

Best Practices and Better Practices for Admins

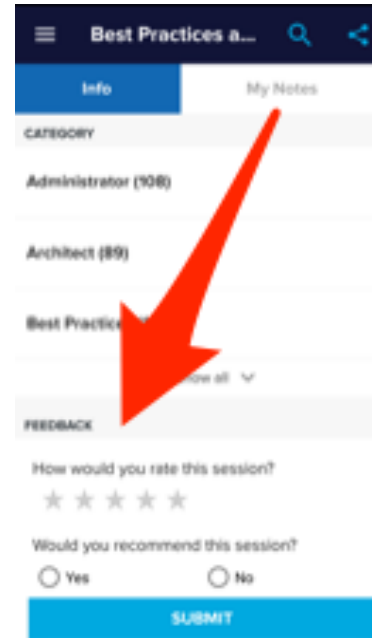
While you get settled...

Download Latest Slides:

<https://splunk.box.com/v/burch-practices-admin>

or ask a neighbor with flash drive

Load Feedback:



The screenshot shows a mobile application interface for 'Best Practices a...'. At the top, there is a navigation bar with a menu icon, the title 'Best Practices a...', a search icon, and a share icon. Below the navigation bar, there are two tabs: 'Info' (selected) and 'My Notes'. The main content area displays a list of categories: 'CARSOCY', 'Administrator (108)', 'Architect (89)', and 'Best Practice'. Below this list, there is a 'FEEDBACK' section. The feedback form includes the question 'How would you rate this session?' with a five-star rating system, and 'Would you recommend this session?' with radio buttons for 'Yes' and 'No'. A blue 'SUBMIT' button is located at the bottom of the form. A large red arrow points from the 'My Notes' tab area down to the 'FEEDBACK' section.

Best Practices and Better Practices for Admins

Burch

Sales Engineer @ Splunk

.conf2016

splunk >

Disclaimer

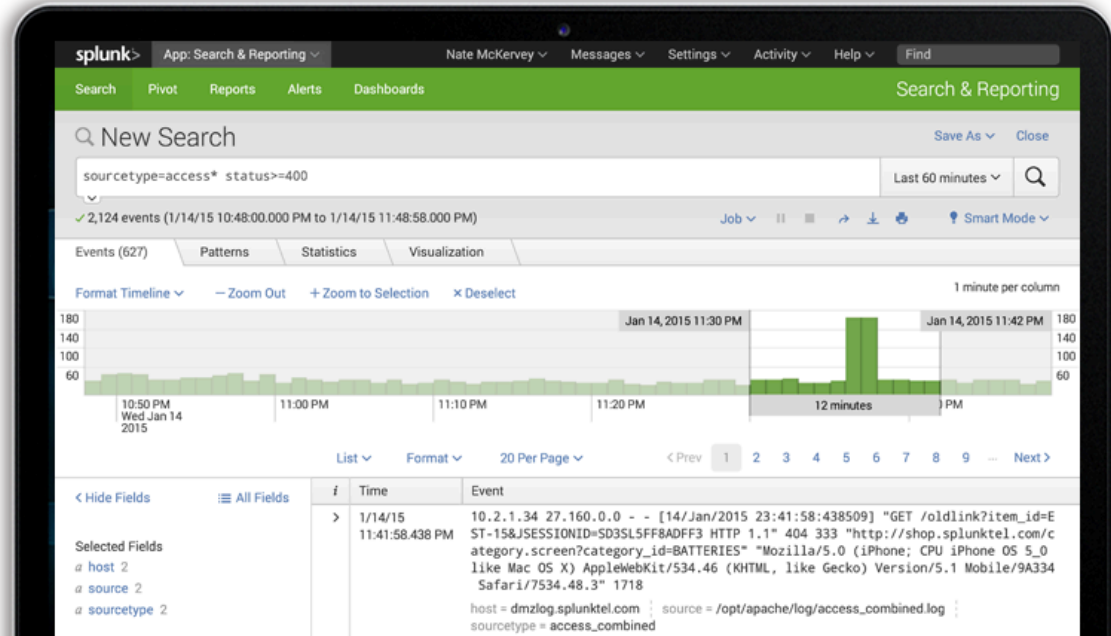
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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.

