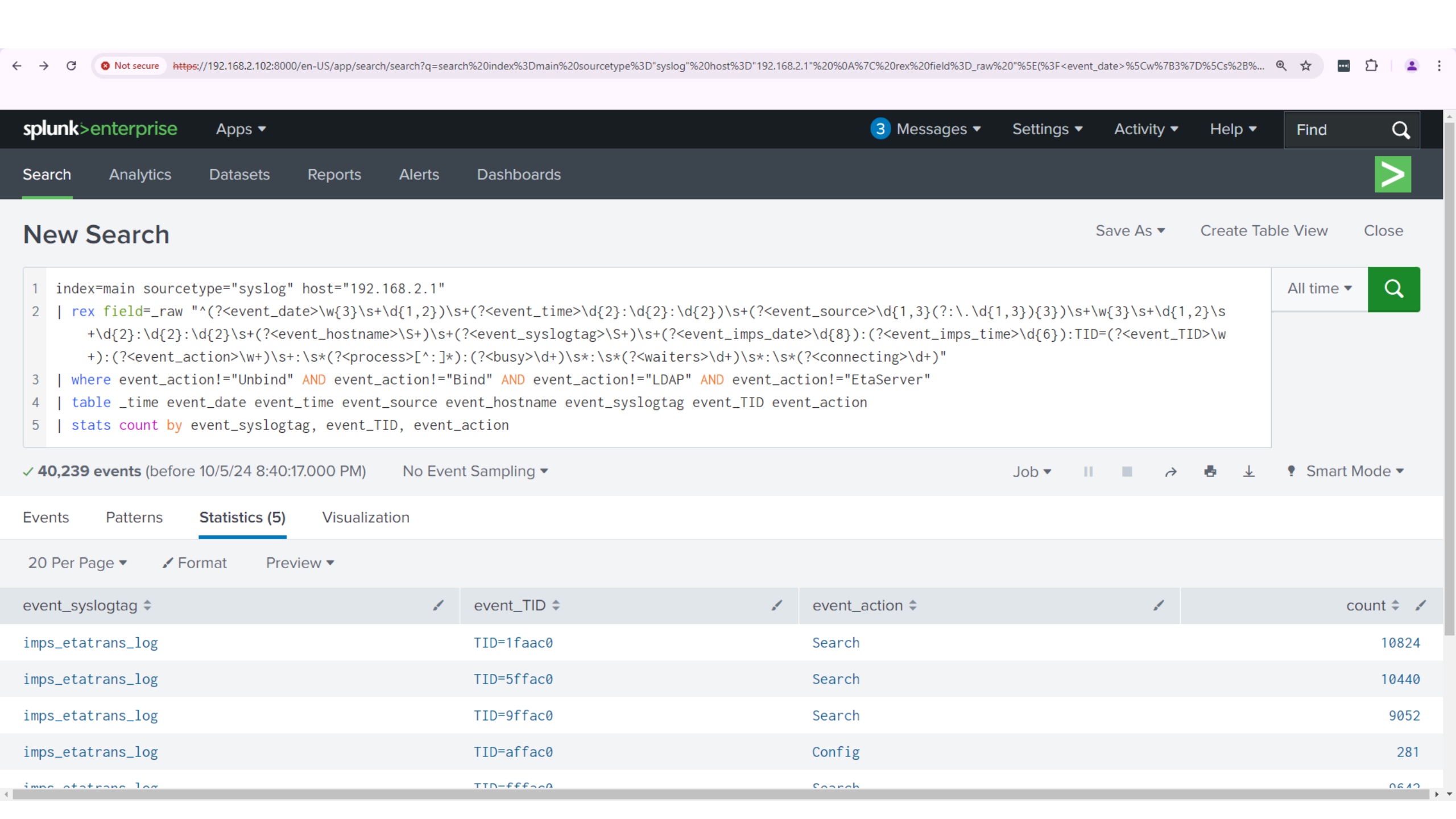
```
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

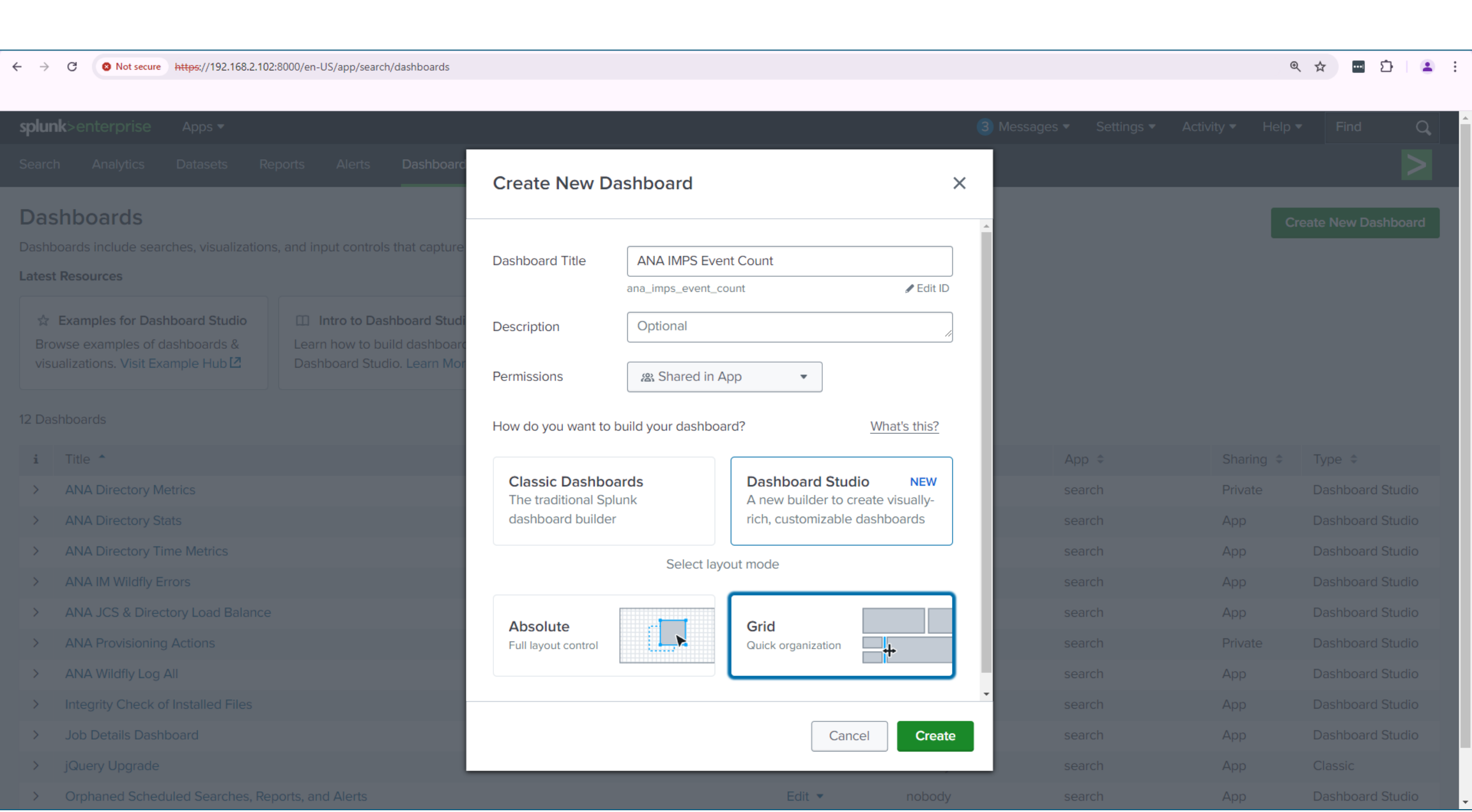
2) Noise from imjournal being forwarded to imfile for "action"

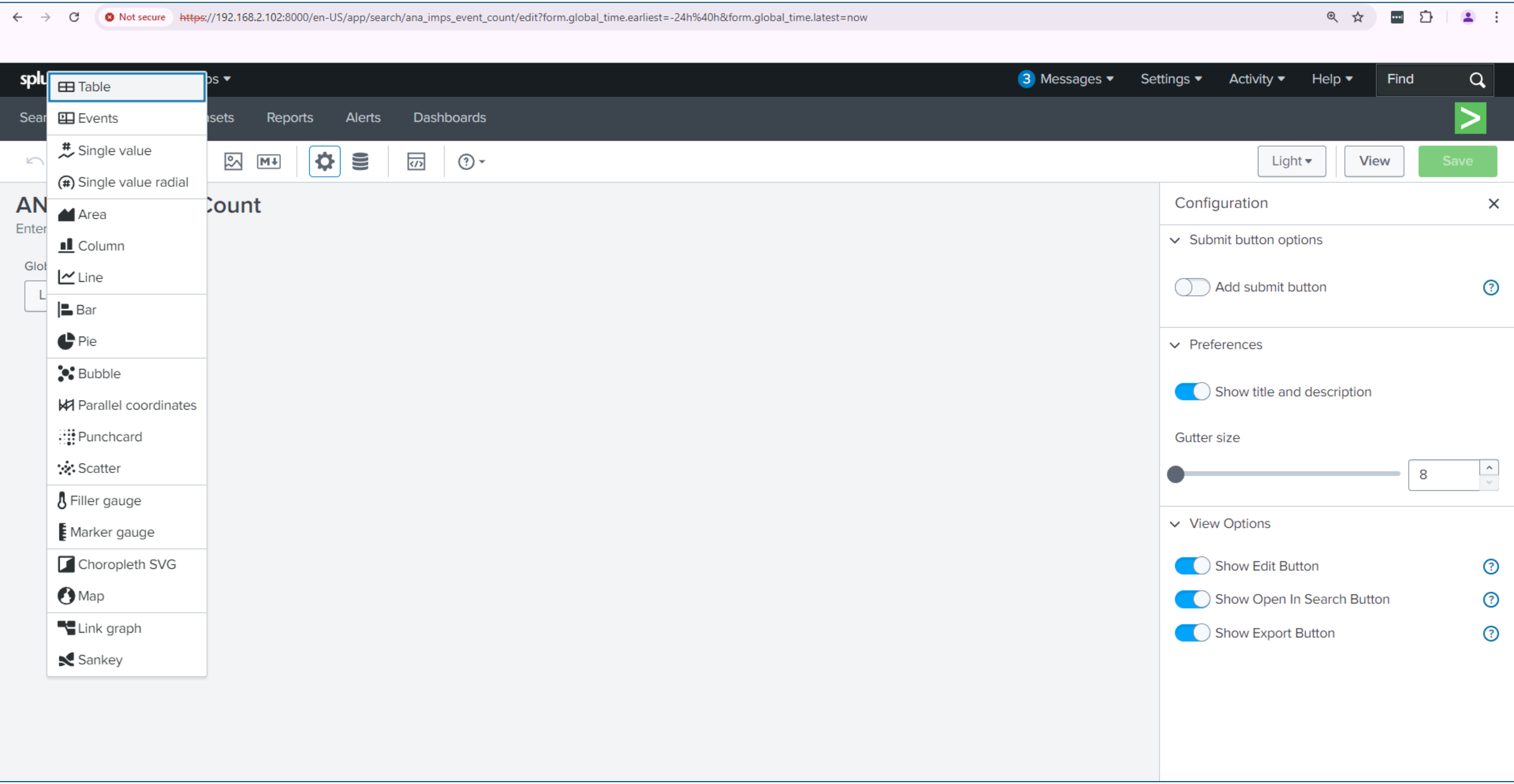
```
config@vapp145 VAPP-14.5.1 (192.168.2.102):/etc/rsyslog.d > cat rsyslog-custom.conf

# Send logs to remote syslog server using TCP (reliable transmission)
# Adding an action queue for better reliability and buffering in case of connection issues with TCP
# Larger queue configuration with disk-based queue if needed
# Only allow logs with Facility local5 to be forwarded
if ($syslogfacility-text == "local5") then {
  action(
    type="omfwd"
    target="log-srv"
    port="10514"
    protocol="tcp"
    action.resumeRetryCount="-1"     # Retry indefinitely if the connection is lost
