

# Your Splunk Sandbox

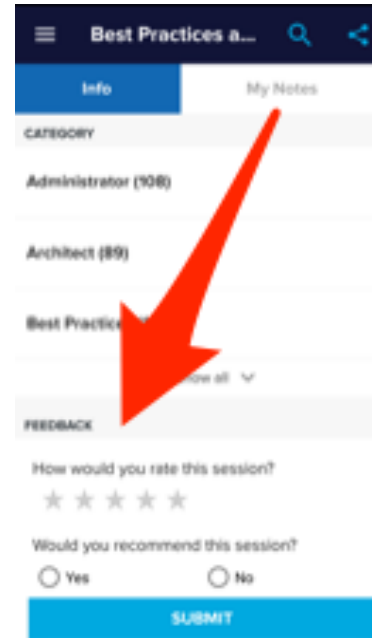
While you get settled...

Download Latest Slides:

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

or ask a neighbor with flash drive

Load Feedback:



The screenshot shows a mobile application interface for 'Best Practices a...'. It features a navigation bar with 'Info' and 'My Notes' tabs. Below the navigation bar, there is a list of categories: 'CATEGORY', 'Administrator (108)', 'Architect (89)', and 'Best Practice'. A red arrow points to the 'FEEDBACK' section, which contains a rating question: 'How would you rate this session?' with five stars, and a recommendation question: 'Would you recommend this session?' with 'Yes' and 'No' radio buttons. A blue 'SUBMIT' button is at the bottom.

Related Blog:

Search: [blogs.splunk.com](https://blogs.splunk.com) your splunk  
sandbox

<http://blogs.splunk.com/2016/03/22/your-splunk-sandbox>

# Your Splunk Sandbox

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.

# 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



# Burch's Goal

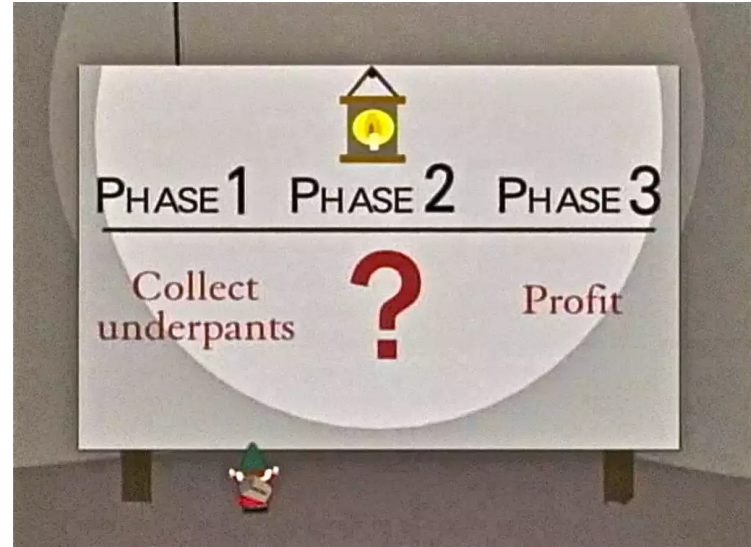
Hesitate no more

# Burch's Goal



# Agenda

- Stage 1: Build
- Stage 2: Play
- ?
- Stage 4: Profit
  
- Config Tricks
- NOT sandbox



# Your Splunk Sandbox

Build



# Build a Splunk Sandbox: Options



Localhost

Admin Rights?



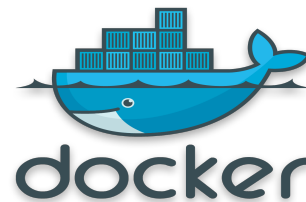
Cloud

Exfiltration?



Virtual

Effort?

