



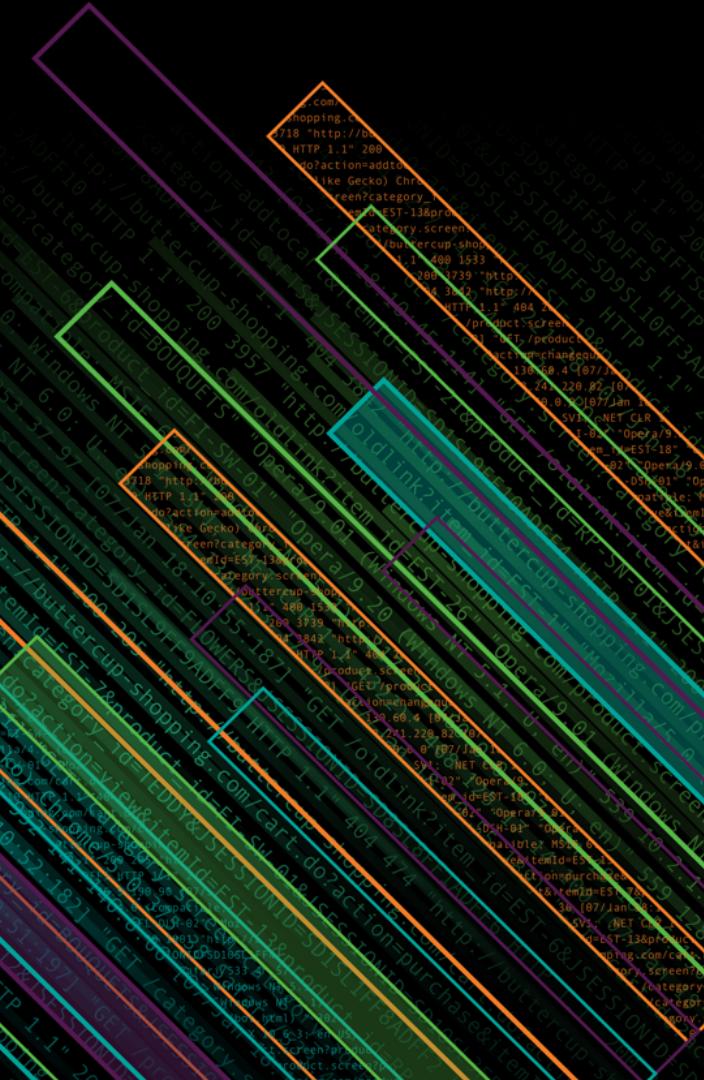
splunk>

# Splunk .conf18

## DevOps in the Enterprise

### Defense Agency Gains Push-Button Process for Repetitive Splunk Tasks

Bill Ern | Lockheed Martin  
Eric Nicholson | August Schell  
October 2018



# 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. © 2018 Splunk Inc. All rights reserved.

# Our Speakers

**BILL ERN**

Splunk Admin, Lockheed Martin

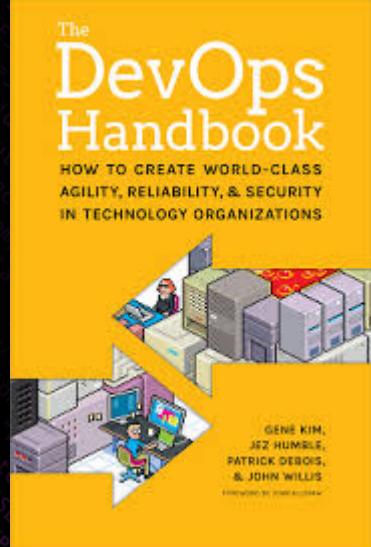
**ERIC NICHOLSON**

Splunk PS, August Schell

DEVOPS RISES TO THE OCCASION

splunk> .conf18

“Currently, DevOps is more like a philosophical movement, not yet a precise collection of practices, descriptive or prescriptive.”



