

# 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](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

<b>Problem Statement</b>	<b>1</b>
<b>System Informations</b>	<b>3</b>
Operating System Used	3
Installed Splunk Version	3
Running Splunk and connecting to Splunk using browser	5
<b>Creation of an App in Splunk to capture System Data</b>	<b>5</b>
<b>Task Set 1</b>	<b>7</b>
Indexes Created	7
Events Log Search	8
Security Logs	8
Applications	9
System Logs	11
<b>Task Set 2</b>	<b>11</b>
Search Query List for Memory and CPU	12
Disk I/O performance Data	13
15 Minutes char for disk and CPU utilization	14
Charting feature to showcase the output and save them to dash board	15
<b>Conclusion</b>	<b>15</b>
<b>References</b>	<b>15</b>

## 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 options to 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.

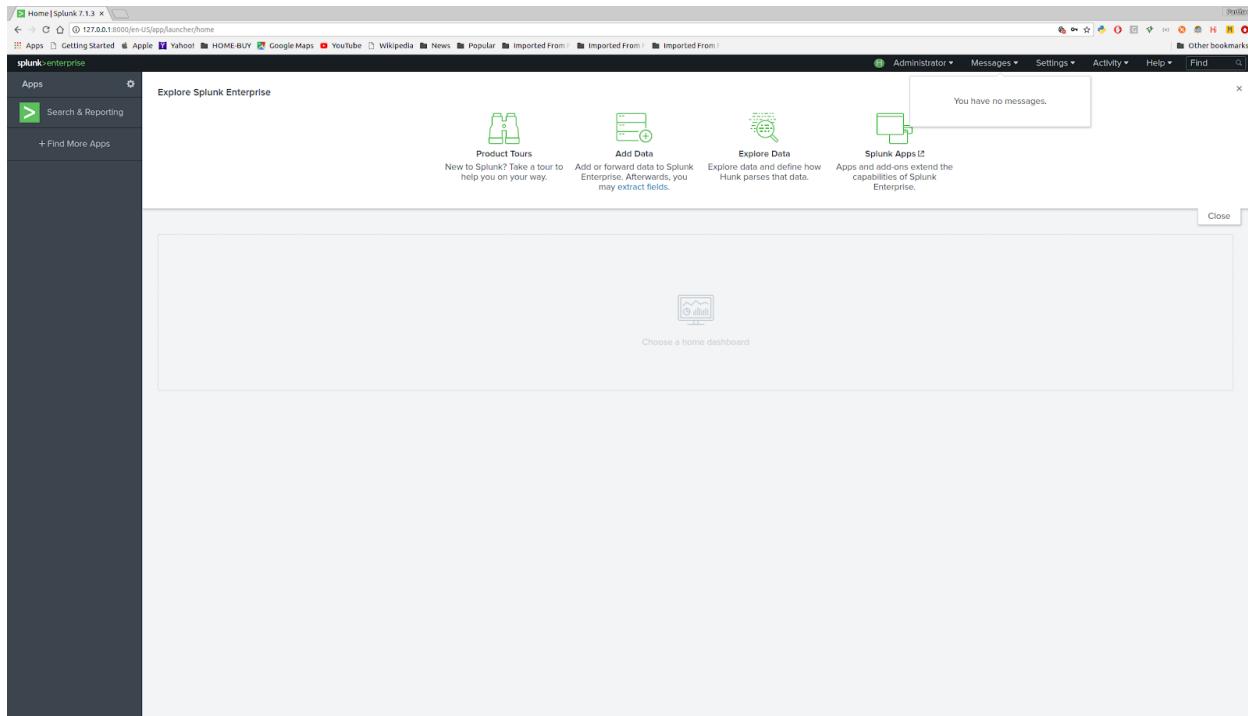
Starting splunk server daemon (splunkd)...
