

.conf2015

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...



.conf2015

Distributed Management Console 6.2 Recap

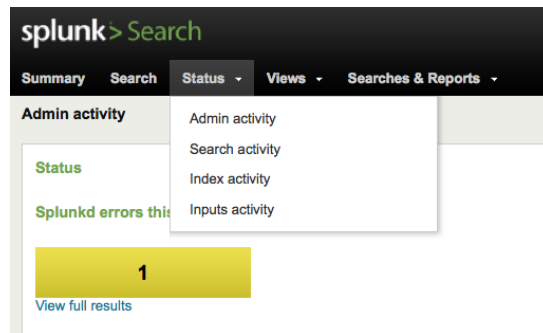
splunk>

Continuous Investment in Management/Monitoring

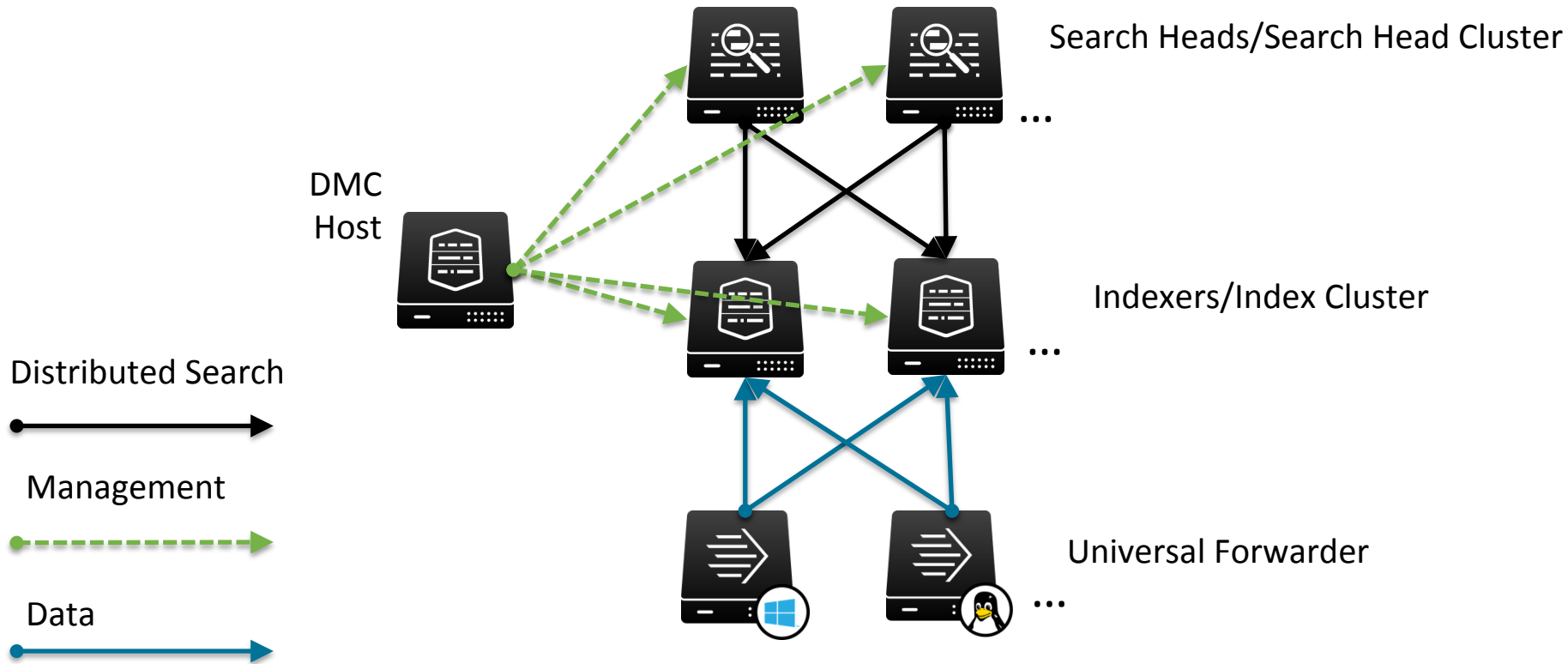
- Started with Introspection in 6.1
- Items in 6.3 that will make Admins happy
 - Event hashing
 - <insert theatre schedule>
 - Forwarder director
 - <insert theatre schedule>
- The future
 - Radically simplified setup/expansion
 - Granular controls in distributed deployment
 - Standard flows for common 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!