    queue.type="LinkedList"          # Use a linked list for the queue
    queue.size="50000"               # Buffer up to 50,000 log messages in memory
    queue.dequeueBatchSize="100"     # Process 100 messages at a time when the queue is being flushed
    queue.highWatermark="40000"      # Start applying flow control when the queue size reaches 40,000
    queue.lowWatermark="10000"       # Resume normal operations when the queue size drops to 10,000
    queue.timeoutEnqueue="0"         # Do not drop messages, wait indefinitely if the queue is full
    queue.workerThreads="4"          # Use multiple worker threads to improve message throughput

    # Disk-based queue settings to handle overflow when memory queue fills up
    queue.spoolDirectory="/var/log/rsyslog-queue"  # Directory for disk-backed queue
    queue.maxDiskSpace="10g"                 # Maximum disk space for the queue
    queue.fileName="largequeue"              # Name for disk queue files
    queue.saveOnShutdown="on"                # Save queue to disk on shutdown to prevent data loss
  )
  stop  # Prevent further processing of local5 logs
}
```

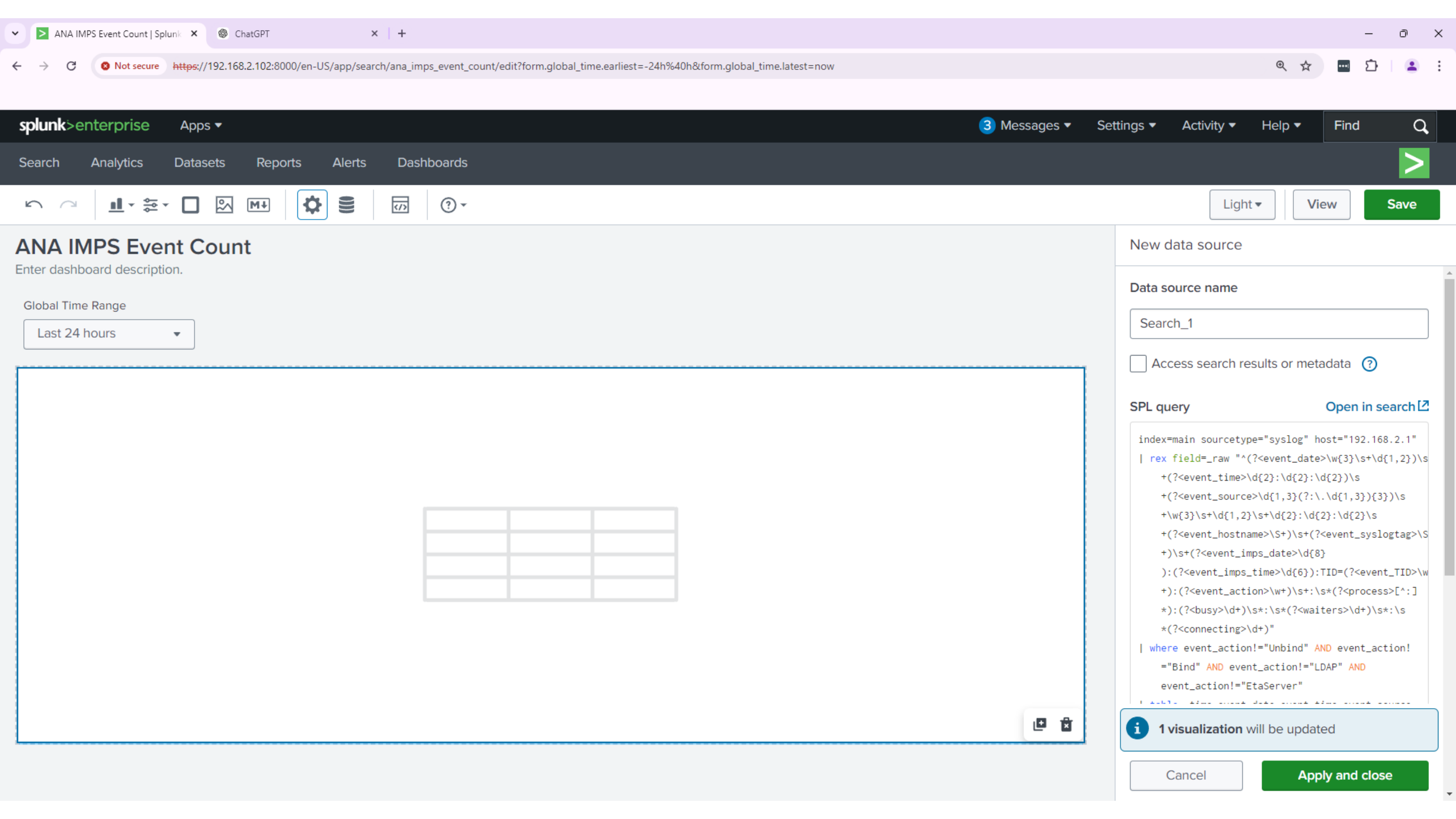
3) Syslog indexes were being defaulted to GMT/UTC TZ - impacted queries

```
config@vapp145 VAPP-14.5.1 (192.168.2.102):/etc/rsyslog.d > podman exec -it -u splunk splunk bash -c 'cat ./etc/system/local/props.conf'
[syslog]
TZ = US/Central
```


Not secure
https://192.168.2.102:8000/en-US/app/search/search?q=search%20index%3Dmain%20sourcetype%3D"syslog"%20host%3D"192.168.2.1"%20%0A%7C%20rex%20field%3D_raw%20"%5E(%3F<event_date>%5Cw%7B3%7D%5Cs%2B%...