Done

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 : psqlinux@gmail.com
# script : script to store a file every second with the to
#####
#!/bin/bash

collect_iotop() {
```

```
iotop -n 1 -b  
}  
  
collect_iotop  
#!/bin/bash  
#####  
# author : psqlinux@gmail.com  
# script : script to store a file every second with the to  
#####  
  
#!/bin/bash  
  
collect_top() {  
    top -n 1 -b  
}  
  
collect_top  
root@psg:/opt/splunk/etc#
```

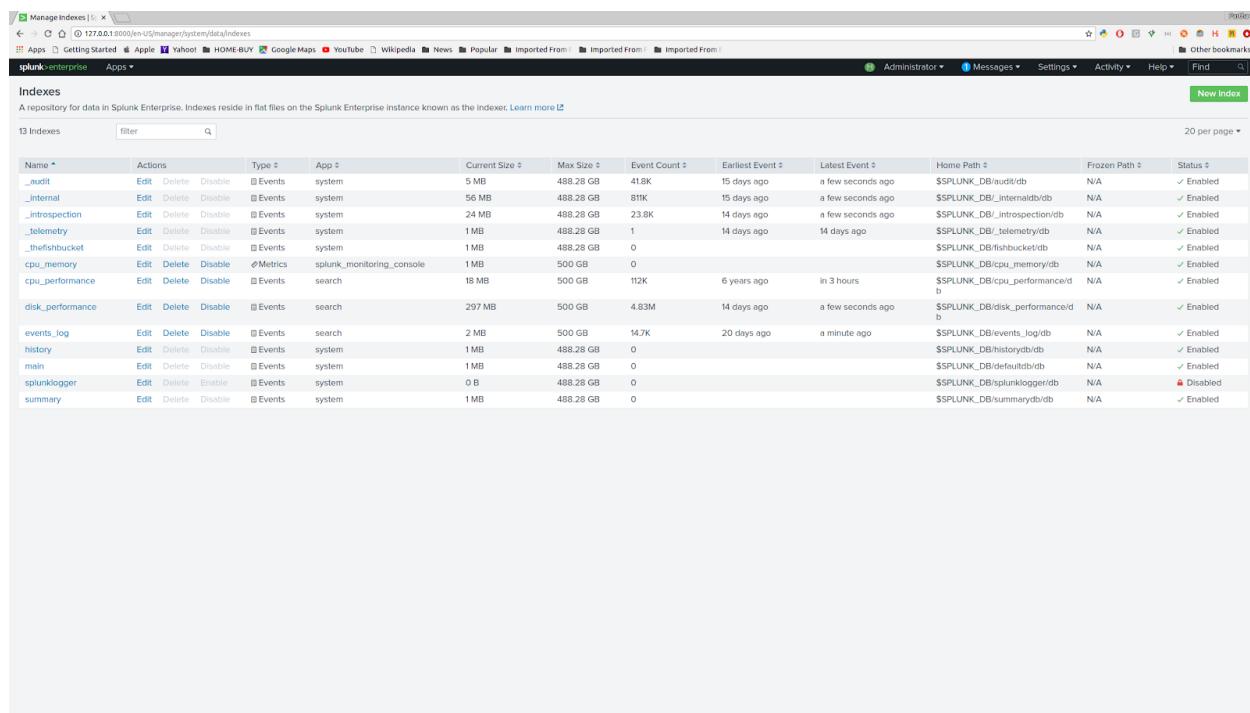
Command	Interval	Source type	App	Status	Actions
\$SPLUNK_HOME/etc/apps/scripts/bin/top.sh	1	top-too_small	search	Disabled   Enable	Clone   Delete
\$SPLUNK_HOME/etc/apps/splunk_instrumentation/bin/instrumentation.py	0 * * * *	splunk_telemetry_log	splunk_instrumentation	Enabled   Disable	Clone
\$SPLUNK_HOME/etc/apps/splunk_instrumentation/bin/on_splunk_start.py	-1	script	splunk_instrumentation	Enabled   Disable	Clone
\$SPLUNK_HOME/etc/apps/splunk_instrumentation/bin/schedule_delete.py	0 0 * * *	script	splunk_instrumentation	Enabled   Disable	Clone
/opt/splunk/etc/apps/introspection_generator-addon/bin/collector.path	0	splunk_resource_usage__internal	introspection_generator_addon	Enabled   Disable	Clone
/opt/splunk/etc/apps/splunk_monitoring_console/bin/dmc_config.py	-1	script	splunk_monitoring_console	Enabled   Disable	Clone
/opt/splunk/etc/apps/scripts/bin/iotop.sh	1	top # set sourcetype to top	scripts	Enabled   Disable	Clone   Delete
/opt/splunk/etc/apps/scripts/bin/top.sh	1	top # set sourcetype to top	scripts	Enabled   Disable	Clone   Delete

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

## 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



The screenshot shows the Splunk Enterprise 'Manage Indexes' page. At the top, there's a header bar with various icons and links. Below it, a navigation bar has 'splunk.enterprise' and 'Apps' selected. The main content area is titled 'Indexes' and contains a table with 13 rows. The columns in the table are: Name, Actions, Type, App, Current Size, Max Size, Event Count, Earliest Event, Latest Event, Home Path, Frozen Path, and Status. The table lists various system and monitoring indexes like '\_audit', '\_internal', '\_introspection', '\_telemetry', '\_thefishbucket', 'cpu\_memory', 'cpu\_performance', 'disk\_performance', 'events\_log', 'history', 'mem', 'splunklogger', and 'summary'. Most indexes are of type 'Events' and are associated with the 'system' app. The status column shows most are enabled, except for 'mem' which is disabled.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	5 MB	488.28 GB	41.8K	15 days ago	a few seconds ago	\$SPLUNK_DB/audit/db	N/A	✓ Enabled
