splunk> .conf2017

You've Inherited a Splunk Enterprise Deployment… Now What?

A Seminar for Admins Who Are All "What is this? I Can't Even…."

Jessica Law | Senior Staff Technical Writer

Matthew Ness | Principal Technical Writer

September 2017 | Washington, DC

Forward-Looking Statements

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.

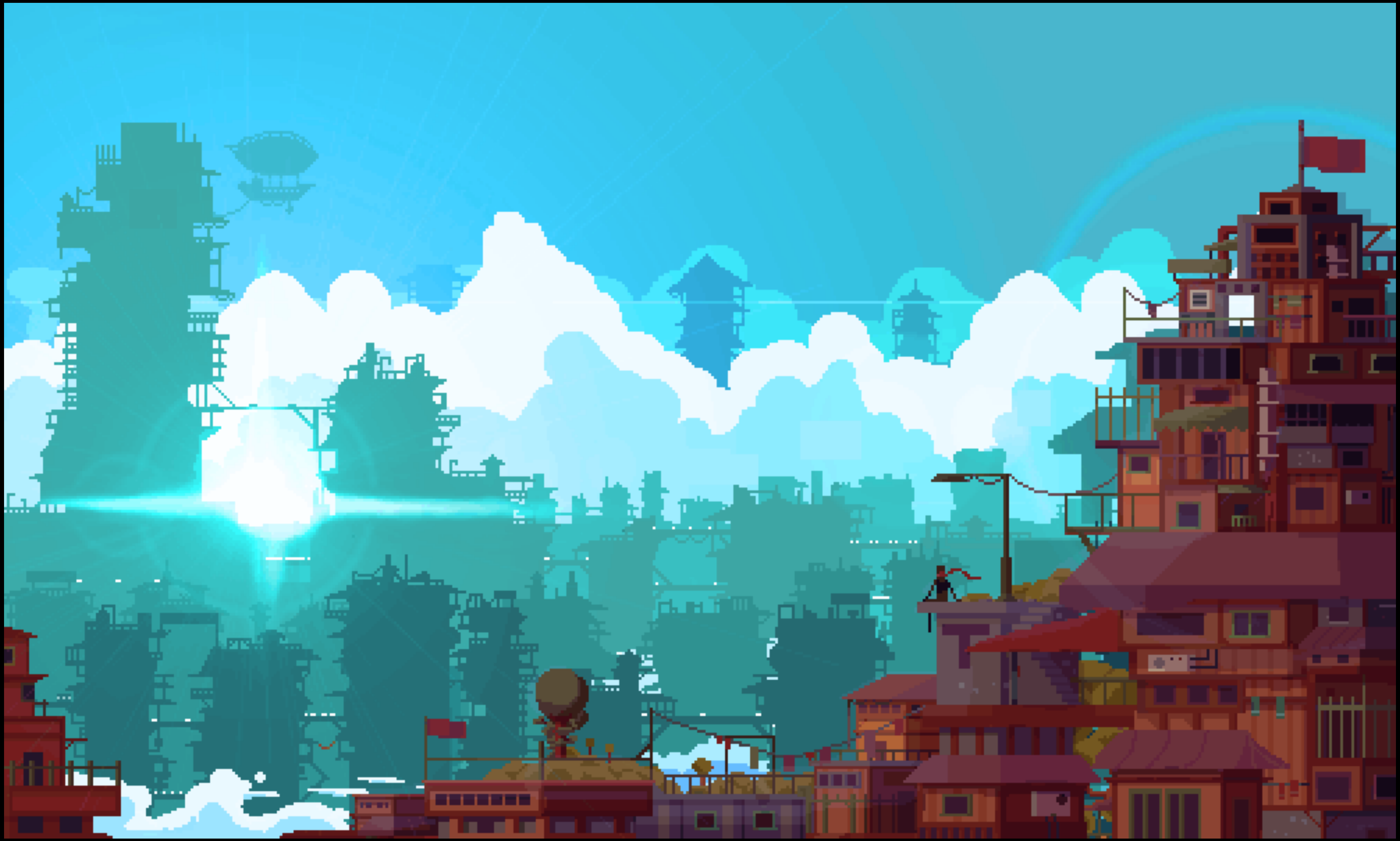
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements 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.

You’ve Inherited a Splunk Enterprise Deployment …Now What?

A Seminar for Admins Who Are All
“What is this? I Can’t Even….”

RELAX

We are here to help



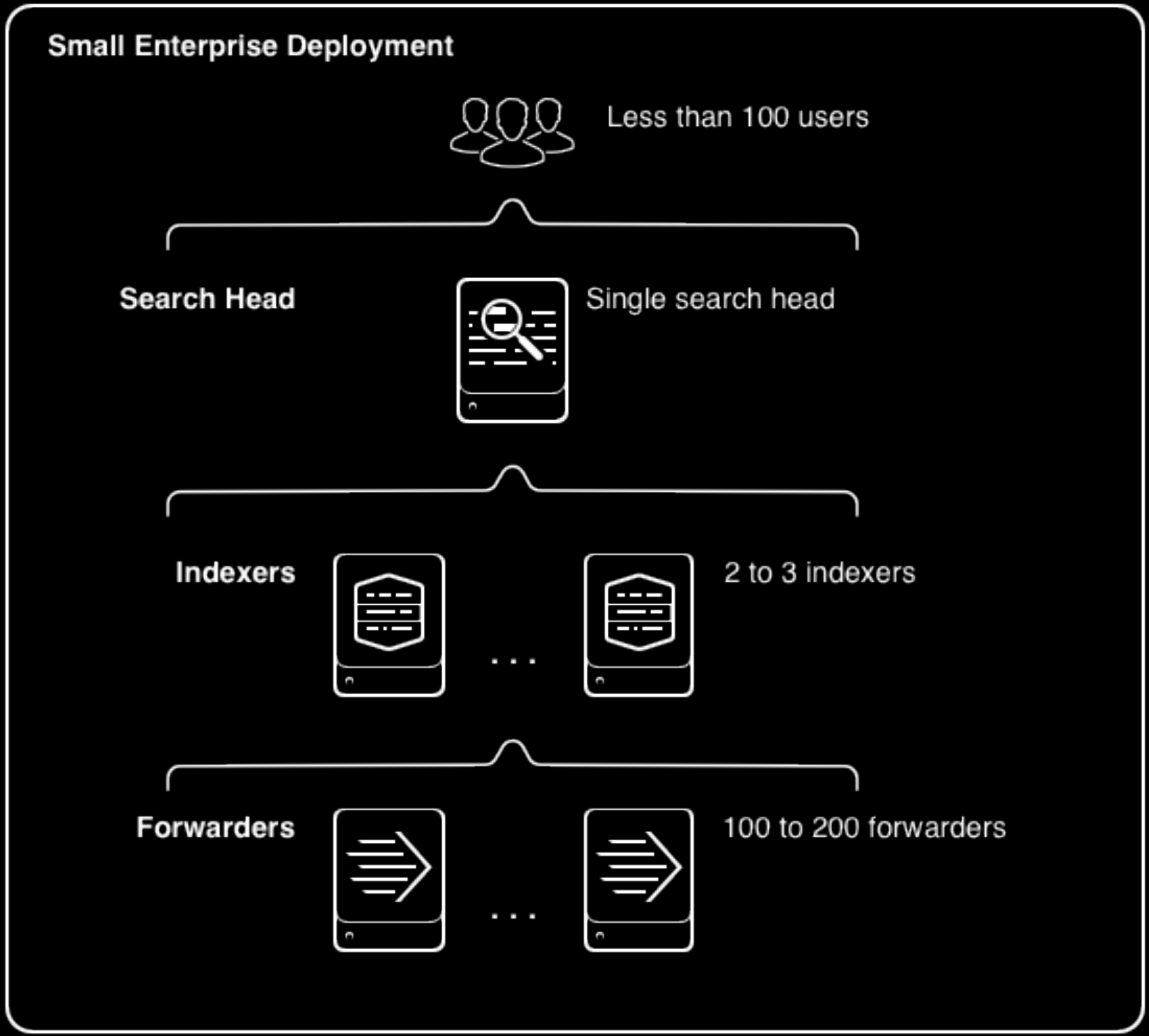
Agenda

- Part 1: Diagram your deployment topology.
- Part 2: Get to know your data.
- Part 3: Survey your apps and add-ons.
- Part 4: Check your licenses.
- Part 5: Study your user authentication methods.
- Part 6: Review the security of your deployment.
- Part 7: Monitor the health of your system.
- Part 8: Investigate your knowledge objects.

1

Diagram Your Deployment Topology

Example Small Deployment



Small Enterprise Deployment

Less than 100 users

Search Head

Single search head

Indexers

2 to 3 indexers

Forwarders

100 to 200 forwarders

Splunk Enterprise Components

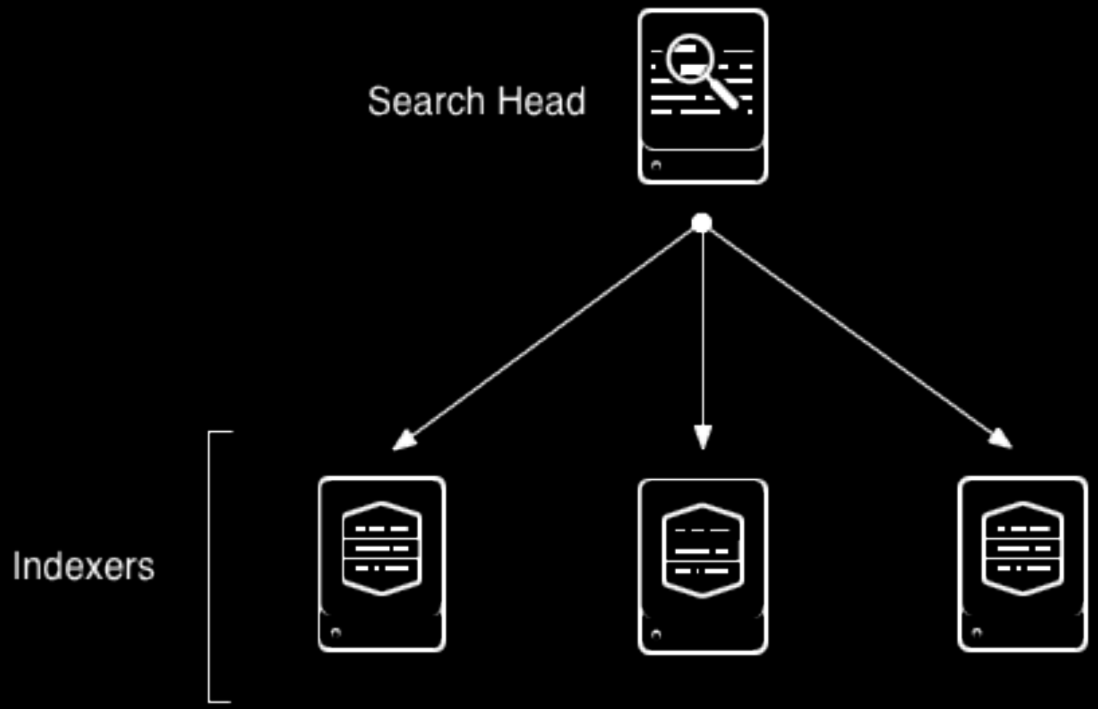
Processing components

- Forwarders
- Indexers
- Search heads

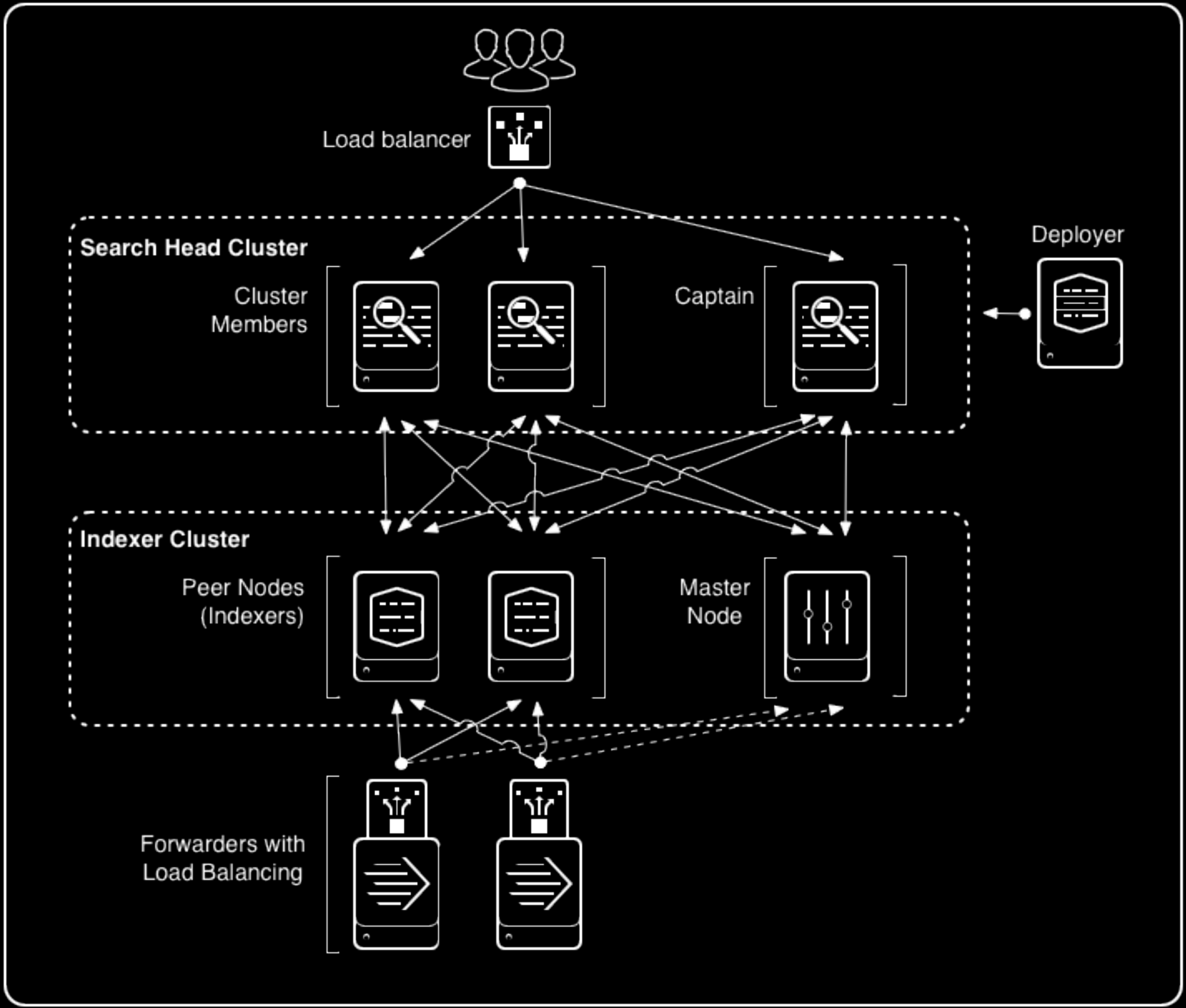
Management components

- License master
- Monitoring console
- Deployment server
- Indexer cluster master
- Search head cluster deployer

