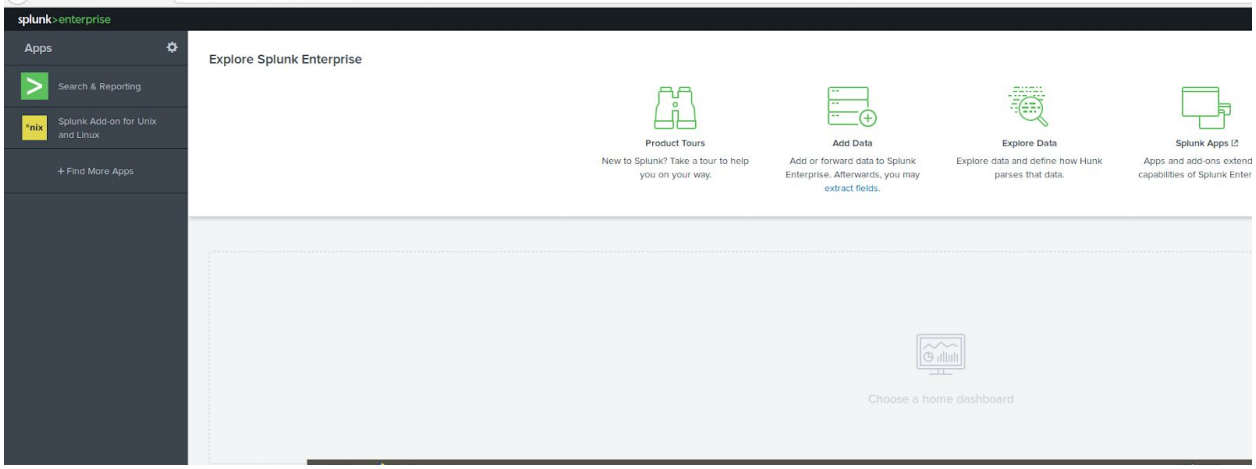
Cyber Defense Organization

SIEM Workshop Worksheet - Jonathan Matza 11/08/2019

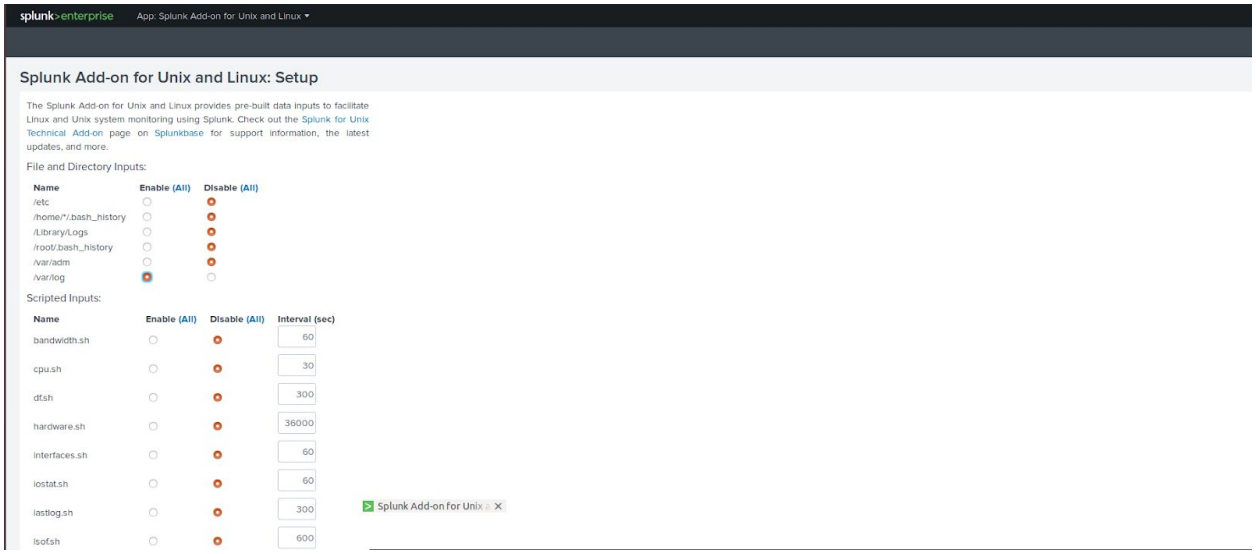
Splunk Workshop

1. Type in this command: **sudo /opt/splunk/bin/splunk start**
    a. to start up Splunk
2. Go to a firefox browser and type in: localhost:8000 (or port Splunk is going to bind to)
    a. admin
    b. bb123#123



