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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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. © 2017 Splunk Inc. All rights reserved.
You’ve Inherited a Splunk Enterprise Deployment ...Now What?

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

You are now the administrator of a Splunk Enterprise deployment!

▶ It's up and running already! Great!
▶ Lots of employees are using it!
▶ Everyone loves the dashboards!
▶ And the alerts!
▶ It's indexing a whole bunch of data!
▶ It's a distributed search setup
▶ Clusters of indexers and search heads
▶ Something called Enterprise Security… and KV Store…
▶ OMG… what is this thing?
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.
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

Indexers
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
Discover Topology with Configuration Files

START

- Does server.conf contain a [clustering] stanza? (YES/NO)
- Is mode set to "master"? (YES/NO)

- YES (Indexer cluster master node)
- NO

© 2017 SPLUNK INC.
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`

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

[sslConfig] [conf demos]
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

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

Cluster master / monitoring console / deployment server / license master

- 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

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

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

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

[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
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
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.
Deployment Diagram Checkpoint

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

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

Cluster master / Monitoring console / deployment server / license master

docs-unix-6a
- 8 CPU cores

Splunk web port 8000
Management port 8089
App server port 8065
KV store port 8191

SE 6.6.2
Linux RHEL 7
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
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
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.
Users, Roles, and Authentication
Roles Determine Actions Users Can Perform

Roles

- **Team Leader**
  - assemble_avengers
  - set_HQ_passwords
  - call_in_SHIELD
  - (and inherits **Team Member** role capabilities)

- **Team Member**
  - developBattle_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
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
  ```

© 2017 SPLUNK INC.
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
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
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
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Config type</th>
<th>Owner</th>
<th>App</th>
<th>Sharing</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors in the last 24 hours</td>
<td>savedsearch</td>
<td>No-owner</td>
<td>search</td>
<td>App</td>
<td>Permissions</td>
</tr>
<tr>
<td>Errors in the last hour</td>
<td>savedsearch</td>
<td>No-owner</td>
<td>search</td>
<td>App</td>
<td>Permissions</td>
</tr>
<tr>
<td>KV store lookup</td>
<td>transformslookup</td>
<td>admin</td>
<td>search</td>
<td>Private</td>
<td>Permissions</td>
</tr>
<tr>
<td>License Usage Data Cube</td>
<td>savedsearch</td>
<td>No-owner</td>
<td>search</td>
<td>App</td>
<td>Permissions</td>
</tr>
<tr>
<td>Messages by minute last 24 hours</td>
<td>savedsearch</td>
<td>No-owner</td>
<td>search</td>
<td>App</td>
<td>Permissions</td>
</tr>
<tr>
<td>Orphaned scheduled searches</td>
<td>savedsearch</td>
<td>No-owner</td>
<td>search</td>
<td>App</td>
<td>Permissions</td>
</tr>
<tr>
<td>Splunk errors last 24 hours</td>
<td>savedsearch</td>
<td>No-owner</td>
<td>search</td>
<td>App</td>
<td>Permissions</td>
</tr>
<tr>
<td>alert</td>
<td>views</td>
<td>No-owner</td>
<td>search</td>
<td>Global</td>
<td>Permissions</td>
</tr>
<tr>
<td>alerts</td>
<td>views</td>
<td>No-owner</td>
<td>search</td>
<td>Global</td>
<td>Permissions</td>
</tr>
<tr>
<td>anomaly</td>
<td>commands</td>
<td>No-owner</td>
<td>search</td>
<td>Global</td>
<td>Permissions</td>
</tr>
<tr>
<td>asciasfia</td>
<td>views</td>
<td>No-owner</td>
<td>search</td>
<td>App</td>
<td>Permissions</td>
</tr>
<tr>
<td>bucketdir</td>
<td>commands</td>
<td>No-owner</td>
<td>search</td>
<td>Global</td>
<td>Permissions</td>
</tr>
<tr>
<td>charting</td>
<td>views</td>
<td>No-owner</td>
<td>search</td>
<td>Global</td>
<td>Permissions</td>
</tr>
<tr>
<td>crawl</td>
<td>commands</td>
<td>No-owner</td>
<td>search</td>
<td>Global</td>
<td>Permissions</td>
</tr>
<tr>
<td>facessp</td>
<td>commands</td>
<td>No-owner</td>
<td>search</td>
<td>Global</td>
<td>Permissions</td>
</tr>
</tbody>
</table>

Survey Your Knowledge Objects
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
Demo of Orphaned Object Reassignment

Presented by Matt Ness
## Orphaned Object Reassignment

### Let’s Set The Stage

<table>
<thead>
<tr>
<th>Object Owner</th>
<th>Shared, Scheduled Searches</th>
<th>Related Dashboard Panels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tulip O’Hare</td>
<td>• Successful Webstore Purchases, Last 30d</td>
<td>• Buttercup Games Purchases, last 30 days</td>
</tr>
<tr>
<td></td>
<td>• Failed Webstore Purchases, Last 30d</td>
<td>• Top Buttercup Games Product Categories</td>
</tr>
<tr>
<td>Jesse Custer</td>
<td>• Top Purchase Categories</td>
<td>• Failed Webstore Purchases, last 30 days</td>
</tr>
<tr>
<td></td>
<td>• ARCADE Product Purchases</td>
<td>• Top Arcade Items</td>
</tr>
</tbody>
</table>
Orphaned Object Reassignment

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.

New Owner: Select an owner

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

Save
You’ve heard the talk
Now read the manual!

- 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.
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
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