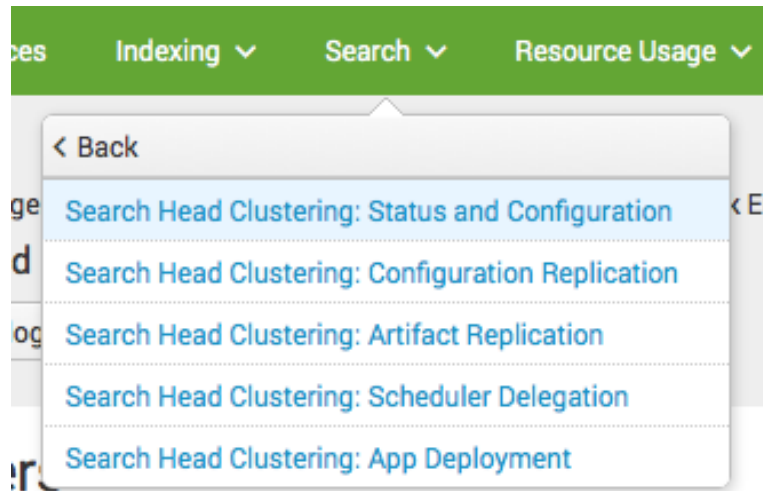
.conf2015

Search Head Clustering Views

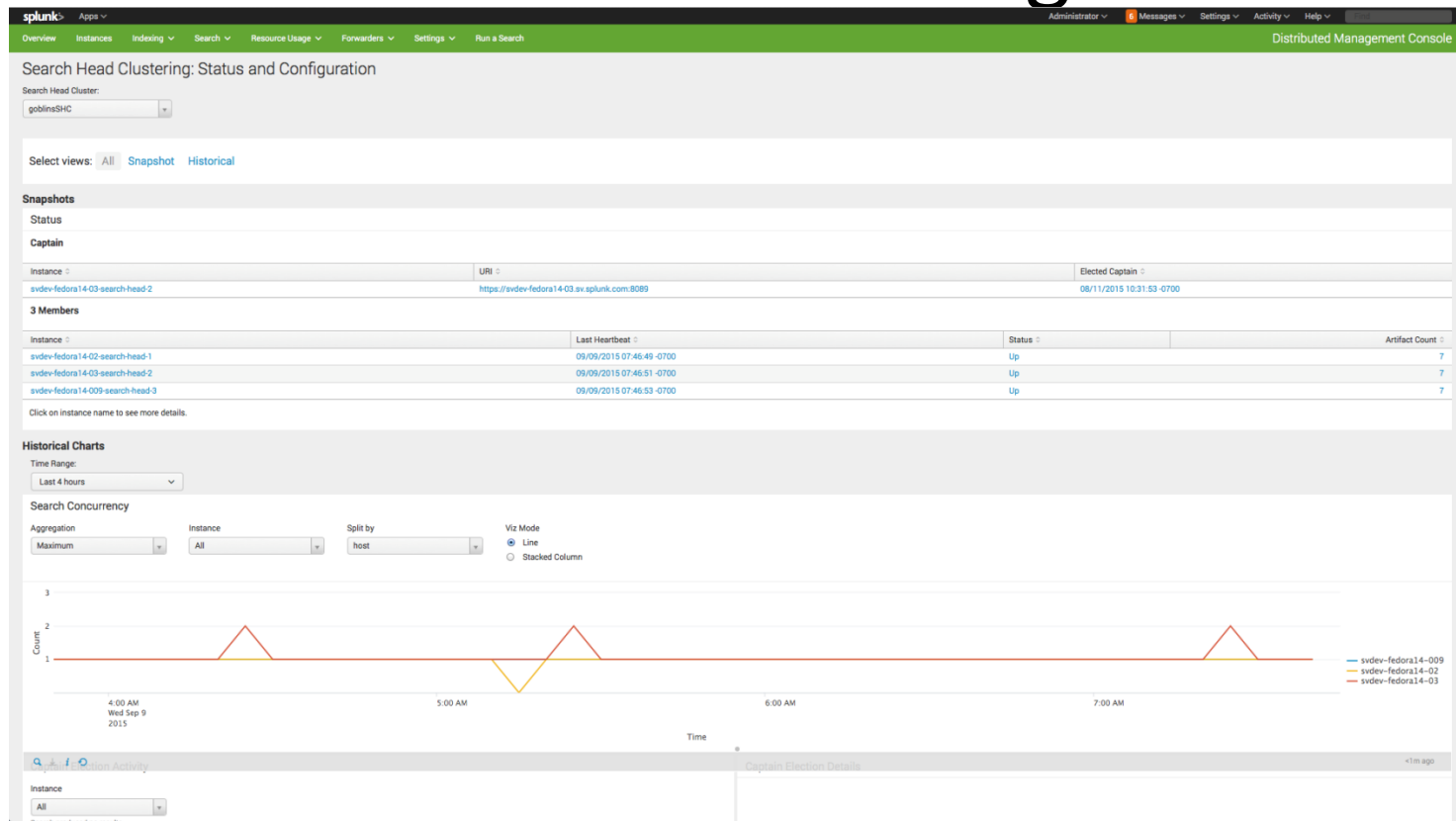
splunk>

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



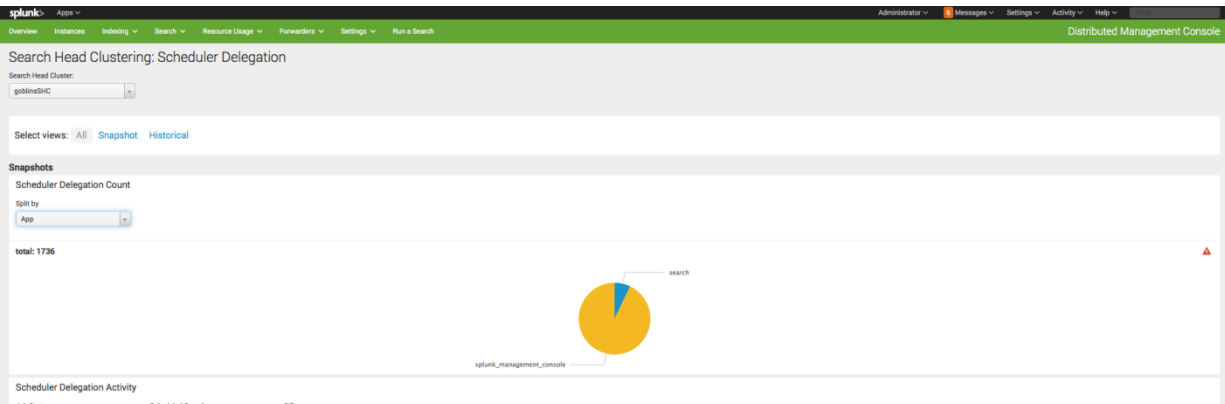
SHC – Status and Configuration



SHC – Configuration Replication

SHC – Artifact Replication

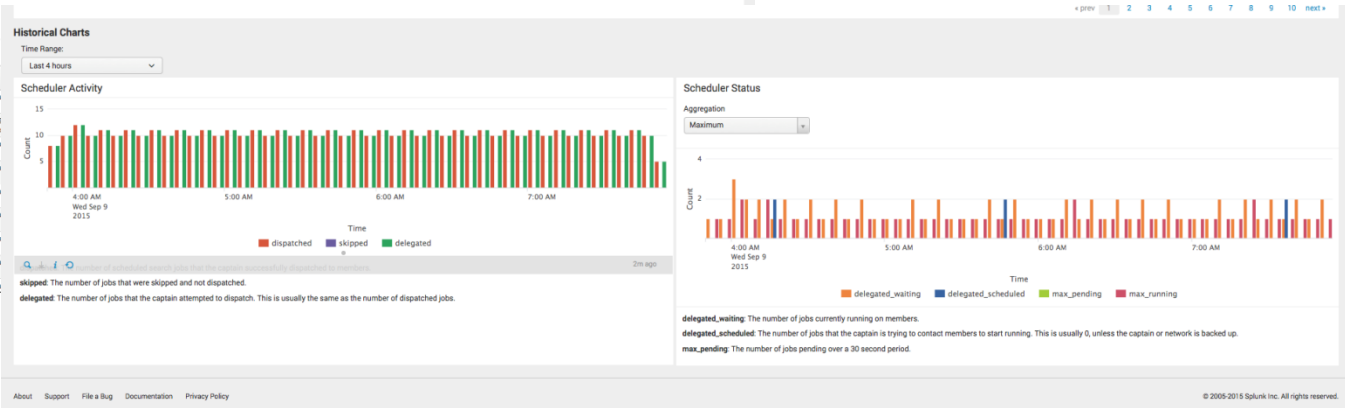
SHC – Scheduler Delegation



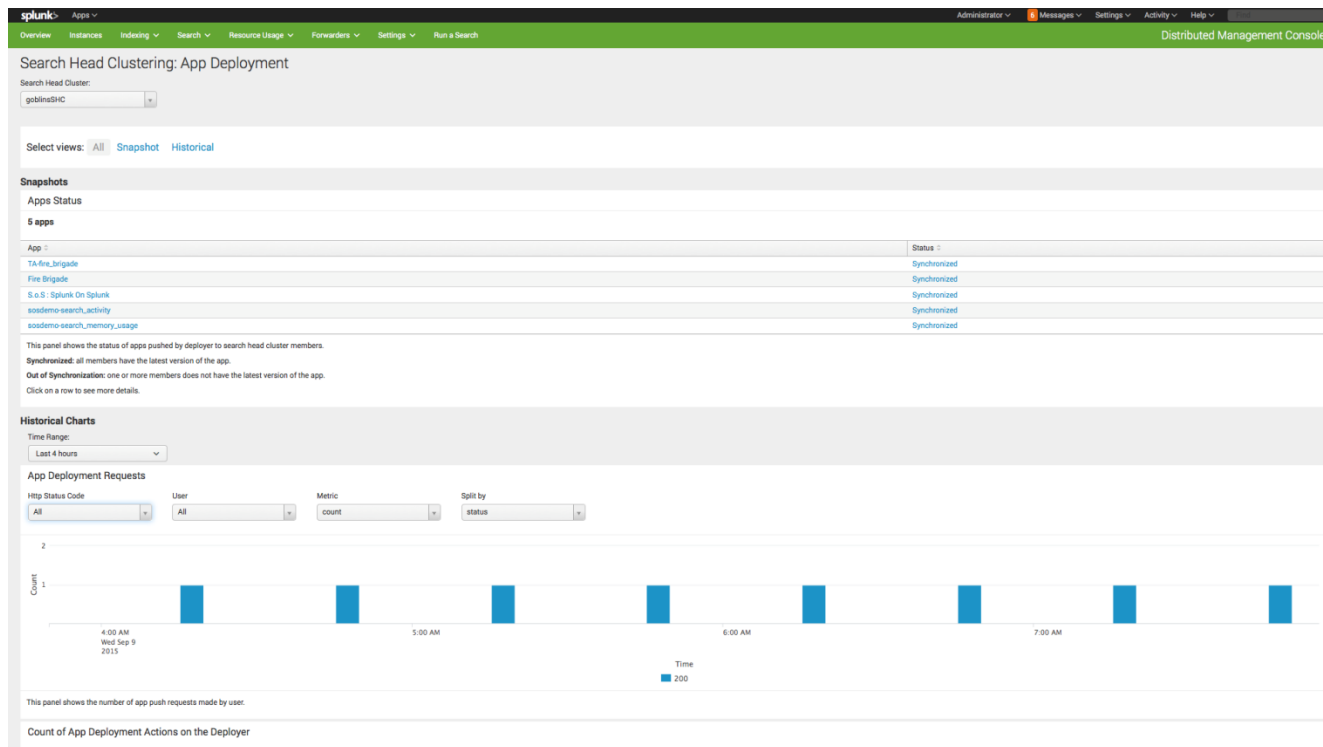
Scheduler Delegation Activity

Job State: All Scheduled Search: All SID: *

Dispatch Time	Job State	Success	Delegating Instance (Captain)	Delegated Instance	Scheduled Search
09/09/2015 07:51:00 -0700	DISPATCHED	Failed	evdev-fedora14-03-search-head-2	285C99A2-A3D4-43DD-9D70-ED51096FC5D0	SHC - internal stats coo
