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> .conf18

Our Speakers

BILL ERN

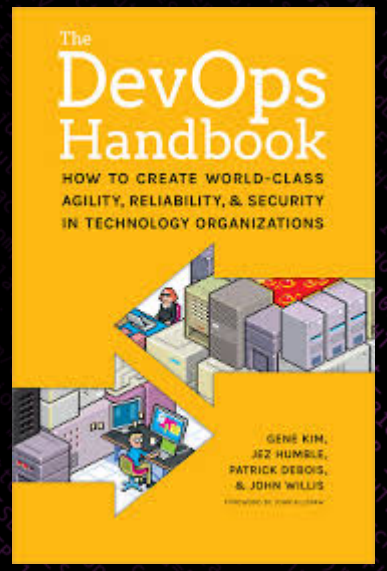
Splunk Admin, Lockheed Martin

ERIC NICHOLSON

Splunk PS, August Schell

DEVOPS RISES TO THE OCCASION

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



—Gene Kim

splunk> .conf18

Challenges

What Problems Exist?

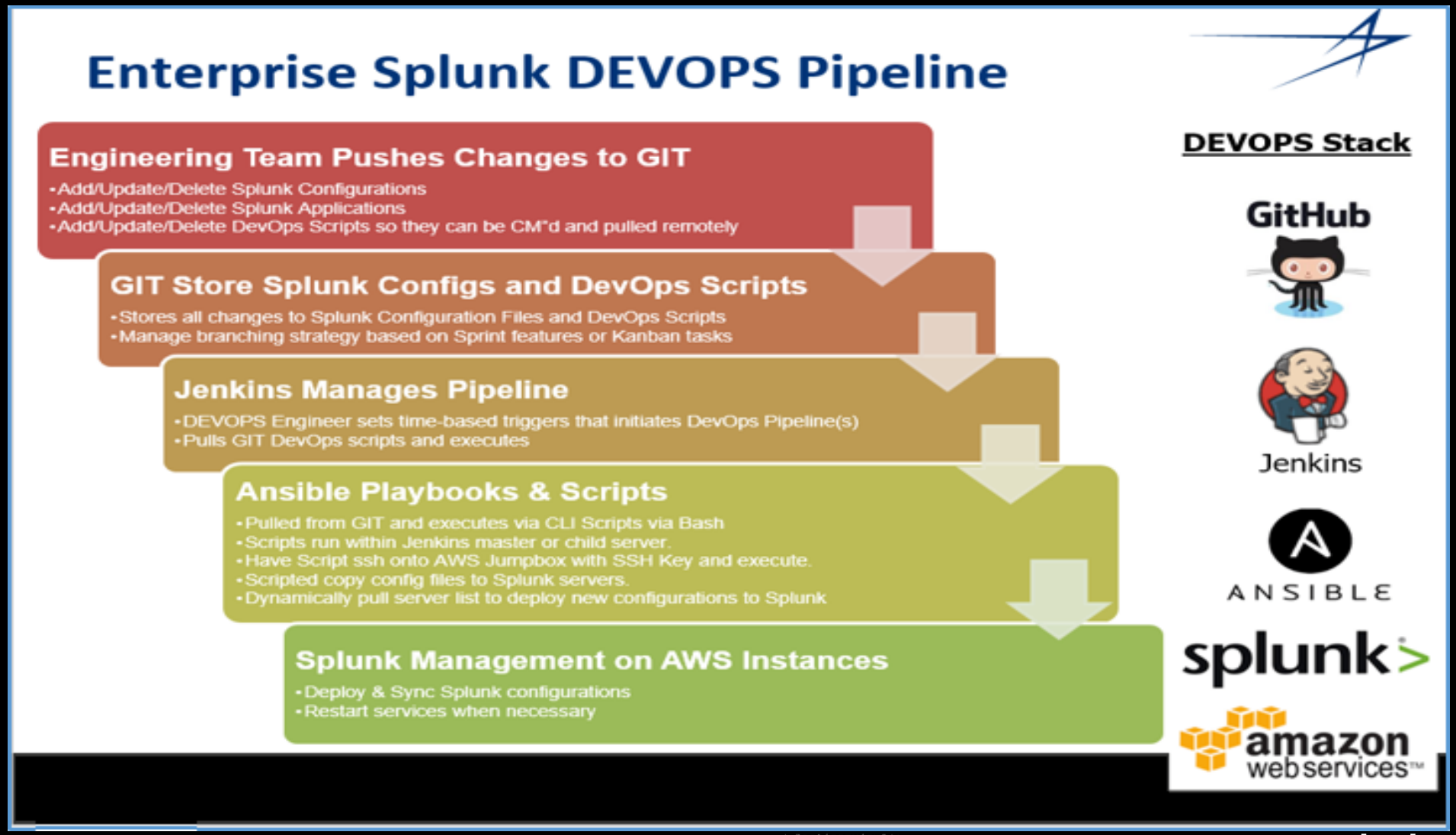
1. A large scale Splunk infrastructure growing at an extremely fast pace
2. Set up repository - software and configuration Files
3. Make updates continuously through a user-friendly file editor
4. Necessary that the cost be kept at a minimum
5. Automated by a click of a button during maintenance windows

