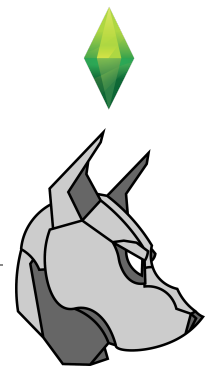


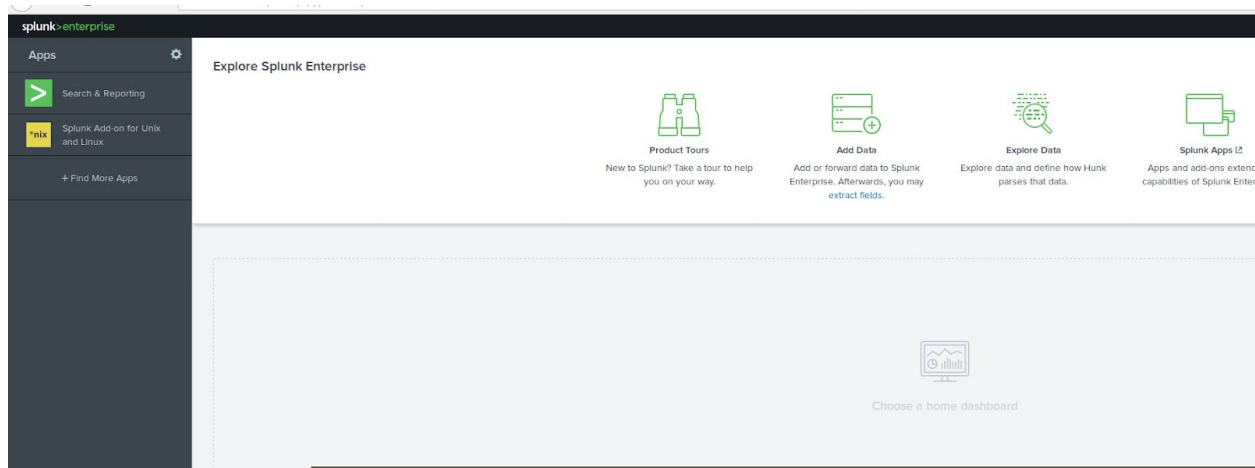
Cyber Defense Organization



SIEM Workshop Worksheet - Jonathan Matza 11/08/2019

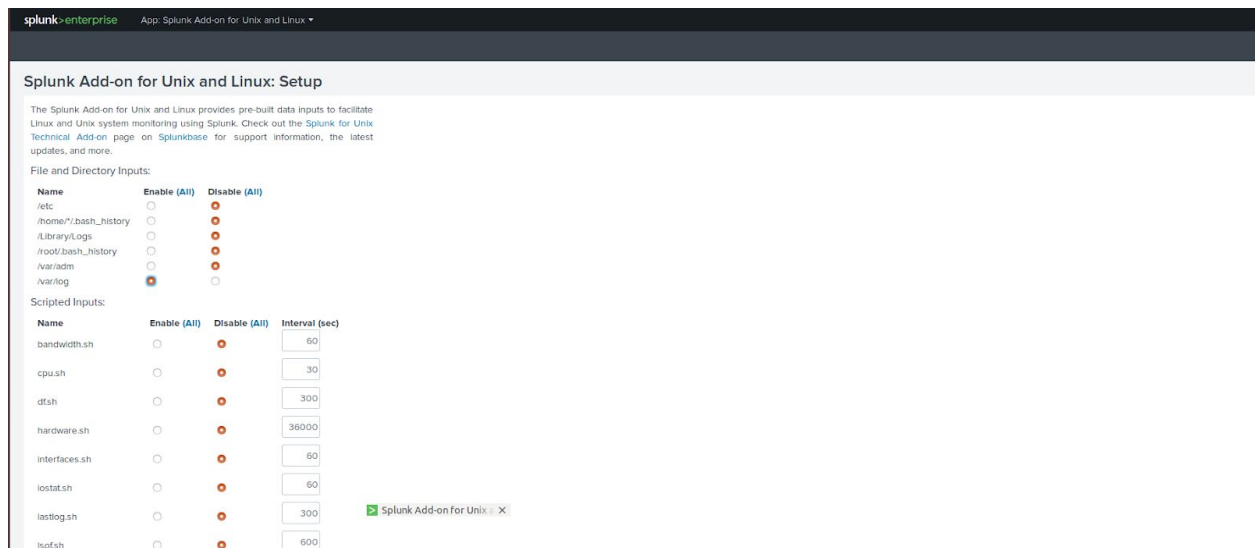
Splunk Workshop

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=*`

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query `sourcetype=* AND boot`. The results are displayed in a list view, showing various system logs and boot-related events. The interface includes a search bar, a results table, and a sidebar with field lists.