splunk>enterprise
Apps
3 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table View
Close
1 index=main sourcetype="syslog" host="192.168.2.1"
2 | rex field=_raw "^(?<event_date>\w{3}\s+\d{1,2})\s+(?<event_time>\d{2}:\d{2}:\d{2})\s+(?<event_source>\d{1,3}(?:\.\d{1,3}){3})\s+\w{3}\s+\d{1,2}\s
+\d{2}:\d{2}:\d{2}\s+(?<event_hostname>\S+)\s+(?<event_syslogtag>\S+)\s+(?<event_imps_date>\d{8}):(?<event_imps_time>\d{6}):TID=(?<event_TID>\w
+):(?<event_action>\w+)\s+:\s*(?<process>[^:]*):(?<busy>\d+)\s*:\s*(?<waiters>\d+)\s*:\s*(?<connecting>\d+)"
3 | where event_action!="Unbind" AND event_action!="Bind" AND event_action!="LDAP" AND event_action!="EtaServer"
4 | table _time event_date event_time event_source event_hostname event_syslogtag event_TID event_action
5 | stats count by event_syslogtag, event_TID, event_action
All time
40,239 events (before 10/5/24 8:40:17.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (5)
Visualization
20 Per Page
Format
Preview
event_syslogtag
event_TID
event_action
count
imps_etatrans_log TID=1faac0 Search 10824
imps_etatrans_log TID=5ffac0 Search 10440
imps_etatrans_log TID=9ffac0 Search 9052
imps_etatrans_log TID=affac0 Config 281


Not secure
https://192.168.2.102:8000/en-US/app/search/dashboards
splunk>enterprise
Apps
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboard
Dashboards
Dashboards include searches, visualizations, and input controls that capture
Latest Resources
Examples for Dashboard Studio
Browse examples of dashboards & visualizations. Visit Example Hub
Intro to Dashboard Studi
Learn how to build dashboard
Dashboard Studio. Learn Mor
Create New Dashboard
12 Dashboards
Title
App
Sharing
Type
ANA Directory Metrics
ANA Directory Stats
ANA Directory Time Metrics
ANA IM Wildfly Errors
ANA JCS & Directory Load Balance
ANA Provisioning Actions
ANA Wildfly Log All
Integrity Check of Installed Files
Job Details Dashboard
jQuery Upgrade
Orphaned Scheduled Searches, Reports, and Alerts
Edit
nobody
search
Private
App
Classic
Dashboard Studio
Create New Dashboard
Dashboard Title
ANA IMPS Event Count
ana_imps_event_count
Edit ID
Description
Optional
Permissions
Shared in App
How do you want to build your dashboard?
What's this?
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
NEW
A new builder to create visually-rich, customizable dashboards
Select layout mode
Absolute
Full layout control
Grid
Quick organization
Cancel
Create


Not secure
https://192.168.2.102:8000/en-US/app/search/ana_imps_event_count/edit?form.global_time.earliest=-24h%40h&form.global_time.latest=now
Messages
Settings
Activity
Help
Find
Reports
Alerts
Dashboards
Light
View
Save
Table
Events
Single value
Single value radial
Area
Column
Line
Bar
Pie
Bubble
Parallel coordinates
Punchcard
Scatter
Filler gauge
Marker gauge
Choropleth SVG
Map
Link graph
Sankey
Configuration
Submit button options
Add submit button
Preferences
Show title and description
Gutter size
8
View Options
Show Edit Button
Show Open In Search Button
Show Export Button


ANA IMPS Event Count | Splunk
ChatGPT
Not secure
https://192.168.2.102:8000/en-US/app/search/ana_imps_event_count/edit?form.global_time.earliest=-24h%40h&form.global_time.latest=now
splunk>enterprise
Apps
3 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Light
View
Save
ANA IMPS Event Count
Enter dashboard description.