09/09/2015 07:50:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	287C5A46-24FC-41E1-A712-B2CAAAD4B84F	_ACCELERATE_669091918E-35809029C0D
09/09/2015 07:50:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	2C2C5FFF-1408-4BC4-908C-E4C7F960D10	SHC - internal stats coo
09/09/2015 07:49:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	287C5A46-24FC-41E1-A712-B2CAAAD4B84F	SHC - internal stats coo
09/09/2015 07:48:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	285C99A2-A3D4-43DD-9D70-ED51096FC5D0	SHC - internal stats coo
09/09/2015 07:47:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	287C5A46-24FC-41E1-A712-B2CAAAD4B84F	SHC - internal stats coo
09/09/2015 07:46:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	287C5A46-24FC-41E1-A712-B2CAAAD4B84F	SHC - internal stats coo
09/09/2015 07:45:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	2C2C5FFF-1408-4BC4-908C-E4C7F960D10	SHC - internal stats coo
09/09/2015 07:44:00 -0700	COMPLETED	Succeeded	evdev-fedora14-03-search-head-2	285C99A2-A3D4-43DD-9D70-ED51096FC5D0	SHC - internal stats coo



SHC – App Deployment





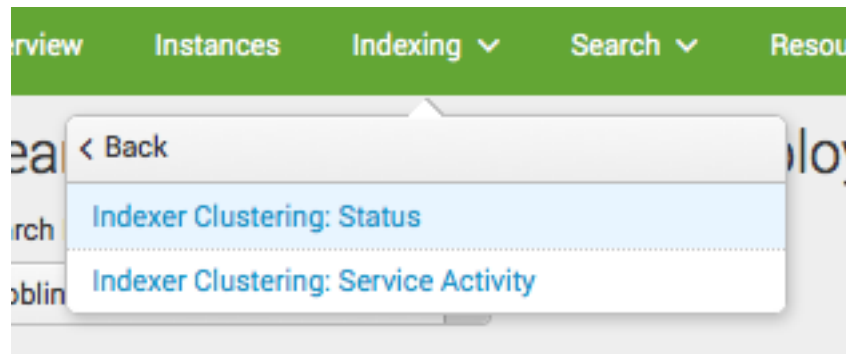
.conf2015

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



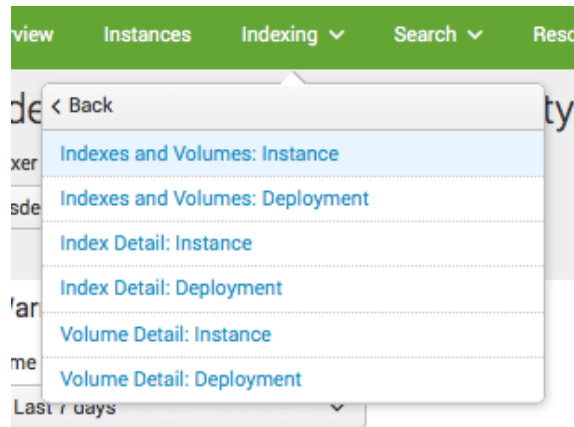
.conf2015

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

splunk Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Distributed Management Console

Overview Instances Indexing ▾ Search ▾ Resource Usage ▾ Forwarders ▾ Settings ▾ Run a Search

Indexes and Volumes: Deployment

Group
All Indexers ▾

Overview

3,004
Total Indexes

24
Non-Empty Indexes

10
Instances

1040.24 GB
Total Across Deployment