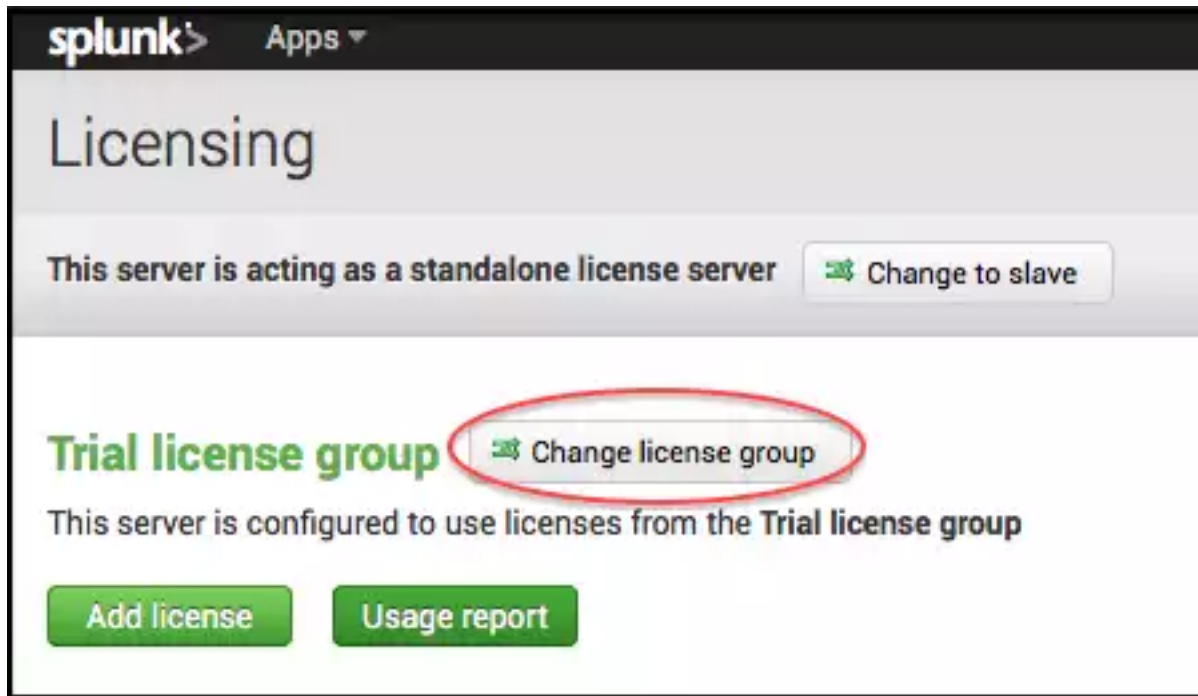


Container

Coolness?

# Build a Splunk Sandbox: License

Settings > Licensing



splunk> Apps ▾

## Licensing

This server is acting as a standalone license server [Change to slave](#)

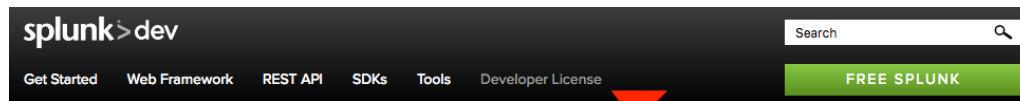
**Trial license group** [Change license group](#)

This server is configured to use licenses from the **Trial license group**

[Add license](#) [Usage report](#)

# Build a Splunk Sandbox: Developer

dev.splunk.com



## Splunk Developer License Signup

With the Splunk developer license, you can use our SDKs and other developer tools to build big data applications that plug into Splunk's map/reduce data-processing pipeline, storage technology, and management facilities. And, you can extend and enhance Splunk Web through our app framework. Just follow a few simple steps below and you'll be on your way.

### 1. Get Splunk Enterprise.

You want to build applications that work on top of Splunk platform, then you need a license to Splunk Enterprise software, which is our flagship core product. Splunk Enterprise is a snap to install and easy to configure. Download it [here](#).

### 2. Get your developer license.

You'll need to [request your developer license](#).

### 3. Get started and stay connected.

- Learn how to [install your license](#).
- Get the SDKs from [Splunk GitHub](#).
- Check out the apps on [Splunkbase](#).
- Follow us on Twitter for latest updates [@splunkdev](#).
- Join our [Google Group](#).

# Build a Splunk Sandbox: STOP



# Your Splunk Sandbox

Play

# Play in your Splunk Sandbox: Tutorial



The image shows a screenshot of the Splunk Docs website. At the top, there is a dark blue header with the text "splunk > docs" and a search bar. Below the header, the page is organized into several sections: "Core products", "Premium solutions", "Apps and add-ons", "Developer tools", "Legacy", and "Docs Latest". A large, green, 3D-style text overlay reads "Installation & Sample Data Included!". A red arrow points from the top of the page down to the "Search Tutorial" link in the "Docs Latest" section.

**Installation & Sample Data Included!**

**Search Tutorial**  
If you are new to Splunk software, start here! The [Search Tutorial](#) guides you through adding data, searching, and creating simple dashboards.

**Visit Splunk Answers**  
Have questions about how to do something with Splunk software? [Engage with the Splunk community](#) to get answers fast!

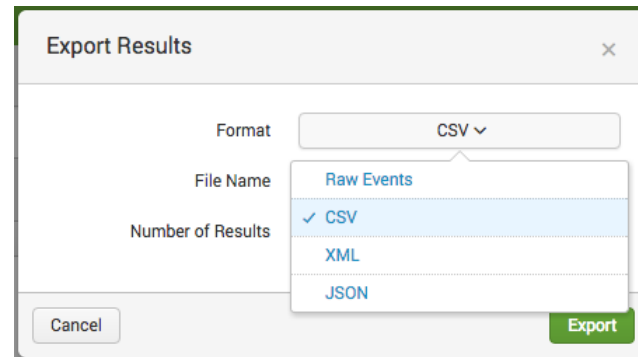
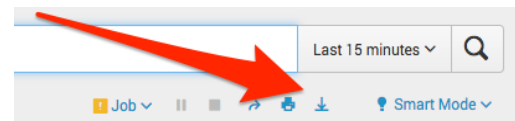
**Docs Latest**

**Splunk Docs on Twitter**  
Tweets by @splunkdocs

**splunk docs** @splunkdocs  
The @splunk docs team, learning from and sharing with the tech writing community <3 [twitter.com/smorewithface/...](#)

# Play in your Splunk Sandbox: Prod Data

- Export prod data
- Gotchas:
  - Huge data volume could timeout
  - Export as raw unless you just want to play with fields
- Add to your sandbox



# Your Splunk Sandbox

## Config Tricks



# Apply Config without Restart

Warning: Not necessarily supported

- | `extract reload=true`
- `/debug/refresh`
  - Force relogin?
- `/en-US/_bump`
- Development mode settings
  - Search “docs.splunk.com development mode settings”

# Your Splunk Sandbox

NOT sandbox

# When to Avoid the Sandbox

- New Search:
  - Time selector
  - | head
- Edit Knowledge Object (Dashboard, Report, etc...)
  - Clone
  - Default to private

# Burch's Goal



# What Now?

Related breakout sessions and activities...

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



# Free Discussion

Questions, ideas, experiences  
...have you?



# THANK YOU

.conf2016