Time	Event
Nov 8 12:30:08 PM	cdo-VirtualBox /usr/lib/gdm3/gdm-x-session[1140]: Kernel command line: <code>BOOT_IMAGE=/boot/vmlinuz-5.0.0-23-generic root=UUID=0d7903d7-7f35-40dd-8365-ab7738703432 ro quiet splash</code>
Nov 8 12:29:47 PM	cdo-VirtualBox systemd[1]: Started Hold until boot process finishes up.
Nov 8 12:29:24 PM	cdo-VirtualBox systemd[1]: Starting Hold until boot process finishes up...
Nov 8 12:29:23 PM	cdo-VirtualBox systemd[1]: Started LSB: Record successful boot for GRUB.
Nov 8 12:29:22 PM	cdo-VirtualBox Is boot vga? yes
Nov 8 12:29:22 PM	cdo-VirtualBox new_boot_file: /var/lib/ubuntu-drivers-common/last_gfx_boot
Nov 8 12:29:22 PM	cdo-VirtualBox last_boot_file: /var/lib/ubuntu-drivers-common/last_gfx_boot

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

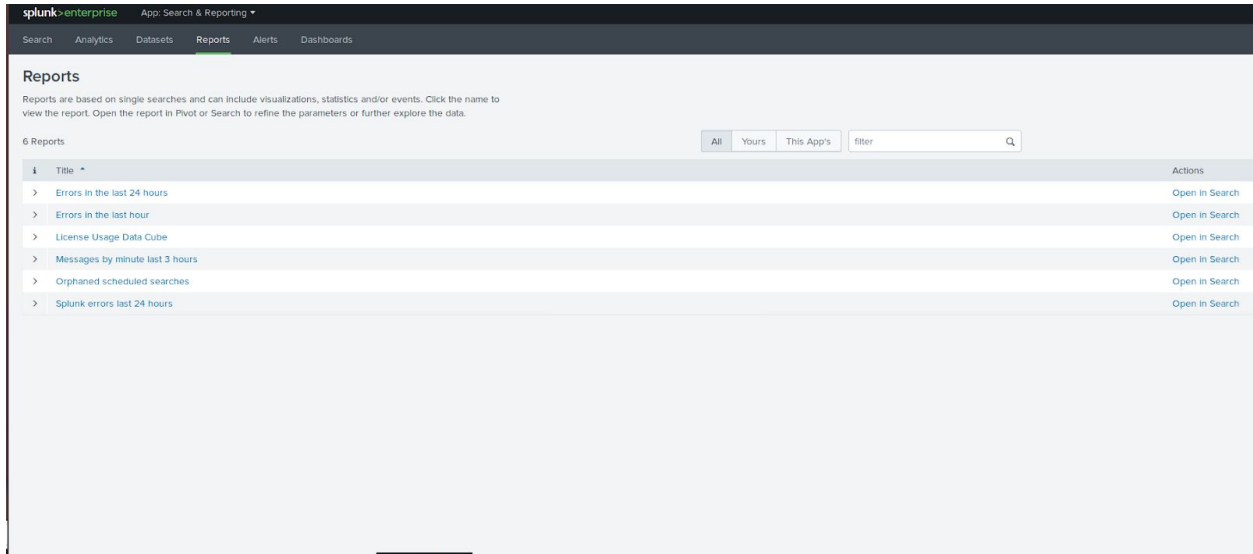
The screenshot shows the Splunk Search & Reporting interface with a detailed view of a search result. The interface displays the event details, including the host, source, sourcetype, and various fields like `BOOT_IMAGE`, `dest`, `eventtype`, `pid`, `process`, `root`, and `src`. The interface also shows the time, default, and punct fields.