Basic Distributed Environment



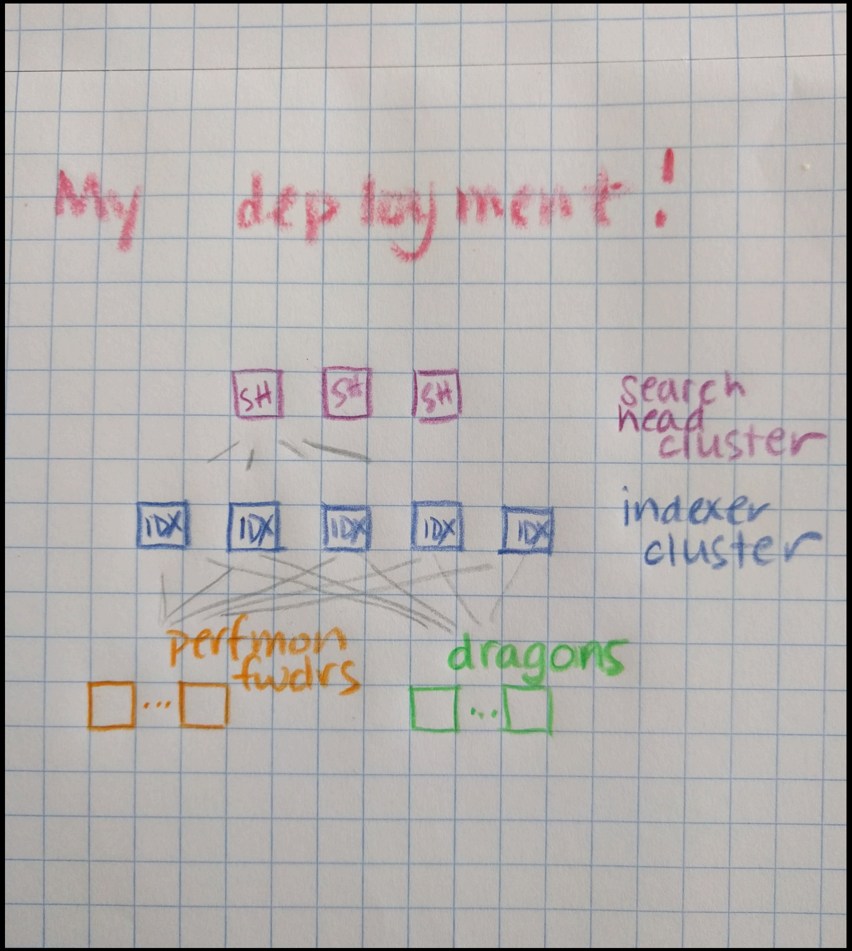
Search Head Cluster and Indexer Cluster



Draw a Diagram of Your Deployment

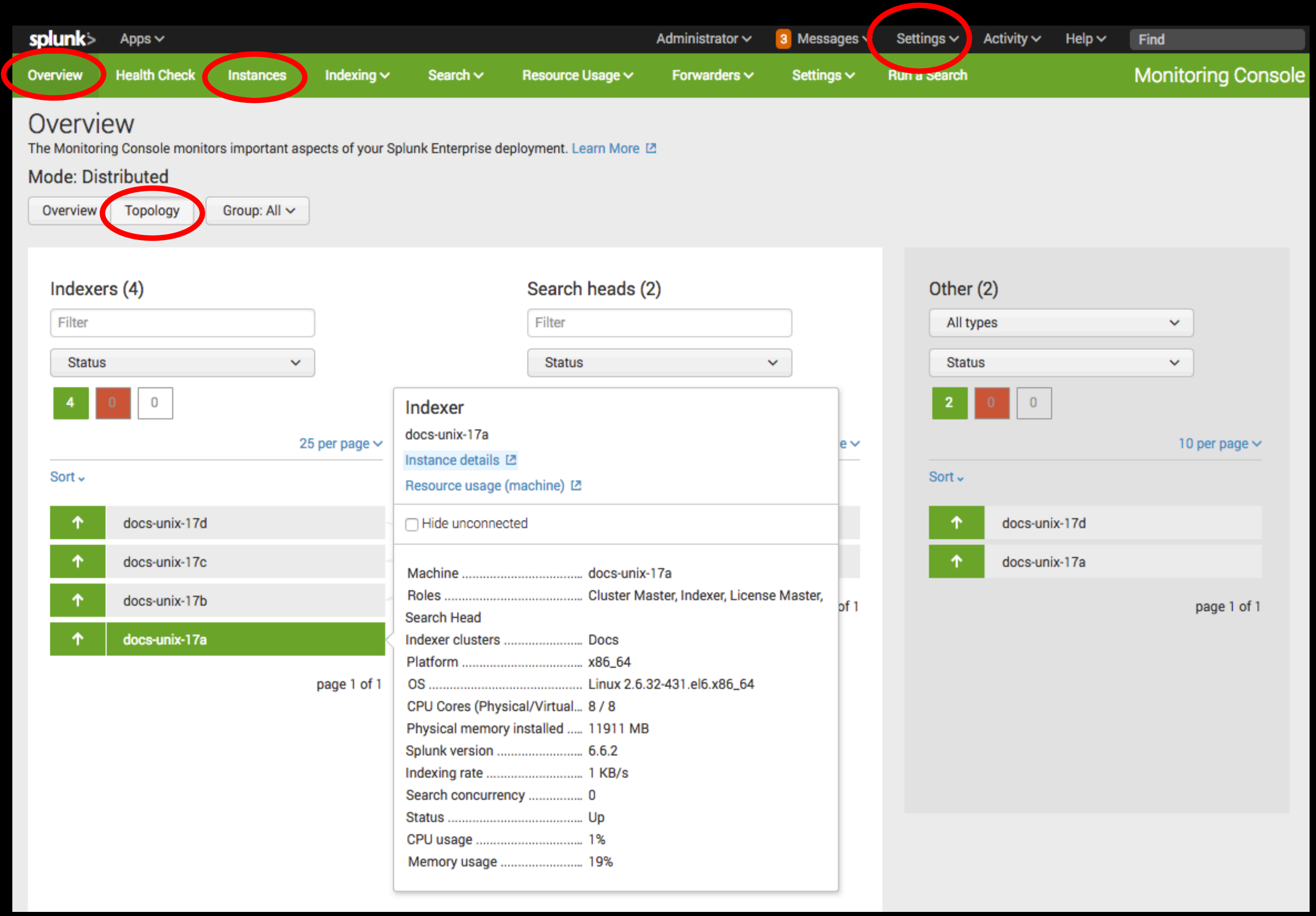
- Include every component
  - Search heads and indexers
  - Management components
  - Forwarders or groups of forwarders

- For each component, include details
  - Splunk Enterprise version
  - Whether it is running KV store
  - All open ports
  - Machine information



Discover Topology with the Monitoring Console

- Access the monitoring console
  - Click Settings > Monitoring Console
- Use the Instances page
  - Record instance, machine name, roles, cluster labels
- Use the Topology view
  - Click Overview > Topology
  - Record roles, Splunk version, OS, CPU cores



Overview

The Monitoring Console monitors important aspects of your Splunk Enterprise deployment. Learn More

Mode: Distributed

Indexer

docs-unix-17a

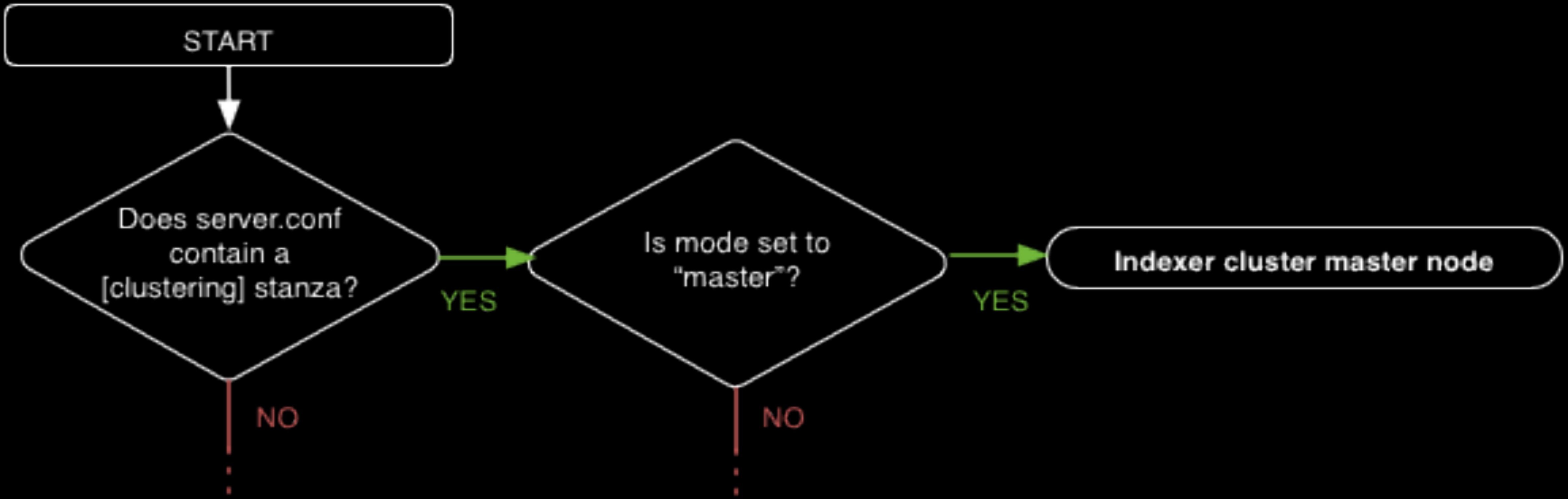
Instance details

Resource usage (machine)

☐ Hide unconnected

```
Machine ............................ docs-unix-17a
Roles .............................. Cluster Master, Indexer, License Master,
Search Head
Indexer clusters ................... Docs
Platform ........................... x86_64
OS ................................. Linux 2.6.32-431.el6.x86_64
CPU Cores (Physical/Virtual... 8 / 8
Physical memory installed ..... 11911 MB
Splunk version ..................... 6.6.2
Indexing rate ...................... 1 KB/s
Search concurrency ................. 0
Status ............................. Up
CPU usage .......................... 1%
Memory usage ....................... 19%
```

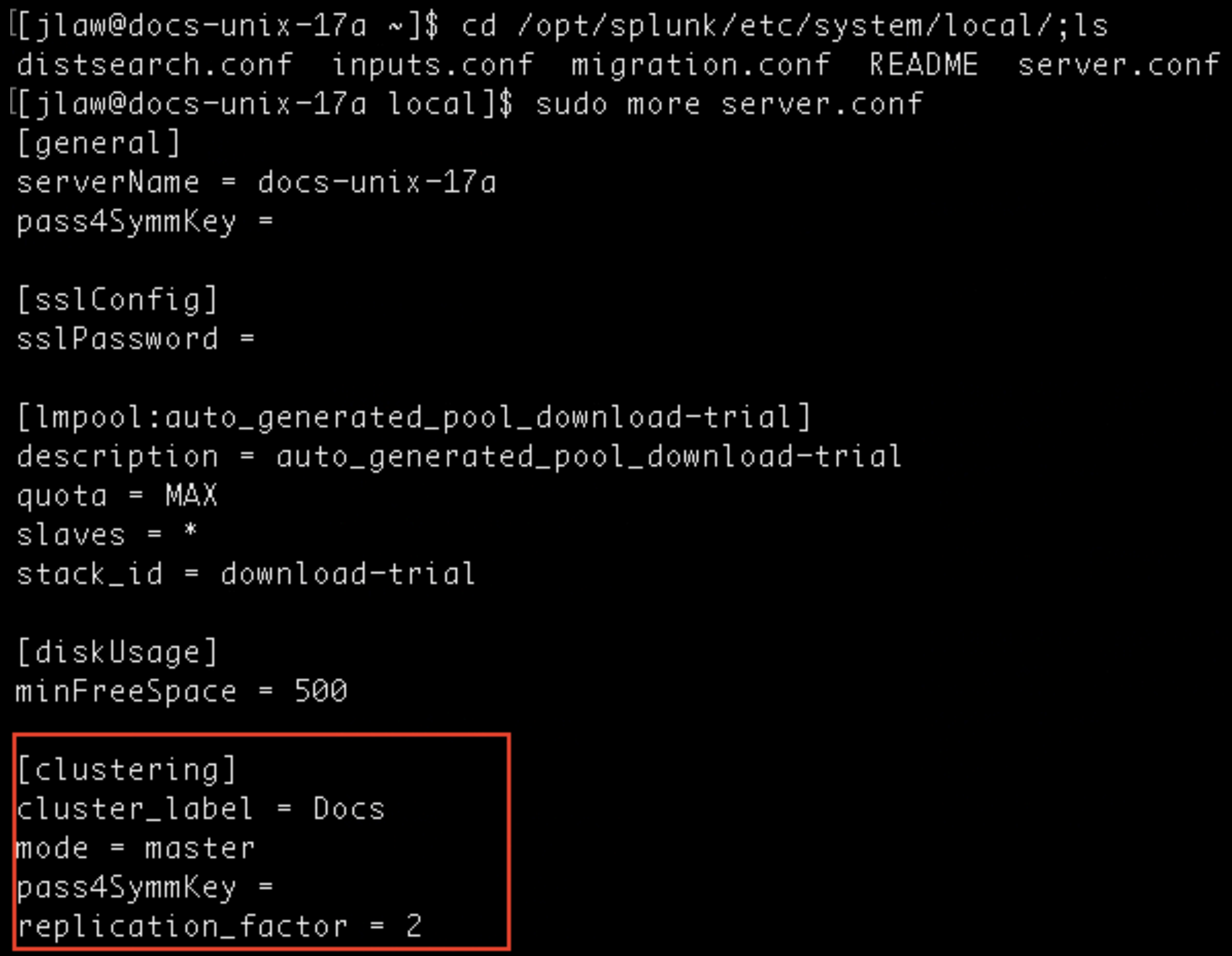
Discover Topology with Configuration Files



START
Does server.conf contain a [clustering] stanza?
YES
NO
Is mode set to "master"?
YES
NO
Indexer cluster master node

