Creating Welcome Pages
...while you get settled...

► Latest Slides:
  • https://splunk.box.com/v/blueprints-wpc-hol

► Collaborate: #success
  • Sign Up @ http://splk.it/slack

► Load Feedback ---------------------------------------
Creating Welcome Pages
With the Welcome Page Creator

Burch | Senior Best Practices Engineer

.conf2017 | 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.
The Problem

This is why you’re here....
report on how popular splunk is

No results found. Try expanding the time range.
<table>
<thead>
<tr>
<th>Title</th>
<th>Actions</th>
<th>Owner</th>
<th>App</th>
<th>Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Model Audit</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Detect Journal Clearing</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Detect Lateral Movement With WMI</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Detect Log Clearing With wenvutil</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Error Details</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Fake Windows Processes</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_TA_aws</td>
<td>Global</td>
</tr>
<tr>
<td>Health Overview</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Introduction</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Malicious Command Line Executions</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Monitor AutoRun Registry Keys</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Monitor Successful Backups</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Monitor Successful Windows Updates</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Monitor Unsuccessful Backups</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Monitor Unsuccessful Windows Updates</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Predictive Analytics</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Ransomware Extensions</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
<tr>
<td>Ransomware Note Files</td>
<td>Edit</td>
<td>nobody</td>
<td>Splunk_SA_CIM</td>
<td>Global</td>
</tr>
</tbody>
</table>
Are you in the right place?

- Experience those challenges
- Comfortable navigating Splunk
- Comfortable creating dashboards

Tots cool to bounce!
Background
What’s a “Burch”? 

Senior Best Practices Engineer

- Was a Senior Sales Engineer
- Before that, Splunk Customer
- Before that, Middleware Eng
- Before that, Computer Science
- Before that, an idea of my parents
- Did this as a customer!
Update to $\neq$ Prerequisite

What is a Workspace? In my mind, it’s a well defined area within which one can construct and create without impact to or by externalities.

Implemented in Splunk, it’s your logging into Splunk, getting escorted to content for their domain, and not being distracted or impacted by the activities of others.

As you might have guessed, this concept is implemented already in Splunk by means of variable “apps.” Unfortunately, many of us don’t embrace apps in this fashion — and for good reason! We often associate apps with the rich contributions available on Splunkbase and rarely consider the simplest of apps, as a Workspace for user groups.
New Concept
Welcome Page
New Concept

Workspace
Welcome Page Creator
Now with easier setup!

Overview

Users often land in Splunk with no clue where to begin. Use this app and its over 20 pre-built panels to create an effective starting page for your users.

This app builds upon the concepts and philosophies outlined in the blog posts Introducing the "Welcome Page Creator" (https://www.splunk.com/blog/2016/06/01/introducing-the-welcome-page-creator) and Your Splunk Workspace (https://www.splunk.com/blog/2017/02/01/your-splunk-workspace)

Subscribe to this app button on bottom right of this page for notifications of updates.

Release Notes
Welcome New Users!

Learning Splunk
If you’re new to splunk, please review these pages:
1. Product Overview: What is Splunk Enterprise?
2. Video: Splunk Enterprise 6.3 Basic Search
3. Splunk Tutorial
4. Quick Reference Guide
5. Splunk Education & Classes

Splunk Community: Questions & Help
- answers.splunk.com - Q&A Forum
- docs.splunk.com - Official Product Documentation
- Plan to join Splunk at conf2016
- Join a local Splunk User Group

Waiting on your Splunk Admins?
Questions?
- Get better and faster answers by posting on answers.splunk.com.
- Follow the answers.splunk.com usernames of peers and friends for greater collaboration. Simply click the "Follow" button within a user’s profile within answers.splunk.com.

Field Extractions?
- Did you know you can extract fields yourself? Without any technical skill!
- With the Field Extractor, you can point and click what you want made into a field.

Splunk Education Videos
If you’re new to splunk, please review these pages:
1. Splunk Demo
2. Education Videos
3. Splunk EDU: How To Videos (YouTube)
4. Creating Alerts Overview
5. Creating Reports Overview
6. Creating Pivot Reports Overview

Explore the data accessible by this Splunk instance
Reset and show all:
- Sources

Learn about sourcetypes and indexes

Select a source to explore:

<table>
<thead>
<tr>
<th>Source</th>
<th>Quantity of Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Users/emeicher/product/test/splunk-welcome/var/log/introspection/disk_objects.log</td>
<td>610</td>
</tr>
<tr>
<td>/Users/emeicher/product/test/splunk-welcome/var/log/introspection/http_event_collector_metrics.log</td>
<td>441</td>
</tr>
<tr>
<td>/Users/emeicher/product/test/splunk-welcome/var/log/introspection/kvstore.log</td>
<td>1504</td>
</tr>
<tr>
<td>/Users/emeicher/product/test/splunk-welcome/var/log/splunk/conf.log</td>
<td>24</td>
</tr>
<tr>
<td>/Users/emeicher/product/test/splunk-welcome/var/log/splunk/first_install.log</td>
<td>4</td>
</tr>
<tr>
<td>/Users/emeicher/product/test/splunk-welcome/var/log/splunk/license_usage.log</td>
<td>2</td>
</tr>
<tr>
<td>/Users/emeicher/product/test/splunk-welcome/var/log/splunk/metrics.log</td>
<td>1393611</td>
</tr>
</tbody>
</table>
Rock & Roll

All night. And party every day.
Download and Install
See Details tab for Instructions

Overview

Users oftenland in Splunk with no clue where to begin. Use this app and it's over 20 pre-built panels to create an effective starting page for your users.

This app builds upon the concepts and philosophies outlined in the blog posts Introducing the "Welcome Page Creator" (https://www.splunk.com/blog/2016/06/01/introducing-the-welcome-page-creator) and Your Splunk Workspace (https://www.splunk.com/blog/2017/02/01/your-splunk-workspace)

Subscribe to this app button on bottom right of this page for notifications of updates.

Release Notes

2012

276

Download

Rate this App

VERSION

2.6.1

BUILT BY

Splunk Works
Welcome Page for Welcome Page Creation

Instructions

What is the Welcome Page Creator?
Not sure how you got here?
- Introducing the Welcome Page Creator
- Your Splunk Workspace

Step 1: Stage the Workspace App Template
The Welcome Page Creator contains a Workspace app template. To take advantage of it, copy the folder
$SPLUNK_HOME/etc/apps/welcome/static/workspace to
$SPLUNK_HOME/share/splunk/app_templates/workspace
(FYI: Restart not required)

Step 2: Create a Workspace
Select the 'workspace' template while creating a Splunk app.
What's a Workspace?

Step 3: Customize the Workspace's Welcome Page
Navigate to that new Workspace (app). Notice that you were automatically directed to a 'welcome' page.
Edit that 'welcome' page as desired by adding from prebuilt panels included with this app or customize panels as described in this post on answers.splunk.com

Still Confused?
- Explore relevant Q&A on answers.splunk.com

Step Fun: Optional Polish
Some best practices for added fun!
- Set the new workspace as the default app for the respective user group's role
- Hide this Welcome Page Creator app so as not to distract your users. You can do so here by toggling the Visible item to "No."
  (Don't worry, the prebuilt panels referenced by other dashboards will continue to work.)
Step 1
Completed by us

Step 1: Stage the Workspace App Template

The Welcome Page Creator contains a Workspace app template. To take advantage of it, copy the folder

`
$SPLUNK_HOME/etc/apps/welcome/static/workspace
`

to

`
$SPLUNK_HOME/share/splunk/app_templates/workspace
`

(PFY: Restart not required)
Step 2

Manage Apps -> Create App

Step 2: Create a Workspace

Select the 'workspace' template while creating a Splunk app.

What's a Workspace?
Step 3: Customize the Workspace's Welcome Page

Navigate to that new Workspace (app). Notice that you were automatically directed to a 'welcome' page.

Edit that 'welcome' page as desired by adding from pre-built panels included with this app or customize panels as described in this post on answers.splunk.com.
Your Mission

Scenario

- ‘User’ role are non Technical Users
- ‘Power’ role are Technical Users
- Make “effective” workspaces for both
- Discussion questions after

Do Now:

- Step 2: Create a Workspace
- Step 3: Customize
- Step Fun++: Appreciate
  - Visibility?
  - Role play as each role
Images for Step Fun++

power
Access controls » Roles » power

Permissions
Apps » hol » Permissions

App permissions
Users with read access can only save objects for themselves, and require write

<table>
<thead>
<tr>
<th>Roles</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td></td>
<td>☑</td>
</tr>
<tr>
<td>can_delete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>power</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>splunk-system-role</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. ...create custom app template?

2. ...create an app in a Search Head Cluster?

3. ...get a date with Buttercup?
1. Rate this! (be honest)

2. Collaborate: #success
   • Sign Up @ http://splk.it/slack

3. Customer Success Studio

4. More talks, search for
   • Blueprints
   • Burch
   • Champagne
   • Delaney
   • Optimization
   • Best Practices
   • Veuve
Questions & Discussion?

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