—Gene Kim

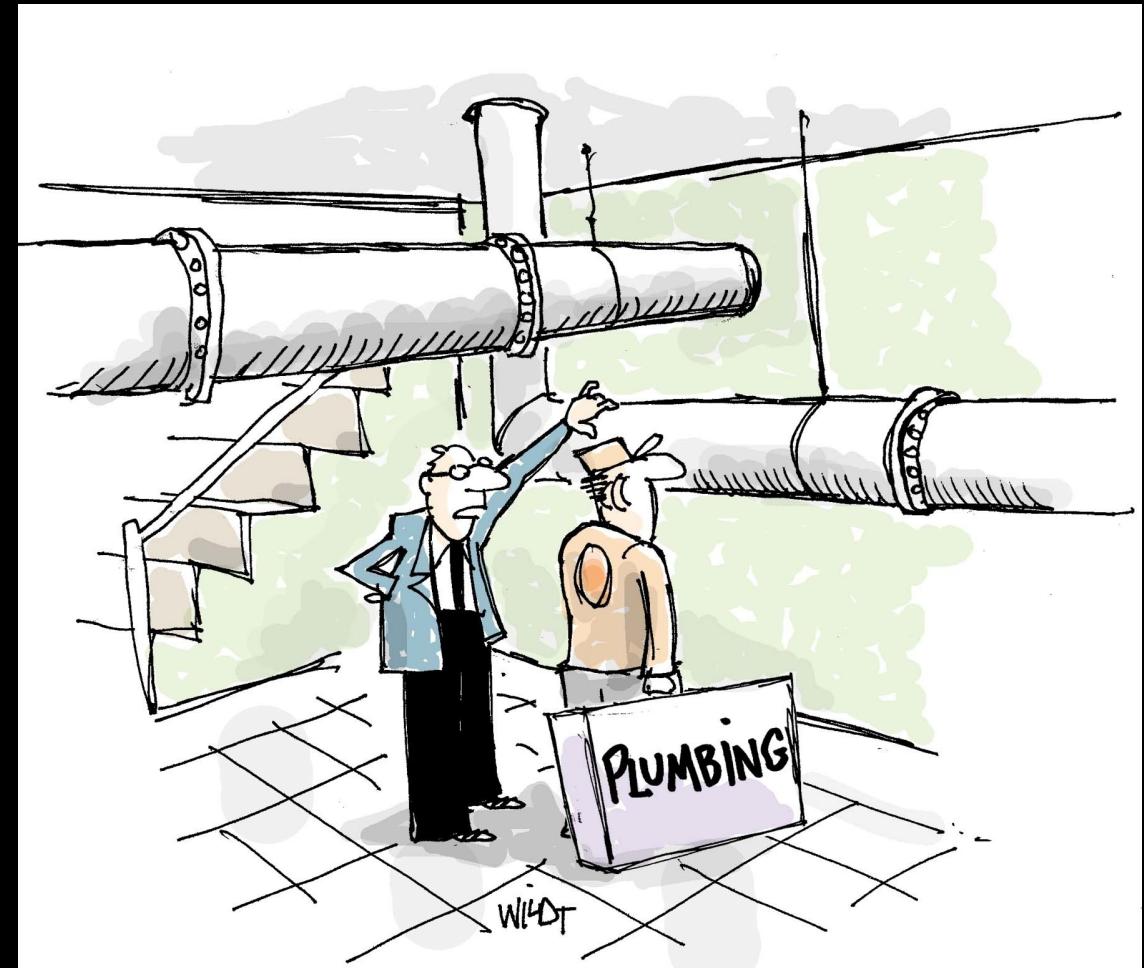
# Challenges

## What Problems Exist?

1. A large scale Splunk infrastructure growing at an extremely fast pace
2. Set up repository - software and configuration Files
3. Make updates continuously through a user-friendly file editor
4. Necessary that the cost be kept at a minimum
5. Automated by a click of a button during maintenance windows