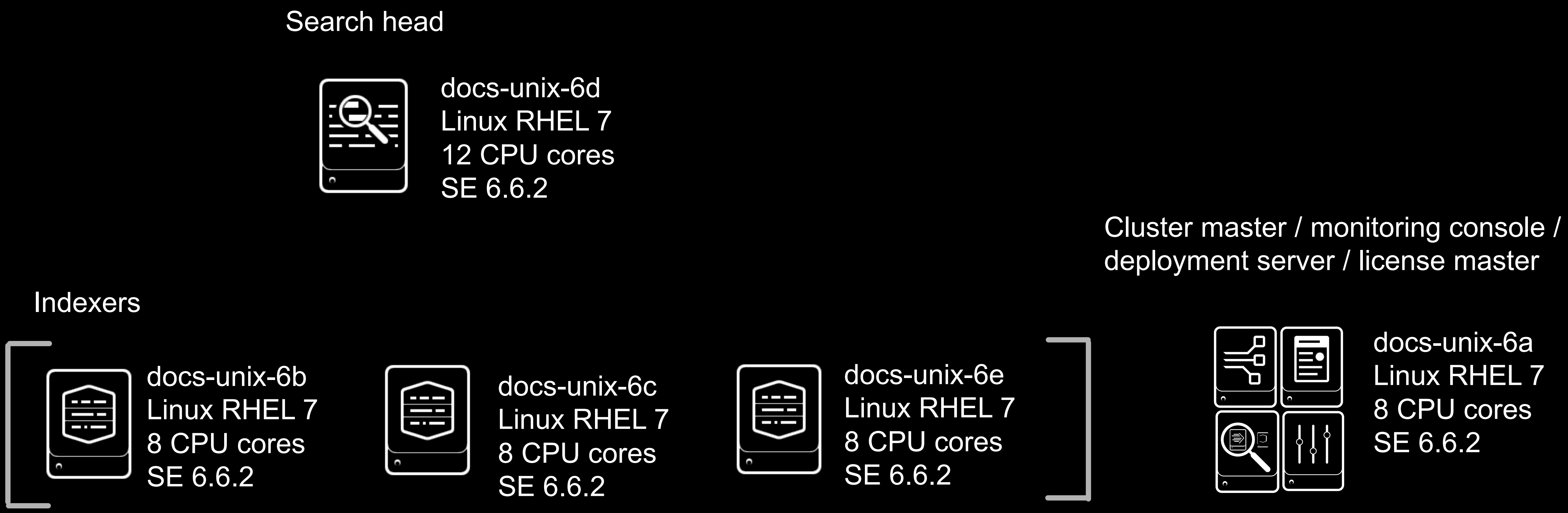
Conf File Discovery Example

- Determine whether each instance is a search head or indexer.
  - Examine `$SPLUNK_HOME/etc/system/local/server.conf`
  - Look for a `[clustering]` stanza.
  - Examine `mode` setting.
- Record findings on diagram.
- Find Splunk Enterprise version with `splunk version`



```
[jlaw@docs-unix-17a ~]$ cd /opt/splunk/etc/system/local/;ls
distsearch.conf  inputs.conf  migration.conf  README  server.conf
[jlaw@docs-unix-17a local]$ sudo more server.conf
[general]
serverName = docs-unix-17a
pass4SymmKey =

[sslConfig]
sslPassword =

[lmpool:auto_generated_pool_download-trial]
description = auto_generated_pool_download-trial
quota = MAX
slaves = *
stack_id = download-trial

[diskUsage]
minFreeSpace = 500

[clustering]
cluster_label = Docs
mode = master
pass4SymmKey =
replication_factor = 2
```

Deployment Diagram Checkpoint



Search head

docs-unix-6d
Linux RHEL 7
12 CPU cores
SE 6.6.2

Cluster master / monitoring console / deployment server / license master

Indexers

docs-unix-6b
Linux RHEL 7
8 CPU cores
SE 6.6.2

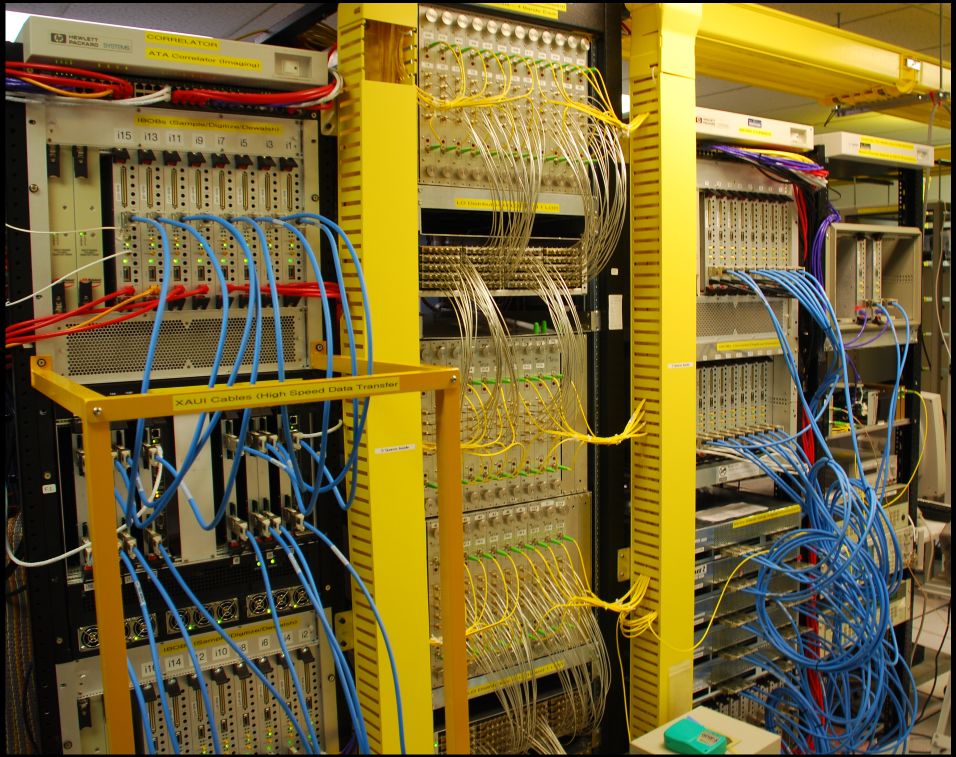
docs-unix-6c
Linux RHEL 7
8 CPU cores
SE 6.6.2

docs-unix-6e
Linux RHEL 7
8 CPU cores
SE 6.6.2

docs-unix-6a
Linux RHEL 7
8 CPU cores
SE 6.6.2

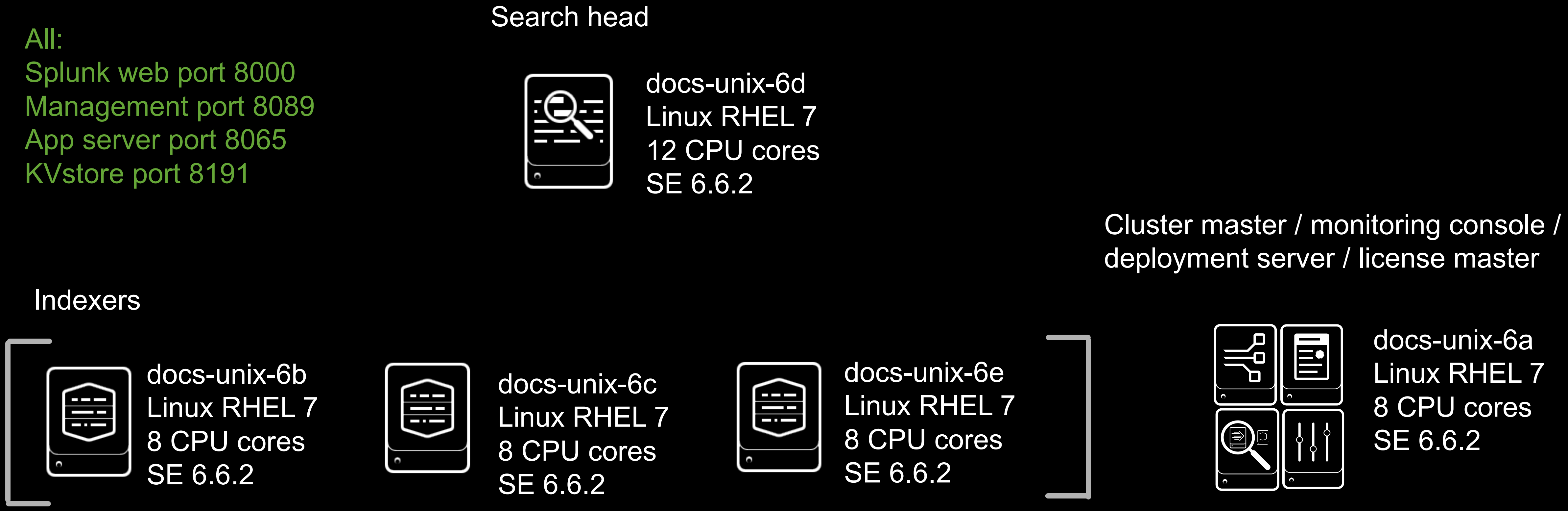
Splunk and Its Environment

- Splunk processes require open ports
  - Conventions can be reconfigured
- Find used ports for a search head
  - In Splunk Web, click Settings > Server settings > General settings
  - Record port numbers
- Find used ports for an indexer
  - On *nix, netstat or lsof system utilities
  - On Windows, netstat, netsh, or cmdlets utilities



Deployment Diagram Checkpoint

All:
Splunk web port 8000
Management port 8089
App server port 8065
KVstore port 8191



Search head

docs-unix-6d
Linux RHEL 7
12 CPU cores
SE 6.6.2

Cluster master / monitoring console / deployment server / license master

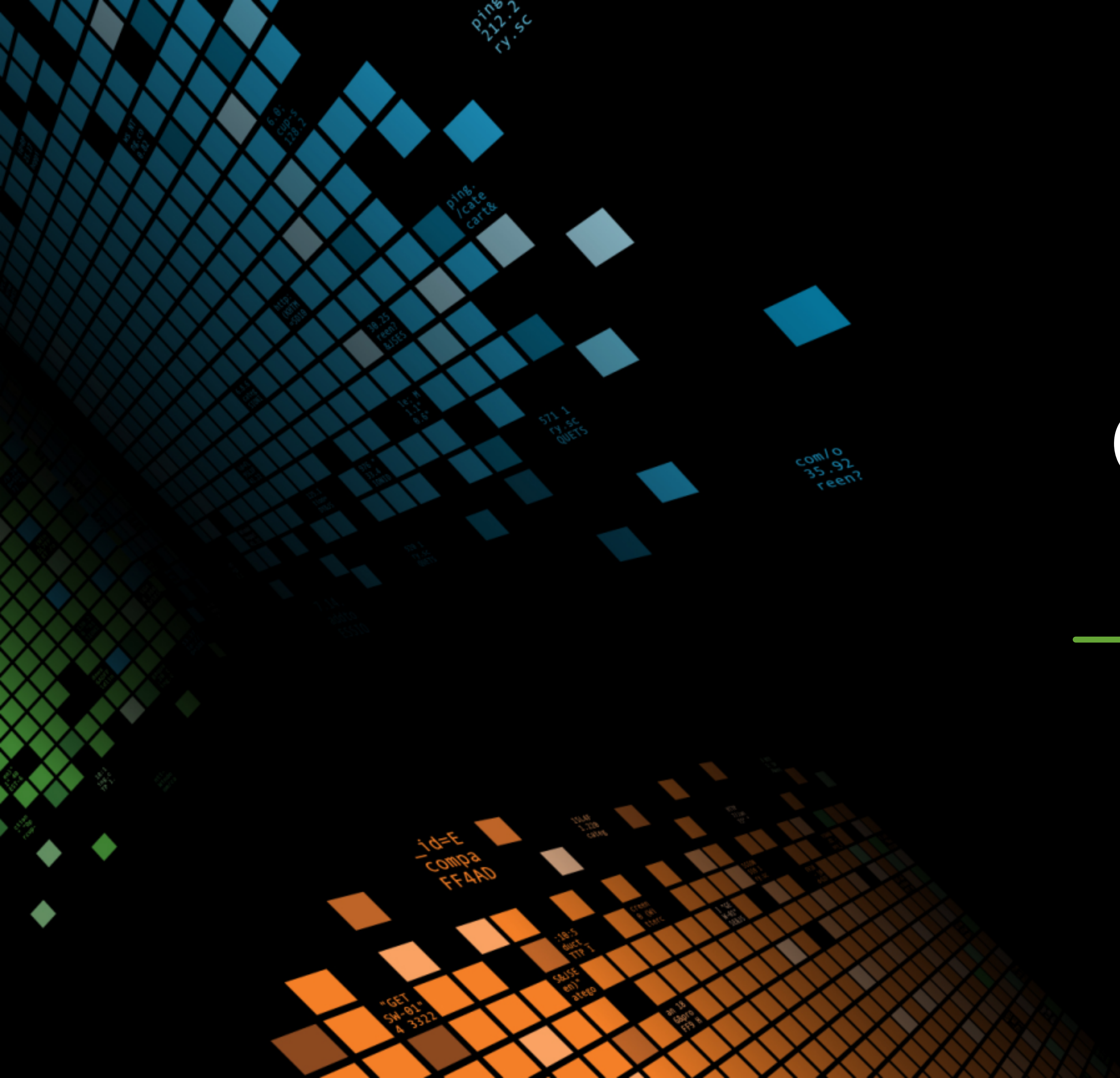
docs-unix-6a
Linux RHEL 7
8 CPU cores
SE 6.6.2

Indexers

docs-unix-6b
Linux RHEL 7
8 CPU cores
SE 6.6.2

docs-unix-6c
Linux RHEL 7
8 CPU cores
SE 6.6.2

docs-unix-6e
Linux RHEL 7
8 CPU cores
SE 6.6.2



2

Get To Know Your Data

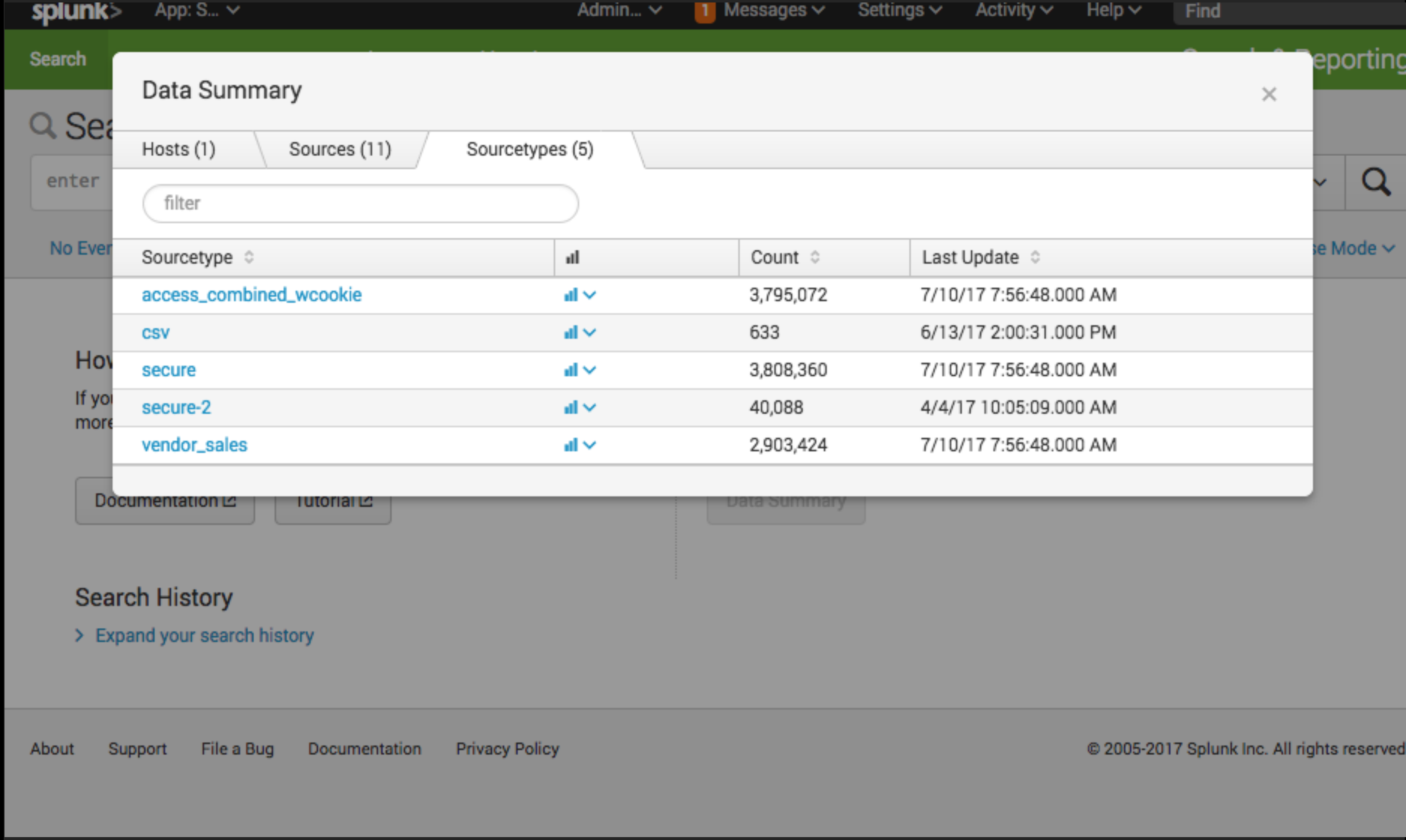
You Have Data

Learn All About It

- What kinds of data does your deployment store?
- Where does that data come from?
- What management rules have been set up for this data?