_internal	Edit Delete Disable	Events	system	56 MB	488.28 GB	811K	15 days ago	a few seconds ago	\$SPLUNK_DB/internaldb/db	N/A	✓ Enabled
_introspection	Edit Delete Disable	Events	system	24 MB	488.28 GB	23.8K	14 days ago	a few seconds ago	\$SPLUNK_DB/introspection/db	N/A	✓ Enabled
_telemetry	Edit Delete Disable	Events	system	1MB	488.28 GB	1	14 days ago	14 days ago	\$SPLUNK_DB/telemetry/db	N/A	✓ Enabled
_thefishbucket	Edit Delete Disable	Events	system	1MB	488.28 GB	0			\$SPLUNK_DB/fishbucket/db	N/A	✓ Enabled
cpu_memory	Edit Delete Disable	Metrics	splunk_monitoring_console	1MB	500 GB	0			\$SPLUNK_DB/cpu_memory/db	N/A	✓ Enabled
cpu_performance	Edit Delete Disable	Events	search	18 MB	500 GB	112K	6 years ago	in 3 hours	\$SPLUNK_DB/cpu_performance/db	N/A	✓ Enabled
disk_performance	Edit Delete Disable	Events	search	297 MB	500 GB	4.83M	14 days ago	a few seconds ago	\$SPLUNK_DB/disk_performance/db	N/A	✓ Enabled
events_log	Edit Delete Disable	Events	search	2 MB	500 GB	14.7K	20 days ago	a minute ago	\$SPLUNK_DB/events_log/db	N/A	✓ Enabled
history	Edit Delete Disable	Events	system	1MB	488.28 GB	0			\$SPLUNK_DB/history/db	N/A	✓ Enabled
mem	Edit Delete Disable	Events	system	1MB	488.28 GB	0			\$SPLUNK_DB/default/db	N/A	✓ Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB/splunklogger/db	N/A	✗ Disabled
summary	Edit Delete Disable	Events	system	1MB	488.28 GB	0			\$SPLUNK_DB/summarydb/db	N/A	✓ Enabled

## Events Log Search

# Security Logs

## Applications

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

Search | Splunk 7.1

① 127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D"events\_log"&id=1538963690.36

Apps Getting Started Apple Yahoo! HOME-BUY Google Maps YouTube Wikipedia News Popular Imported From Imported From Imported From

splunk>enterprise App: Search & Reporting

New Search

Index="events\_log" AND system AND host="pgc-cumulus"

✓ 90 events (10/6/18 6:00:00,000 PM to 10/7/18 6:54:50,000 PM) No Event Sampling ▾

Events (90) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection X Deselect

1 hour per column

List Format 20 Per Page ▾

< Hide Fields ▄ All Fields

**SELECTED FIELDS**

- #date\_hour 2
- #host 1
- #index 1
- #linecount 1
- #process 4
- #source 2
- #sourceType 2
- #splunk\_server 1

**INTERESTING FIELDS**

- #date\_mday 1
- #date\_minute 14
- #date\_month 1
- #date\_second 20
- #date\_wday 1
- #date\_zone 1
- #pid 9
- #punct 24
- #timeendpos 2
- #timestartpos 1

2 more fields + Extract New Fields

Time	Event
Oct 6:53:15.000 PM	Oct 7 18:53:15 psg-cumulus system[1]: Started Hostname Service.