104.02 GB
Averaged Across All Indexers

328 days
Median

4507 days
Oldest

Index Size

Indexes (3004)

Index ▾	Instances ▾	Non-Empty Instances ▾	Total Size (GB) ▾	Average Size (GB) ▾	Average Usage (%) ▾	90th Percentile Usage (%) ▾	Instances Freezing Due To Size* ▾	Median Data Age (days) ▾	Oldest Data Age (days) ▾	Instances Freezing Due To Age ▾
_audit	10	10	161.03	16.10	3.30%	6.70%	0	198	911	0
_internal	10	10	125.49	12.55	2.57%	4.22%	0	44	181	10
_introspection	10	10	17.79	1.78	0.36%	0.51%	0	17	278	10
case_160555	4	0	0	0	N/A	N/A	N/A	N/A	N/A	0
case_160874	4	0	0	0	N/A	N/A	N/A	N/A	N/A	0
case_160975	4	0	0	0	N/A	N/A	N/A	N/A	N/A	0
case_161087	4	0	0	0	N/A	N/A	N/A	N/A	N/A	0
case_161204	4	0	0	0	N/A	N/A	N/A	N/A	N/A	0
case_161427	4	0	0	0	N/A	N/A	N/A	N/A	N/A	0
case_161449	4	0	0	0	N/A	N/A	N/A	N/A	N/A	0

