Problem Statement

1. Finding Logs, Indexing them to Splunk, Performing simple Search.

- Install Splunk Enterprise
- https://www.splunk.com/en_us/download/splunk-enterprise.html#tabs/windows (Links to an external site.)Links to an external site.
- Configure Data inputs from UI or inputs.conf file to capture Event Viewer Logs CPU, Memory, Disk
- Create an index name “event_logs” under indexes
- Perform a search to Identify fields - “host”, “source”, “sourcetypes” from the index name- “event_logs”
- Identify “Security”, “System”, & “Application” from the index

2. Using Splunk SPL Create Dashboards showing CPU, Memory to use the data

- Perform a search query to list values found of Disk, Memory and CPU
- Use stats or timechart syntax to depict actual values on a chart OR
- Use stats or timechart syntax to show avg utilization of Disk, memory & cpu in the last 15 minutes
- Use appropriate charting features to showcase the output and save them to a Dashboard
- Show the values on the graph (Optional)

Dashboard Monitoring And Reporting using Splunk

Author : Partha S Ghosh

System Informations

Operating System Used

```
Linux psg 4.13.0-39-generic #44~16.04.1-Ubuntu SMP Thu Apr 5 16:43:10 U
x86_64 x86_64 GNU/Linux
```

Note here that since i'm completing the assignment in Linux enviornment, there are 2 optio
capture the system data like CPU information/memory Information and Disk IO.

1. Use an available app in splunk store to do it, or
2. Create a small app with help of shell script to capture the system information data

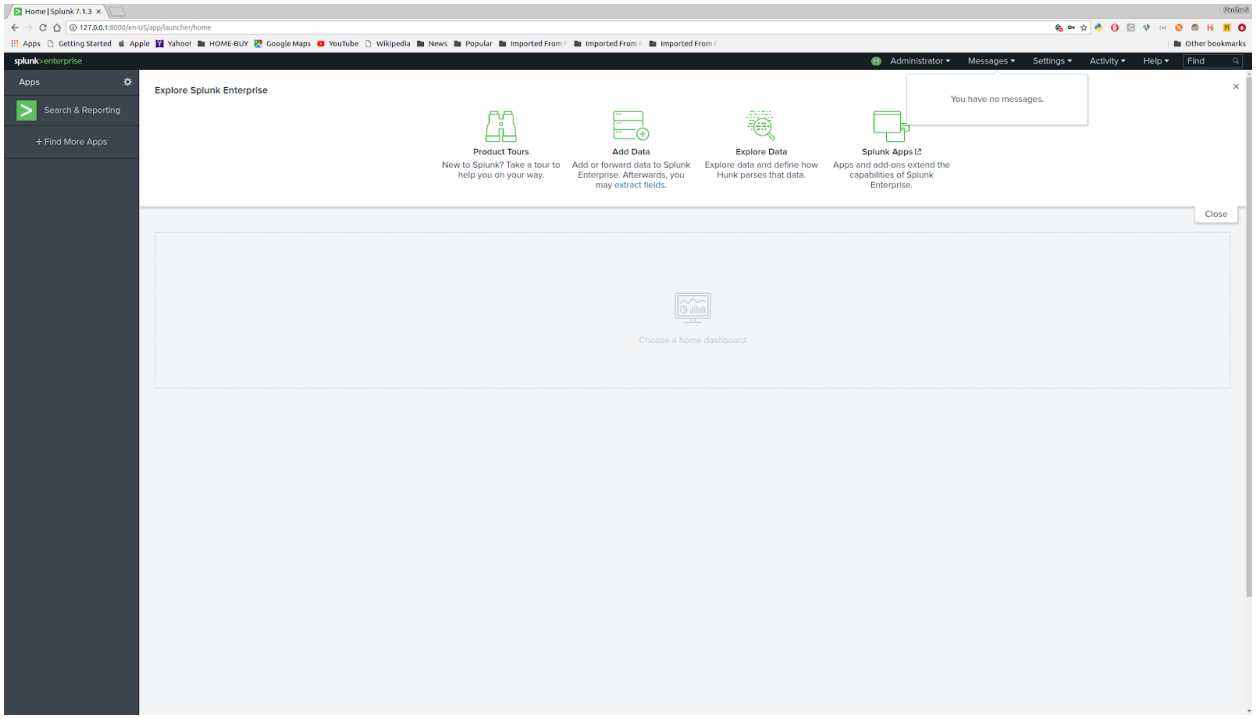
I choose to **follow step 2** as that would provide me some visibility into how the Splunk application work and also adds a degree of difficulty to this exercise.

Installed Splunk Version

```
root@psg:/opt/splunk# ./bin/splunk version
Splunk 7.1.3 (build 51d9cac7b837)

root@psg:/opt/splunk# ./bin/splunk start

Splunk> Australian for grep.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration...  Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _internal _introspectio
_thefishbucket cpu_memory cpu_performance disk_performanc
history main summary
        Done
```

```
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from
'/opt/splunk/splunk-7.1.3-51d9cac7b837-linux-2.6-x86_64-m
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done


Waiting for web server at http://127.0.0.1:8000 to be ava
Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://psg:8000

root@psg:/opt/splunk#
```