Burch's Goal

Learn from my _(our) mistakes

Agenda

- Who are we?
- Common Pitfalls
- MC (a.k.a DMC)
- Resources
- Tipz + Trickz
- Next Steps



Best Practices

Who are we?

What's a Burch?

- Senior Sales Engineer in Boston
- Education
 - CS @ Boston University
 - MBA @ Northeastern University
- Splunk Customer
 - Middleware for 8 years (+splunk)
 - Splunk Admin for 1.5 years (splunk 4.3+)
- Certs: Knowledge, Admin, Architect
- @Splunk since Dec 14
- Splunkbase apps



About you

- Name
- User?
- Power User?
- Admin?
- Groupie?



Best Practices

Common Pitfalls

Support Tickets

1. Open Cases
 - break/fix only
 - support.splunk.com
 - Search: docs.splunk.com -> support
 - Details, details, details
2. Immediate Diags
 - Search: docs.splunk.com -> diag
3. Schedule webex



Configuration Distribution Recap

| Deployment Server | Deployer | Master Node |
|-------------------|---------------------|---------------|
| Forwarders | Search Head Cluster | Index Cluster |

- In a mature environment



Separate Installs:

- Scalability
- Avoid reload deploy-server on restart
- Cheap VMs
- Not in critical path

Bonus points:

```
excludeFromUpdate
DS -> Master -> IDXC
DS -> Deployer -> SHC
```

Deployer

Not your old-timey Deployment Server

Requirements

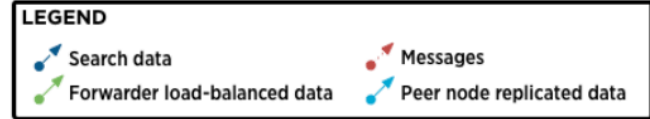
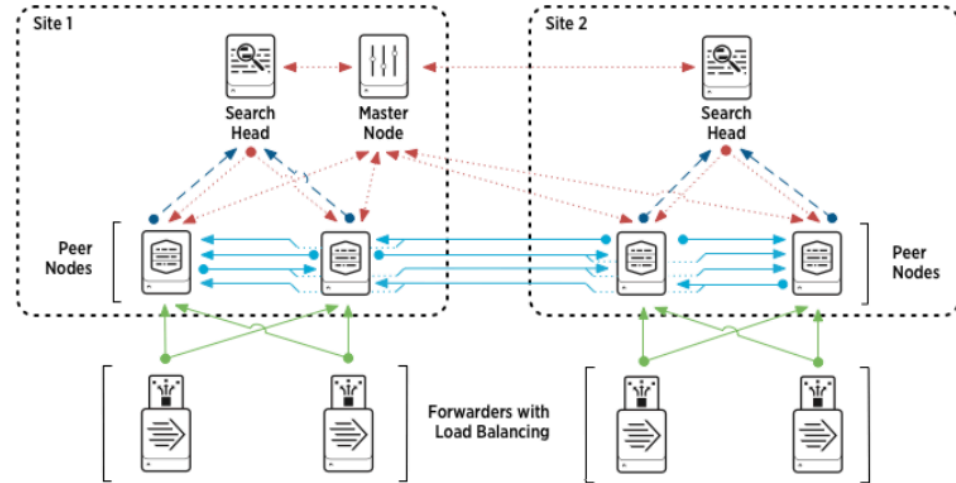
- Min 3+ SHs*
- Same specs
- **No manual conf edits**

Coolness

- Not critical path
- Config -> default
- No alerting servers

Architecture: Data Management

- **Non PROD data** -> PROD SPLUNK!
 - Or Search Head traverses envs
- Logical Separation:
 - Role Based Access Control
 - Separate indexes per env
 - Use event types/tags
- Traversing with SSL
 - Encryption & compression
- DNS entry for functions



Architecture: Cluster of One

- Multisite!
- Replication & Search Factor of 1
- Same disk space as non-cluster
- Allows replication on old data
- Seamless scalability

