What's New DMC?

Octavio Di Sciullo
Supportability Engineering Liaison

Patrick Ogdin
Senior Product Manager

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. 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, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

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 functionality described or to include any such feature or functionality in a future release.

Personal Introduction

- Octavio Di Sciullo
- Patrick Ogdin
  - Work on the Splunk Core Platform
  - 7 Years with Splunk, 10 years with Sun
  - Concerned with administration, supportability, forwarders, platforms

Agenda

- 6.2 DMC Recap
  - Continuous Investment
  - DMC Deployment Architectures
- So What's Up With My Search Head Cluster
- And that other Clustering thing, the Index Cluster
- Indexes and Volumes Everywhere
- Forwarders (Really Everywhere)
- Oh, and One Other Thing…

Distributed Management Console 6.2 Recap

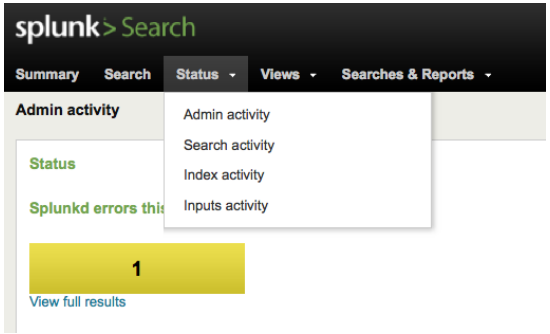
splunk>

Continuous Investment in Management/Monitoring

- Started with Introspection in 6.1
- Items in 6.3 that will make Admins happy
  - Event hashing
    - <insert theatre schedule>
  - Forwarder director
    - <insert theatre schedule>
- The future
  - Radically simplified setup/expansion
  - Granular controls in distributed deployment
  - Standard flows for common tasks in a distributed deployment
  - Better app model for installation/management
- What about S.o.S?