# Solution

# The DevOps Pipeline

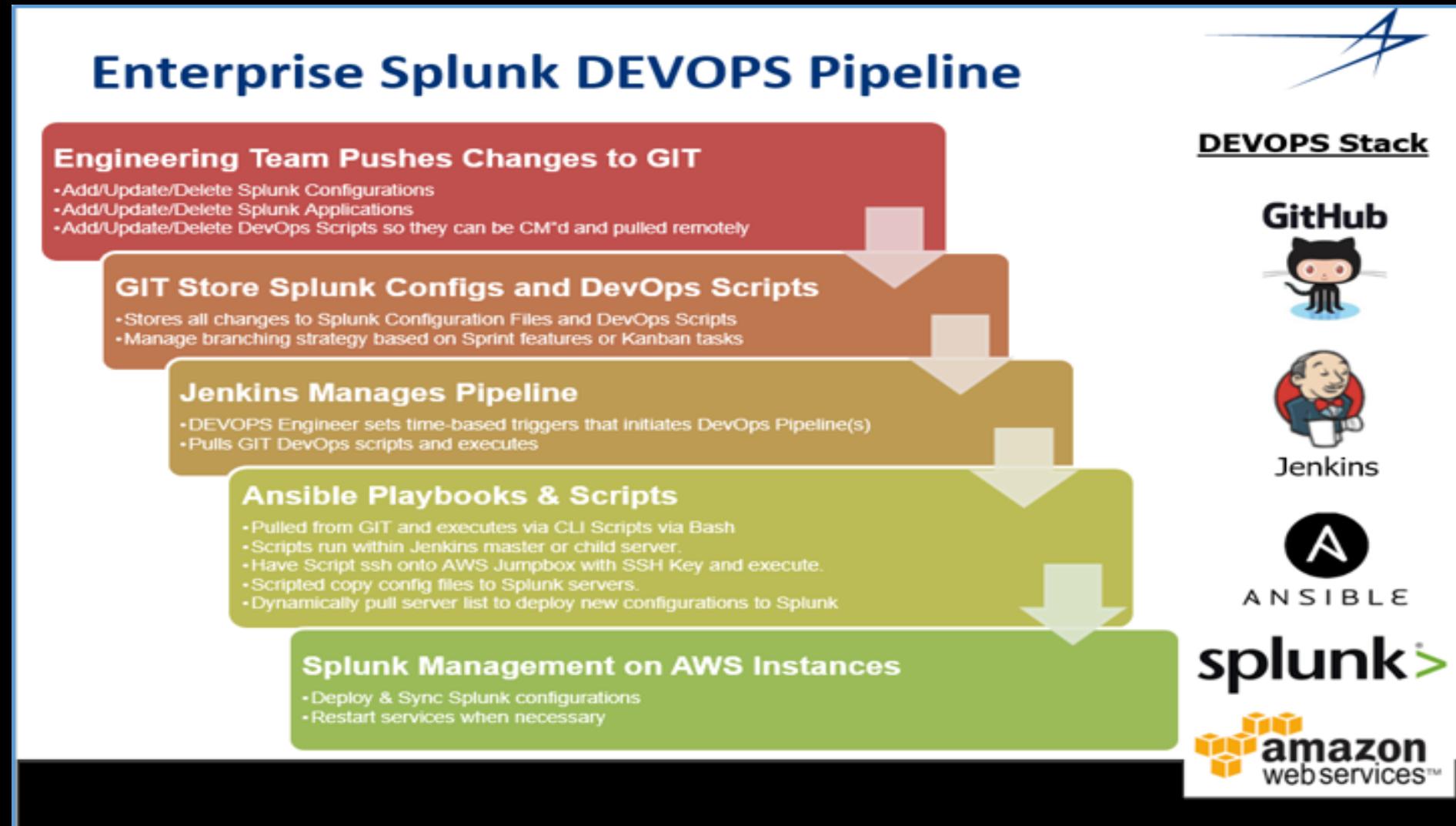


**"Tell me...what IS in the pipeline?"**

CartoonStock.com

# DevOps Pipeline

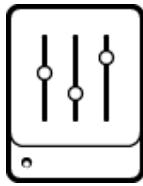
What is it?