AN ARMY OF ONE

Dangerous Capabilities

Weak

- Scheduled Search
- Real Time Search
- Acceleration
 - Summary Indexing
 - Report Acceleration
 - Data Models

Strong

- Everyone a 'user'
- Capabilities only for 'power'+
- Work with you to implement and learn best practices
- Identify & coach & promote to power
- Don't be a data butler

Best Practices

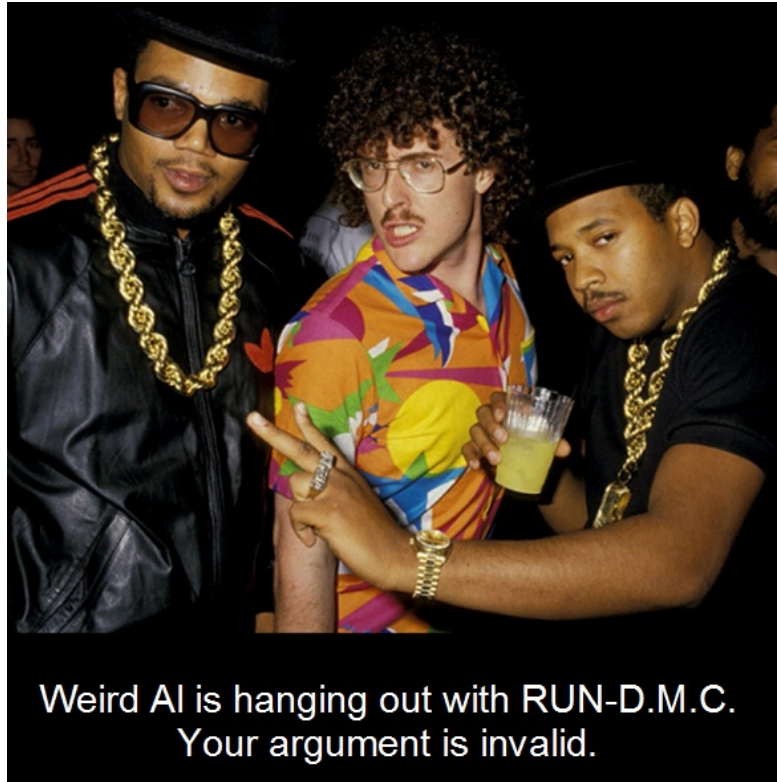
Monitoring Console

Best Practices

The Console Formerly Known As DMC

Run DMC

- Manage Splunk 6.2+ environments
- Replaces Deployment Monitor App
- Incorporates SOS app prior to 6.2+
- Renamed Monitoring Console!



Monitoring Console Setup

docs.splunk.com -> Splunk Enterprise -> Administer -> Monitoring Splunk Enterprise

Manuals Version
6.5.0

Splunk[®] Enterprise

Documentation / Splunk[®] Enterprise

Splunk Enterprise is the data collection, indexing, and visualization engine for operational intelligence.

Get started Search and report **Administer** Deploy Develop

Admin Manual

Starting point for Splunk Enterprise administration. Includes information about managing licenses, configuring Splunk Enterprise, and using the command-line interface. Includes a complete reference to all Splunk Enterprise configuration files.

Getting Data In

How to get your machine data into your Splunk deployment and ensure that it is indexed efficiently and effectively.

Securing Splunk Enterprise

How to create and authenticate users, configure SSL, use audit features to secure your data, and harden Splunk deployments to reduce vulnerability and risk.

Troubleshooting Manual

How to analyze activity and diagnose problems with your Splunk deployment.

Monitoring Splunk Enterprise

Monitor your Splunk Enterprise instance or deployment.

REST API Reference Manual

Reference documentation for Splunk REST API endpoints.