◀ prev 1 2 3 4 5 6 7 8 9 10 next ▶

Click on instance name for more details.
*Number of instances freezing or about to freeze data at 95% or more of configured disk usage capacity.

Volumes (4)

Volume ▾	Instances ▾	Non-Empty Instances ▾	Total Size (GB) ▾	Average Size (GB) ▾	Average Usage (%) ▾	90th Percentile Usage (%) ▾	Volumes Freezing Due To Size ▾
cold	5	5	82.47	16.49	82.47%	98.86%	0
opt	5	5	181.34	36.27	90.67%	98.66%	0
unddiag-coldvol	4	0	0	0	0.00%	0.00%	0
unddiag-hotvol	4	4	49.37	12.34	24.68%	27.38%	0

Click on volume name for more details.

Indexes and Volumes – Index Detail:Deployment

Indexes and Volumes – Volume Detail:Deployment



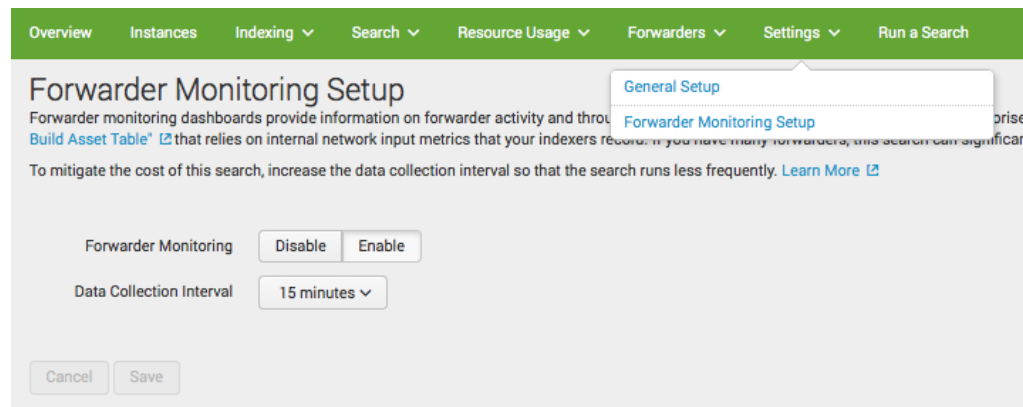
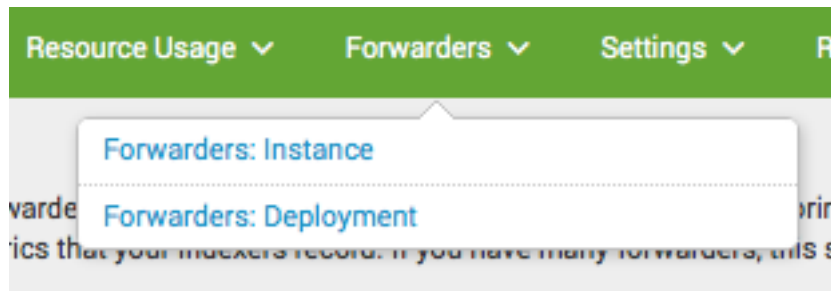
.conf2015