Review The Data Summary

- Find it in the Search and Reporting view.
- Instantly identify the different types of data in your system.
- Generate timecharts for specific hosts, sources, or source types.



Data Summary

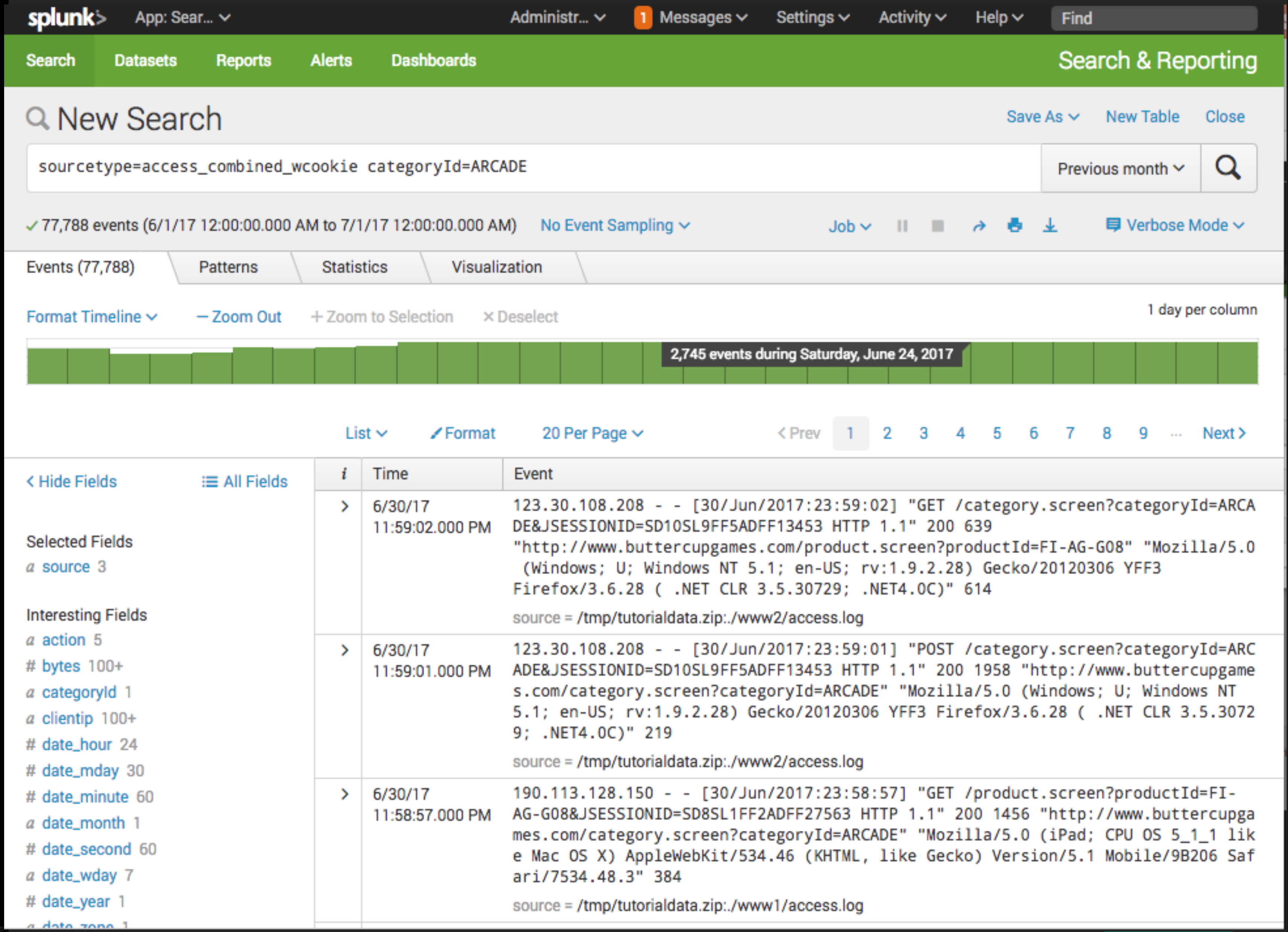
Hosts (1) | Sources (11) | Sourcetypes (5)

filter

Sourcetype		Count	Last Update
access_combined_wcookie		3,795,072	7/10/17 7:56:48.000 AM
csv		633	6/13/17 2:00:31.000 PM
secure		3,808,360	7/10/17 7:56:48.000 AM
secure-2		40,088	4/4/17 10:05:09.000 AM
vendor_sales		2,903,424	7/10/17 7:56:48.000 AM

Run Searches on Your Data

- Explore your data through simple searches.
- Examine the Fields sidebar and study interesting fields.
- Use the Patterns tab to investigate event patterns.



```
sourcetype=access_combined_wcookie categoryId=ARCADE
```

✓ 77,788 events (6/1/17 12:00:00.000 AM to 7/1/17 12:00:00.000 AM)

Selected Fields
a source 3

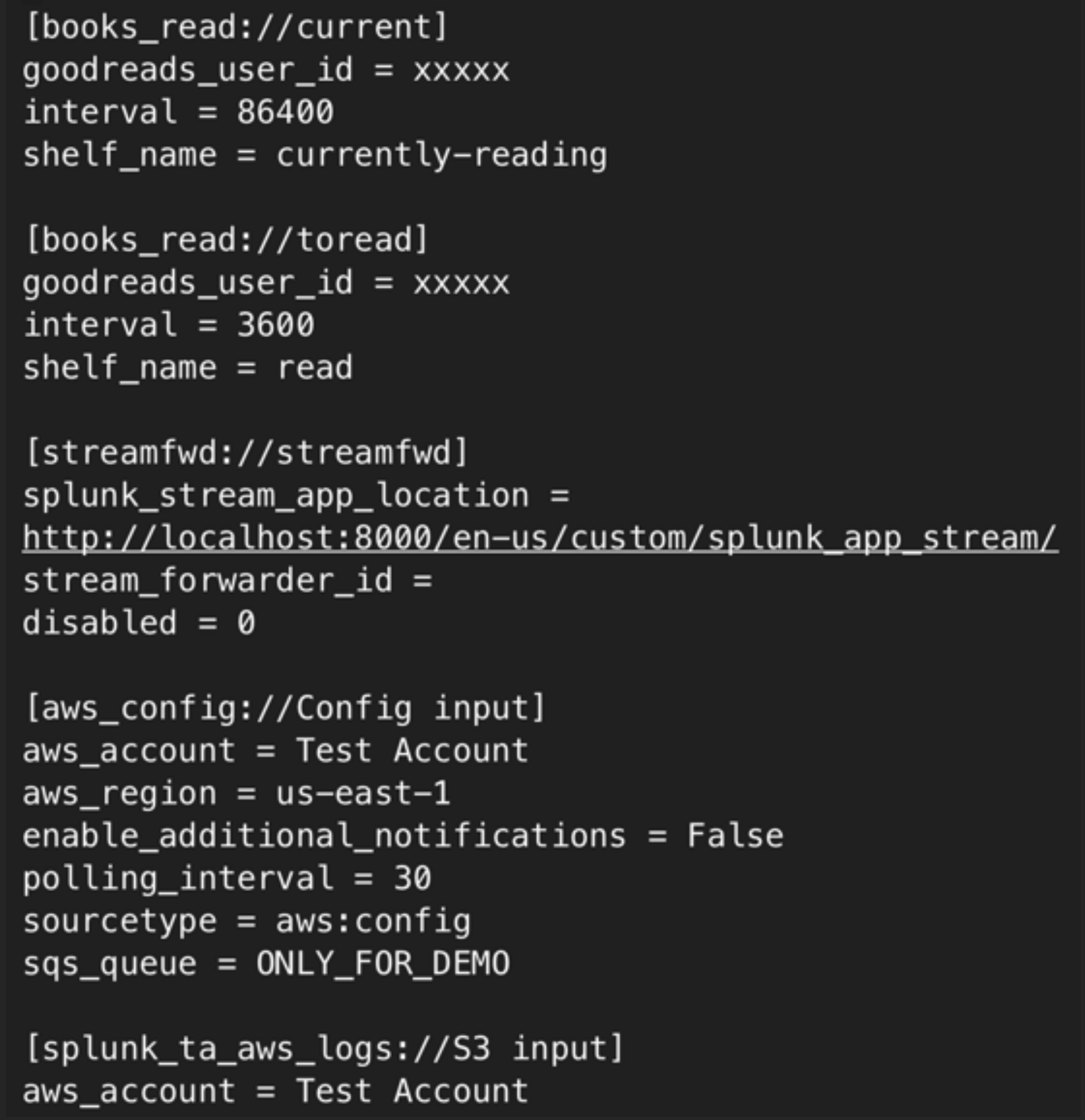
Interesting Fields
a action 5
# bytes 100+
a categoryId 1
a clientip 100+
# date_hour 24
# date_mday 30
# date_minute 60
a date_month 1
# date_second 60
a date_wday 7
# date_year 1
a date_zone 1

Time	Event
6/30/17 11:59:02.000 PM	123.30.108.208 - - [30/Jun/2017:23:59:02] "GET /category.screen?categoryId=ARCADE&JSESSIONID=SD10SL9FF5ADFF13453 HTTP 1.1" 200 639 "http://www.buttercupgames.com/product.screen?productId=FI-AG-G08" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 614 source = /tmp/tutorialdata.zip:./www2/access.log
6/30/17 11:59:01.000 PM	123.30.108.208 - - [30/Jun/2017:23:59:01] "POST /category.screen?categoryId=ARCADE&JSESSIONID=SD10SL9FF5ADFF13453 HTTP 1.1" 200 1958 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 219 source = /tmp/tutorialdata.zip:./www2/access.log
6/30/17 11:58:57.000 PM	190.113.128.150 - - [30/Jun/2017:23:58:57] "GET /product.screen?productId=FI-AG-G08&JSESSIONID=SD8SL1FF2ADFF27563 HTTP 1.1" 200 1456 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 384 source = /tmp/tutorialdata.zip:./www1/access.log

splunk> .conf2017

Study Your Data Inputs

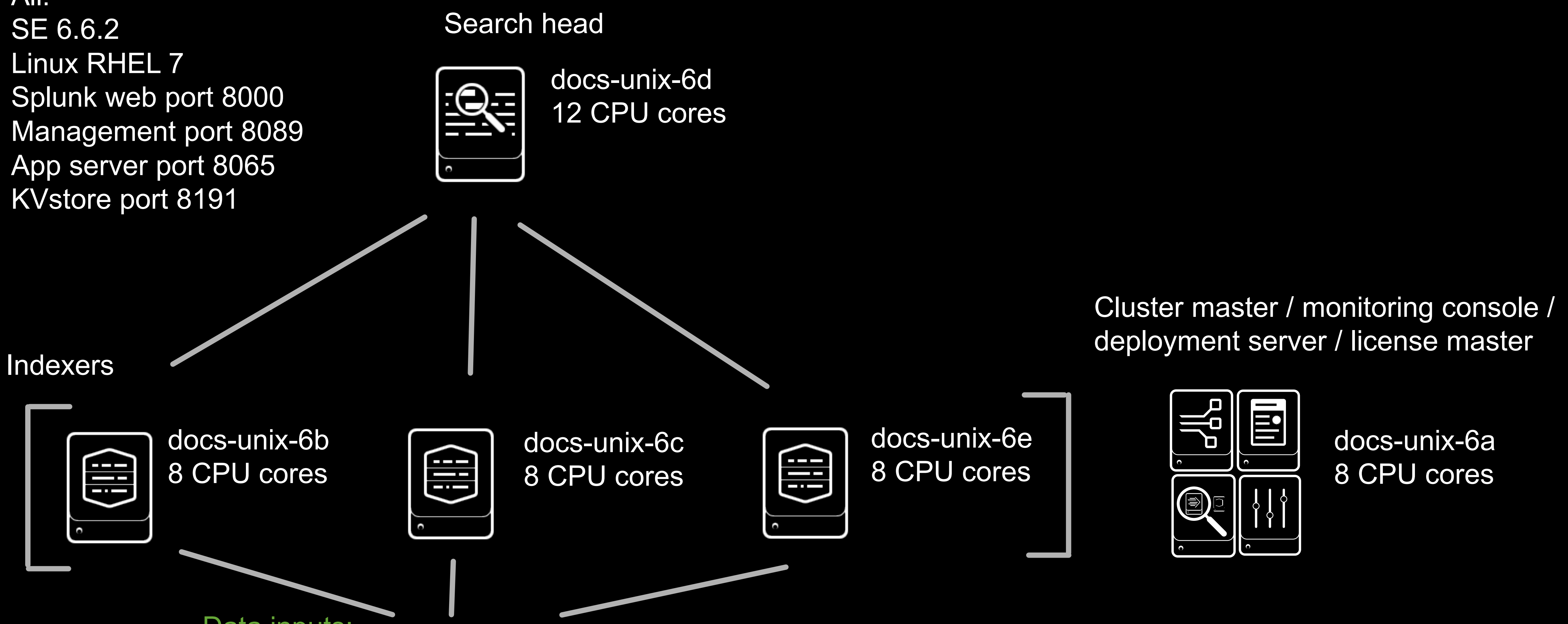
- The inputs.conf file controls:
  - When data is collected
  - What types of data are collected
- Check inputs.conf on:
  - Indexers and forwarders
  - Apps and add-ons
  - Deployment servers



```
[books_read://current]
goodreads_user_id = xxxxx
interval = 86400
shelf_name = currently-reading

[books_read://toread]
goodreads_user_id = xxxxx
interval = 3600
shelf_name = read

[streamfwd://streamfwd]
splunk_stream_app_location =
http://localhost:8000/en-us/custom/splunk_app_stream/
stream_forwarder_id =
disabled = 0

[aws_config://Config input]
aws_account = Test Account
aws_region = us-east-1
enable_additional_notifications = False
polling_interval = 30
sourcetype = aws:config
sqs_queue = ONLY_FOR_DEMO

[splunk_ta_aws_logs://S3 input]
aws_account = Test Account
```

Deployment Diagram Checkpoint

All:
SE 6.6.2
Linux RHEL 7
Splunk web port 8000
Management port 8089
App server port 8065
KVstore port 8191



Search head

docs-unix-6d
12 CPU cores

Indexers

docs-unix-6b
8 CPU cores

docs-unix-6c
8 CPU cores

docs-unix-6e
8 CPU cores

Cluster master / monitoring console / deployment server / license master

docs-unix-6a
8 CPU cores

Data inputs:
HEC: Docteam network monitoring
Stream: Robin's books, Steven's monitoring