Search Activity

Search Activity & Search Usage Statistics

Top 20 Memory-Consuming Searches ⚠

| Name | Memory Usage (MB) | Instance | Runtime | Started | Type | Mode | App | User | Role |
|-----------------------------------|-------------------|---------------|----------|------------------------------|---------------------|------------|--------|--------------------|------|
| 1 SummaryDirector_1469466086.6145 | 1858.50 | ch-demo-cis20 | 21.5 sec | Mon Jul 25 12:01:30 CDT 2016 | report acceleration | historical | system | splunk-system-user | head |
| 2 SummaryDirector_1469462486.5472 | 1858.46 | ch-demo-cis20 | 21.6 sec | Mon Jul 25 11:01:30 CDT 2016 | report acceleration | historical | system | splunk-system-user | head |
| 3 SummaryDirector_1469464287.5813 | 1857.52 | ch-demo-cis20 | 20.4 sec | Mon Jul 25 11:31:29 CDT 2016 | report acceleration | historical | system | splunk-system-user | head |
| 4 SummaryDirector_1469457086.4358 | 1640.81 | ch-demo-cis20 | 21.9 sec | Mon Jul 25 09:31:30 CDT 2016 | report acceleration | historical | system | splunk-system-user | head |
| 5 SummaryDirector_1469460686.5125 | 1640.60 | ch-demo-cis20 | 21.9 sec | Mon Jul 25 10:31:30 CDT 2016 | report acceleration | historical | system | splunk-system-user | head |

Long-running Searches ⚠

| Report Name/Search String | Search Runtime | Search Start | Earliest Time | Latest Time | Type | User | Host | SID |
|---|----------------|--------------------------|---------------|-------------|--------|------------|---------------------------|--|
| metadata type=sourcetypes search totalCount > 0 | 5025.8 sec | 07/25/2016 09:20:44-0500 | all time | all time | ad hoc | demo_owner | ch-demo-dod | rt_1469456444.32 |
| metadata type=sourcetypes search totalCount > 0 | 3185.7 sec | 07/25/2016 09:58:18-0500 | all time | all time | ad hoc | rwalker | ch-demo-bwsd | rt_1469458698.29 |
| search5 | 2863.6 sec | 07/25/2016 09:31:55-0500 | all time | all time | ad hoc | wemmett | ch-demo-appmgmt.hod.cloud | rt_wemmett_wemmett_appmgmt_search5_rt_1469457115.1517 |
| globalSearch | 2584.4 sec | 07/25/2016 10:38:21-0500 | all time | all time | ad hoc | sou | ch-demo-shakeit.hod.cloud | rt_sou_sou_shake_globalSearch_rt_1469461101.1052 |
| search2 | 2584.4 sec | 07/25/2016 10:38:21-0500 | all time | all time | ad hoc | sou | ch-demo-shakeit.hod.cloud | rt_sou_sou_shake_search2_rt_1469461101.1051 |
| search7 | 2584.4 sec | 07/25/2016 10:38:21-0500 | all time | all time | ad hoc | sou | ch-demo-shakeit.hod.cloud | rt_sou_sou_shake_search7_rt_1469461101.1053 |
| search6 | 2461.7 sec | 07/25/2016 12:24:03-0500 | all time | all time | ad hoc | rwalker | ch-demo-pan.hod.cloud | rt_rwalker_rwalker_SplunkforPaloAltoNetworks_search6_rt_1469467443.225 |
| search5 | 2461.4 sec | 07/25/2016 12:24:03-0500 | all time | all time | ad hoc | rwalker | ch-demo-pan.hod.cloud | rt_rwalker_rwalker_SplunkforPaloAltoNetworks_search5_rt_1469467443.224 |

Best Practices

Resources

Search Tutorial

- Free Search Tutorial -> docs.splunk.com -> Search Tutorial

The screenshot shows the Splunk Docs website interface. At the top, there is a navigation bar with links for 'PRODUCTS', 'SOLUTIONS', 'CUSTOMERS', 'COMMUNITY', and 'SPLIXICON'. Below this, there are three main sections: 'Developer tools' (with links to 'Splunk SDKs' and 'Splunk Web Framework'), 'Community' (with links to 'Ponydocs' and 'Splunk Answers and Splunkbase'), and 'Legacy' (with a link to 'Legacy products'). At the bottom, there is a 'Docs Latest' section with a 'Search Tutorial' link highlighted by a red arrow. The 'Search Tutorial' link is part of a paragraph that says: 'If you are new to Splunk software, start here! The [Search Tutorial](#) guides you through adding data, searching, and creating simple dashboards.' To the right of the 'Search Tutorial' link is a 'Visit Splunk Answers' section. On the far right, there is a 'Splunk Docs on Twitter' section showing a tweet from @splunkdocs dated 15 Jan.