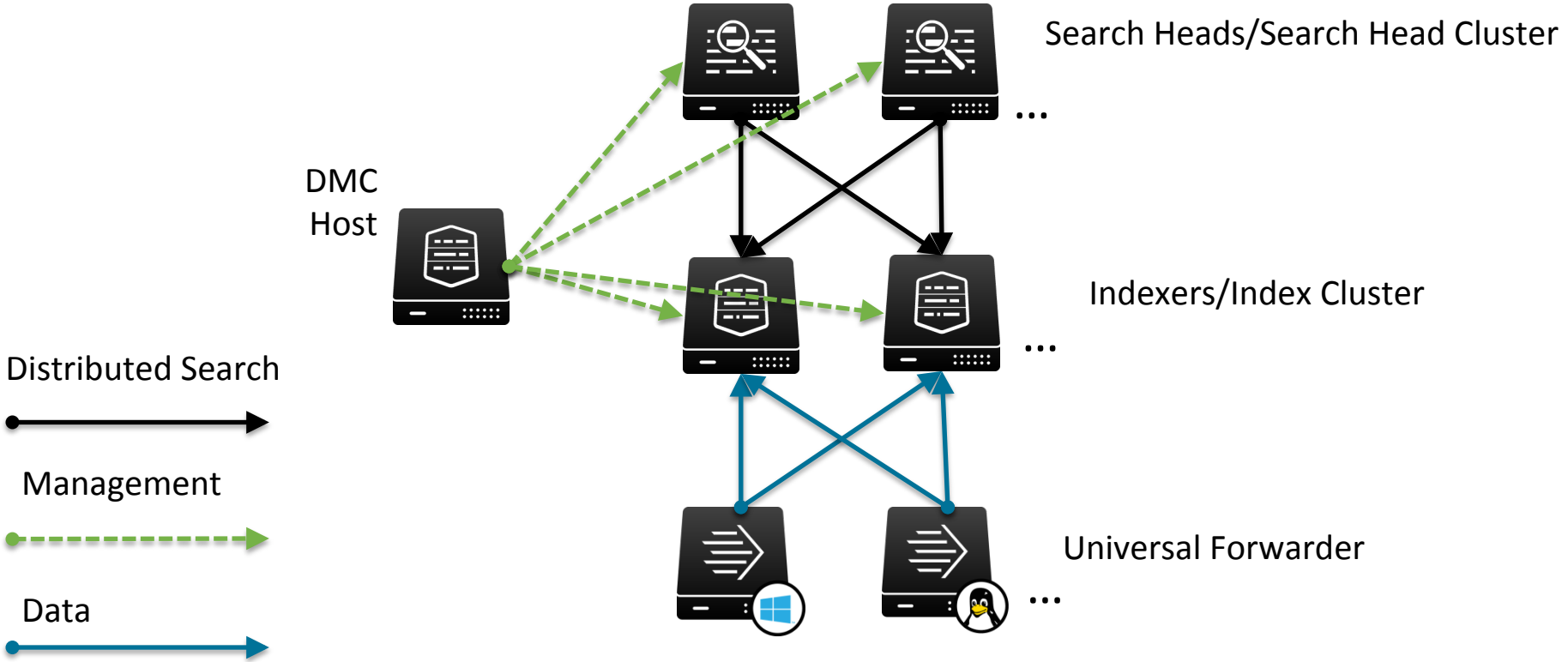
History of Splunk Monitoring Tools

- index=_internal sourcetype=splunkd
  - Go look at the logs!
- Splunkbase Tools
- Status/System activity dashboards
- Deployment Monitor
  - License usage reporting!
  - Alerting, summarization



- S.o.S
  - Developed by Splunk Support for Splunk support and customers
  - Platform resource utilization collection with technology add-ons
  - Topology views

Distributed Management Console Architecture



Setup Tasks

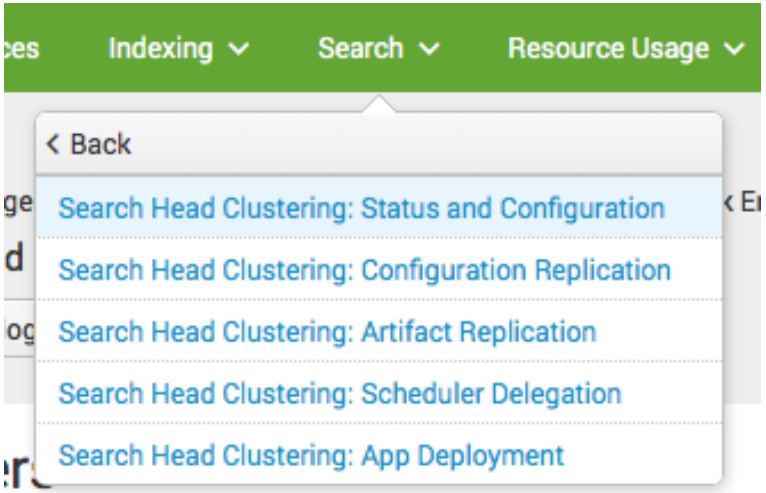
- Prerequisites
  - Where does the DMC live?
  - Topology definition
  - Forward all logs from all components back to the indexing tier
  - All components must be search peers of the DMC host
- Standalone vs. Distributed Mode
  - Server roles
  - Custom groups
  - Cluster labels!