Oct 6:53:15.000 PM	Oct 7 18:53:15 psg-cumulus system[1]: Starting Hostname Service...
Oct 6:53:15.000 PM	Oct 7 18:53:15 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:53:15.000 PM	Oct 7 18:53:15 psg-cumulus [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 6:49:07.000 PM	Oct 7 18:49:07 psg-cumulus index=events_log  linecount=1  process = dbus   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:49:07.000 PM	Oct 7 18:49:07 psg-cumulus system[1]: Started Hostname Service.
Oct 6:49:07.000 PM	Oct 7 18:49:07 psg-cumulus system[1]: Starting Hostname Service...
Oct 6:49:07.000 PM	Oct 7 18:49:07 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:47:44.000 PM	Oct 7 18:47:44 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:47:44.000 PM	Oct 7 18:47:44 psg-cumulus system[1]: Started Hostname Service.
Oct 6:47:44.000 PM	Oct 7 18:47:44 psg-cumulus system[1]: Starting Hostname Service...
Oct 6:47:44.000 PM	Oct 7 18:47:44 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:44:44.000 PM	Oct 7 18:44:44 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:44:44.000 PM	Oct 7 18:44:44 psg-cumulus system[1]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 6:44:07.000 PM	Oct 7 18:44:07 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:44:07.000 PM	Oct 7 18:44:07 psg-cumulus system[1]: Started Hostname Service.
Oct 6:44:07.000 PM	Oct 7 18:44:07 psg-cumulus system[1]: Starting Hostname Service...
Oct 6:44:07.000 PM	Oct 7 18:44:07 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:40:19.000 PM	Oct 7 18:40:19 psg-cumulus system[1]: Started Hostname Service.
Oct 6:40:19.000 PM	Oct 7 18:40:19 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:40:18.000 PM	Oct 7 18:40:18 psg-cumulus system[1]: Starting Hostname Service...
Oct 6:40:18.000 PM	Oct 7 18:40:18 psg-cumulus index=events_log  linecount=1  process =systemd   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:40:18.000 PM	Oct 7 18:40:18 psg-cumulus [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 6:40:18.000 PM	Oct 7 18:40:18 psg-cumulus index=events_log  linecount=1  process = dbus   source = /var/log/syslog   sourcetype = syslog   splunk_server = psg-cumulus
Oct 6:38:38.000 PM	Oct 7 18:38:38 psg-cumulus system[1]: Started Hostname Service.
Oct 6:38:38.000 PM	Oct 7 18:38:38 psg-cumulus system[1]: Starting Hostname Service...