Solution

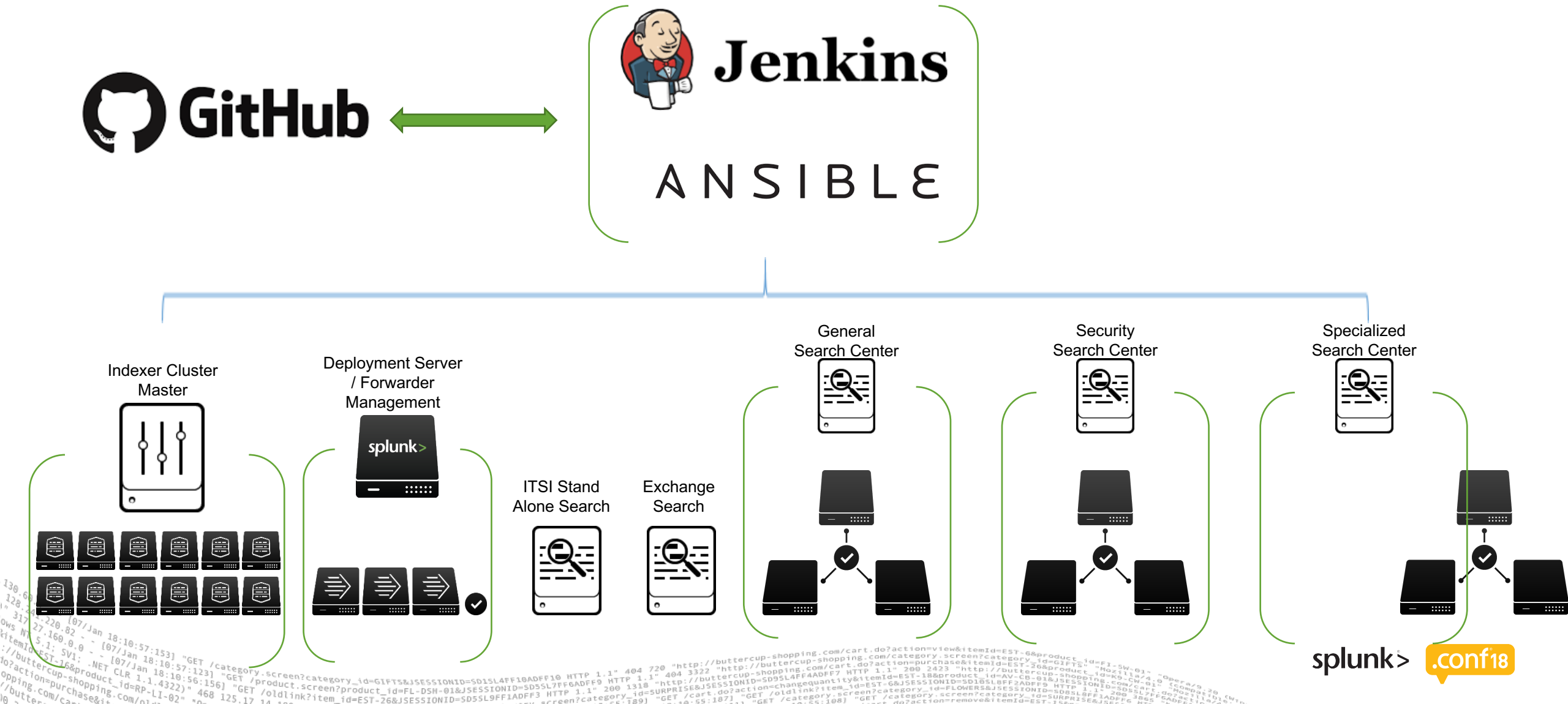
The DevOps Pipeline

DevOps Pipeline

What is it?