Type	Field	Value	Actions
Selected	host	cdo-VirtualBox	
	source	/var/log/syslog	
	sourcetype	syslog	
Event	BOOT_IMAGE	/boot/vmlinuz-5.0.0-23-generic	
	dest	cdo-VirtualBox	
	eventtype	nix-all-logs	
	pid	1140	
	process	/usr/lib/gdm3/gdm-x-session	
	root	UUID=0d7903d7-7f35-40dd-8365-ab7738703432	
	src	cdo-VirtualBox	
Time	_time	2019-11-08T12:30:08.000-05:00	
Default	index	main	
	linecount	1	
	punct		
Activities	splunk_server	cdo-VirtualBox	

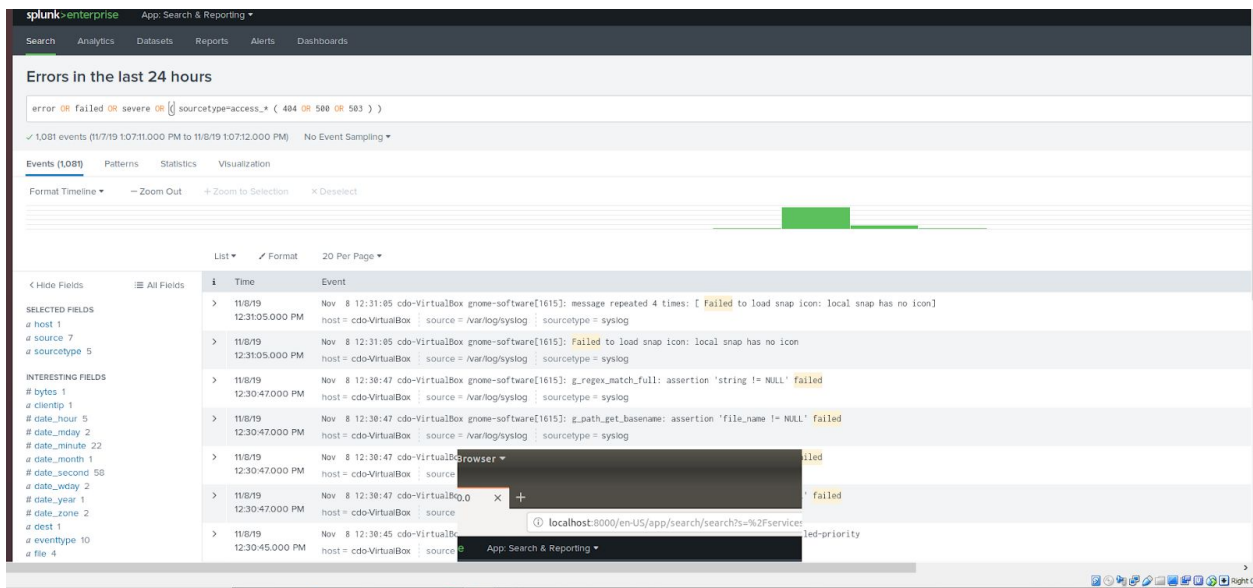
4. Use Event Sampling: 1:100 to see 1 result in 100

