

Cloud Monitoring Console Tips and Tricks

for the Splunk Cloud admin

Andrew Fager

Software Engineer | Splunk

Allen Duet

Product Manager | Splunk



Forward-Looking Statements



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 the 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.

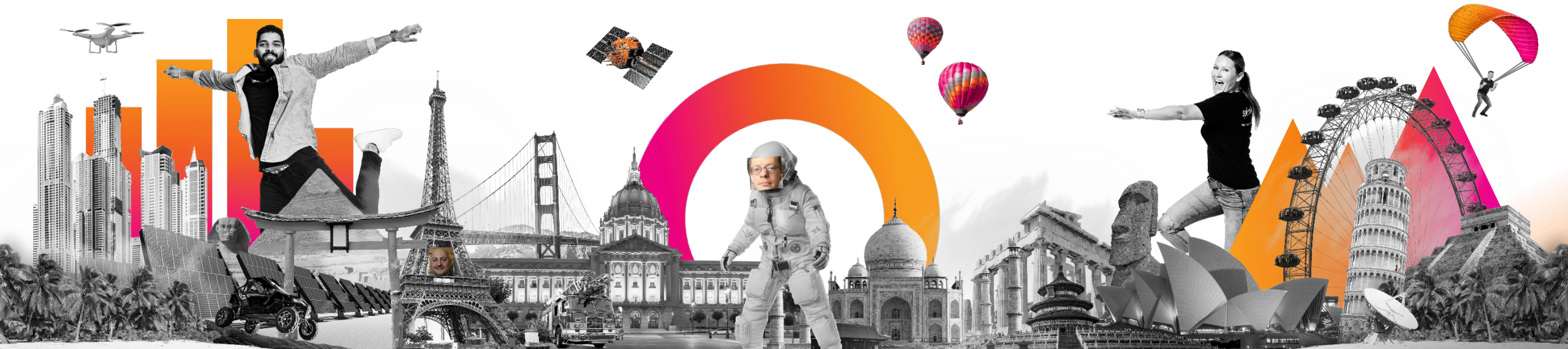
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the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

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2020 Splunk Inc. All rights reserved

Allen Duet

Andrew Fager

We are Splunkers



Agenda

Our approach

We'll show a few slides to help provide some context then dive into some demos as we talk through tips and use cases for the CMC