Search Head Clustering Views

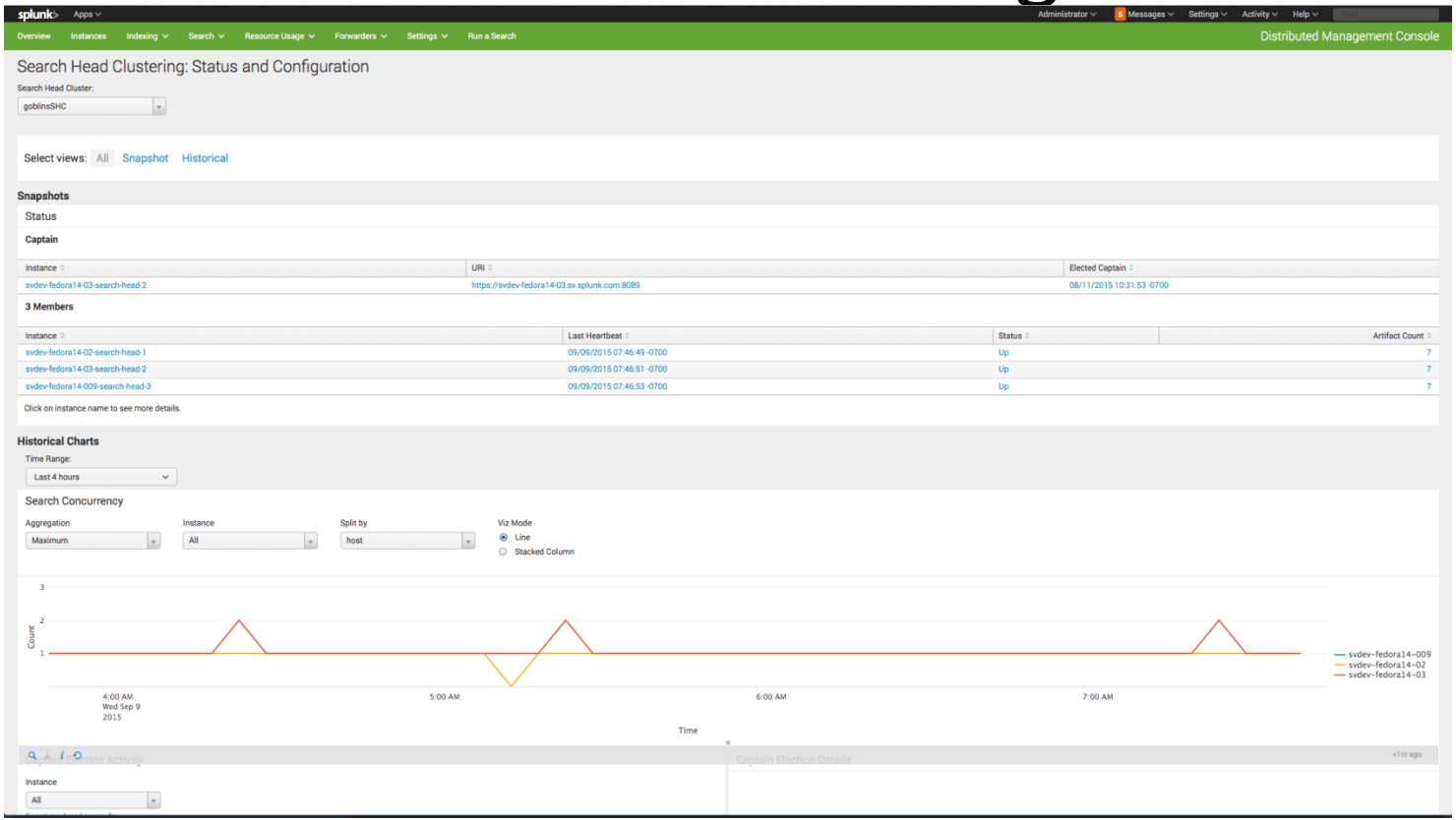
splunk>

Search Head Clustering Views

- Motivation
  - Plenty of data in logs/CLI
  - Lots of customers deploying SHC
  - What is going on in my search head cluster?
- Demo