Getting Log Data into Splunk:

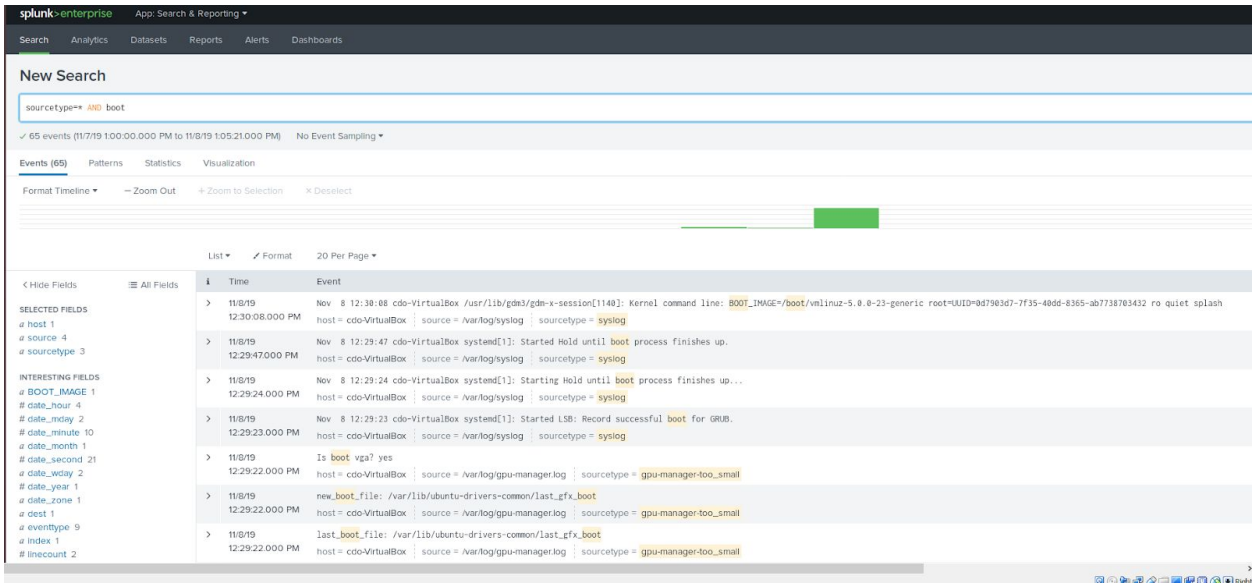
1. Go to the Unix Linux Add-On App (look at board for explanation)
2. Click on enable **/var/log** monitoring. This is where most of your logs are located.



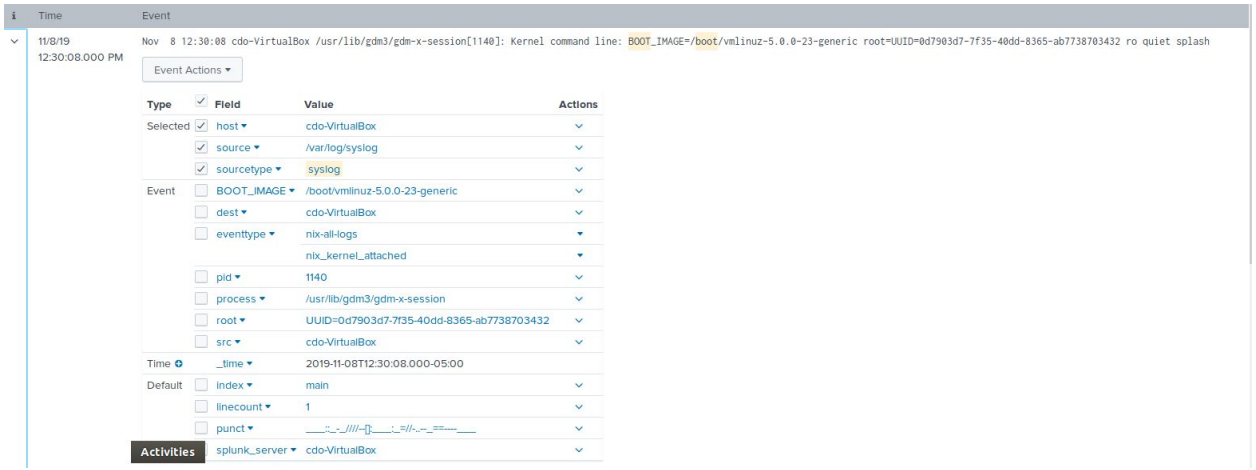
3. Scroll all the way down and click save
4. Wait a minute for Splunk to index the data