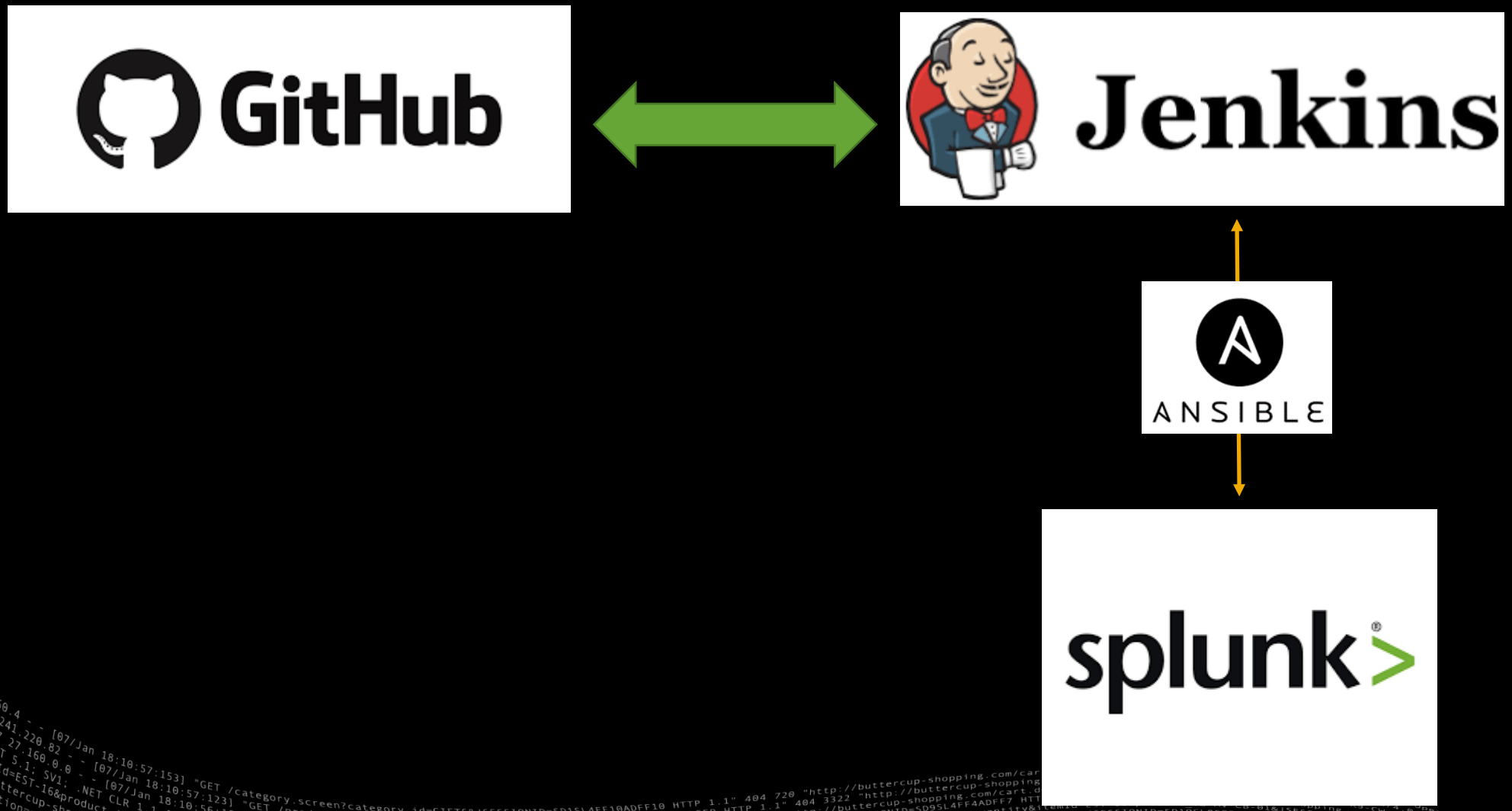


DevOps Workflow



Brief Overview DevOps Workflow

Workflow Diagram



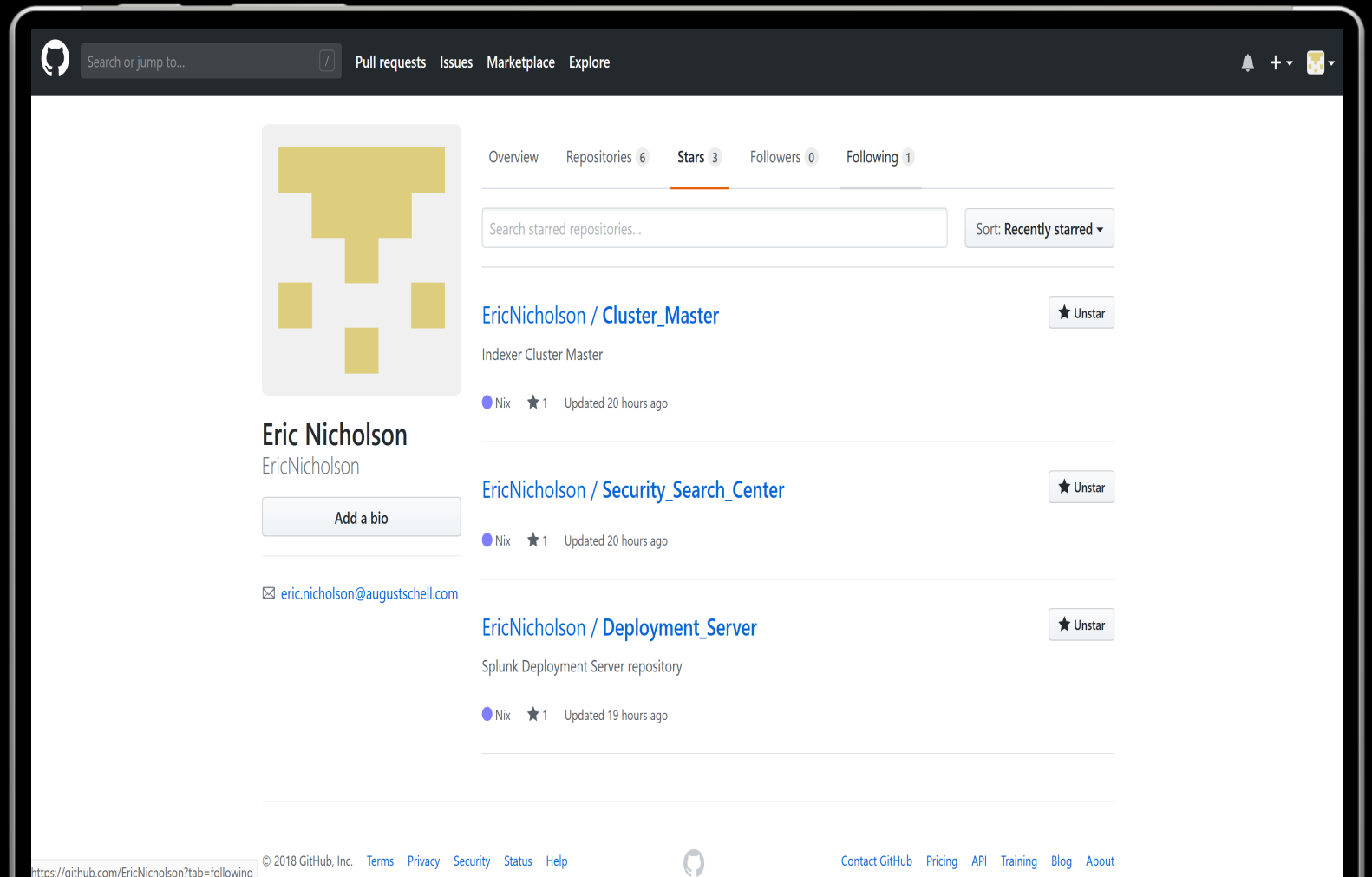
Git Repositories

- 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

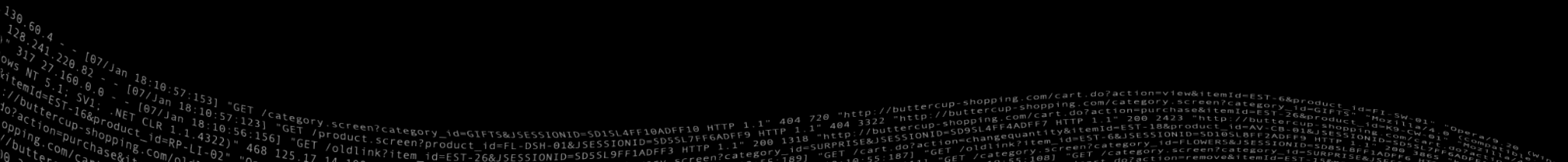


- Repository Names Matched the Search Center Names for Easy Identification
- Within Each Repository are all .conf files, Applications, and TA's
- Members of the team make changes to files in this interface