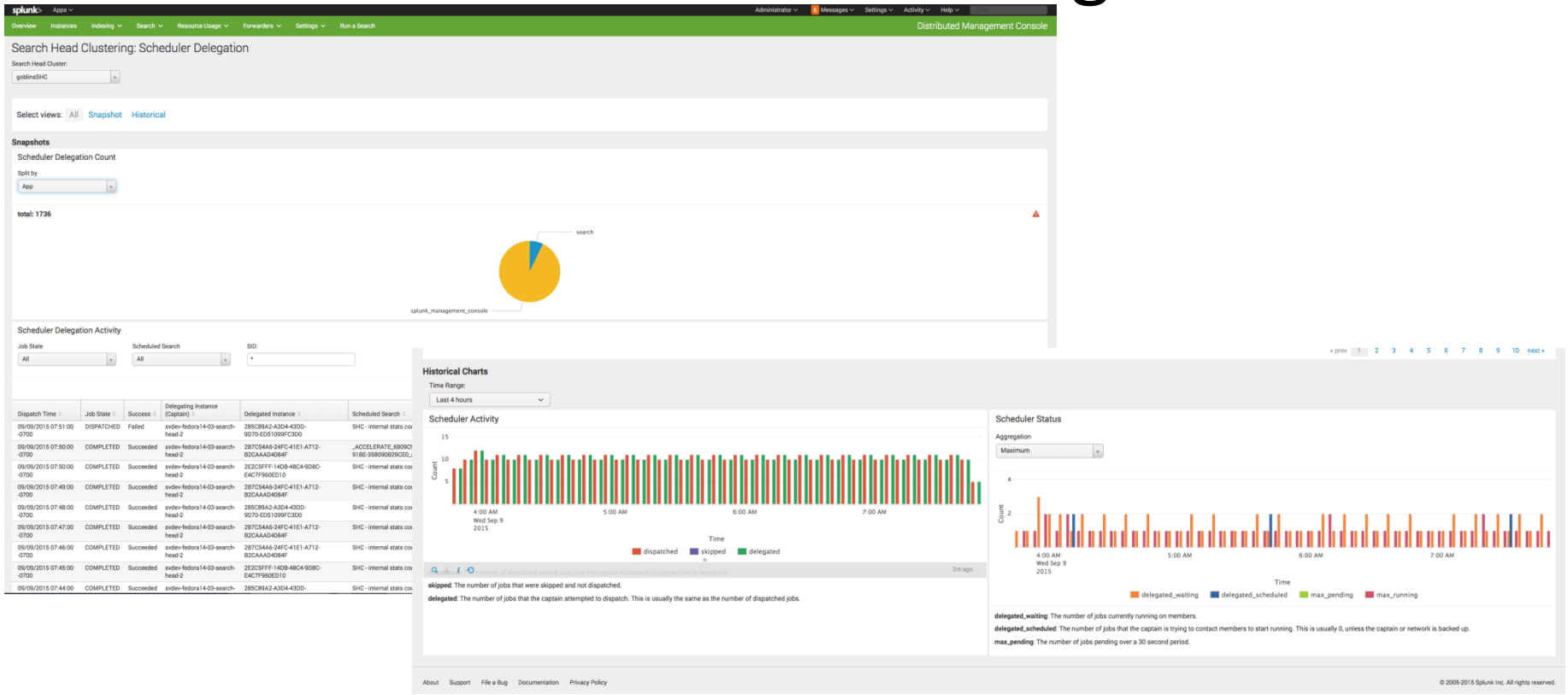
SHC – Status and Configuration



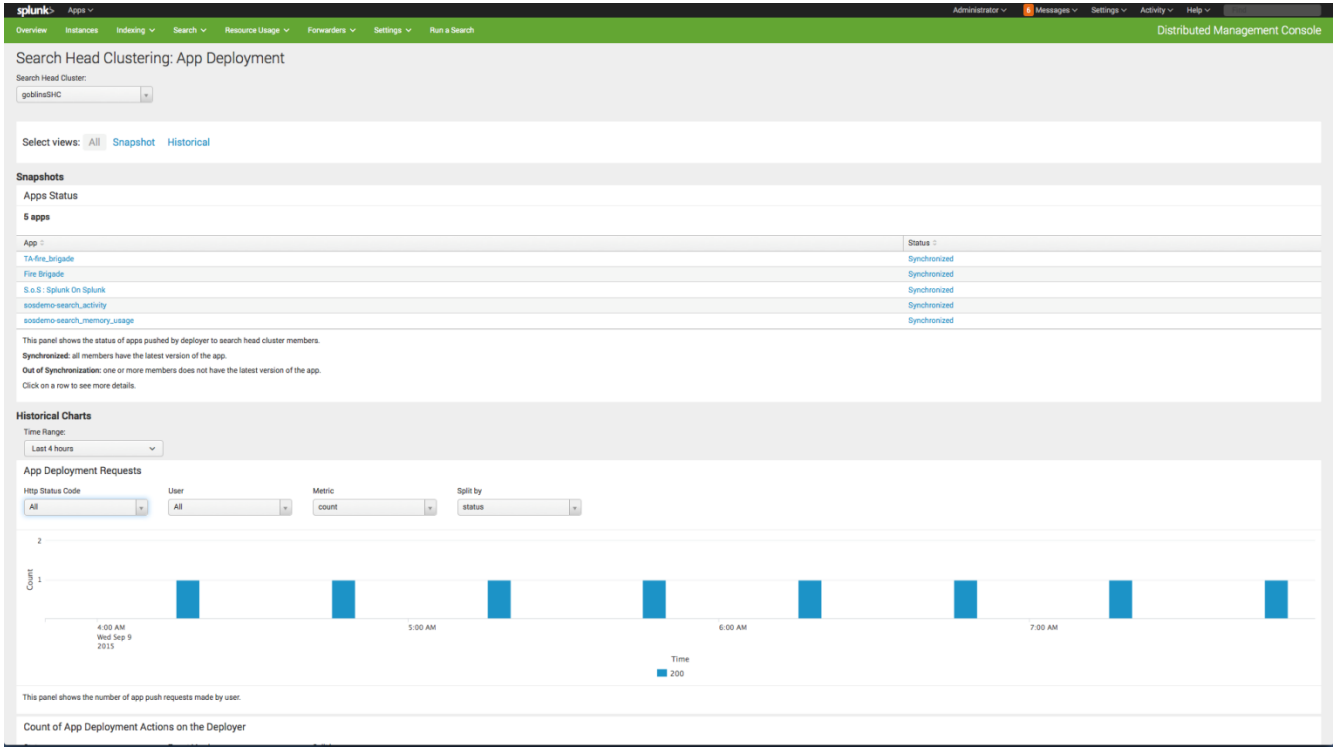
SHC – Configuration Replication

SHC – Artifact Replication

SHC – Scheduler Delegation



SHC – App Deployment

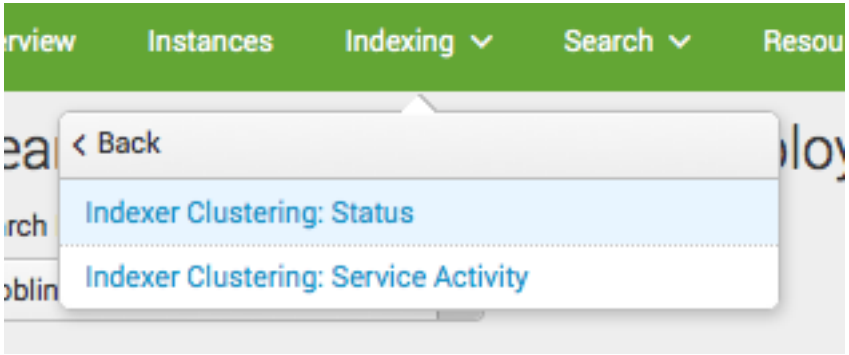


Index Clustering Views

splunk>

Index Clustering Views

- Motivation
  - One layer deeper than originally exposed
  - Dealing with ever expanding indexer counts
- Demo