Looking at Search

1. Go to the search and reporting app
2. Type in this search: boot AND sourcetype=*



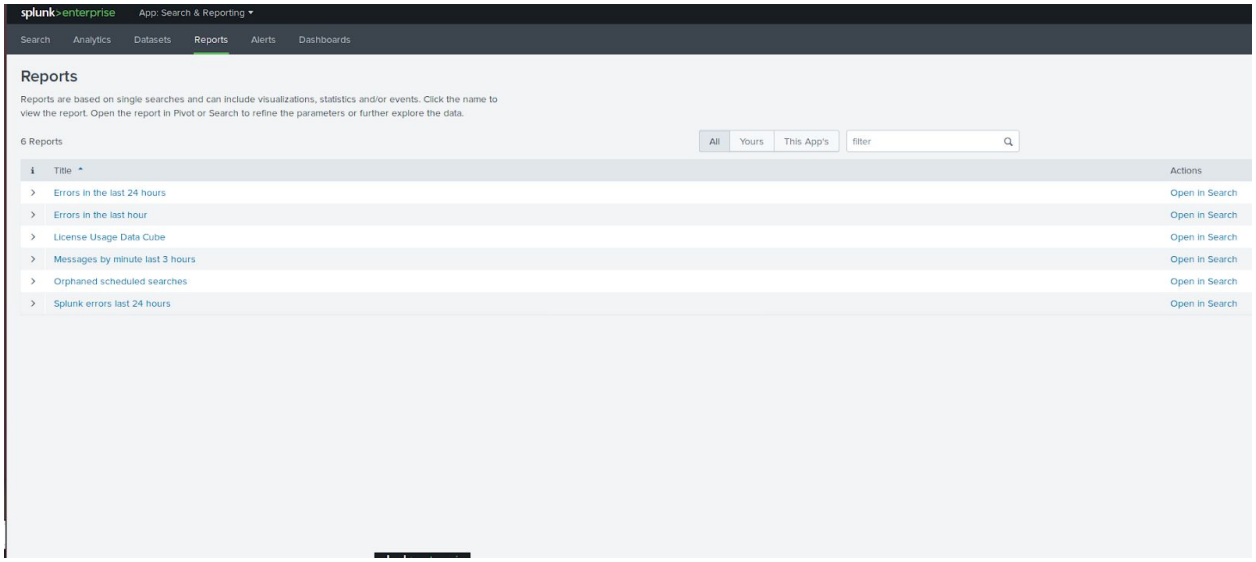
3. Check out the host, the field, and all of the aspects of the results (click arrow button)



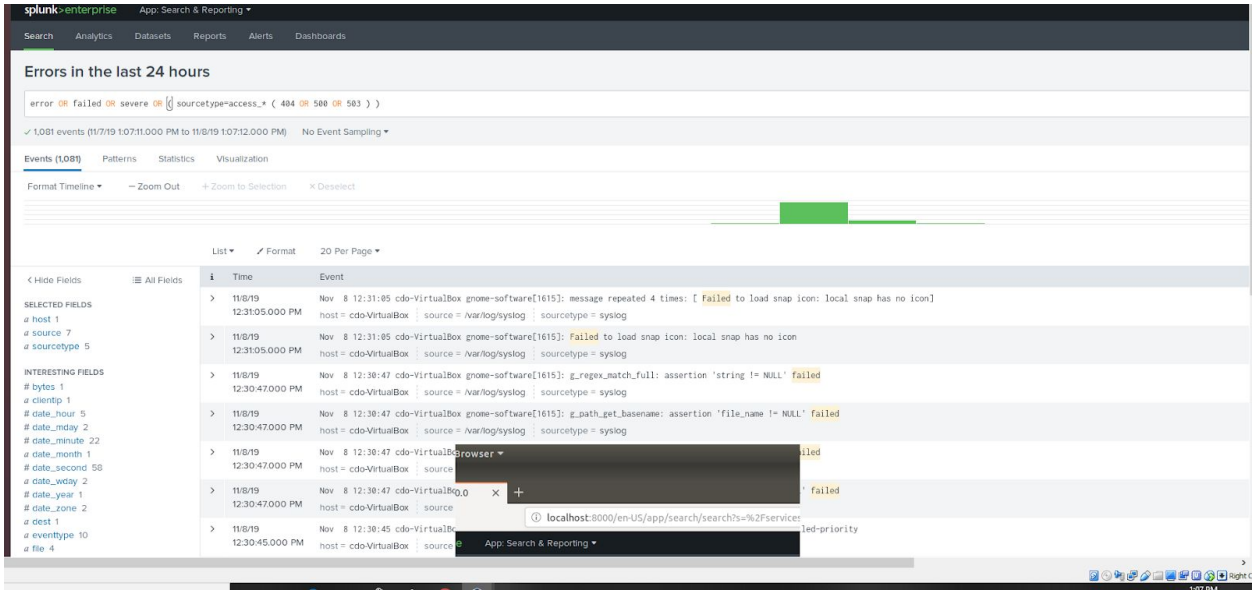
4. Use Event Sampling: 1:100 to see 1 result in 100