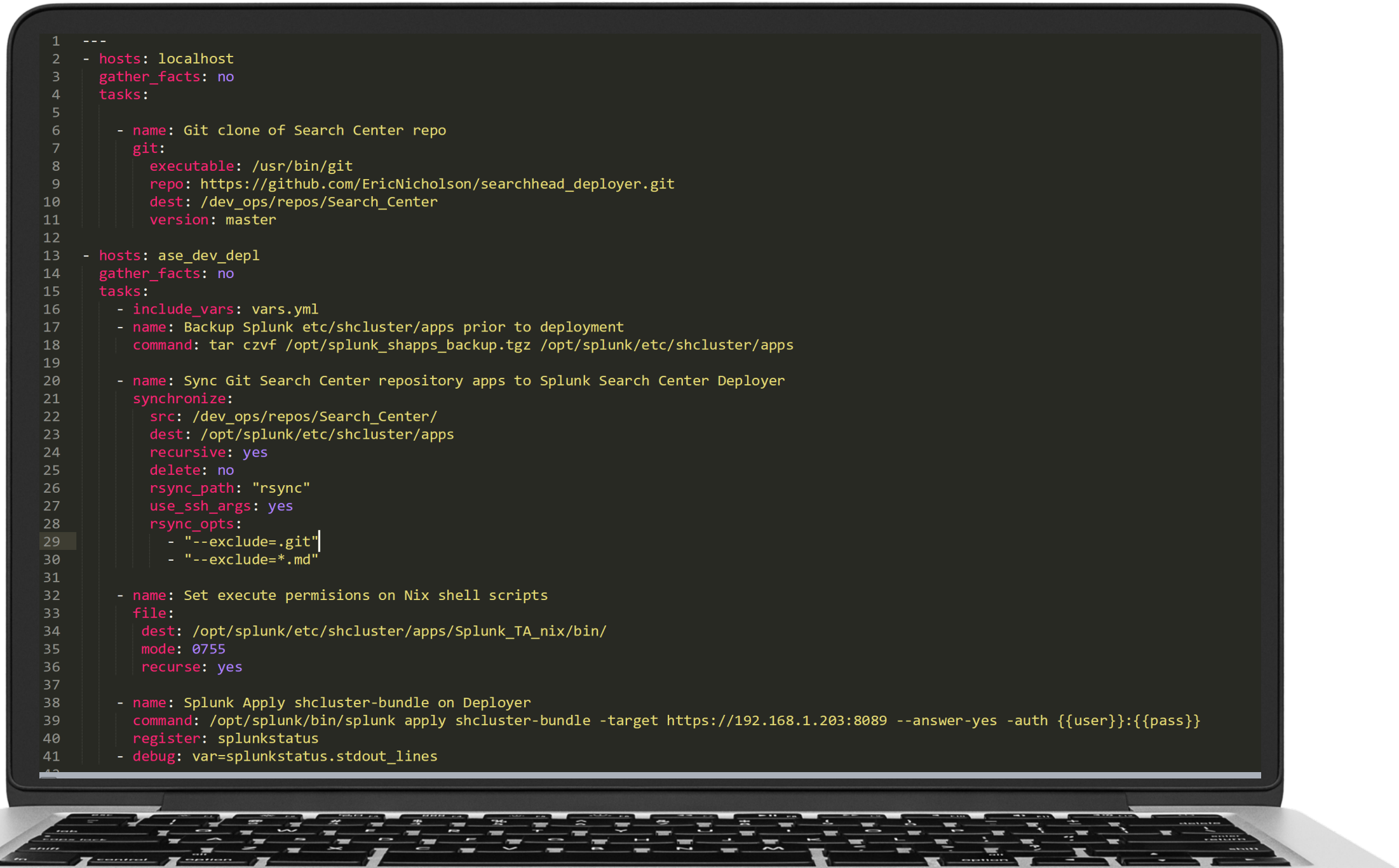
splunk> .conf18

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.