Index Clustering Views - Status

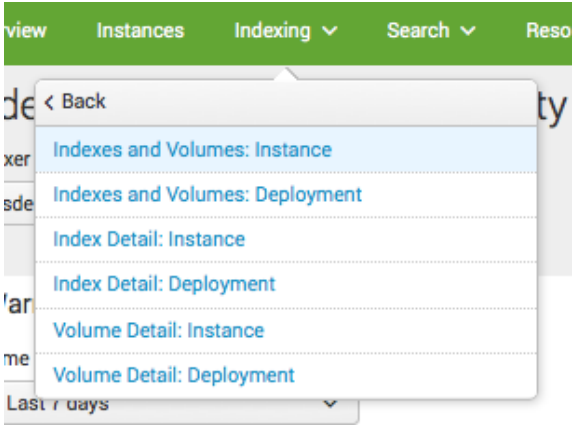
Index Clustering Views – Service Activity

Indexes and Volumes Views

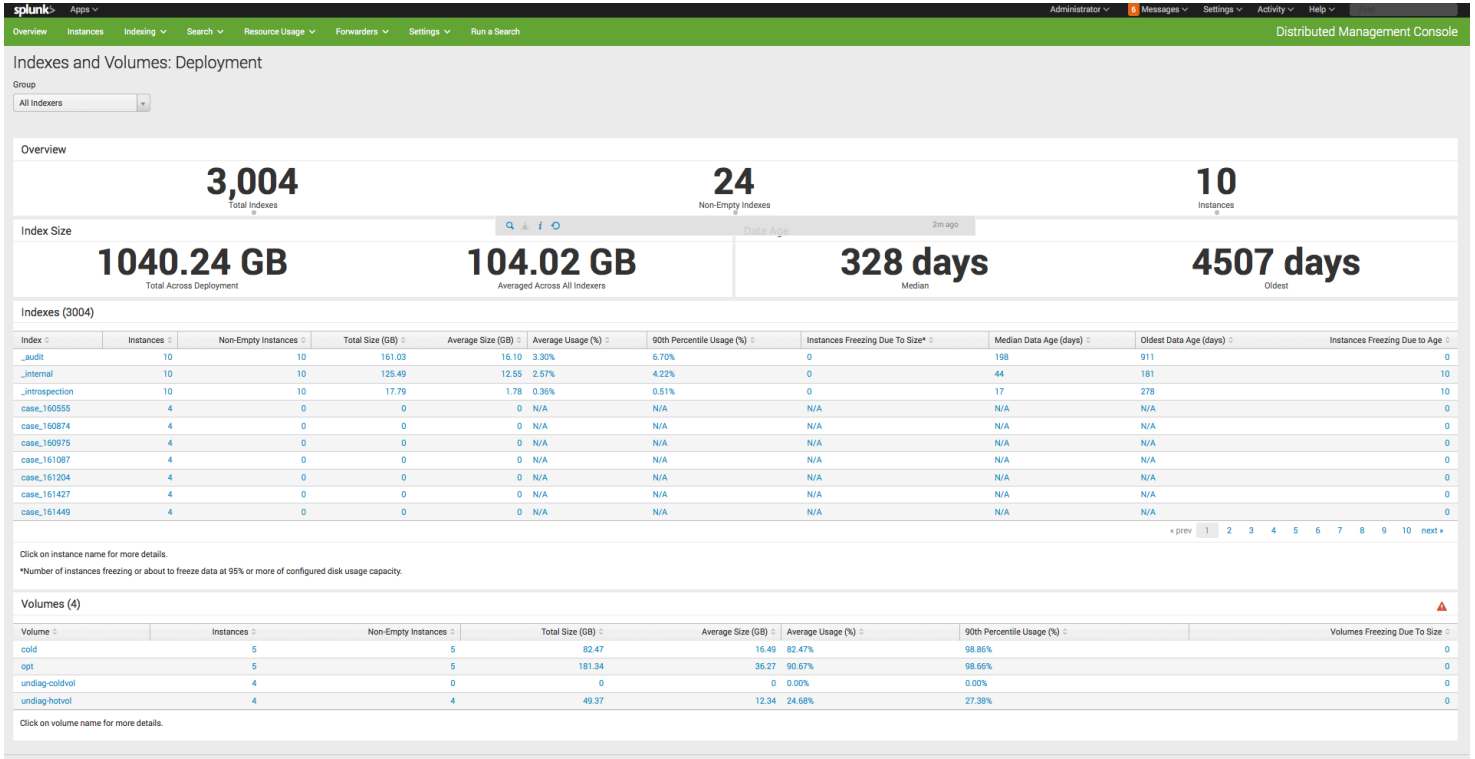
splunk>

Indexes and Volumes Views

- Motivation
  - Customers love Fire Brigade
  - Figuring out if you are meeting your retention policies is tricky
- Demo



Indexes and Volumes - Deployment



Indexes and Volumes – Index Detail:Deployment

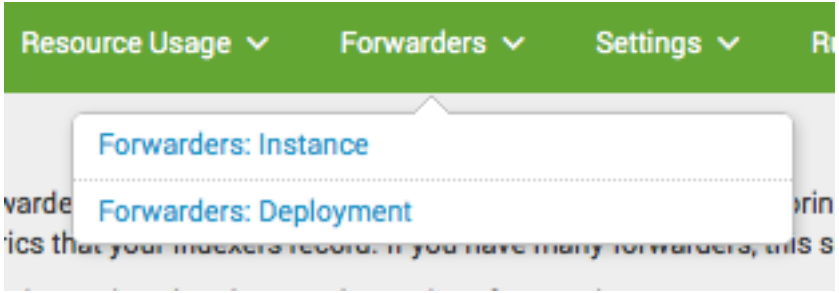
Indexes and Volumes – Volume Detail:Deployment