Global Time Range
Last 24 hours
New data source
Data source name
Search_1
Access search results or metadata
SPL query
Open in search
index=main sourcetype="syslog" host="192.168.2.1"
| rex field=_raw "^(?<event_date>\w{3}\s+\d{1,2})\s
+(?<event_time>\d{2}:\d{2}:\d{2})\s
+(?<event_source>\d{1,3}(?:\.\d{1,3}){3})\s
+\w{3}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2}\s
+(?<event_hostname>\S+)\s+(?<event_syslogtag>\S
+)\s+(?<event_imps_date>\d{8}
):(?<event_imps_time>\d{6}):TID=(?<event_TID>\w
+):(?<event_action>\w+)\s+:\s*(?<process>[^:]
):(?<busy>\d+)\s:\s*(?<waiters>\d+)\s*:\s
*(?<connecting>\d+)"
| where event_action!="Unbind" AND event_action!
="Bind" AND event_action!="LDAP" AND
event_action!="EtaServer"
1 visualization will be updated
Cancel
Apply and close

ANA IMPS Event Count | Splunk

ChatGPT

Not secure https://192.168.2.102:8000/en-US/app/search/ana_imps_event_count/edit

splunk>enterprise Apps

3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Success! Dashboard saved.

Light View Save

ANA IMPS Event Count

Enter dashboard description.

Global Time Range

Last 24 hours

event_syslogtag	event_TID	event_action	count
imps_etatrans_log	TID=1faac0	Search	5548
imps_etatrans_log	TID=5ffac0	Search	5466
imps_etatrans_log	TID=9ffac0	Search	3920
imps_etatrans_log	TID=affac0	Config	139