Search | Splunk 7.1

① 127.0.0.1:8000/en-US/app/search/search?q=search%20index%3D"events\_log"&id=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 F Imported From F Imported From F

splunk>enterprise App: Search & Reporting

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 X Deselect

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%

Oct 6:40:18.000 PM Oct 7 18:40:18 psg-cumulus dbus[831]: Lsystem] Activating via systemd: service name='org.freedesktop.hostname1'. date\_hour = 18 | host = psg-cumulus | index = events\_log | linecount = 1 | process = dbus | source = /var/log/syslog | sourcetype = syslog | splunk\_server = psg-cumulus

Oct 6:38:52.000 PM Oct 7 18:38:52 psg-cumulus gnome-session[1397]: (eog:14809): EOG-WARNING \*\*: Failed to open file '/home/psg. date\_hour = 18 | host = psg-cumulus | index = events\_log | linecount = 1 | process = gnome-session | source = /var/log/syslog | sourcetype = syslog | splunk\_server = psg-cumulus

Oct 6:38:47.000 PM Oct 7 18:38:47 psg-cumulus gnome-session[1397]: (eog:14746): EOG-WARNING \*\*: Failed to open file '/home/psg. date\_hour = 18 | host = psg-cumulus | index = events\_log | linecount = 1 | process = gnome-session | source = /var/log/syslog | sourcetype = syslog | splunk\_server = psg-cumulus

Oct 6:38:38.000 PM Oct 7 18:38:38 psg-cumulus gnome-session[1397]: (eog:14657): EOG-WARNING \*\*: Failed to open file '/home/psg. date\_hour = 18 | host = psg-cumulus | index = events\_log | linecount = 1 | process = gnome-session | source = /var/log/syslog | sourcetype = syslog | splunk\_server = psg-cumulus

# System Logs

Search | Splunk 7.1. x

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.search.tab=events

Apps Getting Started Apple Yahoo! HOME-BUY Google Maps YouTube Wikipedia News Popular Imported From F Imported From F Imported From F

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

List ▾ ✓ Format 20 Per Page ▾		
< Hide Fields	≡ All Fields	i Time Event
<b>SELECTED FIELDS</b>		> 10/7/18 Oct 7 18:40:19 psg-cumulus org.gtk.vfs.Daemon[1256]: ** (process:1704): WARNING **: send_done_cb: No such interface 'org.gtk.vfs.Daemon' [source=psg-cumulus index=events_log linecount=1 process=org.gtkvfs.Daemon source=/var/log/syslog sourcetype=syslog]
#date_hour 2		6:40:19.000 PM
a host 1		
a index 1		
#linecount 1		
a process 27		
a source 2		
a sourcetype 2		
a splunk_server 1		
<b>INTERESTING FIELDS</b>		
#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		

**splunk\_server**

1 Value, 100% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

Values	Count	%
psg-cumulus	875	100%

> 10/7/18 Oct 7 18:40:18 psg-cumulus systemd[1]: Starting Hostname Service...  
6:40:18.000 PM date\_hour = 18 host = psg-cumulus index = events\_log linecount = 1 process = systemd source = /var/log/syslog sourcetype = syslog

> 10/7/18 Oct 7 18:40:18 psg-cumulus dbus[831]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'  
6:40:18.000 PM date\_hour = 18 host = psg-cumulus index = events\_log linecount = 1 process = dbus source = /var/log/syslog sourcetype = syslog

> 10/7/18 Oct 7 18:38:52 psg-cumulus gnome-session[1397]: (eog:14809): EOG-WARNING \*\*: Failed to open file '/home/psg/.cache/thumbnails/  
6:38:52.000 PM date\_hour = 18 host = psg-cumulus index = events\_log linecount = 1 process = gnome-session source = /var/log/syslog sourcetype = syslog

> 10/7/18 Oct 7 18:38:47 psg-cumulus gnome-session[1397]: (eog:14746): EOG-WARNING \*\*: Failed to open file '/home/psg/.cache/thumbnails/  
6:38:47.000 PM date\_hour = 18 host = psg-cumulus index = events\_log linecount = 1 process = gnome-session source = /var/log/syslog sourcetype = syslog

# 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

This screenshot shows a complex interface for monitoring system performance, likely using Splunk or a similar log analysis tool. The top navigation bar includes links for 'Search', 'Databases', 'Reports', 'Alerts', and 'Dashboards'. A search bar at the top left contains the query 'cpu\_performance'. The main area is titled 'New Search' and displays a summary of 2,152 events from October 6, 2018, to October 7, 2018, between 6:00:00 PM and 6:57:16.000 PM. There is no event sampling applied.