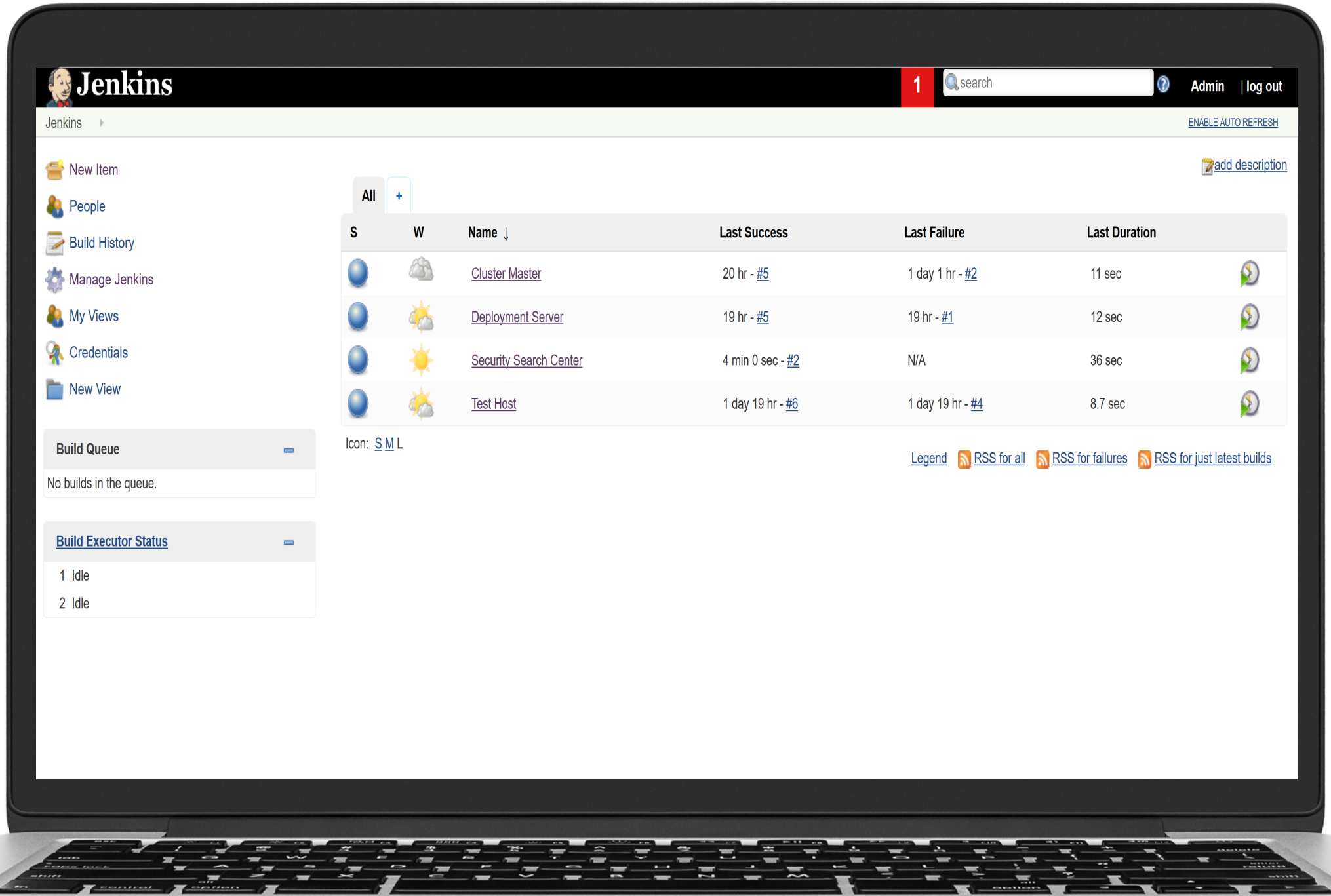
splunk> .conf18

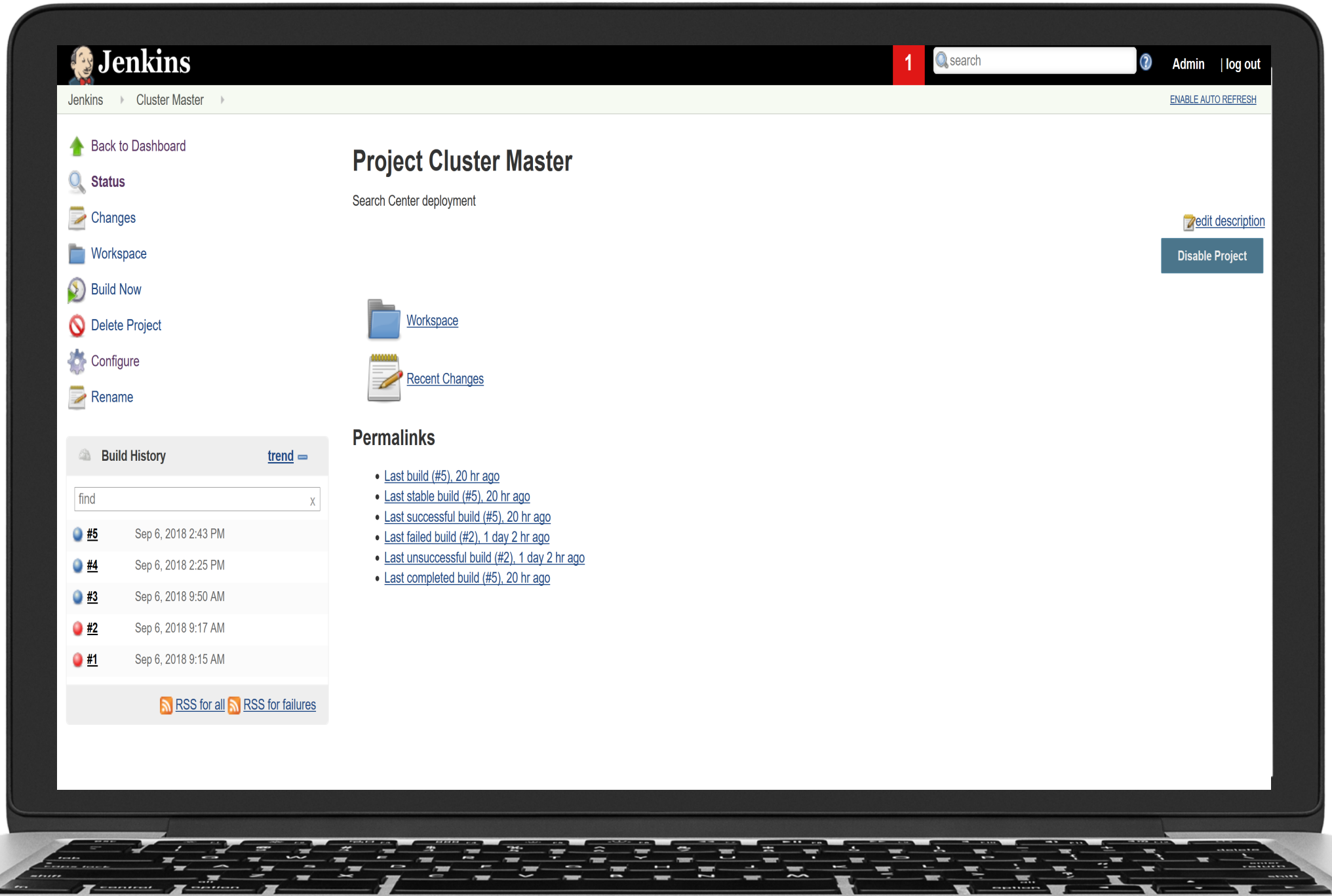


```yaml
---
- hosts: localhost
  gather_facts: no
  tasks:

    - name: Git clone of Search Center repo
      git:
        executable: /usr/bin/git
        repo: https://github.com/EricNicholson/searchhead_deployer.git
        dest: /dev_ops/repos/Search_Center
        version: master

- hosts: ase_dev_depl
  gather_facts: no
  tasks:
    - include_vars: vars.yml
    - name: Backup Splunk etc/shcluster/apps prior to deployment
      command: tar czvf /opt/splunk_shapps_backup.tgz /opt/splunk/etc/shcluster/apps

    - name: Sync Git Search Center repository apps to Splunk Search Center Deployer
      synchronize:
        src: /dev_ops/repos/Search_Center/
        dest: /opt/splunk/etc/shcluster/apps
        recursive: yes
        delete: no
        rsync_path: "rsync"
        use_ssh_args: yes
        rsync_opts:
          - "--exclude=.git"
          - "--exclude=*.md"

    - name: Set execute permisions on Nix shell scripts
      file:
       dest: /opt/splunk/etc/shcluster/apps/Splunk_TA_nix/bin/
       mode: 0755
       recurse: yes

    - name: Splunk Apply shcluster-bundle on Deployer
      command: /opt/splunk/bin/splunk apply shcluster-bundle -target https://192.168.1.203:8089 --answer-yes -auth {{user}}:{{pass}}
      register: splunkstatus
    - debug: var=splunkstatus.stdout_lines
```

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.