Running Splunk and connecting to Splunk using browser

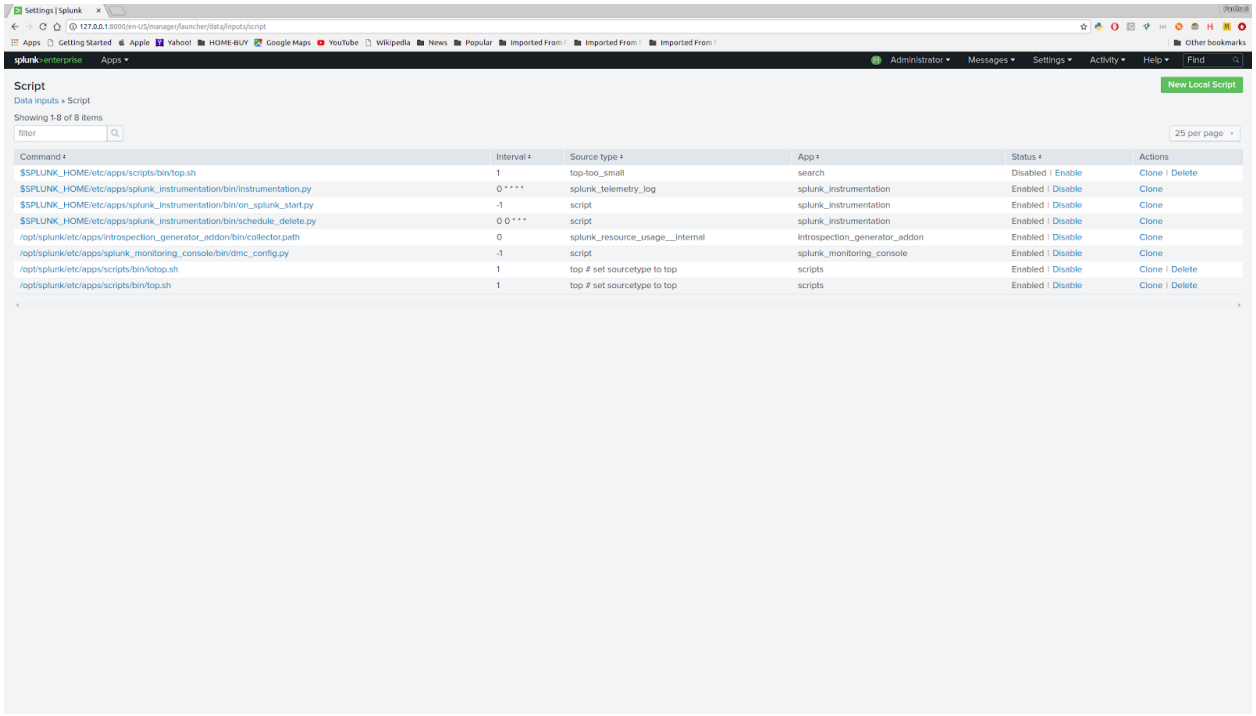


Creation of an App in Splunk to capture System Data

To create an application in splunk followed the steps in Splunk Documentation (1). Here is how the scripts looked like

```
root@psg:/opt/splunk/etc# find . -name "*top.sh"
./apps/scripts/bin/iotop.sh
./apps/scripts/bin/top.sh
root@psg:/opt/splunk/etc# find . -name "*top.sh" | xargs
#!/bin/bash
############
# author : psglinux@gmail.com
# script : script to store a file evey second with the to
############

#!/bin/bash

collect_iotop() {
```

```
    iotop -n 1 -b
}

collect_iotop
#!/bin/bash
############
# author : psglinux@gmail.com
# script : script to store a file evey second with the to
############

#!/bin/bash

collect_top() {
    top -n 1 -b
}

collect_top
root@psg:/opt/splunk/etc#
```

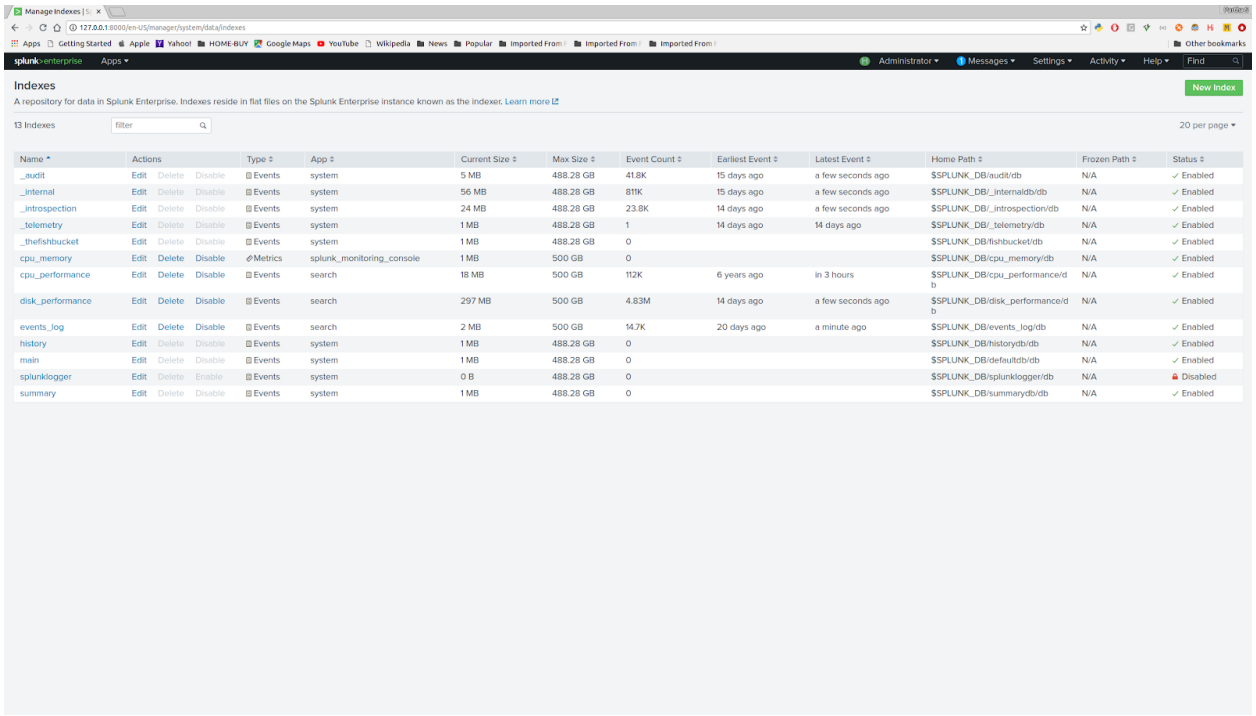


The last 2 scripts that are run every second to capture the system information in ubuntu Lin