The search results are presented in a table format with columns for 'Time' (including 'date\_hour' and 'date\_minsec'), 'Event', and 'Actions'. The table shows several entries, each detailing CPU usage statistics (top command, tasks, running processes, load average, memory usage, swap usage, PID, and source type). One entry is highlighted with a blue border, showing a detailed breakdown of CPU usage by process (psutil) and a specific event action (script://bin/top.sh).

Below the main search results, there is a separate section for 'INTERESTING FIELDS' and 'MORE FIELD' options. The bottom part of the interface shows a detailed log of system activity, with a scrollable list of log entries. The log includes various system logs such as 'kern.log', 'syslog', and 'splunkd.log', showing kernel messages, system calls, and logrotate errors.

## Disk I/O performance Data

Search Splunk 7.1.x | About transforms... More

http://127.0.0.1:8000/en-US/app/search/search?\_index=%20index%20disk\_performance%20linecount=25&\_id=1538964241.61&display=page.search.mode=verbose&dispatch.sample\_ratio=1&earliest=-2hr&latest=-now

Apps Getting Started Apple Yahoo! HOME BUY Google Maps youtube Wikipedia News Popular Imported From Imported From Imported From

splunkenterprise App: Search & Reporting \* Administrator Messages Settings Activity Help Find Search & Reporting

New Search

Search Datasets Reports Alerts Dashboards

index="disk\_performance" linecount=25|

499 of 499 events matched No Event Sampling \*

Events (499) Patterns Statistics Visualization

1 Loading Timeline...

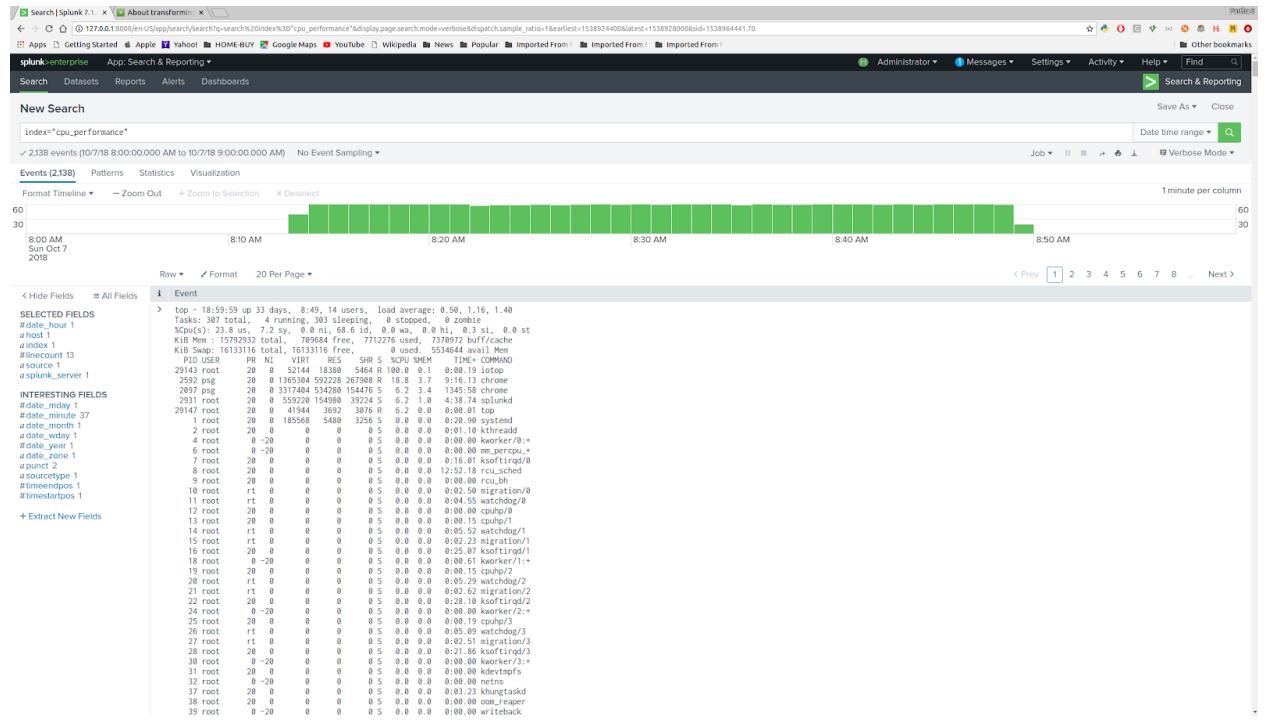
Raw Format 20 Per Page ▾

Event

Event
< Hide Fields □ All Fields
<b>SELECTED FIELDS</b>
#events=499
#host=1
#index=1
#linecount=1
#source=1
a_spunk_server=1
<b>INTERESTING FIELDS</b>
a_address=1
a_enable_crash_reporter=1
#field_trial_handle=1
a_gauge_preferences=4
a_lang=1
#num_rester_threads=1
a_punct=1
a_punct_32=1
#renderer_client_id=25
a_service_pipe_token=25
a_start_request_channel_to_kern=27
a_shared_files=1
a_startup_pipe=1
a_timestamping=1
a_type=2
43 more fields
+ Extract New Fields

Total DISK READ : 0.00 B/s | Total DISK WRITE : 2.35 M/s  
Actual DISK READ : 0.00 B/s | Actual DISK WRITE : 636.92 K/s  
TID PRIO USER DISK READ DISK WRITE SWAPIN IO COMMAND  
2932 be/4 root 0.00 B/s 1.58 K/s 0.00 % 0.00 % splunkd pid=2931] splunkd -p 8889 start [process-runner]  
2933 be/4 root 0.00 B/s 1.859 M/s 0.00 % 0.00 % splunkd pid=2932] splunkd -p 8889 start [process-runner]  
2952 be/4 root 0.00 B/s 917.71 K/s 0.00 % 0.00 % splunkd -p 8889 start [process-runner]  
1 be/4 root 0.00 B/s 0.08 B/s 0.00 % 0.00 % init splash  
2 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/0:0h]  
4 be/8 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/0:0h]  