Forwarder Views

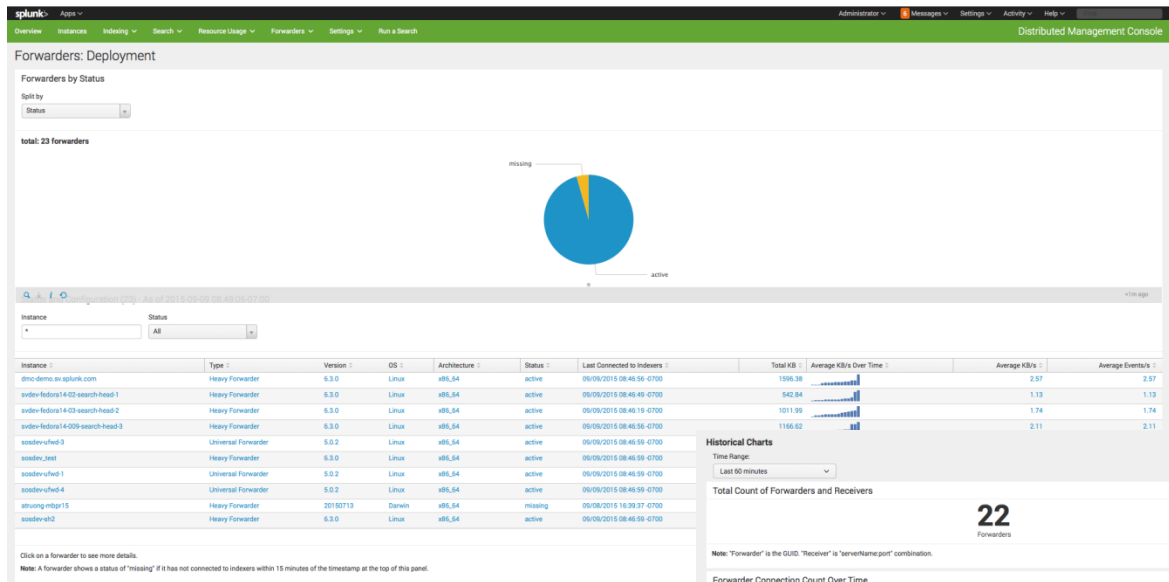
splunk>

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



Historical Charts

Time Range: Last 60 minutes

Total Count of Forwarders and Receivers

22
Forwarders

16
Receivers

Note: "Forwarder" is the GUID, "Receiver" is "serverName:port" combination.

Forwarder Connection Count Over Time

Overlay: KB/s



Note: "Forwarder connection count" is the total number of connections between forwarders and receivers. For example, if a forwarder connects to three receivers, its count is three.