# DevOps Workflow



Indexer Cluster Master



Deployment Server / Forwarder Management



ITSI Stand Alone Search



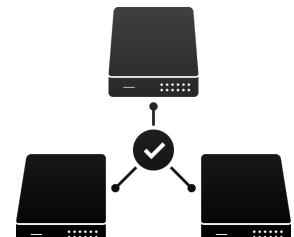
Exchange Search



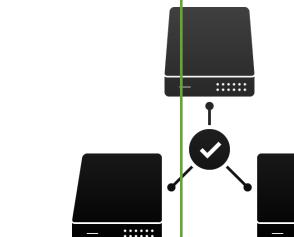
General Search Center



Security Search Center

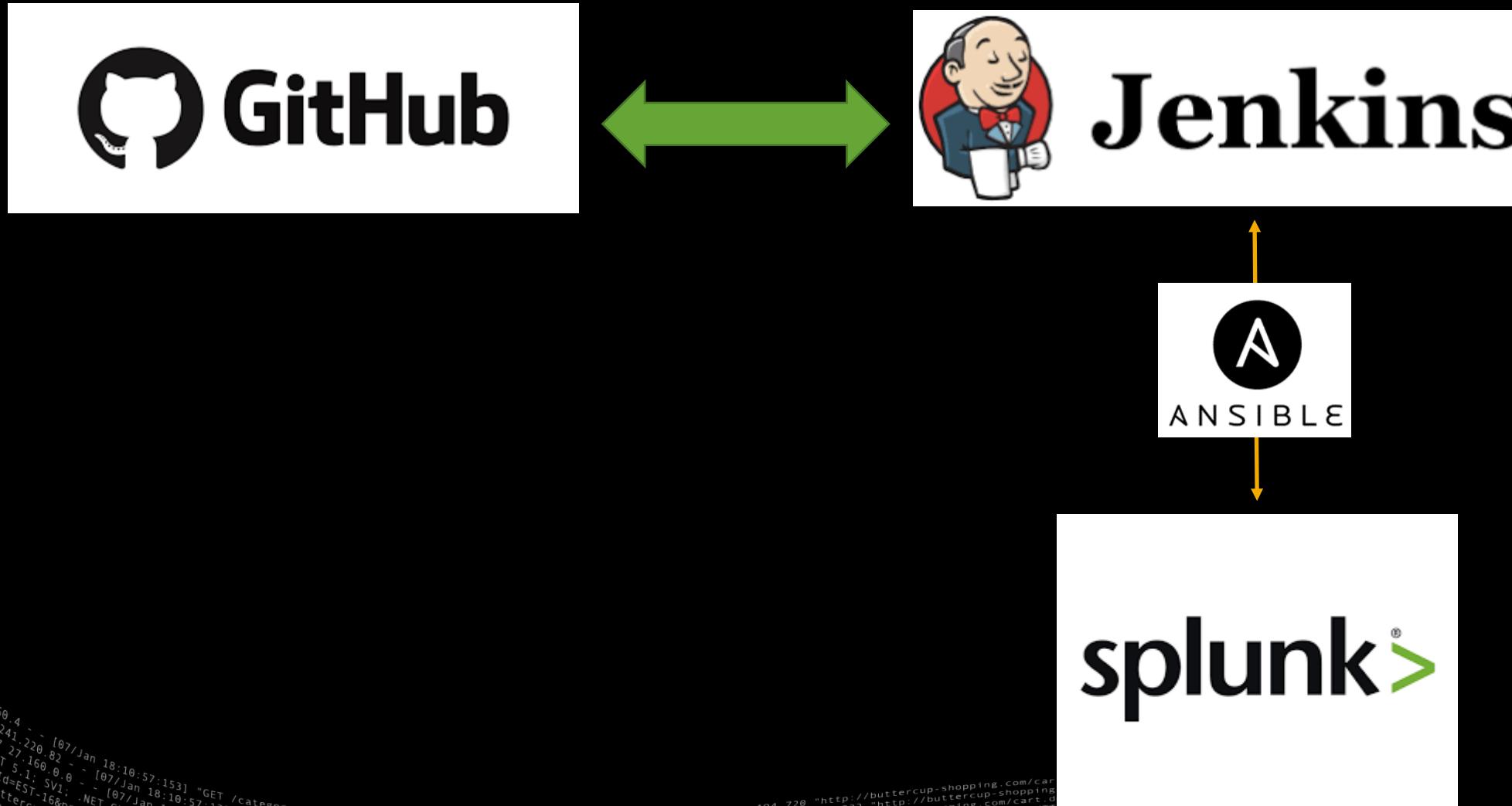


Specialized Search Center



# Brief Overview DevOps Workflow

## Workflow Diagram





# Git Repositories

- ▶ Security Search Center Staging DEV
  - ▶ General Search Center Staging DEV
  - ▶ Security Search Center PROD
  - ▶ General Search Center PROD
  - ▶ ITSI Search Center PROD
  - ▶ Exchange Search Center PROD
  - ▶ Deployment Server Primary PROD

▶ Search Center repositories contain proprietary Apps and Add-ons that pertain only to that Search Center