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

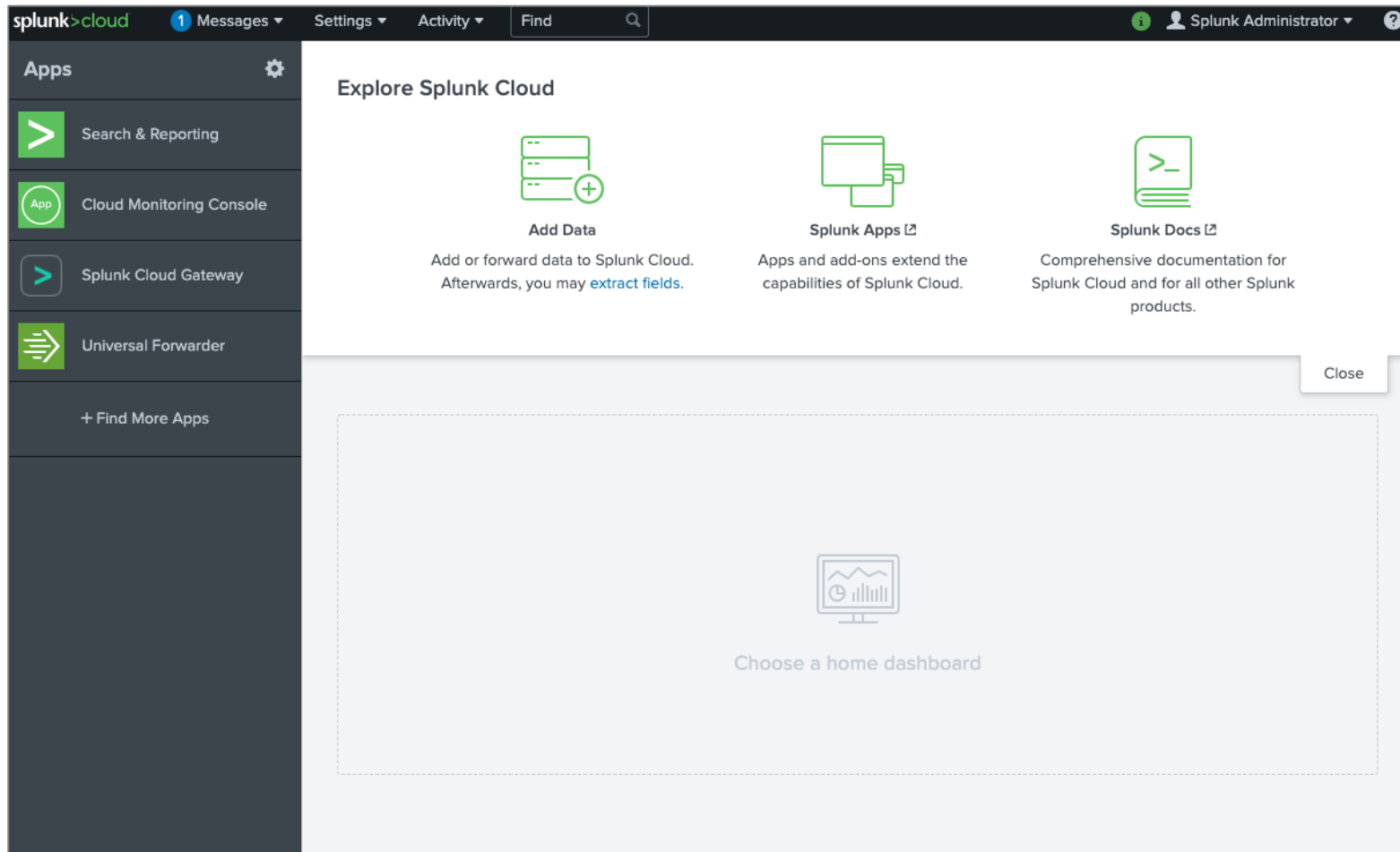
Demo of CMC

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?

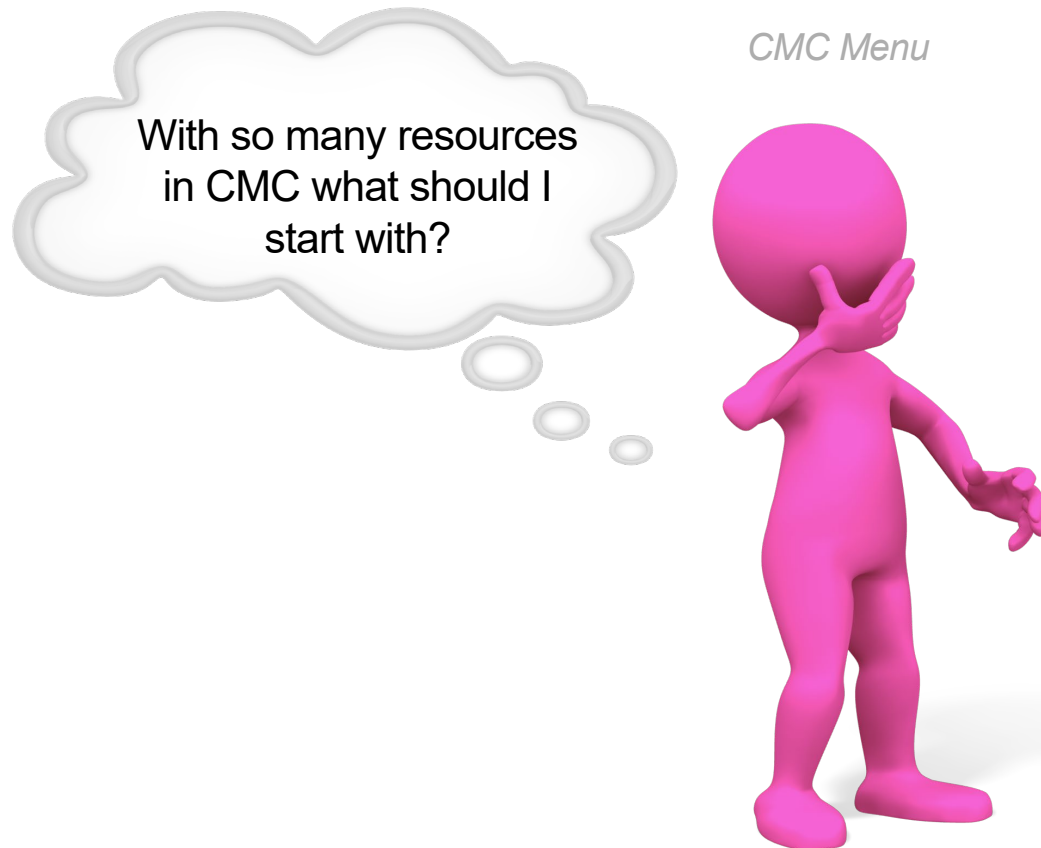
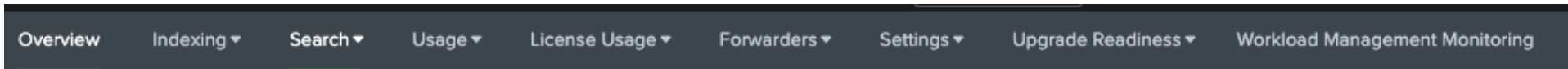
And where to find it



sc_admins

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

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?