Benefits:

- Downloads & Installs Splunk
- Local sandbox
- Add real data

Community Q&A

- answers.splunk.com

Benefits:

- E-mail notifications
- Fast answers
- Larger distribution

The screenshot shows the Karma Leaderboard on answers.splunk.com. At the top right, there is a search bar with 'sloshburch' entered and a 'Refine your search' dropdown menu with options for Questions, Apps, Users (selected), and Tags. Below the search bar, the 'Karma Leaderboard' section has filters for 'last week', 'last 2 weeks', 'current month', 'quarter to date' (selected), and 'all time'. The leaderboard table has columns for Rank, Change, User, and Karma. The top row shows SlosHBurch with Rank 18, a change of 39 (up), and Karma 533. A red arrow points from the Karma value to a user profile card for SlosHBurch. The profile card includes a profile picture, name, location (Boston, MA), a '+ Follow' button, and statistics: 1422 Reputation, 226 Posts, 38 Following, 7 Followers, and 11/11 Joined.

| Rank | Change | User | Karma |
|---------|----------|------------|-------|
| 18 | 39 ↑ | SlosHBurch | 533 |
| 101,108 | 42,782 ↑ | SlosHBurch | |

SlosHBurch
Boston, MA
[+ Follow](#)

1422 Reputation
226 Posts
38 Following
7 Followers
11/11 Joined

Splunk! The Book

- <http://www.splunk.com/goto/book>

Exploring Splunk

SEARCH PROCESSING LANGUAGE (SPL) PRIMER AND COOKBOOK

Splunk is probably the single most powerful tool for searching and exploring data you will ever encounter. Exploring Splunk provides an introduction to Splunk -- a basic understanding of Splunk's most important parts, combined with solutions to real-world problems.

Part I: Exploring Splunk

- Chapter 1 tells you what Splunk is and how it can help you.
- Chapter 2 discusses how to download Splunk and get started.
- Chapter 3 discusses the search user interface and searching with Splunk.
- Chapter 4 covers the most commonly used search commands.
- Chapter 5 explains how to visualize and enrich your data with knowledge.

Part II: Solution Recipes

- Chapter 6 covers the most common monitoring and alerting solutions.
- Chapter 7 covers the most common transaction solutions.
- Chapter 8 covers the most common lookup table solutions.

About the Author

David Carasso, Splunk's Chief Mind, was the third Splunk employee. He has been responsible for innovating and prototyping a class of hard problems at the Splunk core, including developing the Search Processing Language (SPL), dynamic event and source tagging, automatic field extraction, transaction grouping, event aggregation, and timestamping. He holds two patents for his work with Splunk, and lives in Marin County, California, with his wife and three children.



Download the Book: [ePub](#) | [pdf](#) | [Kindle](#)

Purchase a Hardcopy:
[Amazon](#) | [Splunk Store](#)

Benefits:

- Real examples of commands
- Deeper than docs
- Free!

Reference

- Splunk Documentation -> docs.splunk.com
- Smart Answers -> blogs.splunk.com/?s=smart+answers
- User Groups -> usergroups.splunk.com

Welcome Page Creator

<https://splunkbase.splunk.com/app/2991>



Hands on Labs

Welcome App Page Creator

Tuesday, September 27, 2016 | 1:30 PM-1:45 PM

Wednesday, September 28, 2016 | 5:00 PM-5:15 PM

Thursday, September 29, 2016 | 12:00 PM-12:15 PM

BEGINNER | **Industries:** Other | **Role:** Splunk Technical Champion, Administrator | **Track:** Community Theater | **Session Focus:** Deploying Splunk | **Other Topics:** Best Practices