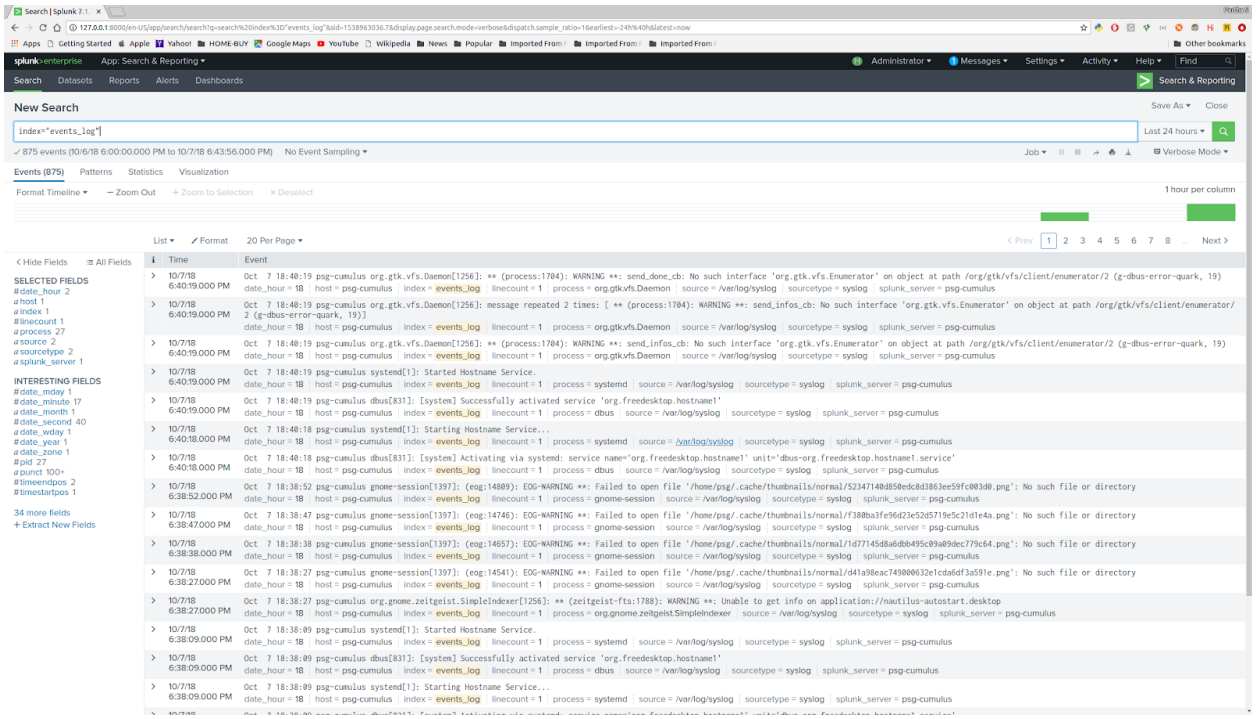
Task Set 1

- Configure Data inputs from UI or inputs.conf file to capture Event Viewer Logs CPU, Memory, Disk
- Create an index name “event_logs” under indexes
- Perform a search to Identify fields - “host”, “source”, “sourcetypes” from the index name- “event_logs”
- Identify “Security”, “System”, & “Application” from the index