3

Survey Your Apps and Add-ons

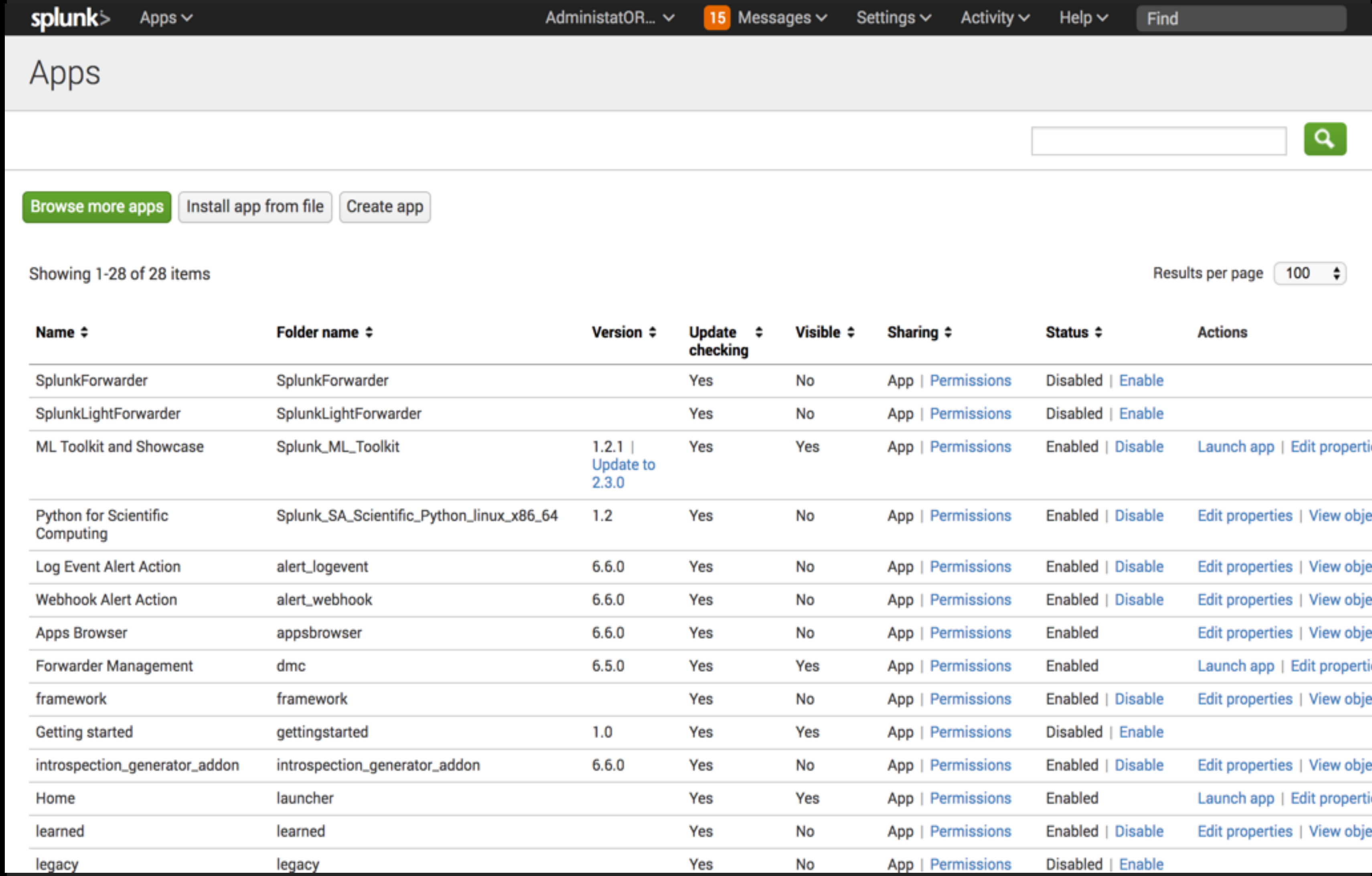
Apps and Add-ons

What's Running In Your Deployment?

- Apps
  - Have their own, often quite specialized UIs
  - Focus on specific business use-cases
- Add-ons
  - Contain knowledge objects that help with data ingestion
  - Often designed to be paired with apps
  - Usually do not have UI elements of their own

See What's Installed

- Open your app list
  - Select Apps > Manage Apps
  - Note which items are disabled
- Review app and add-on objects
  - Select Settings > All configurations
  - Filter the list by app



Apps

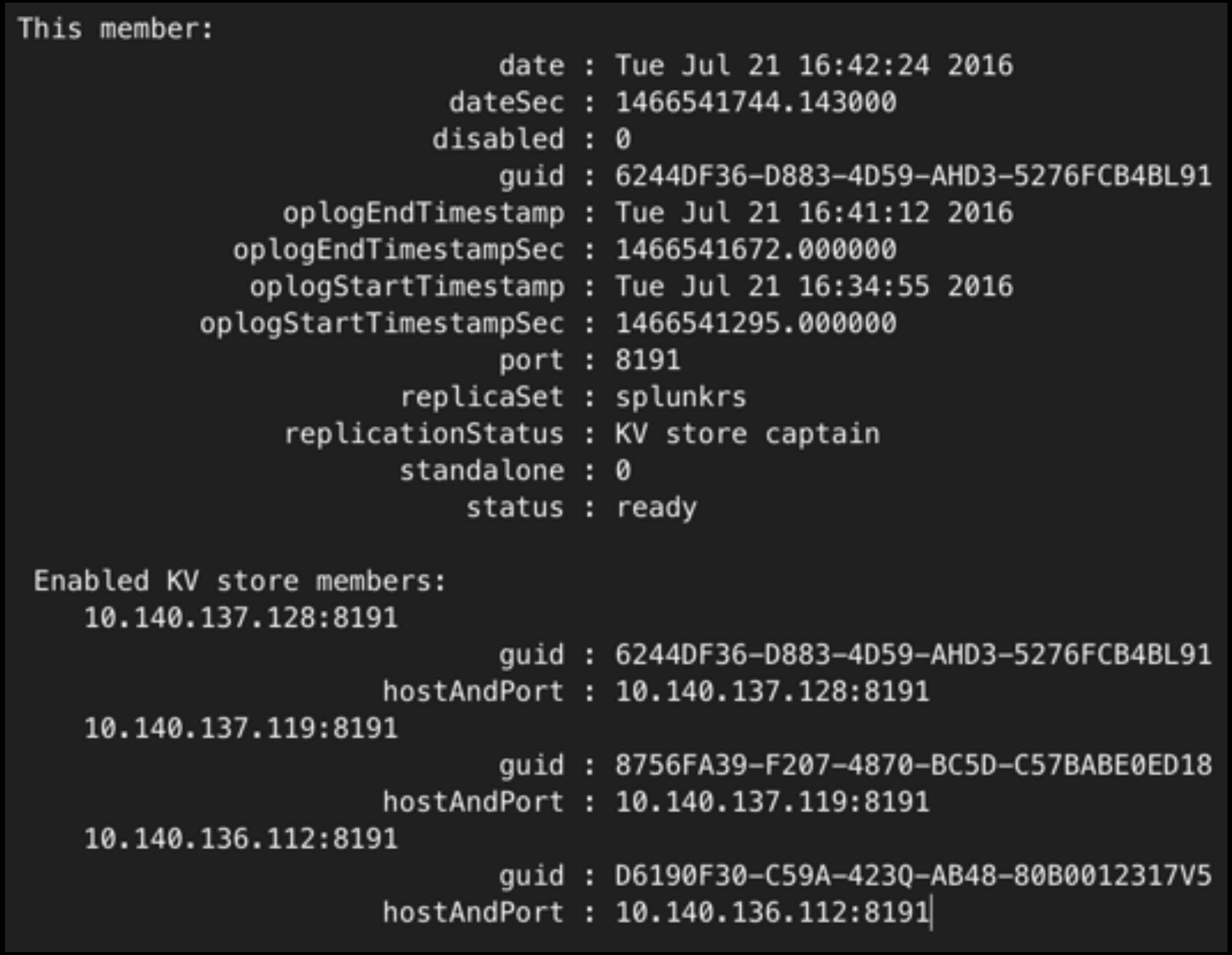
Showing 1-28 of 28 items

Results per page 100

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
ML Toolkit and Showcase	Splunk_ML_Toolkit	1.2.1 | Update to 2.3.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properti
Python for Scientific Computing	Splunk_SA_Scientific_Python_linux_x86_64	1.2	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View obje
Log Event Alert Action	alert_logevent	6.6.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View obje
Webhook Alert Action	alert_webhook	6.6.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View obje
Apps Browser	appsbrowser	6.6.0	Yes	No	App | Permissions	Enabled	Edit properties | View obje
Forwarder Management	dmc	6.5.0	Yes	Yes	App | Permissions	Enabled	Launch app | Edit properti
framework	framework		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View obje
Getting started	gettingstarted	1.0	Yes	Yes	App | Permissions	Disabled | Enable	
introspection_generator_addon	introspection_generator_addon	6.6.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View obje
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properti
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View obje
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable	

The KV Store and Your Apps

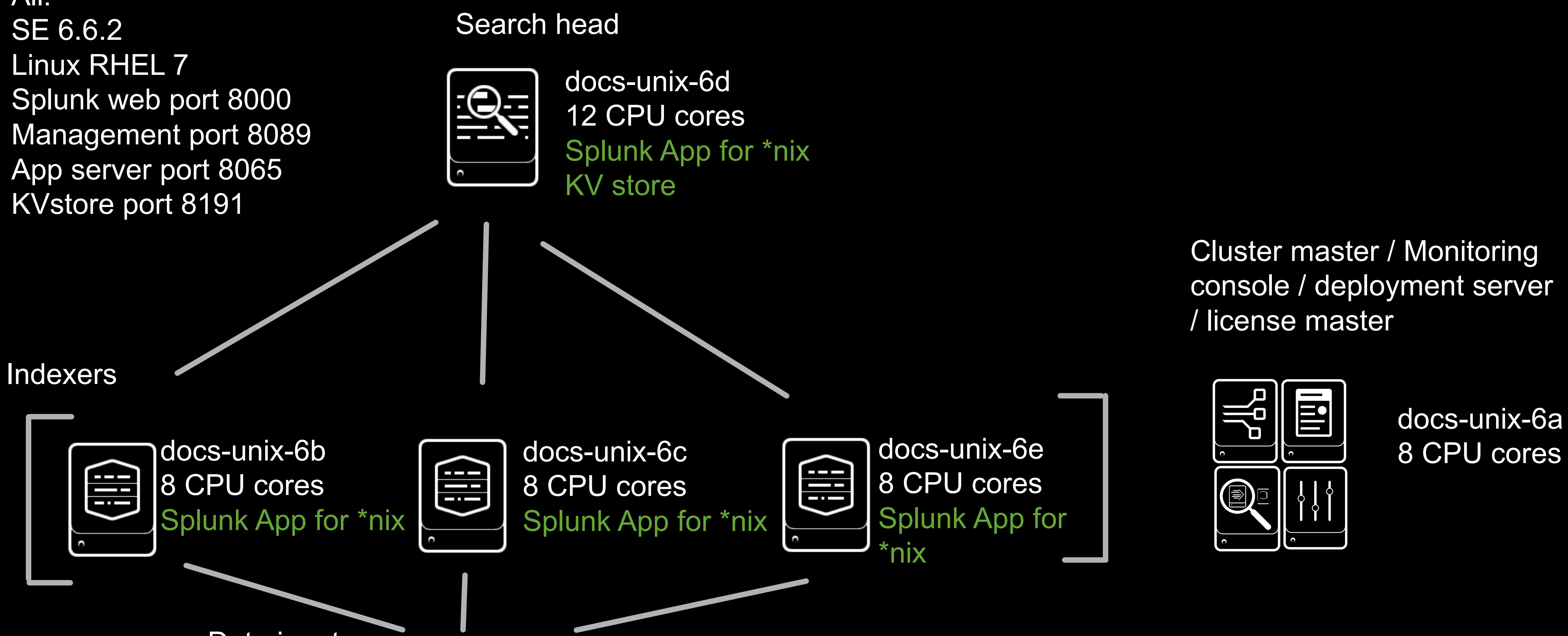
- The app key value store can retain state information about apps
- KV store processes are independent of those of search head clusters
- Find KV Store members
  - `./splunk show kvstore-status`
- Locate apps with KV store collections
  - `./splunk btool collectionslist —debug`
  - In the results, look for items belonging to `$SPLUNK_HOME/etc/apps`.



```
This member:
                          date : Tue Jul 21 16:42:24 2016
                       dateSec : 1466541744.143000
                      disabled : 0
                          guid : 6244DF36-D883-4D59-AHD3-5276FCB4BL91
             oplogEndTimestamp : Tue Jul 21 16:41:12 2016
          oplogEndTimestampSec : 1466541672.000000
           oplogStartTimestamp : Tue Jul 21 16:34:55 2016
        oplogStartTimestampSec : 1466541295.000000
                          port : 8191
                    replicaSet : splunkrs
             replicationStatus : KV store captain
                    standalone : 0
                        status : ready

 Enabled KV store members:
    10.140.137.128:8191
                          guid : 6244DF36-D883-4D59-AHD3-5276FCB4BL91
                   hostAndPort : 10.140.137.128:8191
    10.140.137.119:8191
                          guid : 8756FA39-F207-4870-BC5D-C57BABE0ED18
                   hostAndPort : 10.140.137.119:8191
    10.140.136.112:8191
                          guid : D6190F30-C59A-423Q-AB48-80B0012317V5
                   hostAndPort : 10.140.136.112:8191
```

Deployment Diagram Checkpoint

All:
SE 6.6.2
Linux RHEL 7
Splunk web port 8000
Management port 8089
App server port 8065
KVstore port 8191



Search head

docs-unix-6d
12 CPU cores
Splunk App for *nix
KV store

Indexers

docs-unix-6b
8 CPU cores
Splunk App for *nix

docs-unix-6c
8 CPU cores
Splunk App for *nix

docs-unix-6e
8 CPU cores
Splunk App for *nix

Cluster master / Monitoring console / deployment server / license master

docs-unix-6a
8 CPU cores

Data inputs:
HEC: Docteam network monitoring
Stream: Robin’s books, Steve’s monitoring