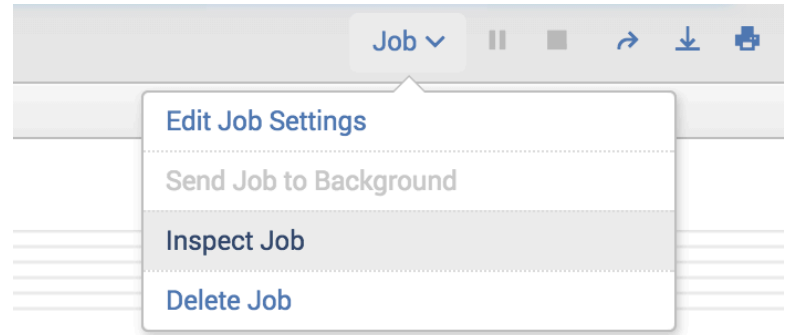
Speakers

Erick Mechler, SE Director, Splunk

Users often land in the Splunk platform with no clue where to begin. In this lab, you'll get hands-on training on how to use the Welcome Page Creator app. You'll be able to use this app and its over 20 prebuilt panels to create an effective starting page for your users. Check out the associated blog post (<http://blogs.splunk.com/2016/09/01/introducing-the-welcome-page-creator>) for more details.

Job Inspector

- Job Inspector
 - docs.splunk.com “Search Job Inspector”



This search has completed and has returned **1,000** results by scanning **22,696** events in **1.049** seconds.

- $\text{events per second} = \text{events} / \text{seconds}$
- $\text{results per second} = \text{results} / \text{seconds}$

Play it safe



Splunk Snacks

Your Splunk Sandbox

Wednesday, September 28, 2016 | 11:00 AM-11:15 AM

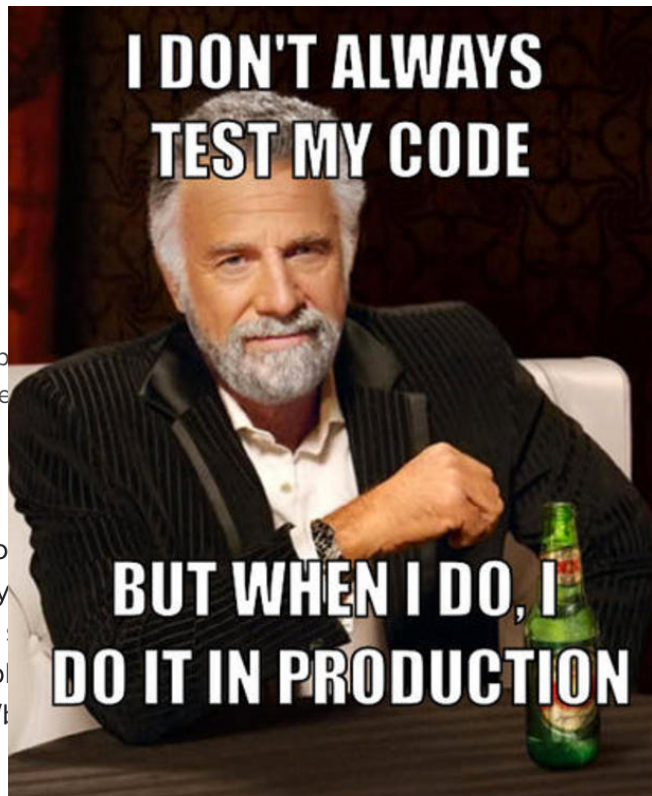
INTERMEDIATE | **Products:** Splunk Enterprise | **Role:** Splunk Technical Champ

Track: Community Theater | **Session Focus:** Using Splunk | **Other Topics:** Ge

Speakers

Burch Simon, Senior Sales Engineer, Splunk Inc.