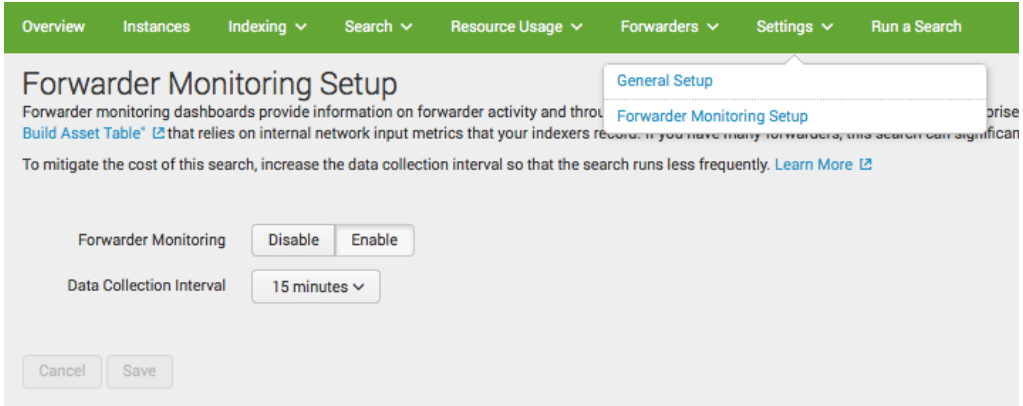
Forwarder Views

splunk>

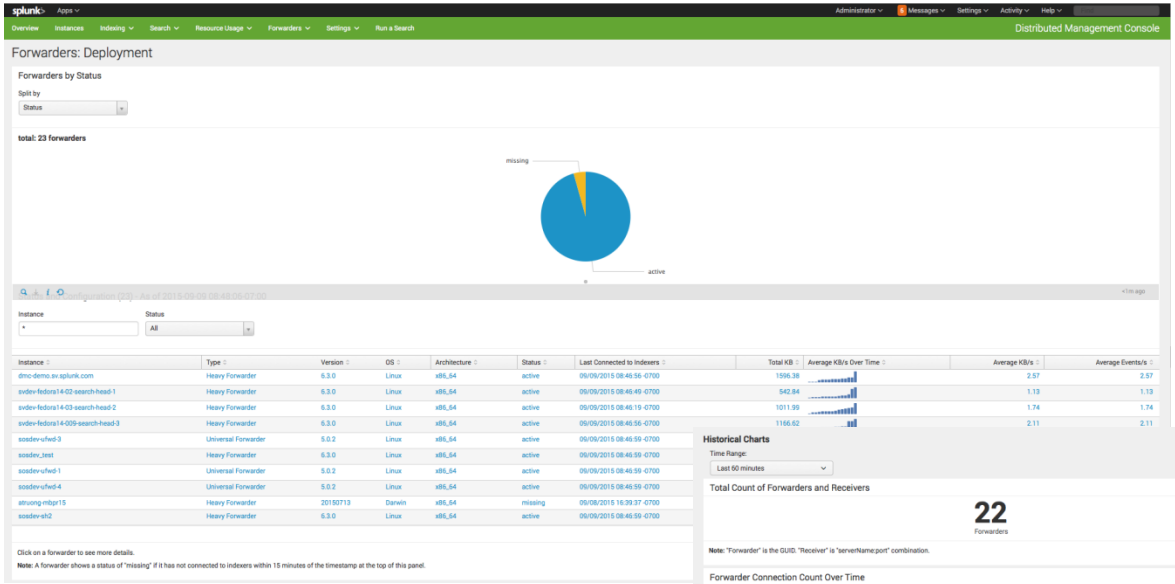
Forwarder Views

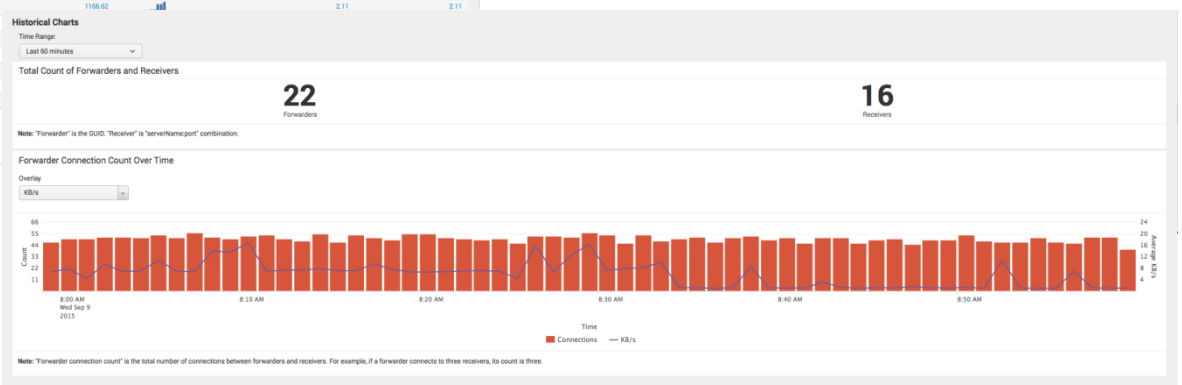
- Motivation
  - No forwarder info in 6.2!
  - Deployment monitor no longer improved/supported
  - Some customers don't use deployment server
- Forwarder Monitoring Setup
  - Runs a search against indexers
  - Configurable period
  - View reads from asset table
- Demo