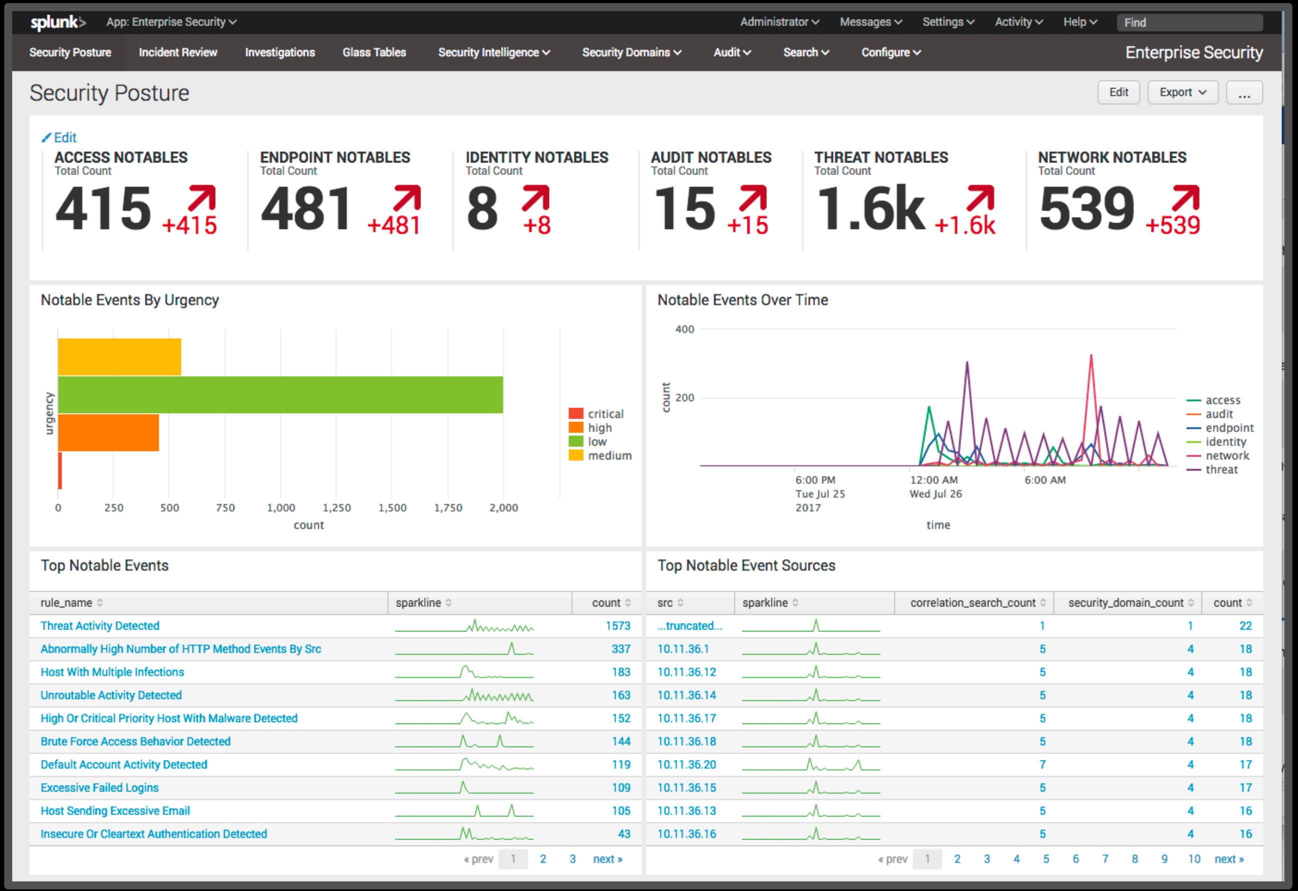
Considerations for Splunk Premium Solutions

- Premium Splunk apps require additional oversight
  - Splunk Enterprise Security (ES)
  - Splunk IT Service Intelligence (ITSI)
  - Splunk User Behavior Analytics (UBA)
- ES and ITSI tend to be resource-intensive
- They can have specific search head and indexer requirements
  - For example, ES needs a dedicated search head

Enterprise Security

What To Watch Out For

- Heavy reliance on data models, lookups, modular inputs, KV Store, and scheduled searches
- Keep an eye on:
  - The Content Profile dashboard
  - The Data Model Audit dashboard
  - Correlation searches



ACCESS NOTABLES Total Count 415 +415

ENDPOINT NOTABLES Total Count 481 +481

IDENTITY NOTABLES Total Count 8 +8

AUDIT NOTABLES Total Count 15 +15

THREAT NOTABLES Total Count 1.6k +1.6k

NETWORK NOTABLES Total Count 539 +539

Top Notable Events

rule_name	sparkline	count
Threat Activity Detected		1573
Abnormally High Number of HTTP Method Events By Src		337
Host With Multiple Infections		183
Unroutable Activity Detected		163
High Or Critical Priority Host With Malware Detected		152
Brute Force Access Behavior Detected		144
Default Account Activity Detected		119
Excessive Failed Logins		109
Host Sending Excessive Email		105
Insecure Or Cleartext Authentication Detected		43

« prev 1 2 3 next »

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
...truncated...		1	1	22
10.11.36.1		5	4	18
10.11.36.12		5	4	18
10.11.36.14		5	4	18
10.11.36.17		5	4	18
10.11.36.18		5	4	18
10.11.36.20		7	4	17
10.11.36.15		5	4	17
10.11.36.13		5	4	16
10.11.36.16		5	4	16

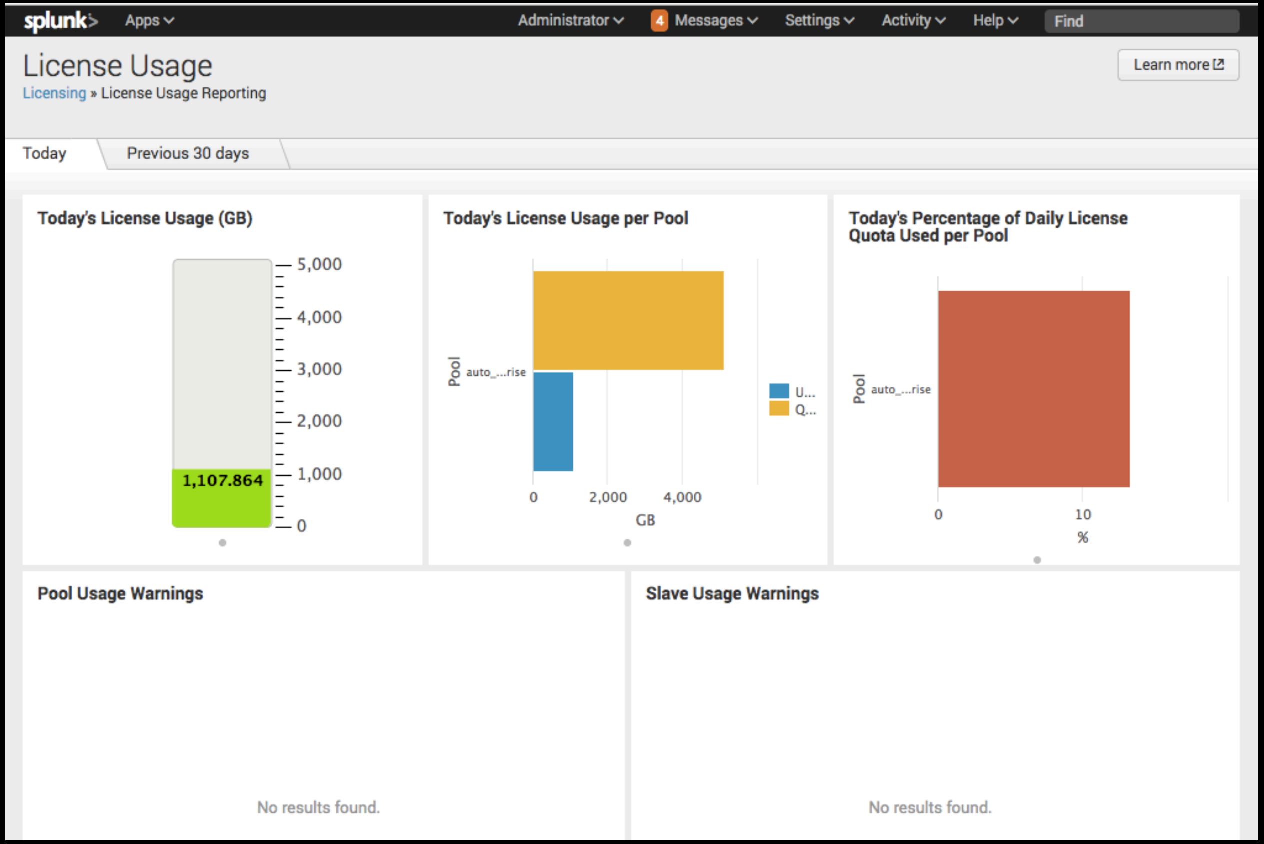
« prev 1 2 3 4 5 6 7 8 9 10 next »

4

Check Your Licenses

Understand Your Licenses

- Survey licenses in Splunk Web on the license master.
  - Settings > Licensing
  - Five warnings in 30 day window = violation
  - If your license master is 6.5.0+, consider asking for a no-enforcement license
- Enable licensing alerts
  - The monitoring console comes with two licensing alerts.
  - Update the alert actions for your notification preferences.



License Usage

Licensing » License Usage Reporting

Today's License Usage (GB)

Today's License Usage per Pool

Today's Percentage of Daily License Quota Used per Pool

Pool Usage Warnings

No results found.

Slave Usage Warnings

No results found.

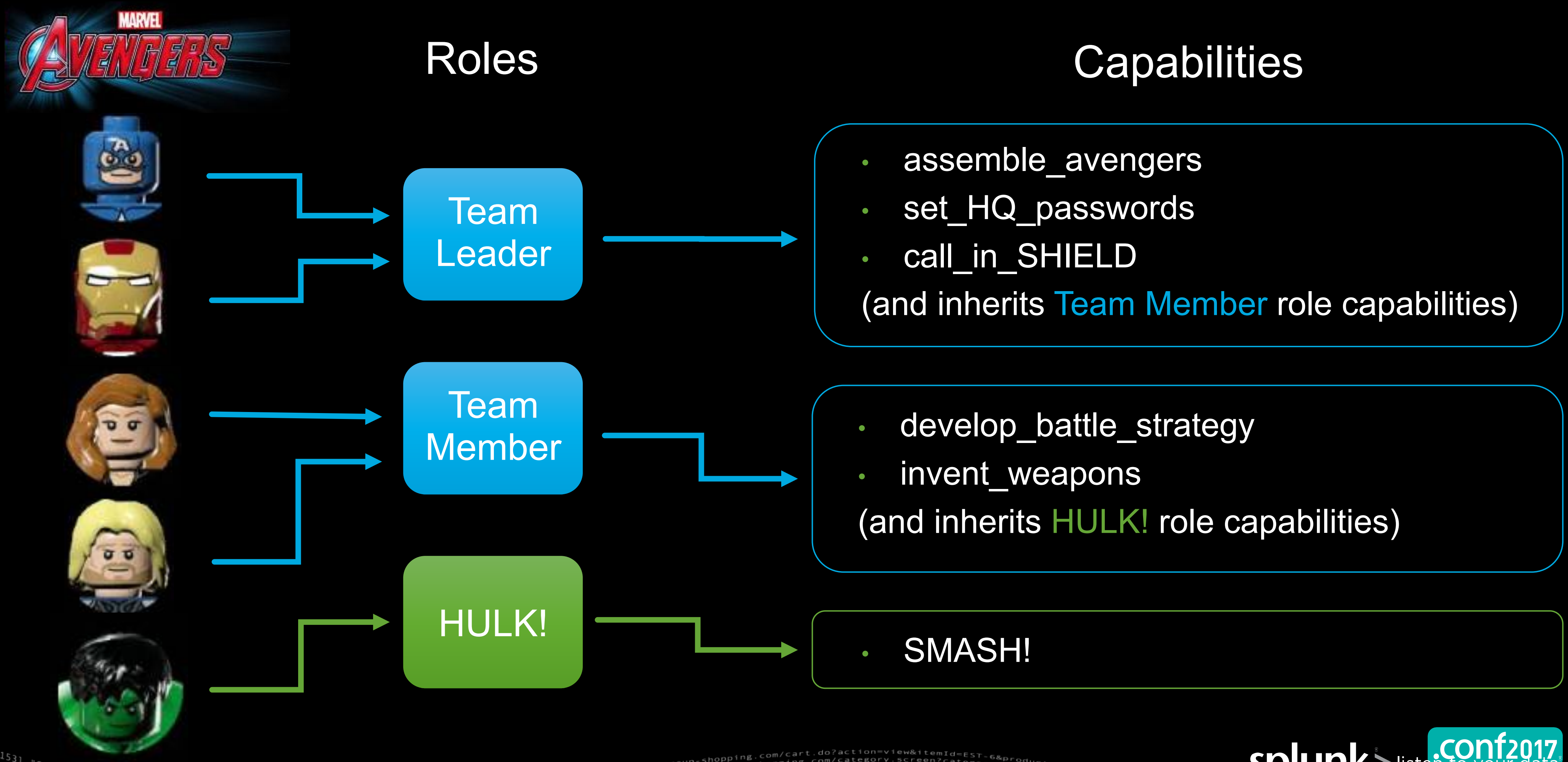
5

Users, Roles, and Authentication

splunk> .conf2017

Users, Roles, and Capabilities

Roles Determine Actions Users Can Perform



Roles

Capabilities

Team Leader

- assemble_avengers
- set_HQ_passwords
- call_in_SHIELD

(and inherits Team Member role capabilities)

Team Member

- develop_battle_strategy
- invent_weapons

(and inherits HULK! role capabilities)

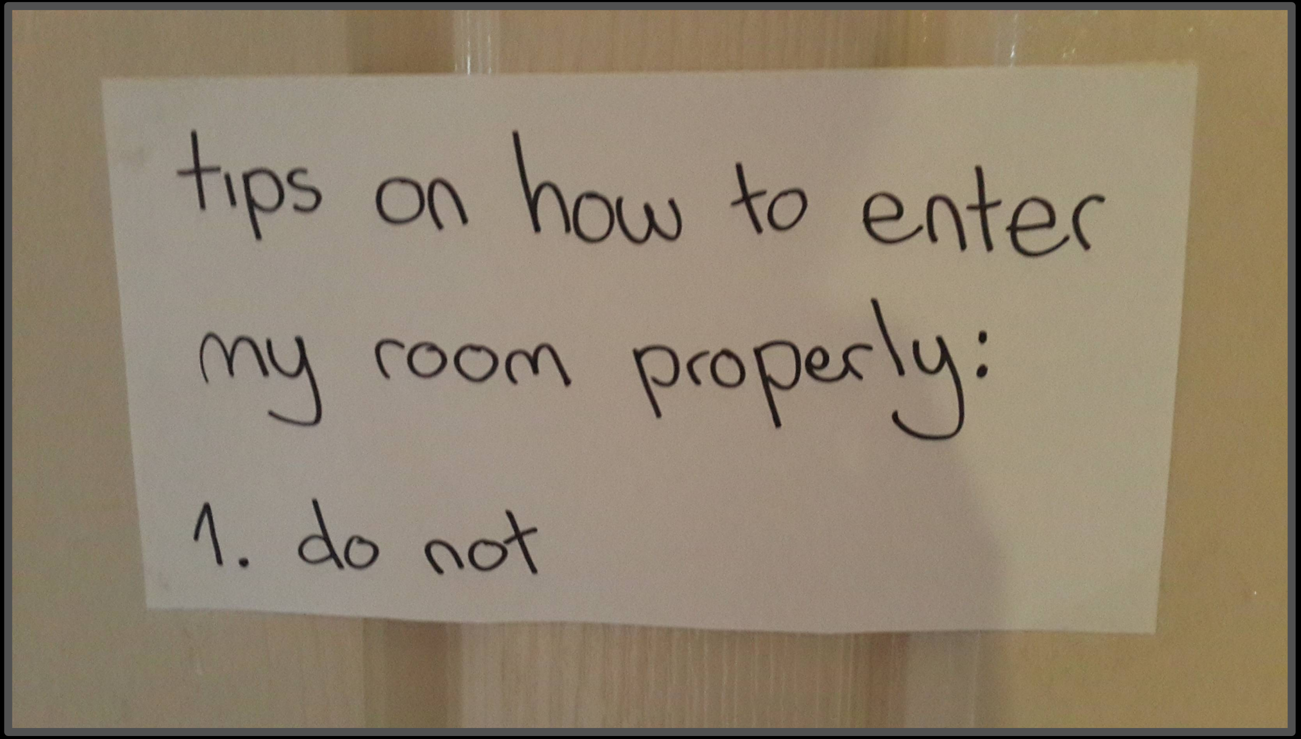
HULK!

- SMASH!