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

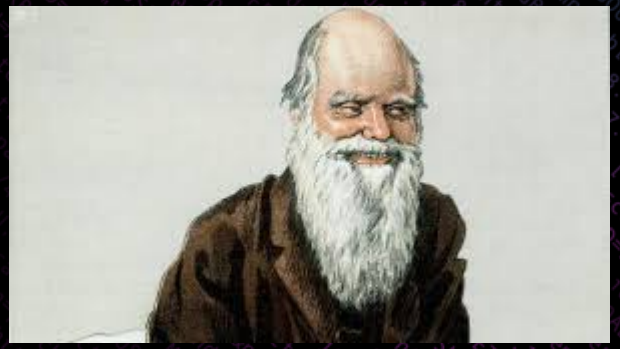
Security

Retain Control and Preserve Compliance

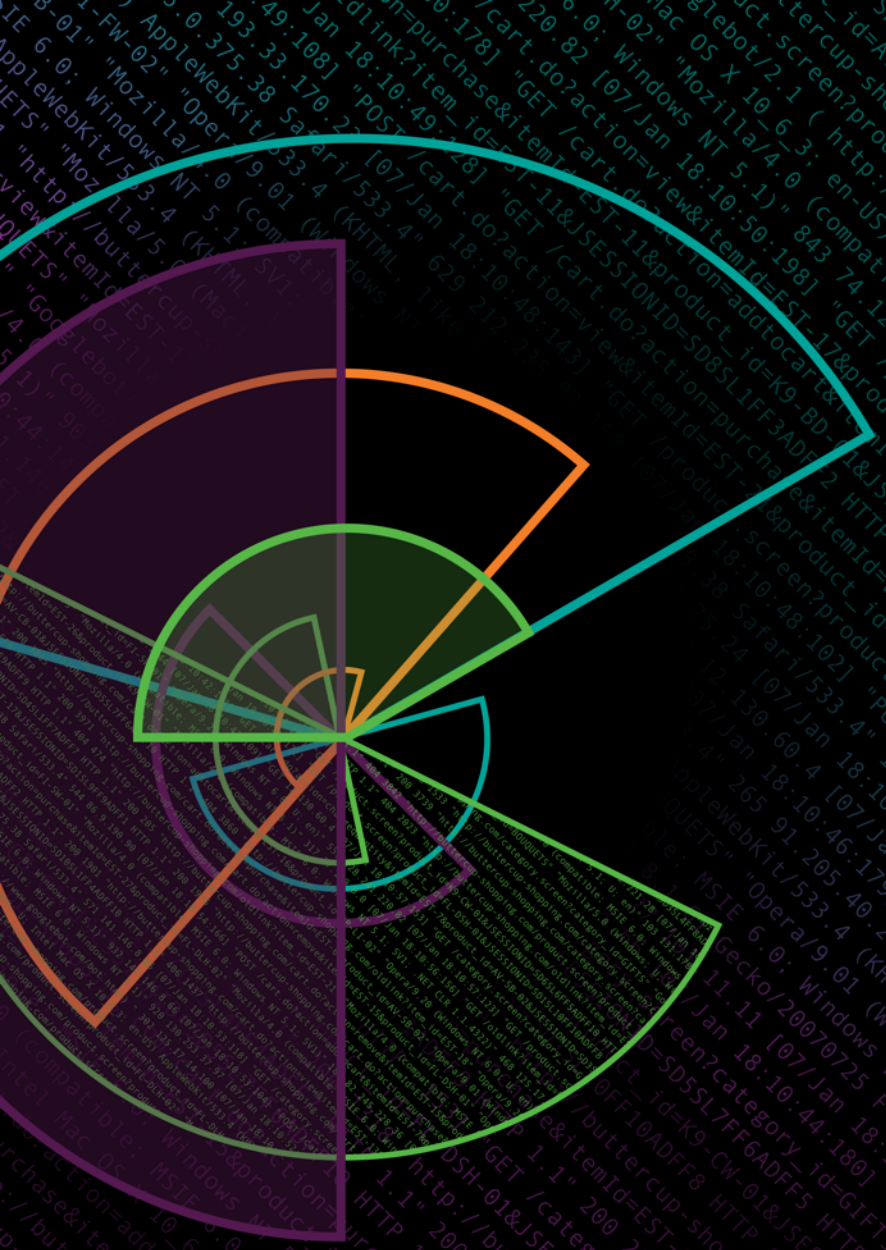
Business Impacts

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

splunk> .conf18

Q&A

Bill Ern | Admin

Eric Nicholson | Splunk PS

splunk> .conf18

Thank You

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