Cloud Monitoring Console Tips and Tricks

for the Splunk Cloud admin

Andrew Fager
Software Engineer | Splunk

Allen Duet
Product Manager | Splunk
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.
Allen Duet

Andrew Fager

We are Splunkers
Agenda

1. What is the CMC?
   Overview of the Cloud Monitoring Console

2. Starting out as a Splunk Cloud admin
   Tips on how to use the CMC when first getting started

3. More advanced uses of CMC
   Demo of CMC

4. How to provide feedback for the CMC
   Contact us if you have an idea to improve the CMC
What Is the Cloud Monitoring Console?
And where to find it
Getting Started With the CMC

Areas to focus on

My top 5 recommendations:

• Overview page
  – What changes are occurring in your stack

• Getting Data into Splunk Cloud
  – Indexing > Data Quality
  – Forwarders > Deployment

• Search Performance
  – Search > Skipped Scheduled Searches
  – Search > Expensive Searches

With so many resources in CMC what should I start with?
Overview

Understanding Change

The Overview dashboard is a collection of panels from throughout CMC with additional information designed to provide context around changes in your cloud deployment.
Data Quality

What errors are occurring while getting data into Splunk?

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Total Issues</th>
<th>Source Count</th>
<th>Line Breaking Issues</th>
<th>Time mapping parking Issues</th>
<th>Aggregation Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>intel_inmon_log</td>
<td>32832</td>
<td>8</td>
<td>32832</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>linux_messages_syslog</td>
<td>1454</td>
<td>4</td>
<td>0</td>
<td>1454</td>
<td>0</td>
</tr>
<tr>
<td>linux_users_accounts</td>
<td>1499</td>
<td>1</td>
<td>0</td>
<td>1499</td>
<td>0</td>
</tr>
<tr>
<td>netstats</td>
<td>796</td>
<td>1</td>
<td>0</td>
<td>796</td>
<td>0</td>
</tr>
<tr>
<td>splunk.config.broker</td>
<td>719</td>
<td>1</td>
<td>0</td>
<td>719</td>
<td>0</td>
</tr>
<tr>
<td>splunk.config.broker</td>
<td>719</td>
<td>1</td>
<td>0</td>
<td>719</td>
<td>0</td>
</tr>
<tr>
<td>cloud-inth-output</td>
<td>178</td>
<td>1</td>
<td>0</td>
<td>178</td>
<td>0</td>
</tr>
<tr>
<td>splunk.config.broker</td>
<td>178</td>
<td>1</td>
<td>0</td>
<td>178</td>
<td>0</td>
</tr>
<tr>
<td>splunk.config.broker</td>
<td>178</td>
<td>1</td>
<td>0</td>
<td>178</td>
<td>0</td>
</tr>
<tr>
<td>splunk.config.broker</td>
<td>178</td>
<td>1</td>
<td>0</td>
<td>178</td>
<td>0</td>
</tr>
</tbody>
</table>

Clicking a source type shows issues by source, helping you locate the origin of this data. [Show more info]
Forwarders: Deployment

How are your forwarders doing?
Skipped Scheduled Searches

The canary of features...

Skipped Scheduled Searches
Assess whether your scheduled searches are running as expected, quantify the fraction of your search workload that is being skipped or delayed, and find pointers for taking corrective action. Learn More...

Time Range

Include Acceleration Searches

Total Skipped Searches

537

Scheduled Search Skip Ratio
2.11%

Count of Skipped Scheduled Searches

Group by

Reason

The maximum number of concurrent running jobs for this historical scheduled search on this instance has been reached

455
91.86%

useradmin/27/1 is not allowed to run historical scheduled search, skipping

16
2.98%

useradmin/27/1/CloudAppDelete me Lookup_stubs/luster_update Clone

useradmin/27/1 is not allowed to run historical scheduled search, skipping

16
2.98%

useradmin/27/1/moby/search; Subscription Alert

useradmin/27/1 is not allowed to run historical scheduled search, skipping

4
0.74%

Count of Skipped Searches Over Time

Group by

Reason
Expensive Searches
Who could use a little SPL coaching?

### Top 20 Most Expensive Ad Hoc Searches

<table>
<thead>
<tr>
<th>Search Time</th>
<th>User</th>
<th>Time Range Start</th>
<th>Time Range End</th>
<th>Search Duration</th>
<th>Events Scanned</th>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-01-08</td>
<td>aduet</td>
<td>ZERO_TIME</td>
<td>ZERO_TIME</td>
<td>02:01:32.98</td>
<td>8,974,907</td>
<td>search index=main</td>
</tr>
</tbody>
</table>

### Potentially Inefficient Searches

<table>
<thead>
<tr>
<th>User</th>
<th>Search SPL</th>
<th>Events Scanned</th>
<th>Search Time Range [days]</th>
<th>Search Duration</th>
<th>Splunk Query Score</th>
<th>Potentially Inefficient Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>aduet</td>
<td>search ''</td>
<td>242,268</td>
<td>7</td>
<td>00:00:2.11</td>
<td>18</td>
<td>Missing Index</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Missing SourceType Missing Host</td>
</tr>
<tr>
<td>aduet</td>
<td>search index=main</td>
<td>8,974,907</td>
<td>00:01:32.98</td>
<td></td>
<td>5</td>
<td>Missing SourceType Missing Host</td>
</tr>
</tbody>
</table>
Enough about the basics.

Bring on Andrew to show us the cool stuff!
In review

Use the CMC to

Understand Change
Look for changes in ingest, search, user behavior, and resource use

Optimize your Deployment
Find inefficiencies and opportunities to improve use

Make Decisions about Configuration
Make data driven decisions about configuration changes and use support
Thank You

Please provide feedback via the SESSION SURVEY