Deploying and Managing Splunk with Ansible

Micah Kemp 2017-07-11

https://github.com/micahkemp/DASUG-20170711

Ansible - What is it?

From the Ansible Documentation:

> Ansible is an IT automation tool. It can configure systems, deploy software, and orchestrate more advanced IT tasks such as continuous deployments or zero downtime rolling updates.

How is it used (typically)?

Push, not pull

Over SSH

Ansible Components

Playbooks

Roles

Dependencies

Tasks

Modules

Playbooks - 0001-initial-deployment.yml

Broad definition of what you want to be done

Define which roles to apply to which groups of servers

```
- hosts: splunk_servers

  roles:

      - role: splunk



- hosts: license_master

  roles:

      - role: splunk_license_master
```

Roles - roles/

Grouping of dependencies and tasks

```
roles/role_name/
      meta/
      tasks/
      files/
      vars/
```

Dependencies - roles/role_name/meta/main.yml

Apply roles X, Y and Z before applying this role

Use to keep your role tasks succinct

```
dependencies:

        -   role: splunk_user
```

Tasks - roles/role_name/tasks/main.yml

Perform the actual role-specific functions

```
- name: unpack splunk.tar.gz
  unarchive:
      src: "{{ splunk_tarball }}"
      dest: "{{ splunk_home }}/.."

- name: start splunk and accept license
  command: "{{ splunk_home }}/bin/splunk start --accept-license"
```

Modules - builtin and in library/

Code that is actually run on the host being configured

Customizeable in any language, but easier in Python due to SDK

```
hostname

user
```

```
library/splunk_user.py

library/splunk_config_stanza.py
```

Modules used in this demo - Builtin

hostname

user

unarchive

command

copy

Modules used in the demo - Custom

splunk_user

splunk_config_stanza

splunk_serverclass

splunk_deployment_application

splunk_search_peer

Summary before the demo

Using just a handful of builtin and custom modules, we can deploy a well configured, standardized, and scalable architecture

The demo will deploy:

- Search Head
- Cluster Master
- Indexers (2)
- Heavy Forwarder
- DMC