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



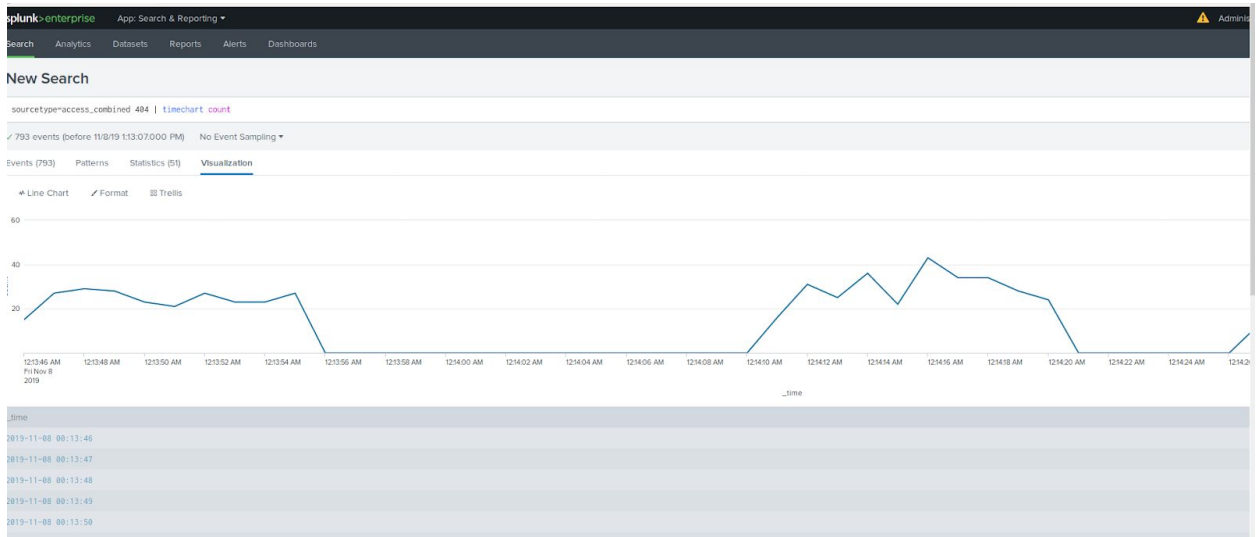
3. Look at the search query, the permissions, scheduling, etc



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

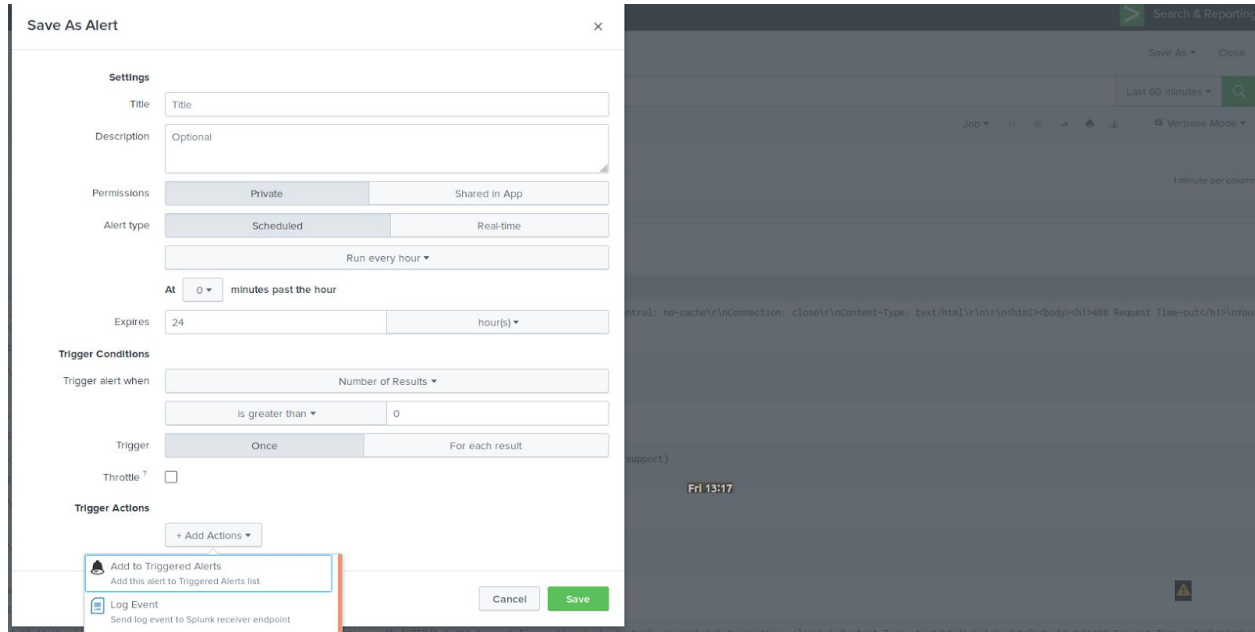
The screenshot shows the 'Save As Dashboard Panel' dialog box. The dialog has several sections: Dashboard (New/Existing), Dashboard Title (optional), Dashboard ID (optional), Dashboard Description (optional), Dashboard Permissions (Private/Shared in App), Panel Title (optional), Panel Powered By (Inline Search), Drilldown (No action), and Panel Content (Statistics/Line Chart). The 'Save' button is highlighted in green.

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