imps_etatrans_log	TID=fffac0	Search	4620

Configuration

General

Visualization type

Table

Title

Description

Data sources

Search_1

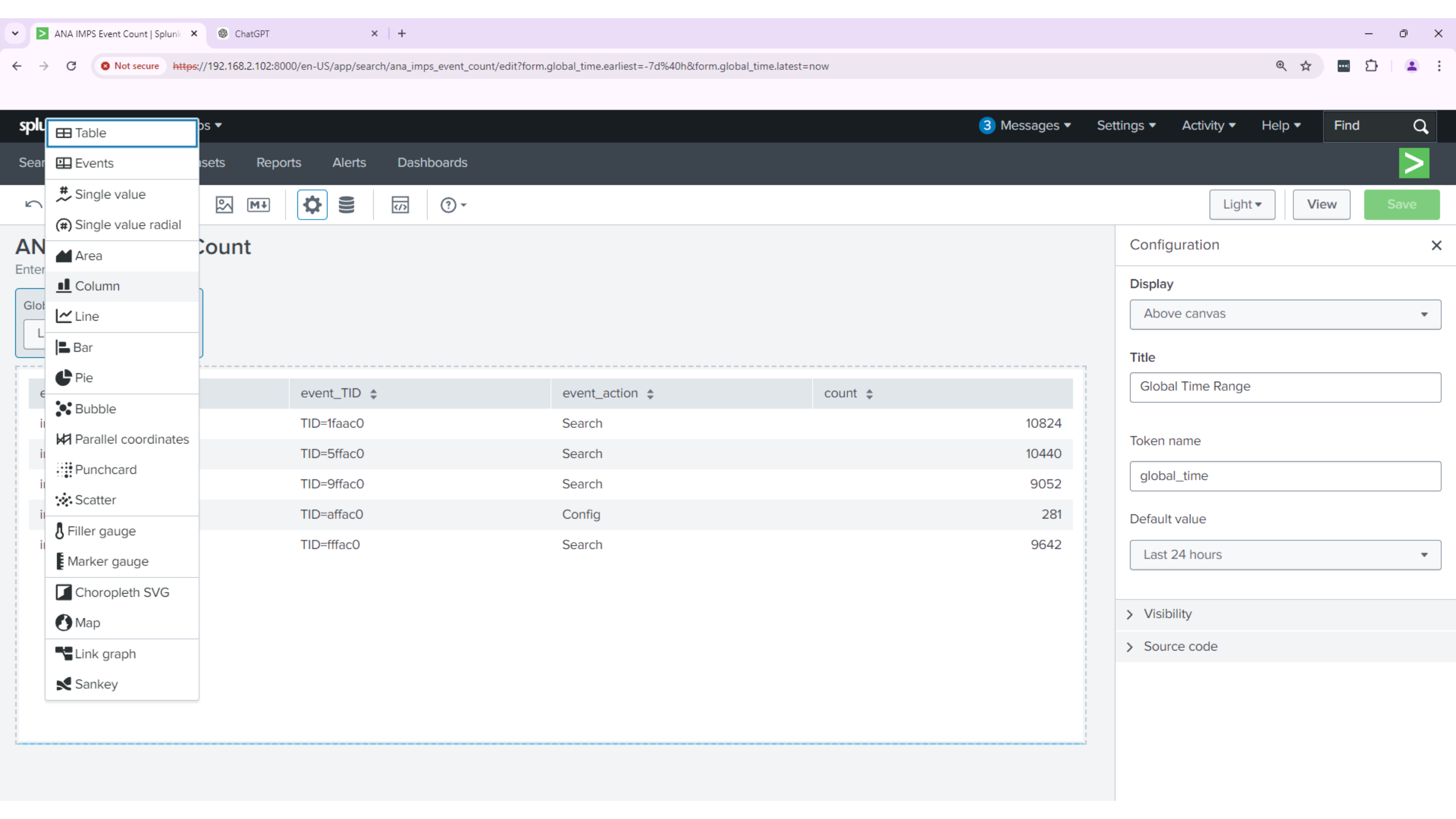
Visibility

Data display

Color and style

Interactions

Source code


ANA IMPS Event Count | Splunk
ChatGPT
Not secure
https://192.168.2.102:8000/en-US/app/search/ana_imps_event_count/edit?form.global_time.earliest=-7d%40h&form.global_time.latest=now
Messages
Settings
Activity
Help
Find
Reports
Alerts
Dashboards
Light
View
Save
Table
Events
Single value
Single value radial
Area
Column
Line
Bar
Pie
Bubble
Parallel coordinates
Punchcard
Scatter
Filler gauge
Marker gauge
Choropleth SVG
Map
Link graph
Sankey
Count
event_TID
event_action
count
TID=1faac0
Search
10824
TID=5ffac0
Search
10440
TID=9ffac0
Search
9052
TID=affac0
Config
281
TID=fffac0
Search
9642
Configuration
Display
Above canvas
Title
Global Time Range
Token name
global_time
Default value
Last 24 hours
Visibility
Source code

ANA IMPS Event Count | Splunk

ChatGPT

Not secure https://192.168.2.102:8000/en-US/app/search/ana_imps_event_count/edit?form.global_time.earliest=-7d%40h&form.global_time.latest=now

splunk>enterprise Apps

3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

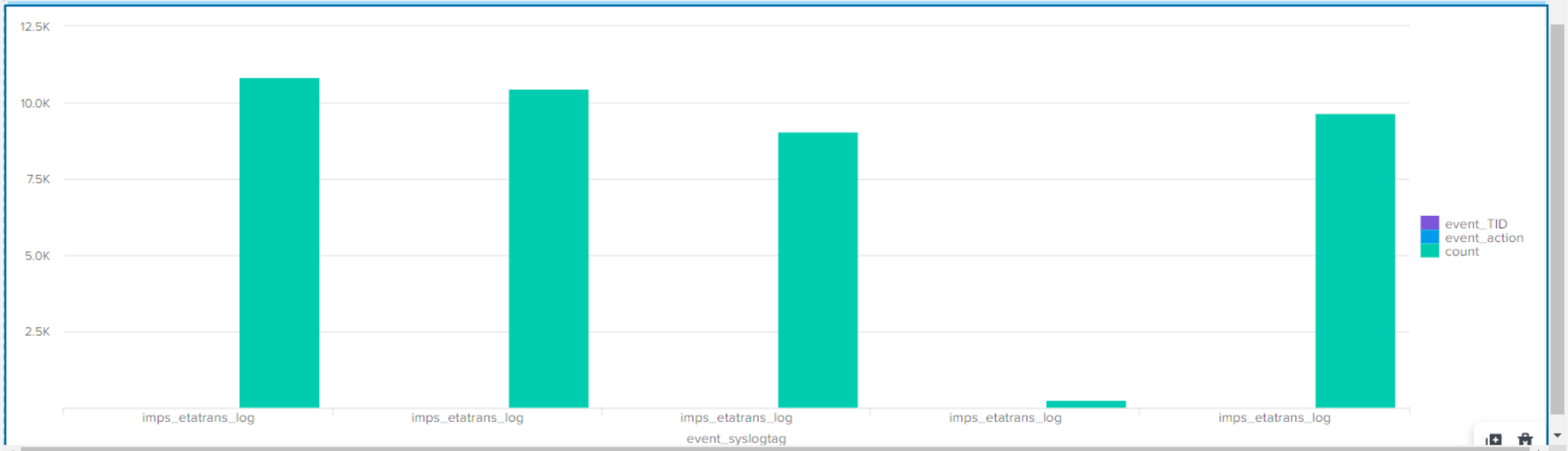
Light View Save

ANA IMPS Event Count

Enter dashboard description.