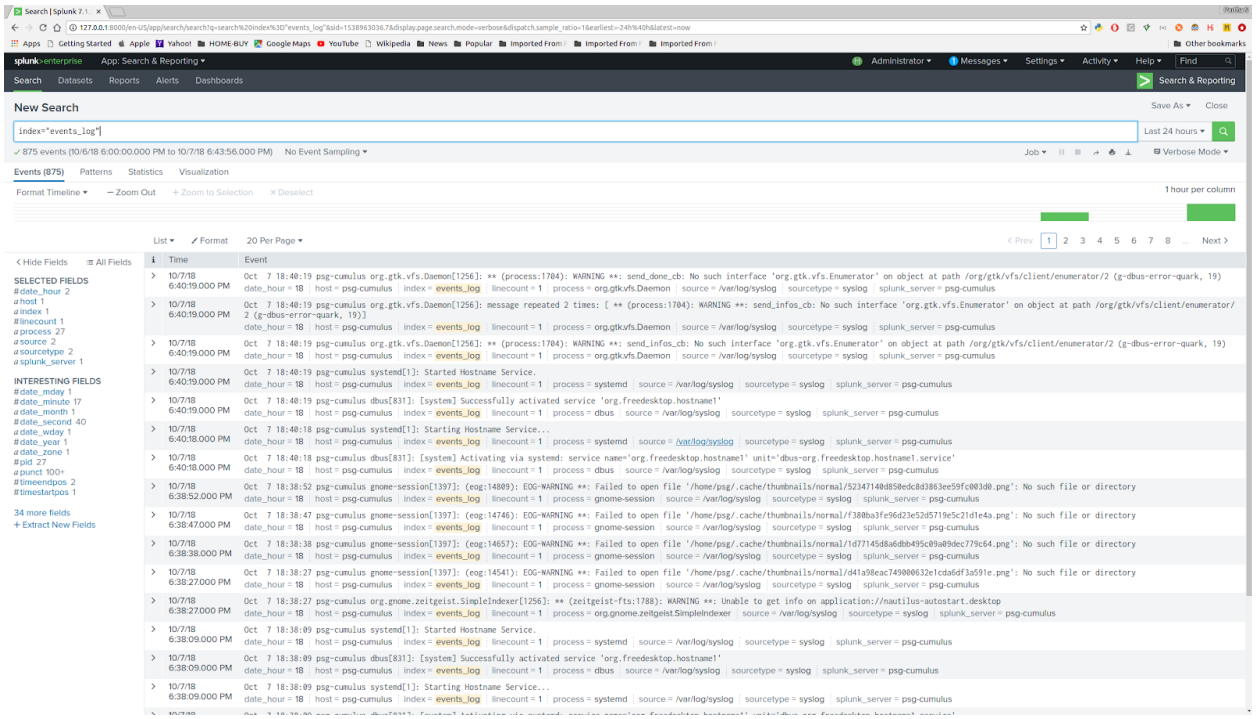
Indexes Created

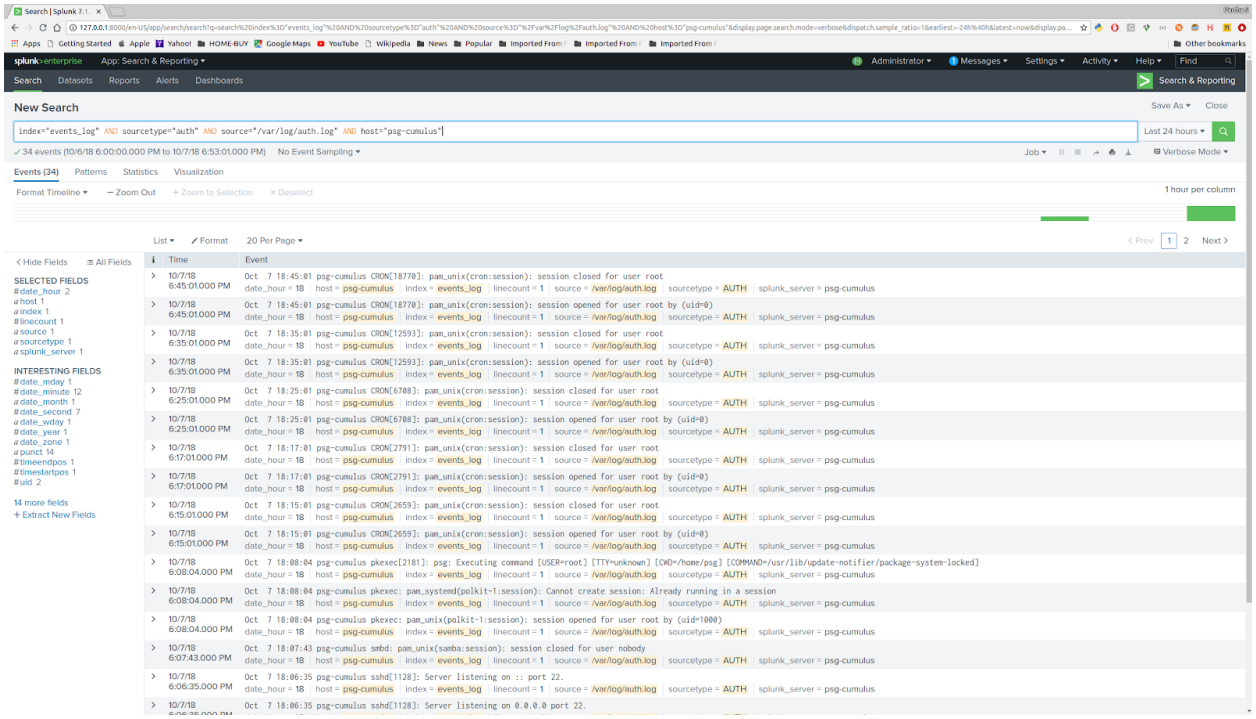


Events Log Search



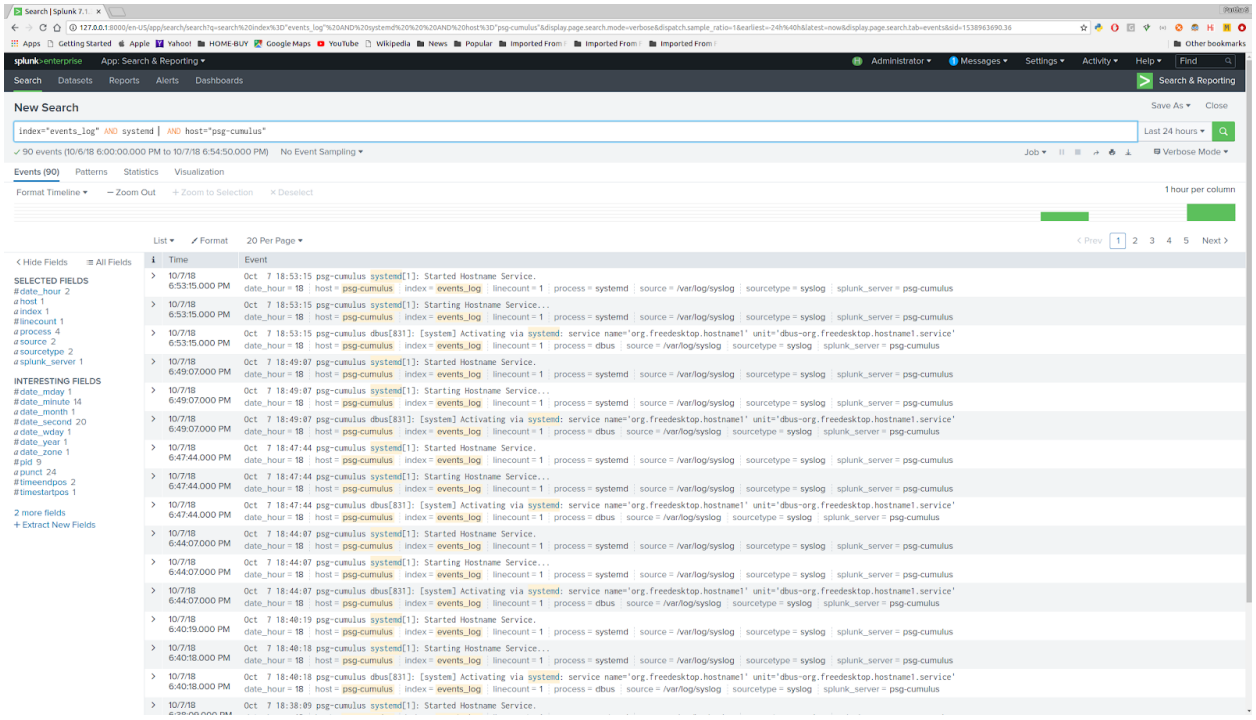
Security Logs

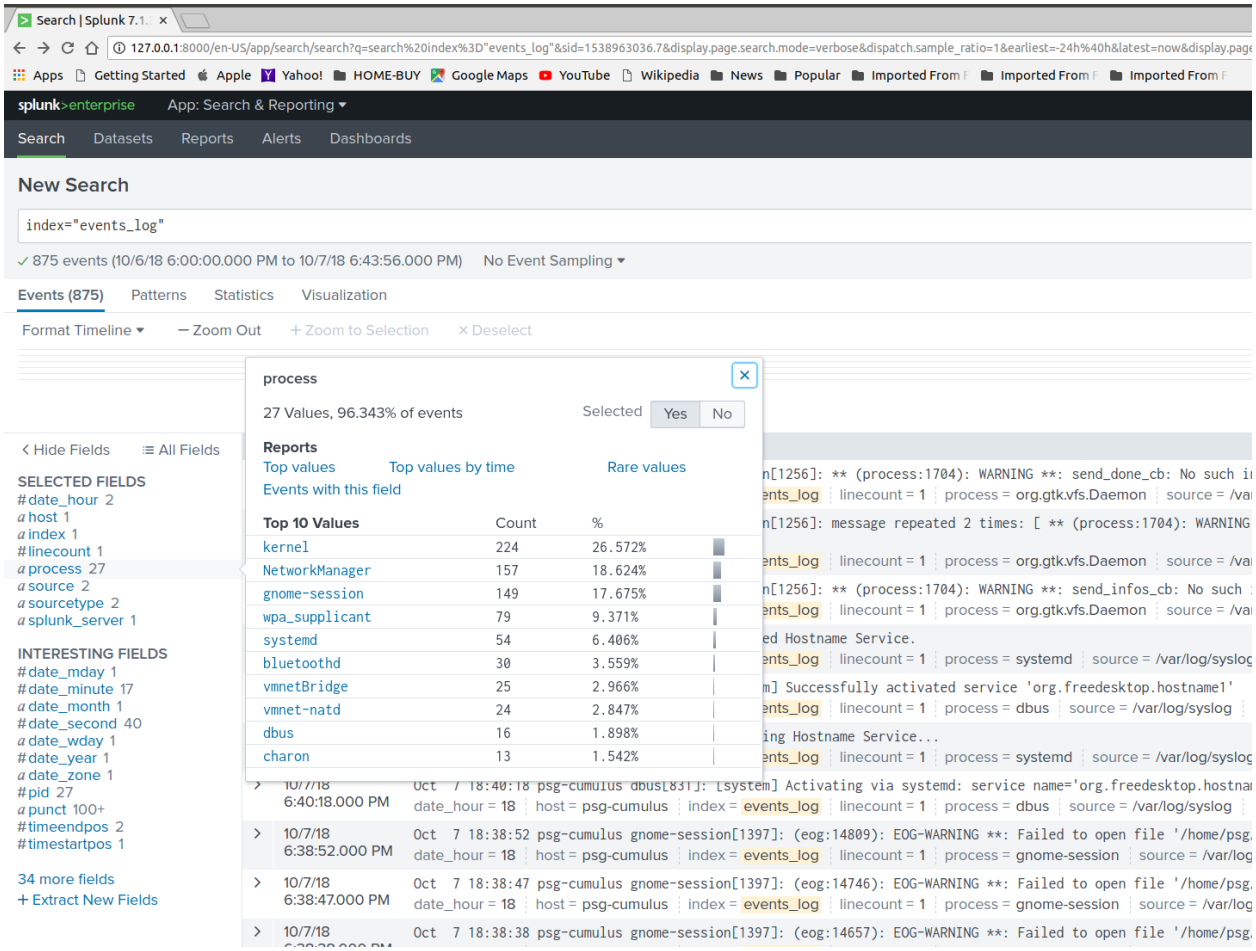




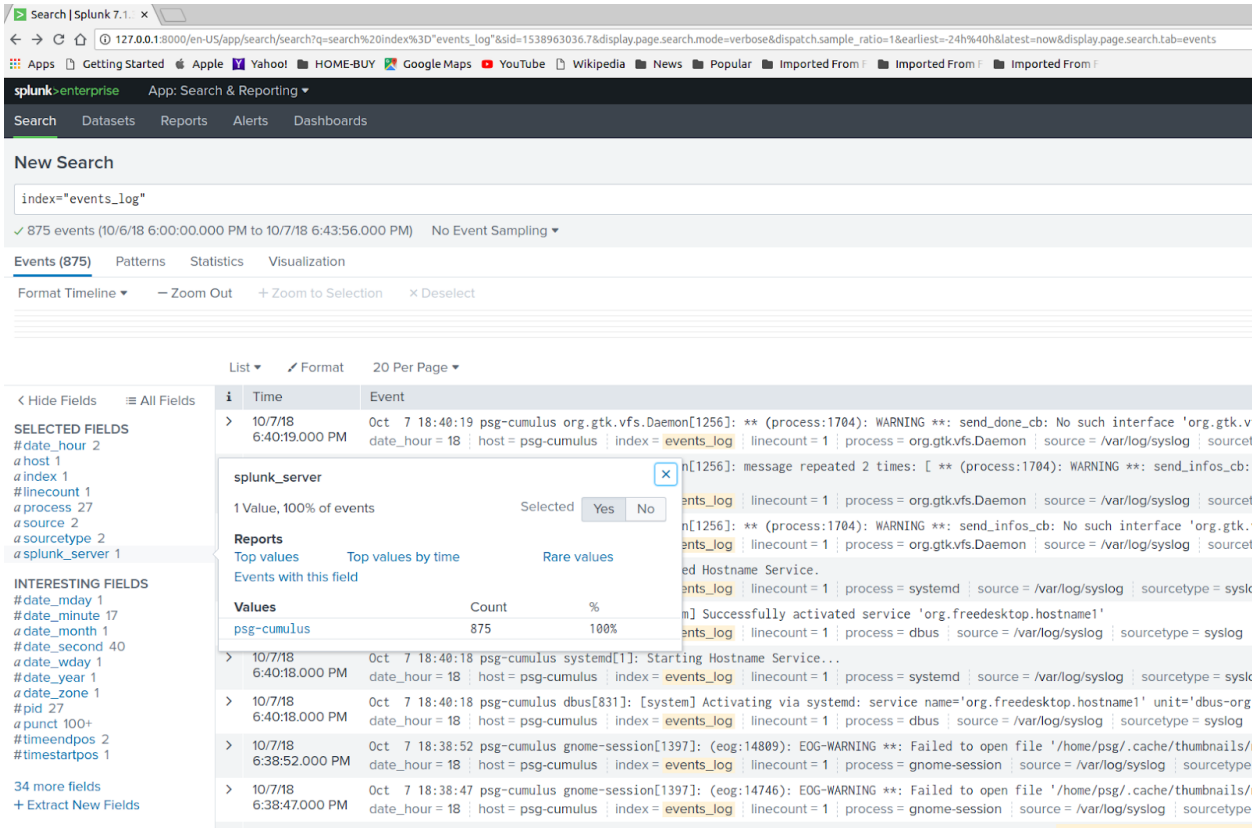
Applications

Captured the systemd logs as well as shown the total number of process info




Search | Splunk 7.1.
127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D"events_log"&sid=1538963036.7&display.page.search.mode=verbose&dispatch.sample_ratio=1&earliest=-24h%40h&latest=now&display.page
Apps
Getting Started
Apple
Yahoo!
HOME-BUY
Google Maps
YouTube
Wikipedia
News
Popular
Imported From
splunk>enterprise
App: Search & Reporting
Search
Datasets
Reports
Alerts
Dashboards
New Search
index="events_log"
875 events (10/6/18 6:00:00.000 PM to 10/7/18 6:43:56.000 PM)
No Event Sampling
Events (875)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
Hide Fields
All Fields
SELECTED FIELDS
#date_hour 2
a host 1
a index 1
#linecount 1
a process 27
a source 2
a sourcetype 2
a splunk_server 1
INTERESTING FIELDS
#date_mday 1
#date_minute 17
a date_month 1
#date_second 40
a date_wday 1
#date_year 1
a date_zone 1
#pid 27
a punct 100+
#timeendpos 2
#timestartpos 1
34 more fields
+ Extract New Fields
process
27 Values, 96.343% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
kernel 224 26.572%
NetworkManager 157 18.624%
gnome-session 149 17.675%
wpa_supplicant 79 9.371%
systemd 54 6.406%
bluetoothd 30 3.559%
vmnetBridge 25 2.966%
vmnet-natd 24 2.847%
dbus 16 1.898%
charon 13 1.542%
10/7/18 6:40:18.000 PM
10/7/18 6:38:52.000 PM
10/7/18 6:38:47.000 PM
10/7/18