When I was an admin, sometimes I wanted to Splunk things, but no wanted to add data and define the corresponding sourcetype. May conf files. Maybe I wanted to muck around with a new version of a reason, I learned a few approaches that may be obvious for the Spl for our adorable n00bs. Learn more about our session here: <http://splunk-sandbox/>



To btool, or not to btool

- `btool <configuration> list <stanza|> <--debug|>`
- **Add to your env path! (source a profile file from an app)**
 - Linux: `export LD_LIBRARY_PATH=$SPLUNK_HOME/lib`
 - Mac: `export DYLD_LIBRARY_PATH=$SPLUNK_HOME/lib`
- No “.conf”
- Use `--debug with | grep -v "system/default"`
- Not current runtime

New Stuff

> Splunk Enterprise 6.5 Overview

DOWNLOAD

Release 6.5 is the latest version of Splunk Enterprise and Splunk Cloud. We have developed an app to guide you through the powerful new features. This is not an in-depth tutorial, rather a guide to help you understand the new features, and to provide examples as well as sample reports, dashboards and visualizations.

The screenshot shows the 'Splunk 6.5 Overview' app interface. It features a navigation menu on the left with 'User Experience' selected. The main content area is titled 'Key Features' and includes several sections:

- User Experience**
 - Table Datasets**: Create and analyze tabular data views without using SPL. Make power users more productive in creating rich data views, while making it simple for anyone to analyze data.
 - Conditional Table Formatting & Number Formatting**: Set table cell coloring determined by cell values straight from the UI. Format numbers and add units while keeping sort order.
 - Table Summaries**: Summarize column totals and calculate percent breakdowns straight from the UI.
 - Dashboard Refresh**: Auto-refresh dashboard elements with minimal flicker using versatile controls.
 - Dashboard Edit Experience**: Preview dashboard before saving. Use new in-page SimpleXML source code editor with inline validation to create custom dashboards.
 - Enhanced Search Assistance**: Improve SPL readability and debugging in search editor, including syntax highlighting, auto-formatting, and autocomplete.

★★★★★ 1 ratings

Rate this app

16 downloads

Unsubscribe

Share this app

VERSION 1.1

Utilities

Splunk Enterprise

App

Splunk 6.5

Splunk Software License Agreement

Platform Independent

Best Practices

Administration

Bootstrap

1. Install splunk binaries
2. Point to DS/Master/Deployer
3. Download config and purpose config
4. Download app with scripted input



Installing Splunk

- Bootstrap to DS
 - Segregates install from config
 - Empowers admin with config
- Scripted input to
 - place: log-local.cfg
 - disable local auth (passwd)
 - touch `.ui_login`
- Global Config App
 - Disable splunkweb
 - Set ports
 - authentication

Remember:

- Transparent Huge Memory Pages
- Source Control

Keep It Clean: Naming Conventions

- Template: <summary|>_<company>_<function>_<environment>
- <company>
 - Yours or from a 3rd party/splunk app
- <function>
 - Nothing that changes (i.e. organization/teams)
- <environment>
 - PROD, DR, QA, TEST, DEV, etc...
- <summary|>
 - Exists as a modifying of corresponding index

Log Management

- “If you log it, then you should Splunk it”
 - App/System performance to write logs
 - Disk to store logs

- Move cronjobs/scheduled tasks to Splunk
 - Scripted Inputs
 - standard output/error captured

Hidden Fields: Time

<http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/SearchTimeModifiers>

| Event Time | Index Time |
|------------|-----------------|
| _time | _indextime |
| earliest | _index_earliest |
| latest | _index_latest |

What does a big difference mean?



I DID ABSOLUTELY NOTHING TODAY

**AND IT WAS EVERYTHING I
THOUGHT IT COULD BE**

Logging Made Easy

- Use clear key-value pairs
- Create events humans can read
- Use developer-friendly formats
- Use timestamps for every event
- Use unique identifiers (IDs)
- Log in text format
- Log more than debug events
- Use categories
- Identify the source
- Minimize multi-line events

Forwarding & Search Heads

- Forward all instances to indexers
 - All indexes – including summary
 - All instances:
 - ▶ * Forwarders
 - ▶ Search Heads
 - ▶ Deployment Server
 - ▶ License Server
 - ▶ Cluster Master
 - ▶ Deployer