Roles and Data Access

Roles Control What Your Users Can See

- Know how your roles define data access rights
  - Index restrictions
  - Search result filters
  - Search time range limits
  - Capability assignment
  - Role inheritance



- Go to Settings > Access Controls > Roles to review your role settings

User Authentication

Let The Right Ones In

- Select Settings > Access Controls > Authentication Method to review or create configurations for
  - LDAP authentication
  - SAML authentication for SSO
  - Multifactor authentication with Duo Security
- ProxySSO
  - Review or create configurations in the settings stanza of web.conf

6

Review Your Deployment Security

Secure Your Communications With SSL

- SSL certificates encrypt and authenticate communications between:
  - The browser and Splunk Web
  - Splunk Enterprise components (except for search heads and peers in distributed search environments)

- Default SSL certificates are located in $SPLUNK_HOME/etc/auth

- Verify your SSL configurations with the following search:

```
index=_internal source=*metrics.log* group=tcpin_connections | dedup hostname |
table _time hostname version sourceIp destPort ssl
```

Key-based Encryption in Splunk Enterprise

- Distributed search
  - Search heads and peers use public-key encryption
  - If necessary, SSL can be configured for each member of a search head cluster
  - Check requireClientCert in server.conf
- The splunk.secret key
  - Collects and encrypts authentication information
  - Stored in .conf files

7

Monitor the Health of Your System

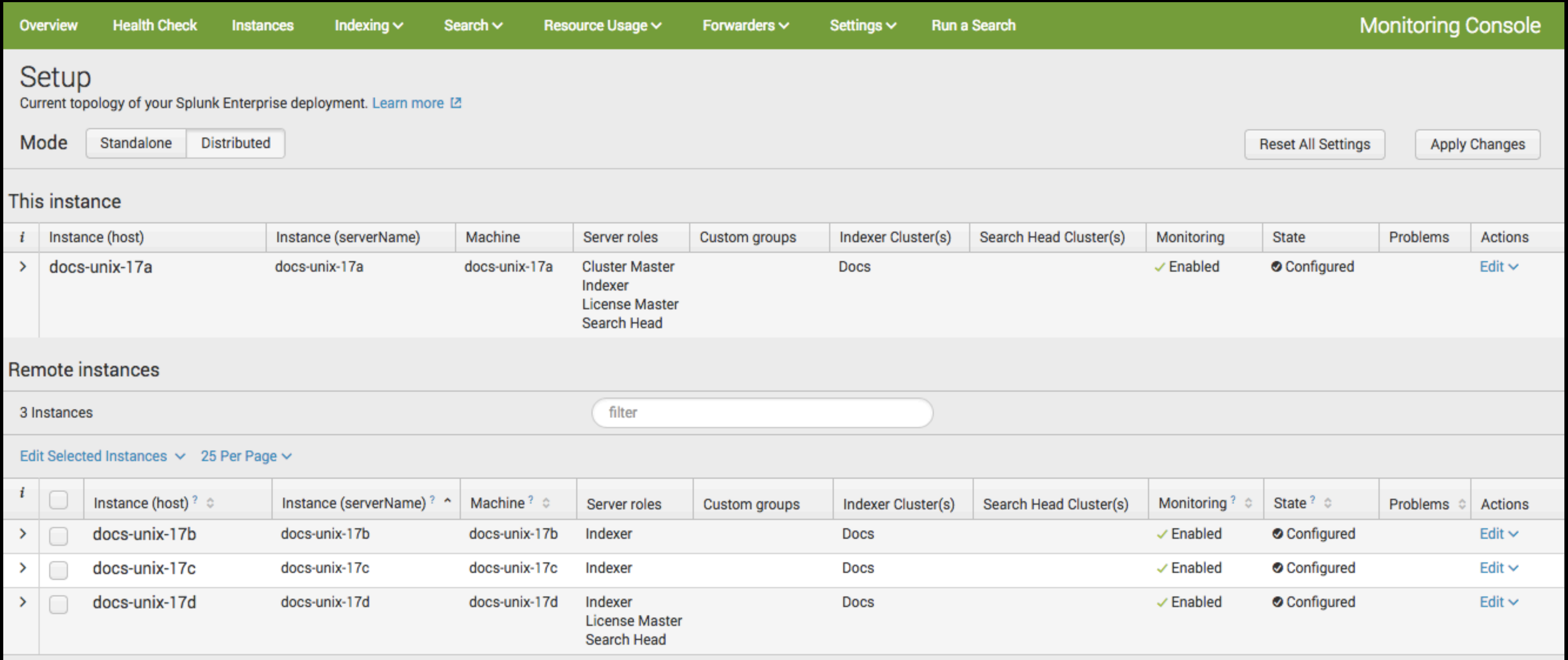
Monitor Your Deployment's Health

- Monitor for these things:
  - CPU load, memory utilization, and disk usage
  - On a *nix system, OS level settings such as THP and ulimits
  - Indexing rate
  - Skipped searches
  - Bad data onboarding practices

- Survey for existing monitoring apps
  - Monitoring console
  - Splunk on Splunk (SoS)
  - Fire Brigade
  - Custom apps

- Set up monitoring console

Demo of Monitoring Console Setup and Health Check



Setup

Current topology of your Splunk Enterprise deployment. Learn more

Mode: Standalone | Distributed

This instance

i	Instance (host)	Instance (serverName)	Machine	Server roles	Custom groups	Indexer Cluster(s)	Search Head Cluster(s)	Monitoring	State	Problems	Actions
>	docs-unix-17a	docs-unix-17a	docs-unix-17a	Cluster Master Indexer License Master Search Head		Docs		✓ Enabled	Configured		Edit

Remote instances

3 Instances

i	□	Instance (host)	Instance (serverName)	Machine	Server roles	Custom groups	Indexer Cluster(s)	Search Head Cluster(s)	Monitoring	State	Problems	Actions
>	□	docs-unix-17b	docs-unix-17b	docs-unix-17b	Indexer		Docs		✓ Enabled	Configured		Edit
>	□	docs-unix-17c	docs-unix-17c	docs-unix-17c	Indexer		Docs		✓ Enabled	Configured		Edit
>	□	docs-unix-17d	docs-unix-17d	docs-unix-17d	Indexer License Master Search Head		Docs		✓ Enabled	Configured		Edit

8

Investigate Your Knowledge Objects

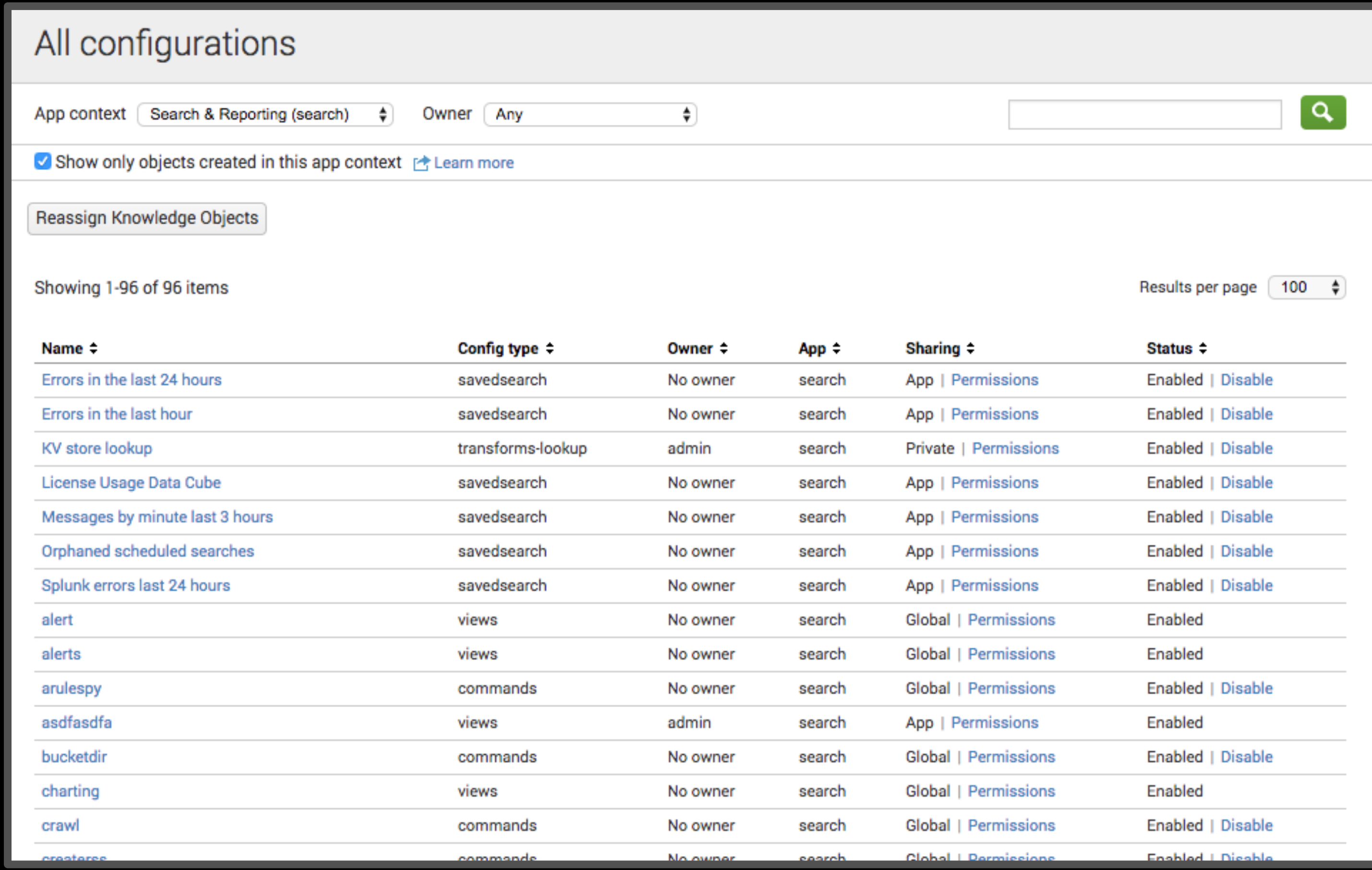
Knowledge Objects

Collect Them All

- Saved searches, reports, and alerts
- Extracted fields
- Calculated fields
- Event types
- Tags
- Aliases
- Lookups
- Search macros
- Data models and datasets
- UI components

Survey Your Knowledge Objects

- The Knowledge section of the Settings menu has all of the object pages
- Open the All Configurations page to see all your objects in one place
  - Filter by app
  - Organize by name, type, or owner
- There are a lot of considerations
  - Naming conflicts
  - Interdependency issues
  - Object sharing and permissions
  - Data model, dataset, and report acceleration



All configurations

App context: Search & Reporting (search)
Owner: Any

☑ Show only objects created in this app context

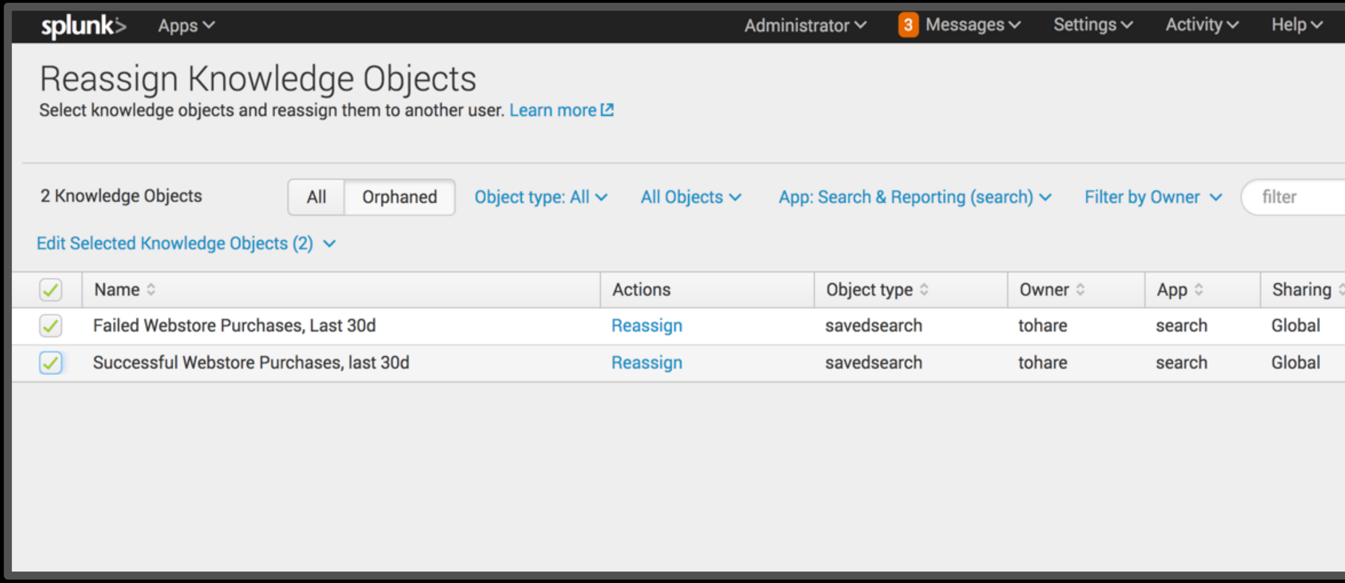
Showing 1-96 of 96 items

Results per page: 100

Name	Config type	Owner	App	Sharing	Status
Errors in the last 24 hours	savedsearch	No owner	search	App | Permissions	Enabled | Disable
Errors in the last hour	savedsearch	No owner	search	App | Permissions	Enabled | Disable
KV store lookup	transforms-lookup	admin	search	Private | Permissions	Enabled | Disable
License Usage Data Cube	savedsearch	No owner	search	App | Permissions	Enabled | Disable
Messages by minute last 3 hours	savedsearch	No owner	search	App | Permissions	Enabled | Disable
Orphaned scheduled searches	savedsearch	No owner	search	App | Permissions	Enabled | Disable
Splunk errors last 24 hours	savedsearch	No owner	search	App | Permissions	Enabled | Disable
alert	views	No owner	search	Global | Permissions	Enabled
alerts	views	No owner	search	Global | Permissions	Enabled
arulespy	commands	No owner	search	Global | Permissions	Enabled | Disable
asdfasdfa	views	admin	search	App | Permissions	Enabled
bucketdir	commands	No owner	search	Global | Permissions	Enabled | Disable
charting	views	No owner	search	Global | Permissions	Enabled
crawl	commands	No owner	search	Global | Permissions	Enabled | Disable

Knowledge Object Ownership

- When a user creates an object:
  - It is unshared, private to that user
  - It is “owned” by that user
- Sharing an object does not change its ownership
- What happens to shared objects when their owners are removed from the system?
  - Not much, in some cases
  - BUT THIS BREAKS SCHEDULED REPORTS, ALERTS, AND SAVED SEARCHES!
- Orphaned knowledge object reassignment is your quick fix to this problem



Reassign Knowledge Objects

Select knowledge objects and reassign them to another user. Learn more

☑	Name	Actions	Object type	Owner	App	Sharing
☑	Failed Webstore Purchases, Last 30d	Reassign	savedsearch	tohare	search	Global
☑	Successful Webstore Purchases, last 30d	Reassign	savedsearch	tohare	search	Global

