# 2017-11-03 - Splunk/1.1 Issues

## Date

03 Nov 2017

## Attendees

- user-c2913
- Doug Newman
- Timothy Goff
- Nathan Clark
- Chris Durbin

## Goals

1. Identify a way to get the logs we need in the right format given the current implementation or...
2. Identify what needs to be done/changed/re-configured to support current reporting needs and enable simple triaging of operational applications.

## Discussion items

- NGAP-2296 - Jira project doesn't exist or you don't have permission to view it.
- Doug noticed a new format in the logs coming from 1.1. Upon so, he noticed that all queries needed to be updated in order to meet the current metric reporting.
  - That's a bit of a beat down given that the hope was just to update sourcetypes and everything just works
  - This works for EDSC with some manual work.
  - The biggest concern for right now is triaging issues.
- Applications are just providing text. Splunk has some logic/black magic that identifies events as such and formats them certain ways.i
- Potential solution that needs to be researched - https://answers.splunk.com/answers/390219/how-to-parse-docker-logs-with-multiple-events-from.html
- Another link from Tim - https://github.com/moby/moby/issues/22920

#### Questions

- What is Splunk doing to format the text file into what we see in Splunk for NGAP 1.0?
  - Marcus: No reformatting is happening. Splunk adds sourcetype and timestamp, but not heavy reformatting or anything.
- What was done in NGAP 1.0 for formatting/sourcetypes and can it be done for 1.1?
  - Who put the sourcetypes together? How did they do it?
  - Marcus suspects it is someone on the NGAP side. Maybe Andrew?
- Did Docker break this? Hard to tell if we don't have sourcetypes.
  - Should be able to use sourcetypes if we want (and configure them).
- Would using Cloudwatch solve our problems? Doesn't solve concatenate, but would provide raw lines.
- Assess what is a go/no-go for EDSC into Prod on Wednesday.

*Type your task here. Use "@" to assign a user and "//" to select a due date.*

## Action items