[Overview](#) [Indexing](#) [Search](#) [Usage](#) [License Usage](#) [Forwarders](#) [Settings](#) [Upgrade Readiness](#) [Workload Management](#) [Monitoring](#) [Cloud Monitoring Console](#)

Data Quality

This dashboard helps you assess the quality of your incoming data by revealing issues that occur when the data is being indexed. These issues appear as warnings and errors in your splunkd.log.

Time Range: Last 15 minutes Include Splunk Source Types: ☒ No ☐ Yes [Hide Filters](#)

Event Processing Issues by Source Type

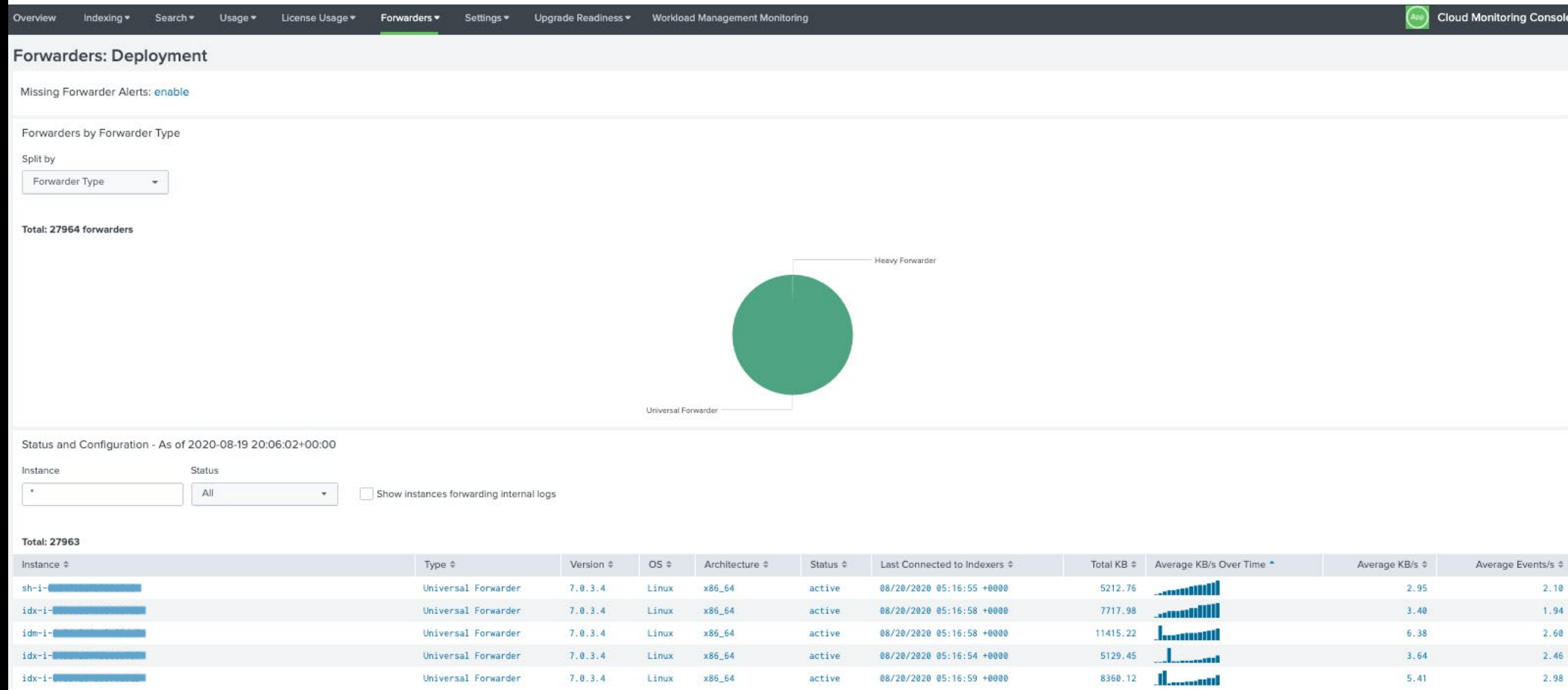
Sourcetype	Total Issues	Source Count	Line Breaking Issues	Timestamp Parsing Issues	Aggregation Issues
itsi_internal_log	32882	8	32882	0	0
linux_messages_syslog	1464	4	0	1464	0
Unix:UserAccounts	1449	1	0	1449	0
suricata	796	1	0	796	0
splunk:config:btool:savedsearches	738	1	8	104	626
splunk:config:btool:macros	201	1	7	2	192
cloud-init-output	178	1	0	116	62
splunk:config:btool:server	176	2	0	0	176
splunk:config:btool:indexes	126	1	0	0	126
splunk:config:btool:props	118	1	0	0	118

« Prev 1 2 3 4 Next »

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...