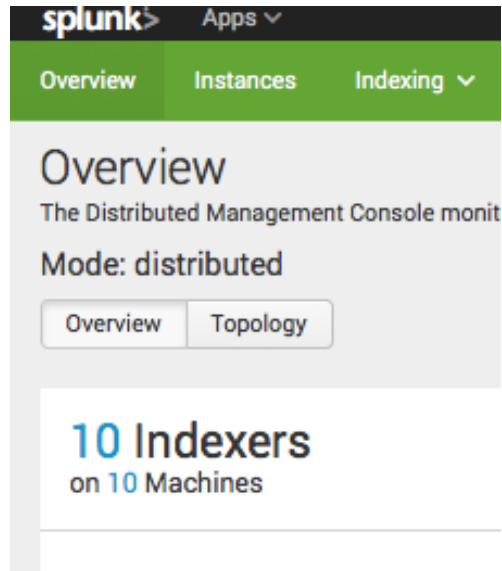
.conf2015

Topology Views

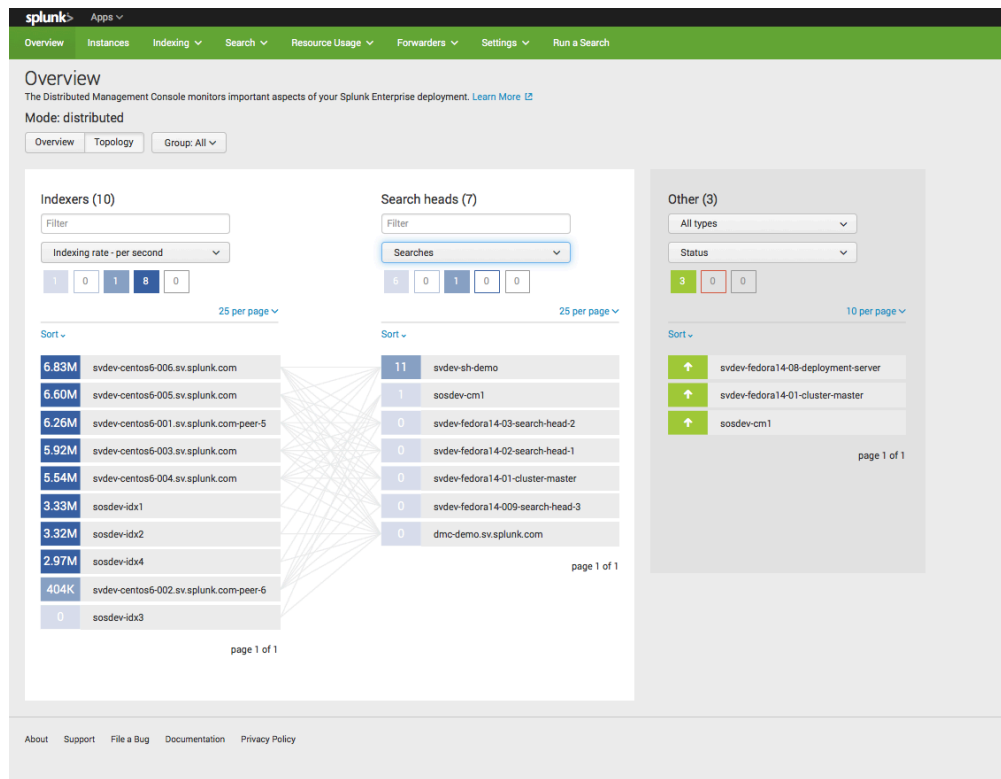
splunk>

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

The screenshot displays the Splunk Enterprise Overview page. The top navigation bar includes links for Overview, Instances, Indexing, Search, Resource Usage, Forwarders, Settings, and Run a Search. The main content area is titled 'Overview' and includes a sub-header 'The Distributed Management Console monitors important aspects of your Splunk Enterprise deployment. [Learn More](#)'. Below this, the 'Mode: distributed' is indicated, and there are tabs for 'Overview' and 'Topology', along with a 'Group: All' dropdown.

The 'Overview' section is divided into three main panels:

- Indexers (10)**: A table showing the performance of 10 indexers. The table has columns for 'Machine', 'Indexer clusters', 'Platform', 'OS', 'CPU core count', 'Physical memory installed', 'Splunk version', 'Indexing rate', 'Status', 'CPU usage', and 'Memory usage'. The 'Memory usage' column is highlighted in green, and the 'Indexing rate' column is highlighted in orange. The 'Indexers' panel includes a 'Filter' input, a 'Memory usage - percentage' dropdown, and a 'Sort' dropdown. The 'Indexers' panel also includes a '25 per page' dropdown and a 'Hide unconnected' checkbox.
- Search heads (7)**: A table showing the performance of 7 search heads. The table has columns for 'Machine', 'Indexer clusters', 'Platform', 'OS', 'CPU core count', 'Physical memory installed', 'Splunk version', 'Indexing rate', 'Status', 'CPU usage', and 'Memory usage'. The 'Memory usage' column is highlighted in green, and the 'Indexing rate' column is highlighted in orange. The 'Search heads' panel includes a 'Filter' input, a 'Memory usage - percentage' dropdown, and a 'Sort' dropdown. The 'Search heads' panel also includes a '10 per page' dropdown and a 'Hide unconnected' checkbox.
- Other (3)**: A table showing the performance of 3 other components. The table has columns for 'Machine', 'Indexer clusters', 'Platform', 'OS', 'CPU core count', 'Physical memory installed', 'Splunk version', 'Indexing rate', 'Status', 'CPU usage', and 'Memory usage'. The 'Memory usage' column is highlighted in green, and the 'Indexing rate' column is highlighted in orange. The 'Other' panel includes a 'Filter' input, a 'Memory usage - percentage' dropdown, and a 'Sort' dropdown. The 'Other' panel also includes a '10 per page' dropdown and a 'Hide unconnected' checkbox.

The 'Indexers' panel shows a list of indexers with their memory usage percentages: 60%, 23%, 23%, 21%, 21%, 19%, 19%, 19%, 17%, and 14%. The 'Search heads' panel shows a list of search heads with their memory usage percentages: 7% and 0%. The 'Other' panel shows a list of other components with their memory usage percentages: 3%, 0%, and 0%.

The footer of the page includes links for About, Support, File a Bug, Documentation, and Privacy Policy.



.conf2015

THANK YOU

splunk>