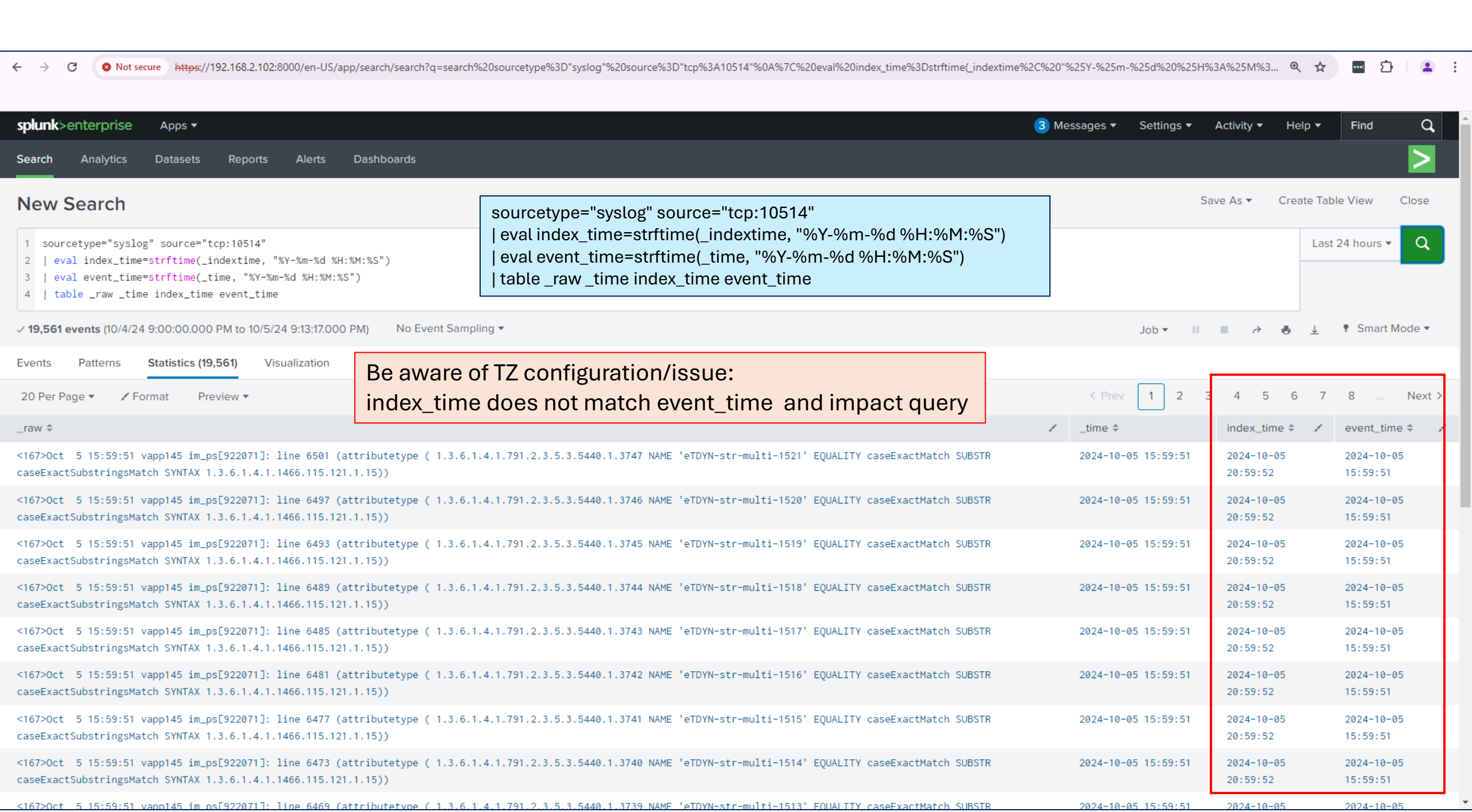
Global Time Range

Last 7 days



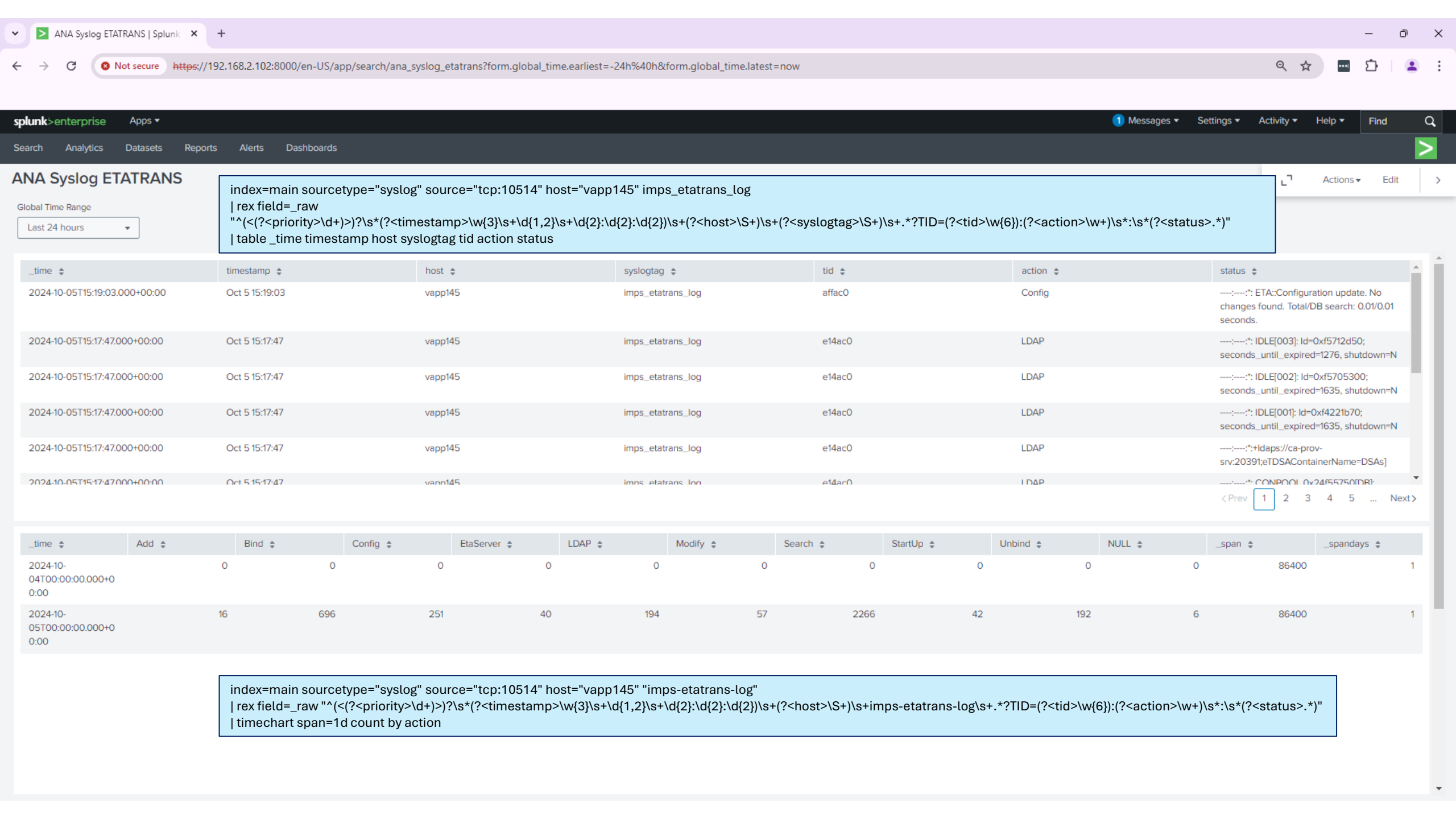
Configuration

- General
- Data sources
  - Search_1
  - + Set up annotation data source
- Visibility
- Data configurations
- Data display
- Color and style
- Legend
- X-axis grid and labels
- Y-axis grid and labels
- Y2-axis grid and labels
- Interactions
- Source code



sourcetype="syslog" source="tcp:10514"
| eval index_time=strftime(_indextime, "%Y-%m-%d %H:%M:%S")
| eval event_time=strftime(_time, "%Y-%m-%d %H:%M:%S")
| table _raw _time index_time event_time

Be aware of TZ configuration/issue:
index_time does not match event_time and impact query


ANA Syslog ETATRANS | Splunk
Not secure
https://192.168.2.102:8000/en-US/app/search/ana_syslog_etatrans?form.global_time.earliest=-24h%40h&form.global_time.latest=now
splunk>enterprise
Apps
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
ANA Syslog ETATRANS
Actions
Edit
Global Time Range
Last 24 hours
index=main sourcetype="syslog" source="tcp:10514" host="vapp145" imps_etatrans_log
| rex field=_raw
"^(<(?<priority>\d+)>)?\s*(?<timestamp>\w{3}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+(?<host>\S+)\s+(?<syslogtag>\S+)\s+.*?TID=(?<tid>\w{6}):(?<action>\w+)\s*:\s*(?<status>.*)"
| table _time timestamp host syslogtag tid action status
_time
timestamp
host
syslogtag
tid
action
status
2024-10-05T15:19:03.000+00:00
Oct 5 15:19:03
vapp145
imps_etatrans_log
affac0
Config
----:----:*: ETA::Configuration update. No changes found. Total/DB search: 0.01/0.01 seconds.
2024-10-05T15:17:47.000+00:00
Oct 5 15:17:47
vapp145
imps_etatrans_log
e14ac0
LDAP
----:----:*: IDLE[003]: Id=0xf5712d50; seconds_until_expired=1276, shutdown=N