Indent Config

Example:

```
[general]
pass4SymmKey = $1$ShiC+P0X
serverName = elBurcho
    sessionTimeout = 30m
```

Benefit

- Easily see system vs hand edits
- Detect hand config updated by system

Search Head limits.conf

Example:

```
[scheduler]  
max_searches_perc = 90
```

Benefit

- Defaults to 50
- Ad Hoc takes precedent
- Additional controls for scheduling

Indexer Discovery

Search docs.splunk.com for “indexerdiscovery”

Pros

- Great for indexers with different volume sizes
- “Rebalances”

Cons

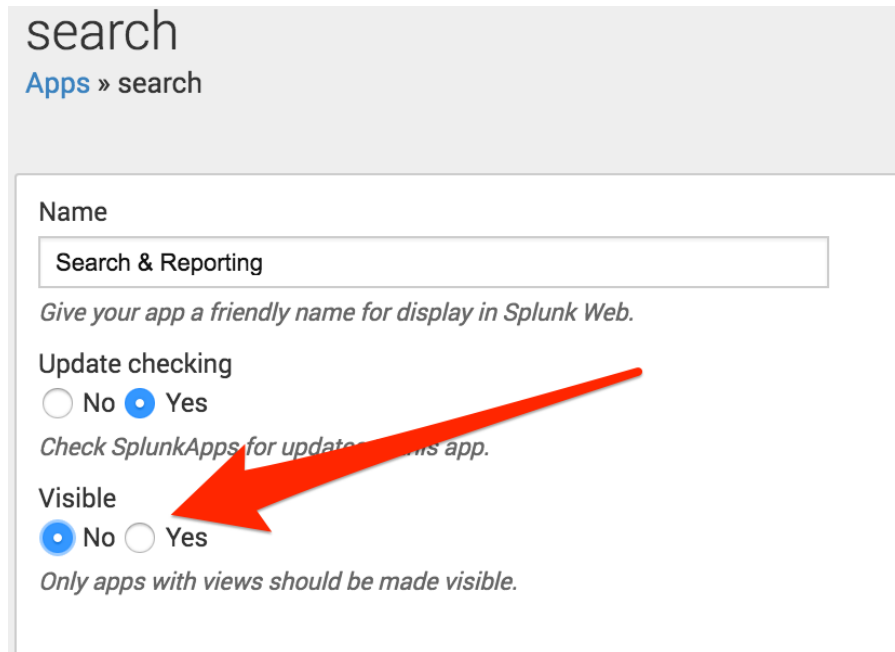
- Requires network traffic to master node
- Forwarder silence if master down

App Development

- Macros
 - allow easy modification
 - Imagine rewriting every search/dashboard
 - Candidates: index, sourcetype, source
- Separate Functions
 - UI vs Data Collection vs index-time
- Permissions:
[]
`export = none`
`owner = nobody`
- Then `export = system` for global stuff (macros, fields, tags, etc...)

User Web-App Experience

- Default App
- Default Dashboard
 - Welcome page
- No search box for new users
- Drive their eyes/focus
 - Hide other apps – even Search!



The screenshot shows the configuration page for the 'search' app in Splunk Web. The page title is 'search' with a breadcrumb 'Apps » search'. The 'Name' field contains 'Search & Reporting'. Below it is a note: 'Give your app a friendly name for display in Splunk Web.' The 'Update checking' section has radio buttons for 'No' and 'Yes', with 'Yes' selected. A note below says 'Check SplunkApps for updates on this app.' The 'Visible' section has radio buttons for 'No' and 'Yes', with 'No' selected. A red arrow points to the 'No' radio button. A note below says 'Only apps with views should be made visible.'

Best Practices

Next Steps

What Now?

Related breakout sessions and activities...

- Rate this! (be honest)
- More talks:
 - conf.splunk.com/speakers.html
 - Search for
 - ▶ Burch
 - ▶ Champagne
 - ▶ Optimization
 - ▶ Practices
 - ▶ tips
 - ▶ Worst



Burch's Goal

Learn from my _(our) mistakes

Free Discussion

Questions, ideas, experiences
...have you?



THANK YOU

.conf2016