Report Creation

1. Go to the search and reporting app.
2. Click on **Reports tab**. Look at the **"Errors in the last 24 hours"** report. Click Open in Search



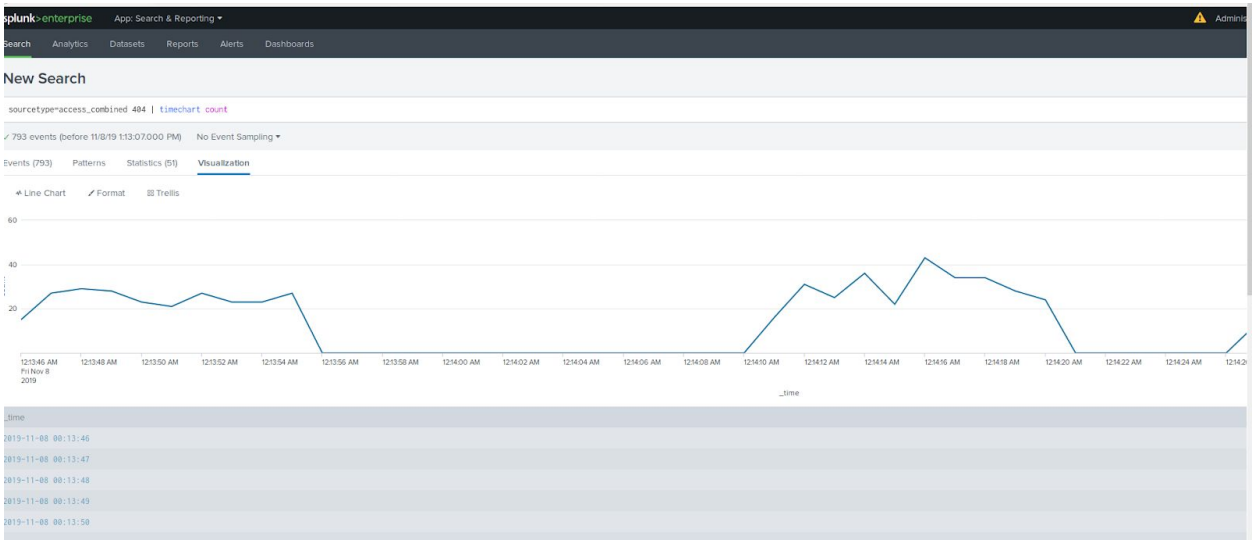
3. Look at the search query, the permissions, scheduling, etc



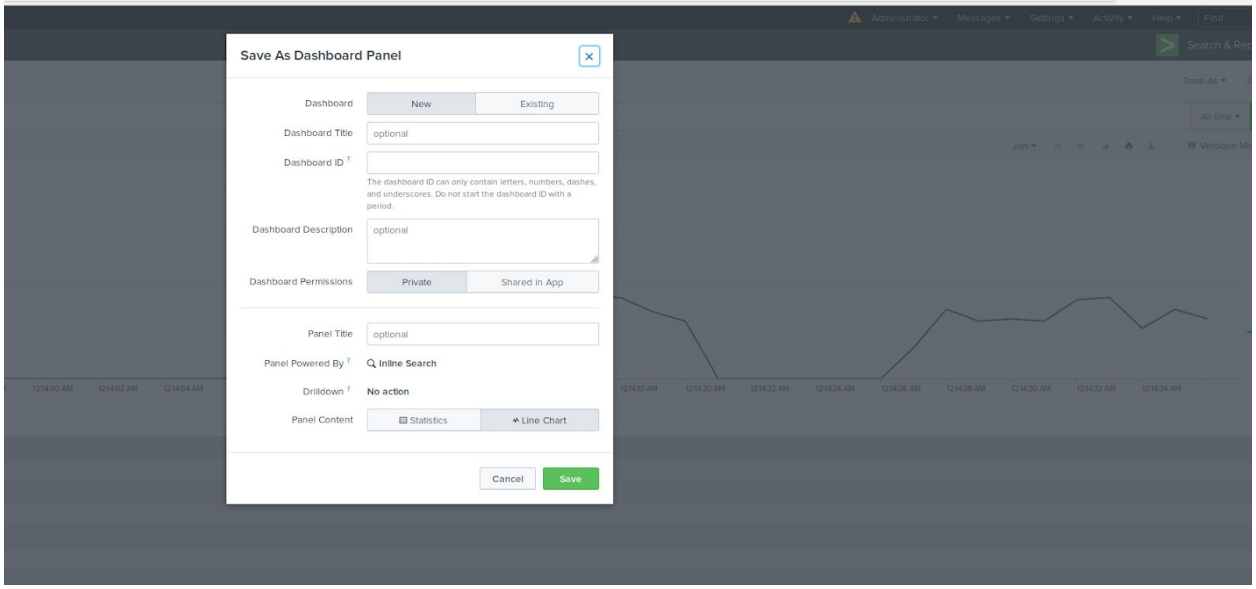
4. Lets Create our own report: go to the search tab and search for this: sourcetype=”access_combined” AND 404
5. Click Save AS and save it as a report