# GitHub

## Repositories Match the Search Centers

The screenshot shows a GitHub user profile for Eric Nicholson. The top navigation bar includes links for Pull requests, Issues, Marketplace, and Explore. Below the header, there's a search bar and a summary of the user's activity: 6 Repositories, 3 Stars, 0 Followers, and 1 Following. A large yellow T-shaped icon serves as the user's profile picture. The main content area displays three starred repositories:

- EricNicholson / Cluster\_Master**: Indexer Cluster Master. Last updated 20 hours ago by Nix. Includes a star/unstar button.
- EricNicholson / Security\_Search\_Center**: Splunk Security Search Center. Last updated 20 hours ago by Nix. Includes a star/unstar button.
- EricNicholson / Deployment\_Server**: Splunk Deployment Server repository. Last updated 19 hours ago by Nix. Includes a star/unstar button.

On the left side of the profile, there's a bio section with a placeholder "Add a bio" and an email address "eric.nicholson@augustschell.com". The footer contains standard GitHub links: Contact GitHub, Pricing, API, Training, Blog, and About.

- ▶ Repository Names Matched the Search Center Names for Easy Identification
- ▶ Within Each Repository are all .conf files, Applications, and TA's
- ▶ Members of the team make changes to files in this interface



# Ansible Playbooks

- ▶ Ansible playbooks are Ansible's configuration, deployment and orchestration language.
  - ▶ Playbooks are used to manage configurations and deployments to remote machines.
  - ▶ In our use case, An Ansible Playbook has been designed specifically to manage repetitive Splunk tasks. These tasks include:
    - Deploying Apps and Add-ons to Splunk Deployers (Search Head Cluster Deployer) and apply the cluster bundle
    - Deploying Apps and Add-ons to Splunk Staging search heads and performing a splunk restart
    - Deploying Apps and Add-ons to Splunk Deployment Server (Forwarder management) and perform the reload deployer
  - ▶ The projects are able to handle pulling the appropriate GitHub repository and then invoke an Ansible playbook to perform tasks such as syncing the repository to the appropriate location on the remote Splunk instance.

```
1  ---
2  - hosts: localhost
3  gather_facts: no
4  tasks:
5
6  - name: Git clone of Search Center repo
7    git:
8      executable: /usr/bin/git
9      repo: https://github.com/EricNicholson/searchhead_deployer.git
10     dest: /dev_ops/repos/Search_Center
11     version: master
12
13 - hosts: ase_dev_depl
14 gather_facts: no
15 tasks:
16   - include_vars: vars.yml
17   - name: Backup Splunk etc/shcluster/apps prior to deployment
18     command: tar czvf /opt/splunk_shapps_backup.tgz /opt/splunk/etc/shcluster/apps
19
20   - name: Sync Git Search Center repository apps to Splunk Search Center Deployer
21     synchronize:
22       src: /dev_ops/repos/Search_Center/
23       dest: /opt/splunk/etc/shcluster/apps
24       recursive: yes
25       delete: no
26       rsync_path: "rsync"
27       use_ssh_args: yes
28       rsync_opts:
29         - "--exclude=.git"
30         - "--exclude=*.md"
31
32   - name: Set execute permissions on Nix shell scripts
33     file:
34       dest: /opt/splunk/etc/shcluster/apps/Splunk_TA_nix/bin/
35       mode: 0755
36       recurse: yes
37
38   - name: Splunk Apply shcluster-bundle on Deployer
39     command: /opt/splunk/bin/splunk apply shcluster-bundle -target https://192.168.1.203:8089 --answer-yes -auth {{user}}:{{pass}}
40     register: splunkstatus
41   - debug: var=splunkstatus.stdout_lines
42
```



# Jenkins Projects

- ▶ Jenkins Projects are jobs that perform tasks such as software builds, run tests, perform repetitive tasks and run scripts
  - ▶ In this use case, Jenkins projects have been created in association with each Ansible Playbook.
  - ▶ Administrators are able to build the Jenkins project that will automatically deploy to Search Head Clusters, Indexer Clusters or Deployment Servers.
  - ▶ Jenkins serves as the “Push Button” answer to the use case.

