
DEV/SECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK FOUR/ LESSON ONE

Agenda

- Splunk Basics
 - Why Splunk?
 - What is an index
 - Data classification
- Splunk commands

Splunk Basics

- Why Splunk?
 - De facto log aggregation and analysis tools
 - Enables us to
 - monitor for security threats across disparate environment
 - analyze and identify anomalous behavior
 - automate initiation of incident response procedures
 - build metrics to visualize our resource
 - Correlate data streams to discover meaningful security events

Splunk Basics

- What is an Index?
 - A bucket of data, commonly logs
 - Default index is main, e.g., `index=main`
- What can you do with an index?
 - Separate and query data type or classification
 - Access controls to data
 - Retention policy, by time or size
 - Performance tuning, sharding

Splunk Basics

- Data classification
 - Index – data bucket
 - Source – where the data came from, e.g., `/var/log/messages`
 - Sourcetype – the data type, often auto detected by Splunk
 - Splunk will attempt to automatically detect the source type based on predefined patterns

Splunk Basics

The screenshot shows the Splunk Enterprise web interface. The top navigation bar includes the Splunk logo, user name 'student1', and links for Messages, Settings, Activity, and Help. A search bar is also present. The left sidebar shows 'Apps' with a gear icon, and 'Search & Reporting' is highlighted with a red box. The main content area is titled 'Explore Splunk Enterprise' and features four circular icons with corresponding text:

- Product Tours**: New to Splunk? Take a tour to help you on your way.
- Search Manual**: Use the Splunk Search Processing Language (SPL).
- Pivot Manual**: Use Pivot to create tables and charts with SPL.
- Dashboards & Visualizations**: Create and edit dashboards using interactive editors or simple XML.

A 'Close' button is located in the top right corner of the main content area. Below the icons, there is a large dashed rectangular box, and at the bottom, there are some abstract bar and line charts.

Splunk Basics

The screenshot shows the Splunk Search & Reporting interface. The top navigation bar includes the Splunk logo, the app name 'Search & Reporting', and user settings for 'student1'. Below this is a green navigation bar with tabs for Search, Pivot, Reports, Alerts, and Dashboards. The main search bar is highlighted with a red rectangle and contains the placeholder text 'enter search here...'. To the right of the search bar are filters for 'Last 4 hours' and a search icon. Below the search bar, a red arrow points to the 'No event Sampling' dropdown menu. The interface is divided into three main sections: 'How to Search' with links to 'Documentation' and 'Tutorial', 'What to Search' with a 'Data Summary' button and event statistics (1,596,412 Events INDEXED, 6 years ago EARLIEST EVENT, a few seconds ago LATEST EVENT), and 'Search History' with a link to 'Expand your search history'.

How to Search
If you aren't familiar with searching in Splunk, or want to learn more, checkout one of the following resources.

[Documentation](#) [Tutorial](#)

What to Search
1,596,412 Events INDEXED
6 years ago EARLIEST EVENT
a few seconds ago LATEST EVENT
[Data Summary](#)

Search History
[Expand your search history.](#)

Splunk Basics

splunk App: Search & Reporting student1 Messages Settings Activity Help Find

Search Pivot Reports Alerts Dashboards Search & Reporting

New Search

index=main | Last 4 hours |

✓ 31,037 events (6/15/16 3:27:00.000 PM to 6/15/16 7:27:56.000 PM) No Event Sampling Job || → ↵ ⬇ ⚡ Smart Mode

Events (31,037) Patterns Statistics Visualization

Format Timeline Zoom Out + Zoom to Selection × Deselect 1 minute per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields All Fields

Selected Fields

- host 3
- invalid_username 28
- remote_host 6
- source 4
- sourcetype 4

Interesting Fields

i	Time	Event
>	6/15/16 7:27:49.775 PM	type=PATH msg=audit(1466018869.775:373532): item=0 name="/var/log/wtmp" inode=265128 dev=ca:01 mode=010066 4 ouid=0 ogid=22 rdev=00:00 obj=system_u:object_r:wtmp_t:s0 nametype=NORMAL host = ip-10-0-0-45 source = /var/log/audit/audit.log sourcetype = linux_audit
>	6/15/16 7:27:49.775 PM	type=CWD msg=audit(1466018869.775:373532): cwd="/" host = ip-10-0-0-45 source = /var/log/audit/audit.log sourcetype = linux_audit
>	6/15/16 7:27:49.775 PM	type=SYSCALL msg=audit(1466018869.775:373532): arch=c0000003e syscall=2 success=yes exit=3 a0=403844 a1=1 a2=2 a3=8 items=1 ppid=1 pid=25267 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="agetty" exe="/sbin/agetty" subj=system_u:system_r:getty_t:s0 key="session" host = ip-10-0-0-45 source = /var/log/audit/audit.log sourcetype = linux_audit

Splunk Commands

- Splunk Search
 - Retrieves events from indexes
 - Filters results of a previous search
 - Uses Search Processing Language
 - Implicit command when a search is performed or can be used further filter search results, e.g., `index=main sourcetype=linux_secure| search field=value`

Splunk Commands

- Field Extraction
 - Key value pairs extracted by Splunk or by custom field extraction
 - Used by splunk to
 - Commands used to perform field extraction: rex, rename, stats, etc.

Questions?

Lab 1

- If you weren't here last week team up with someone who was or quickly do week 3 lab 2 (get AWS credentials from Instructor)
- If you were here last week:
 - Login into AWS, start your instance and note your public IP address (it may have changed)
 - SSH into your instance cd into railsgoat directory and run
 - `export RAILS_ENV=mysql`
 - `bundle exec rake db:setup`