2024-10-05T15:17:47.000+00:00
Oct 5 15:17:47
vapp145
imps_etatrans_log
e14ac0
LDAP
----:----:*: IDLE[002]: Id=0xf5705300; seconds_until_expired=1635, shutdown=N
2024-10-05T15:17:47.000+00:00
Oct 5 15:17:47
vapp145
imps_etatrans_log
e14ac0
LDAP
----:----:*: IDLE[001]: Id=0xf4221b70; seconds_until_expired=1635, shutdown=N
2024-10-05T15:17:47.000+00:00
Oct 5 15:17:47
vapp145
imps_etatrans_log
e14ac0
LDAP
----:----:*:+ldaps://ca-prov-srv:20391;eTDSAContainerName=DSAs]
Prev
1
2
3
4
5
...
Next
_time
Add
Bind
Config
EtaServer
LDAP
Modify
Search
StartUp
Unbind
NULL
_span
_spandays
2024-10-04T00:00:00.000+00:00
0
0
0
0
0
0
0
0
0
0
86400
1
2024-10-05T00:00:00.000+00:00
16
696
251
40
194
57
2266
42
192
6
86400
1
index=main sourcetype="syslog" source="tcp:10514" host="vapp145" "imps-etatrans-log"
| rex field=_raw "^(<(?<priority>\d+)>)?\s*(?<timestamp>\w{3}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+(?<host>\S+)\s+imps-etatrans-log\s+.*?TID=(?<tid>\w{6}):(?<action>\w+)\s*:\s*(?<status>.*)"
| timechart span=1d count by action

ANA Syslog ETATRANS

Actions Edit

Global Time Range

Last 24 hours

_time	Add	Bind	Config	EtaServer	LDAP	Modify	Search	StartUp	Unbind	NULL	_span	_spandays
2024-10-04T00:00:00.000+00:00	0	0	0	0	0	0	0	0	0	0	86400	1
2024-10-05T00:00:00.000+00:00	16	696	251	40	194	57	2266	42	192	6	86400	1

```
index=main sourcetype="syslog" source="tcp:10514" host="vapp145" "imps-etatrans-log"
| rex field=_raw "^(<(?<priority>\d+)>)?\s*(?<timestamp>\w{3}\s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+(?<host>\S+)\s+imps-etatrans-log\s+.*?TID=(?<tid>\w{6}):(?<action>\w+)\s*:\s*(?<status>.*)"
| timechart span=1d count by action useother=f limit=10
```