System Logs



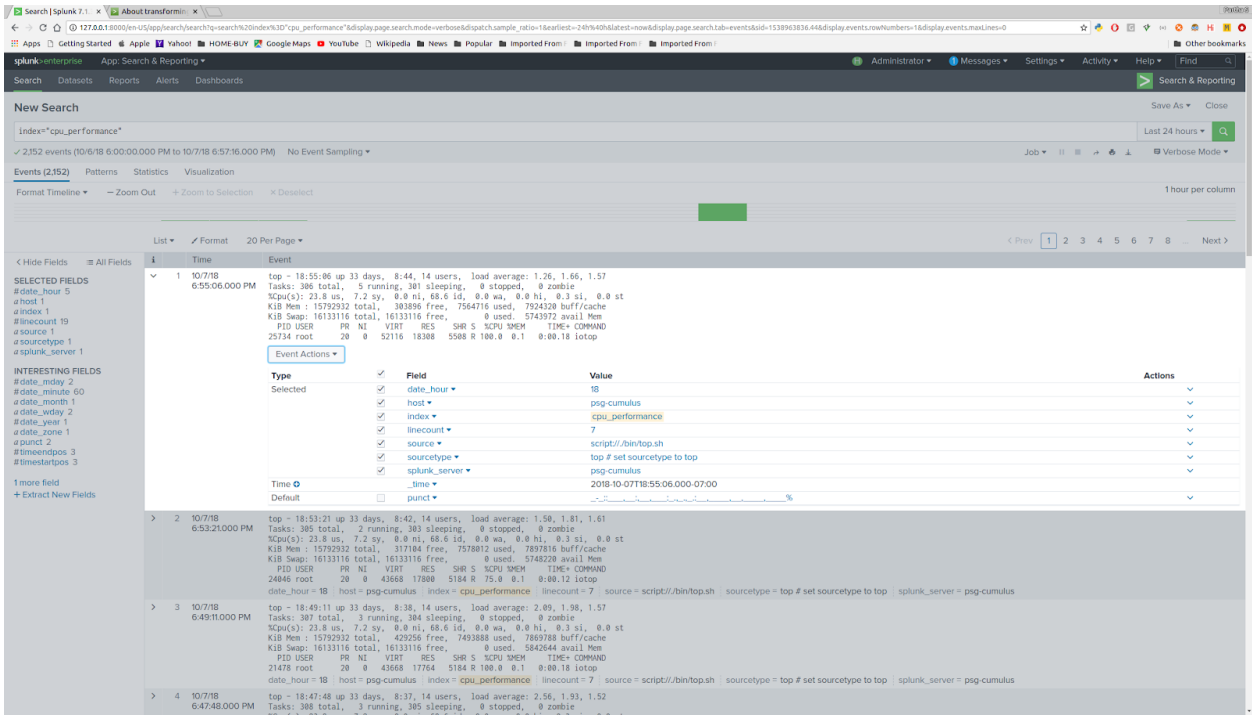
Task Set 2

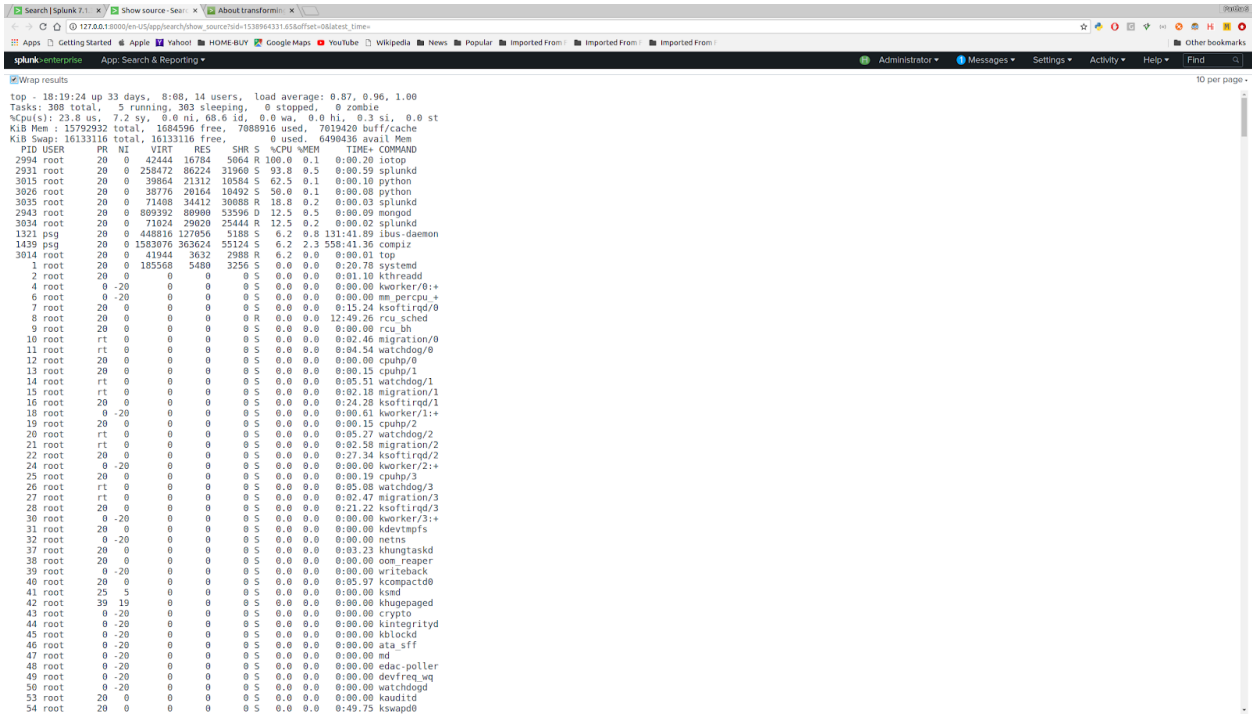
Using Splunk SPL Create Dashboards showing CPU, Memory to use the data