Demo of Orphaned Object Reassignment

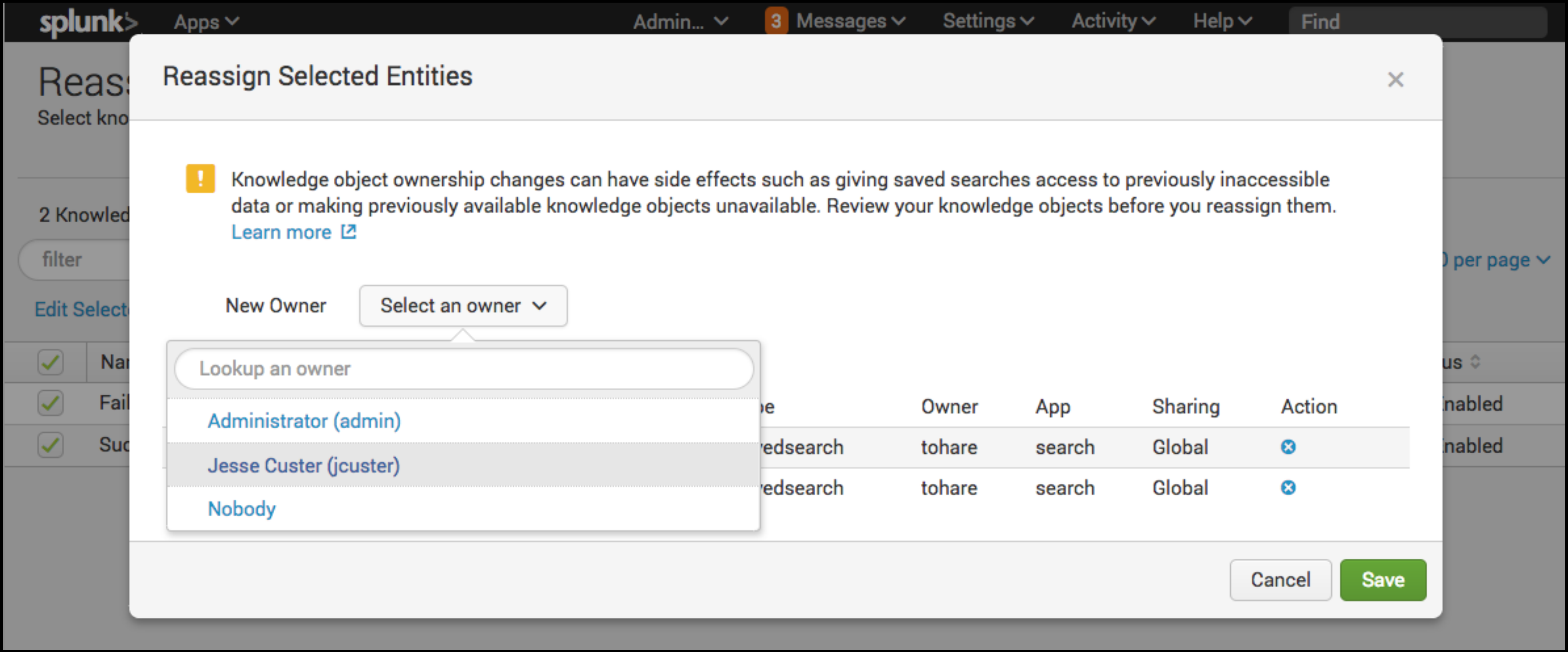
Presented by Matt Ness

Orphaned Object Reassignment

Let's Set The Stage

Object Owner	Shared, Scheduled Searches	Related Dashboard Panels
Tulip O'Hare	• Successful Webstore Purchases, Last 30d • Failed Webstore Purchases, Last 30d	• ~~Buttercup Games Purchases, last 30 days~~ • ~~Top Buttercup Games Product Categories~~
Jesse Custer	• Top Purchase Categories • ARCADE Product Purchases	• Failed Webstore Purchases, last 30 days • Top Arcade Items

Orphaned Object Reassignment



Reassign Selected Entities

! Knowledge object ownership changes can have side effects such as giving saved searches access to previously inaccessible data or making previously available knowledge objects unavailable. Review your knowledge objects before you reassign them. Learn more

New Owner: Select an owner

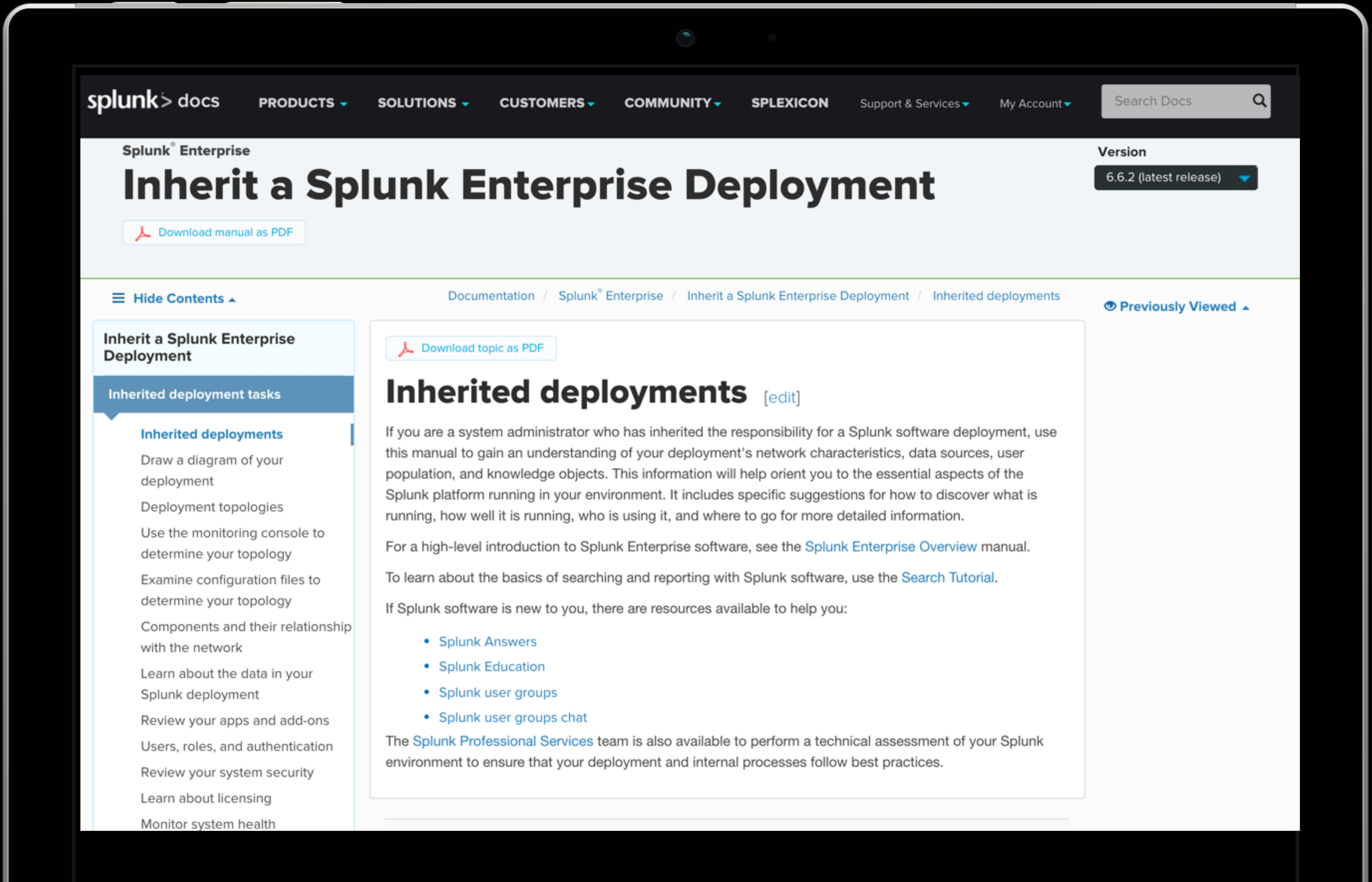
Lookup an owner

- Administrator (admin)
- Jesse Custer (jcuster)
- Nobody

e	Owner	App	Sharing	Action
edsearch	tohare	search	Global	⊗
edsearch	tohare	search	Global	⊗

You’ve heard the talk

Now read the manual!



Splunk® Enterprise

Inherit a Splunk Enterprise Deployment

Inherit a Splunk Enterprise Deployment

Inherited deployment tasks

- Inherited deployments
- Draw a diagram of your deployment
- Deployment topologies
- Use the monitoring console to determine your topology
- Examine configuration files to determine your topology
- Components and their relationship with the network
- Learn about the data in your Splunk deployment
- Review your apps and add-ons
- Users, roles, and authentication
- Review your system security
- Learn about licensing
- Monitor system health

Inherited deployments

If you are a system administrator who has inherited the responsibility for a Splunk software deployment, use this manual to gain an understanding of your deployment's network characteristics, data sources, user population, and knowledge objects. This information will help orient you to the essential aspects of the Splunk platform running in your environment. It includes specific suggestions for how to discover what is running, how well it is running, who is using it, and where to go for more detailed information.

For a high-level introduction to Splunk Enterprise software, see the Splunk Enterprise Overview manual.

To learn about the basics of searching and reporting with Splunk software, use the Search Tutorial.

If Splunk software is new to you, there are resources available to help you:

- Splunk Answers
- Splunk Education
- Splunk user groups
- Splunk user groups chat

The Splunk Professional Services team is also available to perform a technical assessment of your Splunk environment to ensure that your deployment and internal processes follow best practices.

- You can find more information in Inherit a Splunk Enterprise Deployment, at docs.splunk.com.
- If you read it, we’d love to get your feedback.

splunk> .conf2017

And That's It

Thanks To Everyone Who Made This Possible

- The members of the Splunk Doc team who wrote the manual!
- Our friends in Support, Professional Services, Sales Engineering, Product Development, and especially the Splunk Trust, for reviews and suggestions!
- YOU, for taking on the challenge of an existing Splunk Enterprise Deployment!

- Extra-special thanks to Malcolm Moore, our silent presentation partner and resident DJ, for help with slide design and demo environment prep!

Q&A

Jessica Law | Senior Staff Technical Writer
Matt Ness | Principal Technical Writer

Thank You

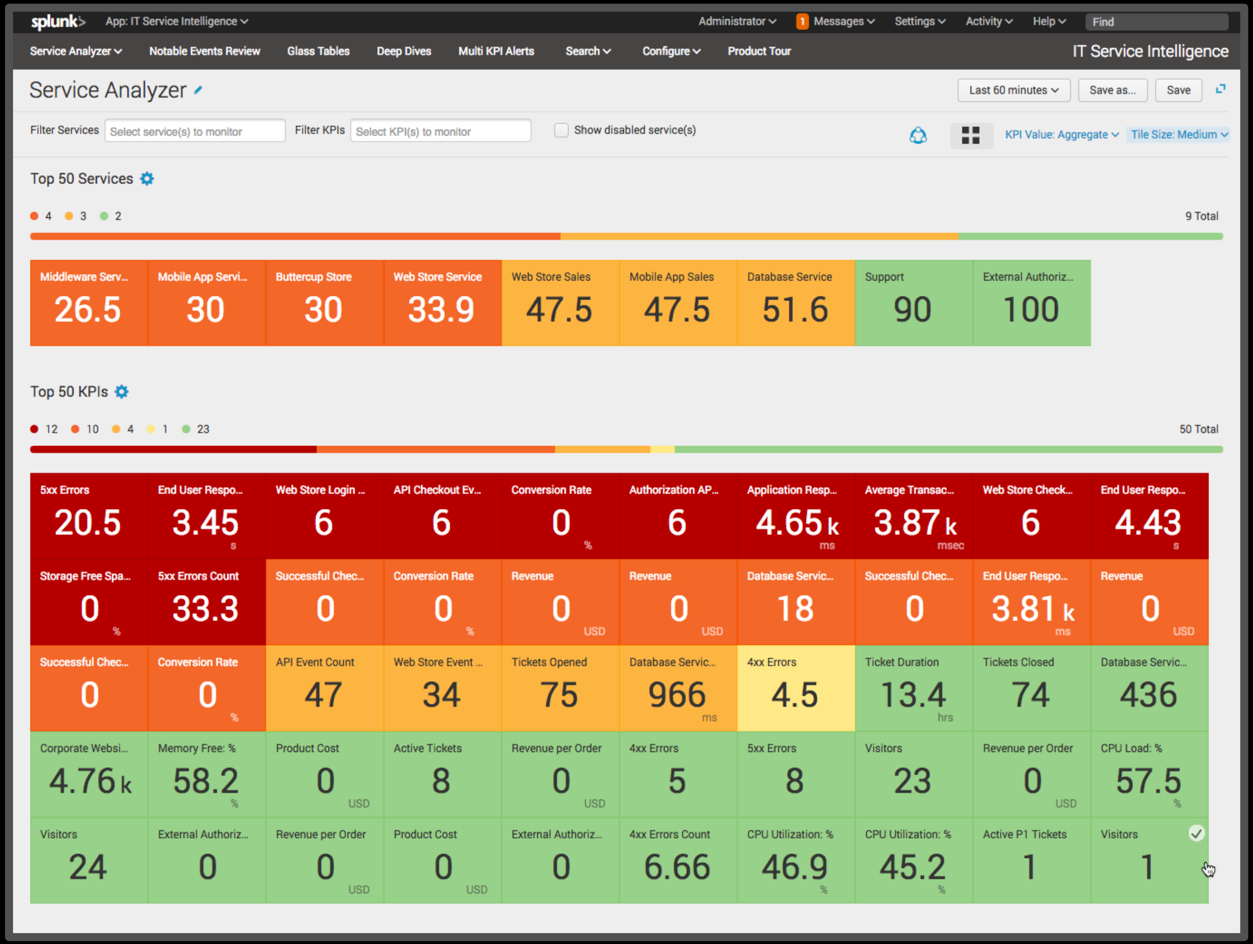
Don't forget to rate this session in the .conf2017 mobile app

splunk> .conf2017

IT Service Intelligence

What To Watch Out For

- Made up of services that monitor IT operations and business processes
- ITSI services are comprised of key performance indicator (KPI) searches that return single value results
- Keep an eye on:
  - Overall KPI search load
  - Entities – data sources for ITSI services and their KPIs



Service Analyzer

Filter Services Select service(s) to monitor Filter KPIs Select KPI(s) to monitor □ Show disabled service(s)

Top 50 Services

● 4 ● 3 ● 2 9 Total

Middleware Serv... 26.5	Mobile App Servi... 30	Buttercup Store 30	Web Store Service 33.9	Web Store Sales 47.5	Mobile App Sales 47.5	Database Service 51.6	Support 90	External Authoriz... 100

Top 50 KPIs

● 12 ● 10 ● 4 ● 1 ● 23 50 Total

5xx Errors 20.5	End User Respo... 3.45 s	Web Store Login ... 6	API Checkout Ev... 6	Conversion Rate 0 %	Authorization AP... 6	Application Resp... 4.65 k ms	Average Transac... 3.87 k msec	Web Store Check... 6	End User Respo... 4.43 s
Storage Free Spa... 0 %	5xx Errors Count 33.3	Successful Chec... 0	Conversion Rate 0 %	Revenue 0 USD	Revenue 0 USD	Database Servic... 18	Successful Chec... 0	End User Respo... 3.81 k ms	Revenue 0 USD
Successful Chec... 0	Conversion Rate 0 %	API Event Count 47	Web Store Event ... 34	Tickets Opened 75	Database Servic... 966 ms	4xx Errors 4.5	Ticket Duration 13.4 hrs	Tickets Closed 74	Database Servic... 436
Corporate Websi... 4.76 k	Memory Free: % 58.2 %	Product Cost 0 USD	Active Tickets 8	Revenue per Order 0 USD	4xx Errors 5	5xx Errors 8	Visitors 23	Revenue per Order 0 USD	CPU Load: % 57.5 %
Visitors 24	External Authoriz... 0	Revenue per Order 0 USD	Product Cost 0 USD	External Authoriz... 0	4xx Errors Count 6.66	CPU Utilization: % 46.9 %	CPU Utilization: % 45.2 %	Active P1 Tickets 1	Visitors 1