Dashboard Creation

1. Type in this search: sourcetype=”access_combined” AND 404 | timechart count
2. Go to the visualization tab, experiment with the chart options, click on line chart



3. Click Save As Dashboard Panel

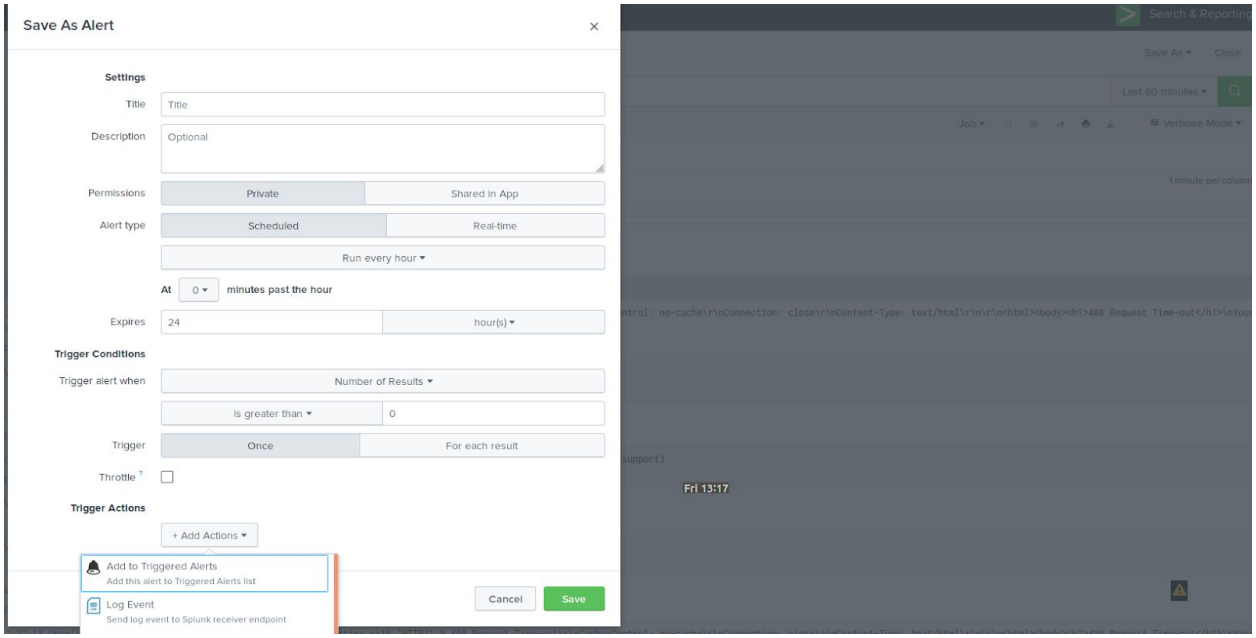


4. Name it something like 404 errors

Alerts

Go to the search and reporting app

1. Go to search app, type in something you want to be alerted about
2. So lets do the same search as before, change it to an 1 hour search window
3. Click Save As Alert
4. Check out Trigger actions and check off “add to triggered alerts”



Lets go digging:

1. Use what you learned above in search to figure out why there are so many 404 errors
2. Think about what you should search to look for logs with 404 data