- Perform a search query to list values found of Disk, Memory and CPU
- Use stats or timechart syntax to depict actual values on a chart OR
- Use stats or timechart syntax to show avg utilization of Disk, memory & cpu in the last 15 minutes
- Use appropriate charting features to showcase the output and save them to a Dashboard

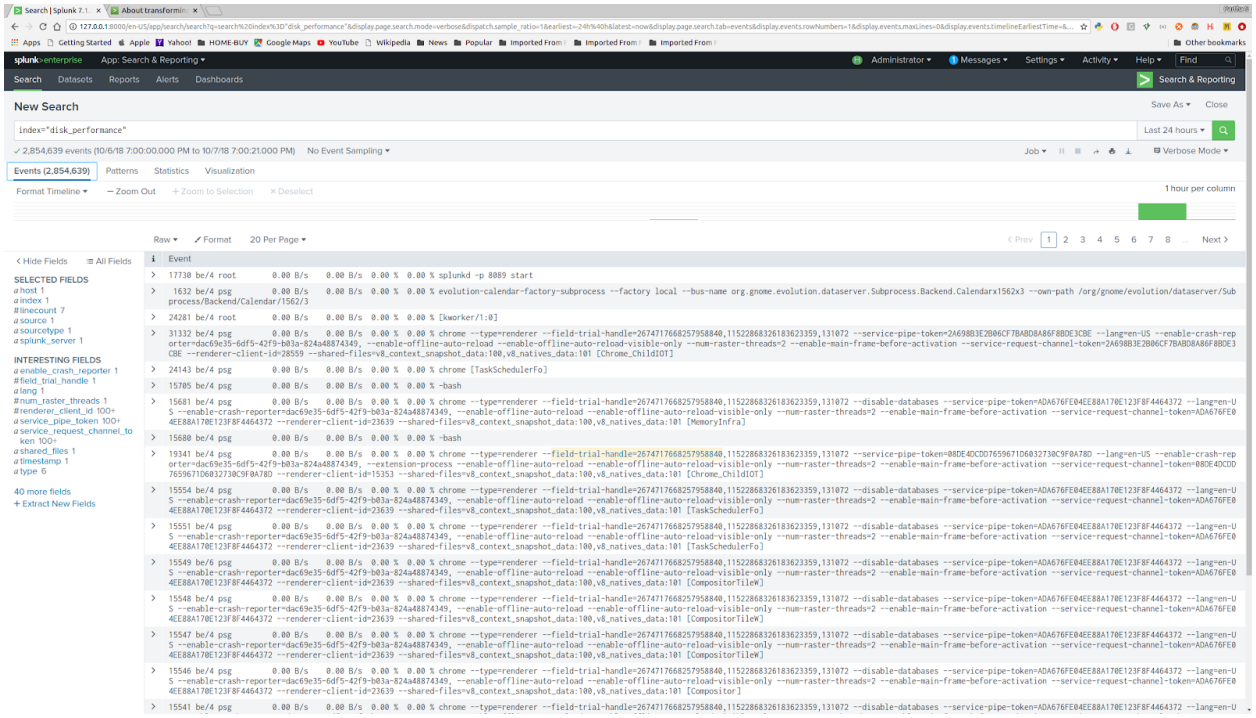
- Show the values on the graph (Optional)