Forwarder Views – Deployment Wide



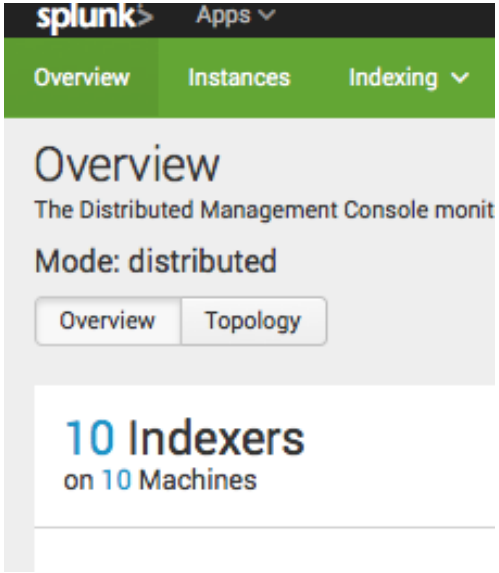


Topology Views

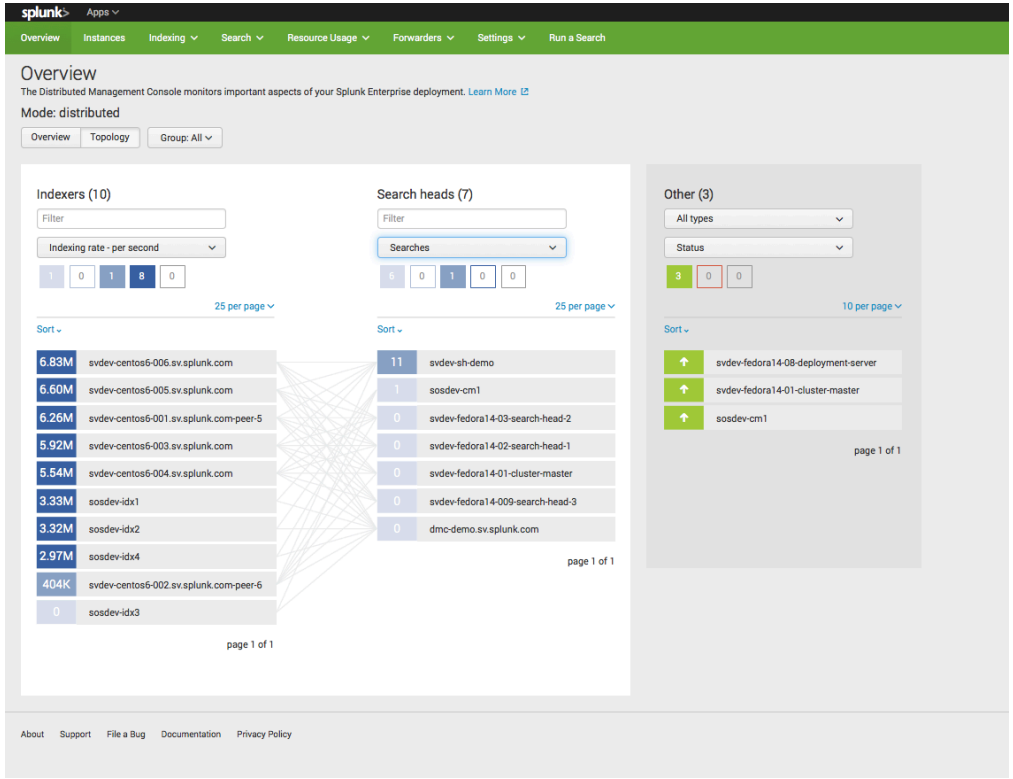
splunk>

Topology Views

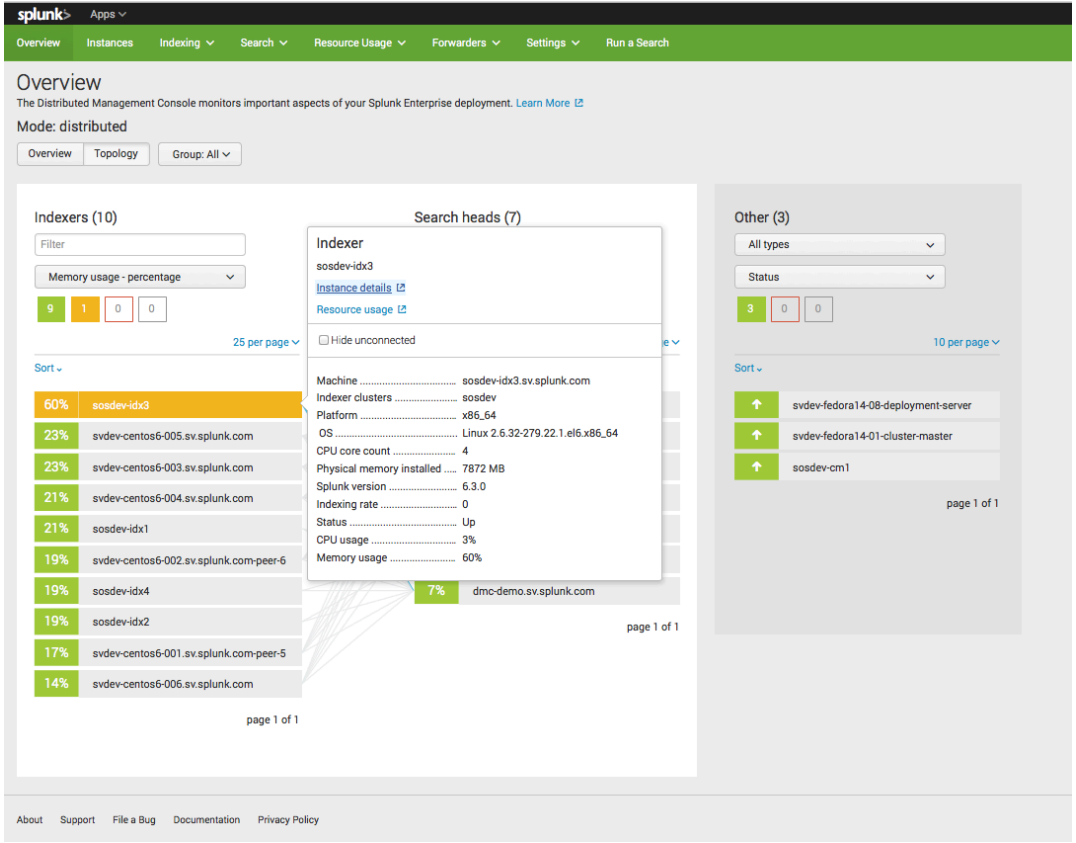
- Motivation
  - Visual representation of deployment
  - Relationships between instances
  - Deployment at-a-glance
  - Troubleshooting
- Demo



Topology Views – KPI Overlays



Topology Views – Performance Overlays/Detail



THANK YOU

splunk>