6 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [mm\_percpu\_wq]  
7 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [ksched\_wq]  
8 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [ksched]  
9 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [rcu\_bh]  
10 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [migration/0]  
11 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [migration/0]  
12 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [cpuhp/0]  
13 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [cpuhp/1]  
14 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [cpuhp/1]  
15 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [migration/1]  
16 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kschedigrq/0]  
18 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/0:0h]  
19 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/0:0h]  
20 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [watchdog]  
21 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [migration/2]  
22 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/0:0h]  
24 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/2:0h]  
25 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [cpuhp/3]  
26 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [migration/3]  
27 rt/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [migration/3]  
28 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kschedigrq/3]  
29 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/3:0h]  
31 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kworker/3:0h]  
32 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [netns]  
1371 be/4 psg 0.00 B/s 0.00 B/s 0.00 % 0.00 % alt-splice-registrtryd --use-gnome-session [main]  
37 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [oom\_reaper]  
38 be/4 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [oom\_reaper]  
39 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [xrtbeck]  
40 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kmemcheckd0]  
41 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kmem]  
42 be/7 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kmemcgated]  
43 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [crypto]  
44 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [alt-splice-registrtryd]  
45 be/0 root 0.00 B/s 0.00 B/s 0.00 % 0.00 % [kblockd]

## 15 Minutes chart for disk and CPU utilization



## Charting feature to showcase the output and save them to dashboard

Title	Actions	Owner	App	Sharing
AUTH LOG	Edit	admin	search	Private
CPU and MEMORY	Edit	admin	search	Private
Disk IO	Edit	admin	search	Private
events_log_query	Edit	admin	search	Private

## 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>