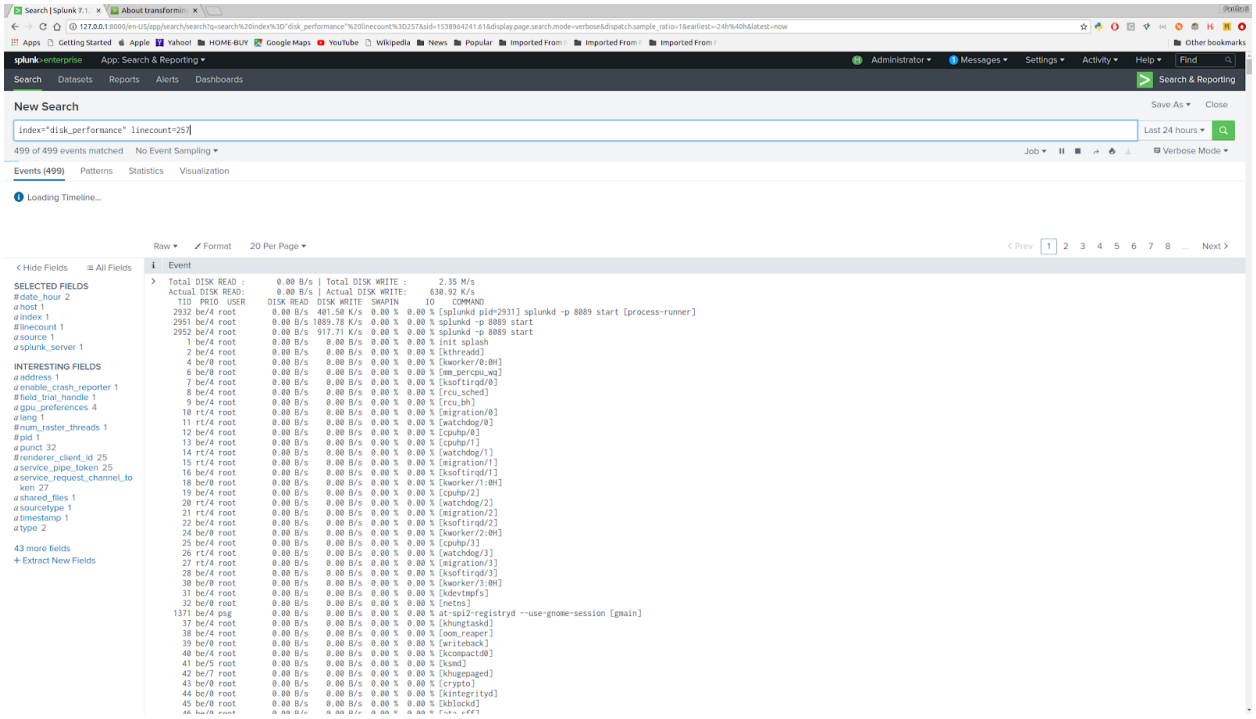
Search Query List for Memory and CPU



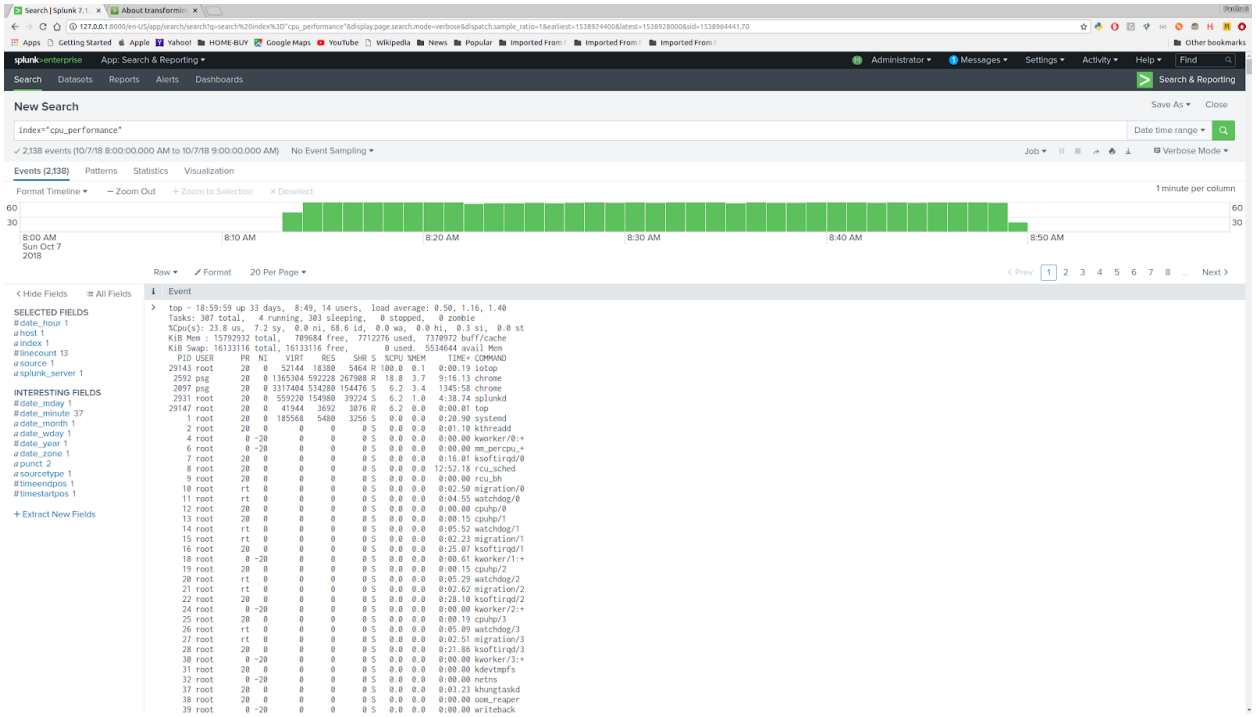


Disk I/O performance Data

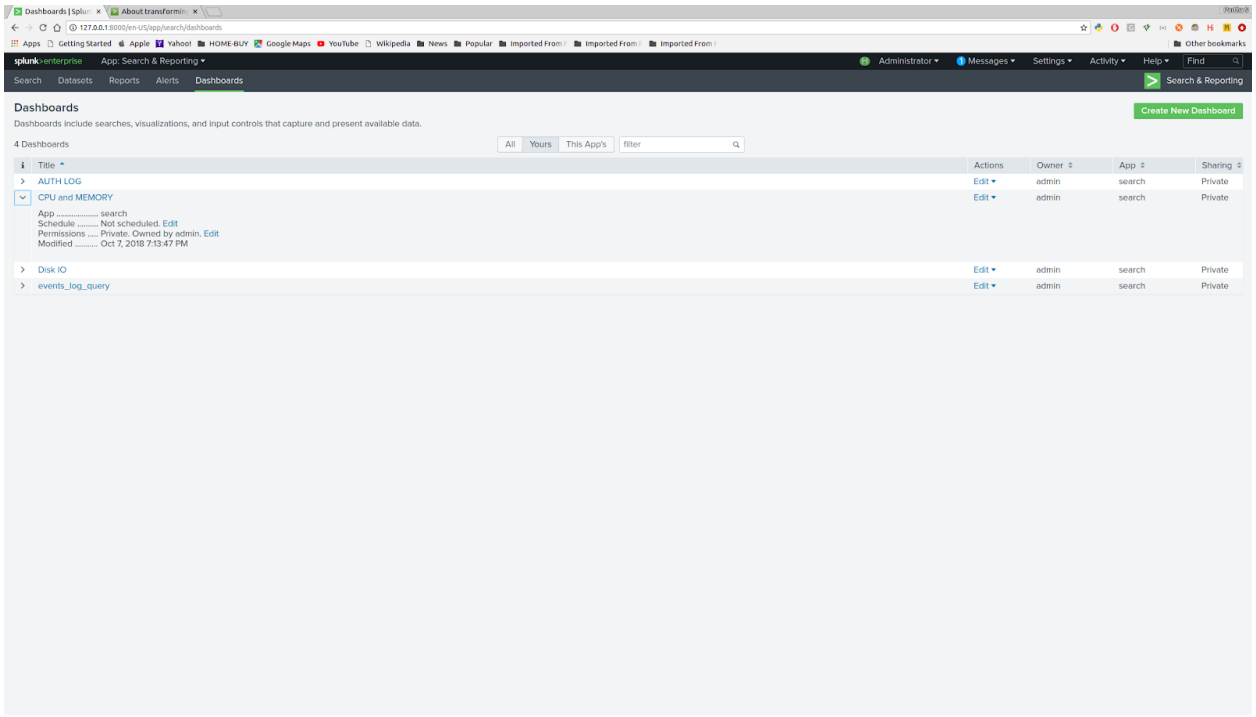




15 Minutes char for disk and CPU utilization



Charting feature to showcase the output and save them to dash board



Conclusion

1. Splunk seems to be a good tool for system monitoring
2. Conversion of Tabular Data to a time series data seems to be not well documented

References

1. Setting up data from a script top/iotop : http://docs.splunk.com/Documentation/Splunk/7.1.3/AdvancedDev/ScriptSetup

2. Formatting the tabular data : http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Multikv

   http://docs.splunk.com/Documentation/Splunk/7.1.3/Admin/Multikvconf#multikv.conf.example