Overview Indexing Search Usage License Usage Forwarders Settings Upgrade Readiness Workload Management Monitoring  Cloud Monitoring Console

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

Last 4 hours

Include Acceleration Searches

☐ Yes

[Hide Filters](#)

☒ No

Total Skipped Searches

537

Scheduled Search Skip Ratio

2.11 %

Count of Skipped Scheduled Searches

Group by

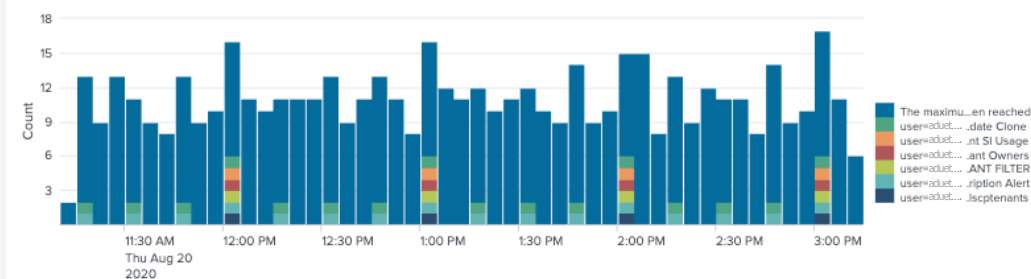
Reason

Reason	Count	Percent of Total
The maximum number of concurrent running jobs for this historical scheduled search on this instance has been reached	489	91.06 %
user=aduetdemo77 is not allowed to run historical scheduled search, skipping savedsearch_id=aduetdemo77;cloudops;Delete me lookup_shcluster_update Clone	16	2.98 %
user=aduetdemo67 is not allowed to run historical scheduled search, skipping savedsearch_id=nobody;search;Subscription Alert	16	2.98 %
user=aduetdemo7 is not allowed to run historical scheduled search, skipping savedsearch_id=aduetdemo7;search;Earliest/Latest Tenant SI Usage	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

Search Time ↕	User ↕	Time Range Start ↕	Time Range End ↕	Search Duration ↕	Search Result Count ↕	Events Scanned ↕	Search ↕
2020-31-08 16:22:53	aduet	ZERO_TIME	ZERO_TIME	00:01:32.98	0	8,974,907	search index=main

Potentially Inefficient Searches

User ^	Search SPL ↕	Events Scanned ↕	Search Time Range (days) ↕	Search Duration ↕	Splunk Query Score ^ ↕	Potentially Inefficient Behavior ↕
aduet	search ''	242,268	7	00:00:2.11	18	Missing Index Missing Sourcetype Missing Host
aduet	search index=main	8,974,907		00:01:32.98	5	Missing Sourcetype Missing Host

Enough about
the basics.

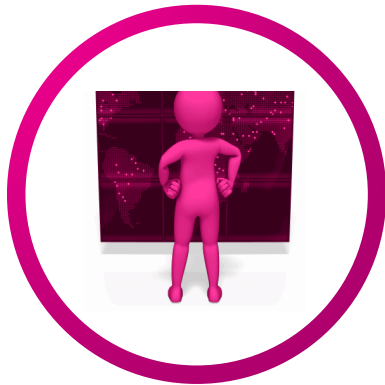


Bring on Andrew
to show us the
cool stuff!

In review

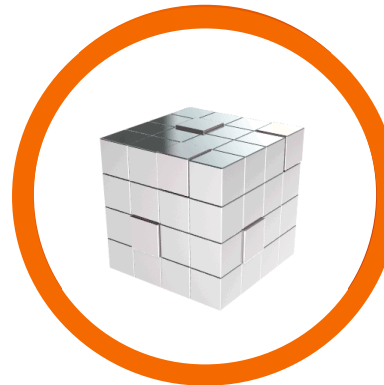
Use the CMC to

Understand Change



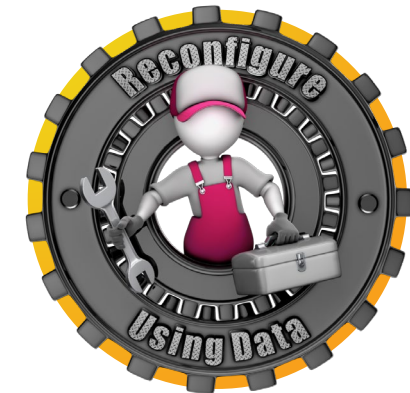
Look for changes in ingest, search, user behavior, and resource use

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