# Jenkins

New Item    People    Build History    Manage Jenkins    My Views    Credentials    New View

1    search    Admin | log out    ENABLE AUTO REFRESH

[add description](#)

S	W	Name ↓	Last Success	Last Failure	Last Duration	
		<a href="#">Cluster Master</a>	20 hr - #5	1 day 1 hr - #2	11 sec	
		<a href="#">Deployment Server</a>	19 hr - #5	19 hr - #1	12 sec	
		<a href="#">Security Search Center</a>	4 min 0 sec - #2	N/A	36 sec	
		<a href="#">Test Host</a>	1 day 19 hr - #6	1 day 19 hr - #4	8.7 sec	

Icon: [S](#) [M](#) [L](#)

Legend: RSS for all RSS for failures RSS for just latest builds

**Build Queue**  
No builds in the queue.

**Build Executor Status**  
1 Idle  
2 Idle

Jenkins

1

search Admin | log out

ENABLE AUTO REFRESH

Back to Dashboard

Status

Changes

Workspace

Build Now

Delete Project

Configure

Rename

Project Cluster Master

Search Center deployment

edit description

Disable Project

Workspace

Recent Changes

Build History

trend —

find

#5 Sep 6, 2018 2:43 PM

#4 Sep 6, 2018 2:25 PM

#3 Sep 6, 2018 9:50 AM

#2 Sep 6, 2018 9:17 AM

#1 Sep 6, 2018 9:15 AM

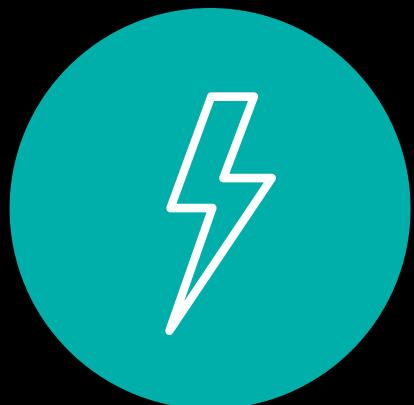
RSS for all RSS for failures

Permalinks

- Last build (#5), 20 hr ago
- Last stable build (#5), 20 hr ago
- Last successful build (#5), 20 hr ago
- Last failed build (#2), 1 day 2 hr ago
- Last unsuccessful build (#2), 1 day 2 hr ago
- Last completed build (#5), 20 hr ago

# Benefits of DevOps

# Why DevOps Matters



# Speed

# Move at a High Velocity



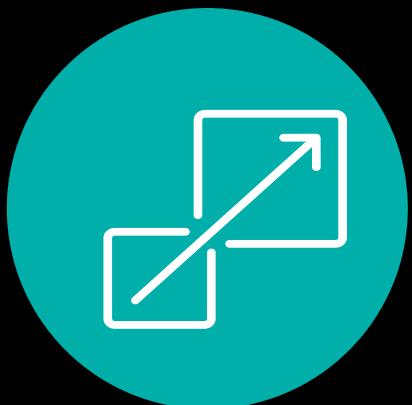
Rapid  
Delivery

**Increase the frequency and pace of releases**



# Reliability

# Continuous Integration & Continuous Delivery



# Scalable

# Manage Complex Changing Infrastructure Systems



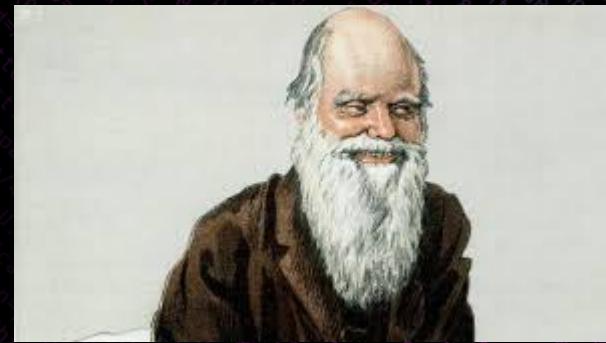
## Security

# Retain Control and Preserve Compliance

# Business Impacts

1. Shortened the maintenance windows from hours to minutes.
2. By automating complex manual tasks, the customer greatly reduced the risk of introducing human error into their environment.
3. Internal staff with less expertise were empowered to use Splunk easily as a result of automation.
4. Daily regular Splunk routines went from complex and risky to the simple click of a button.

“It is not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change.”



—Charles Darwin

# DevOps Demo

Presented by Eric Nicholson

# Q&A

**Bill Ern | Admin**

**Eric Nicholson | Splunk PS**

# Thank You

Don't forget to rate this session  
in the .conf18 mobile app

