Splunk and Ansible

Joining forces to increase implementation power

Rodrigo Santos Silva | Head of Professional Services, Tempest Security Intelligence

09/28/2017 | 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.
Rodrigo Silva  
@rodsansil

- Manager of Professional Services Team at Tempest Security Intelligence

- +10 year experience in information security

- Head of incident response team experienced with major Brazilians financial institutions, industries, insurance companies, e-commerce, etc.
The purpose of this talk is to show how automation can be a close friend to the Splunk administrator. We will see how to create a Splunk cluster environment in minutes using Ansible playbooks.
Agenda

- Differences between Single Instance and Cluster Environment
- Orchestration
- What is Ansible?
- Why Ansible?
- Playbook definition and examples
- Demo
- Lessons Learned
- Q&A
Single instance

Sources

People > splunk > Source
Single instance

- Easy installation
- Minimum administration
- Everything works out of the box
- Small business
Cluster Environment

- Search Head Cluster
- Indexer Cluster
- Deployer
- License Server
- Master Node

Sources
Cluster Environment

- Complex setup
- Large amount of data
- Supported by specialist team
- Continuous increase by client’s demand
- Administration of different servers and services
- Minimal outage accepted
Not everyone working with Splunk has to be a Splunk administration specialist

So, how can we support cluster environment when not every Splunk administrator has the same know-how?

How can we deploy new Splunk nodes with the same configuration and always following the same recipe?
Orchestration

▶ Is the ability to execute and coordinate several automation workflows to reach higher goals

▶ Can be achieved with a lot of different tools (Ansible, SaltStack, Puppet, Chef)

▶ Deploying a new node or a new service doesn't have to be a heavy task. After creating a template, all work should be the automation of this workflow
Create a **unique role** for every node of your environment

Everyone should be able to execute the preset roles

Changes have to be applied only at the **workflows**, and after the certification process, deployed to the target servers
What is Ansible?

- Automated tool released in 2012 by Michael DeHaan
- Works by deploying customized modules (tasks, hosts, roles, playbooks)
- Generates log output for troubleshooting
- Centralized inventory
- Agentless
- Communicates through SSH
- No database required
- Python
- Easy to install and operate
# Why Ansible?

<table>
<thead>
<tr>
<th></th>
<th>Ansible</th>
<th>Chef</th>
<th>Salt</th>
<th>Puppet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support</strong></td>
<td>Ansible Works</td>
<td>Opscode</td>
<td>SaltStack</td>
<td>Puppet Labs</td>
</tr>
<tr>
<td><strong>Control Interface</strong></td>
<td>Playbook (YAML)</td>
<td>Recipes (DSL)</td>
<td>SLS (YAML)</td>
<td>Manifest (DSL)</td>
</tr>
<tr>
<td><strong>Agent</strong></td>
<td>Agentless</td>
<td>Server-Client or Standalone</td>
<td>Master-Agent or Standalone</td>
<td>Master-Agent or Standalone</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Python</td>
<td>Ruby</td>
<td>Python</td>
<td>Ruby</td>
</tr>
<tr>
<td><strong>Communication</strong></td>
<td>SSH</td>
<td>SSL</td>
<td>ZeroMQ</td>
<td>HTTP/ SSH / SSL</td>
</tr>
<tr>
<td><strong>Remote Execution</strong></td>
<td>Built-in</td>
<td>Challenging</td>
<td>Built-in</td>
<td>Challenging</td>
</tr>
<tr>
<td><strong>In Operation Since</strong></td>
<td>2012</td>
<td>2009</td>
<td>2011</td>
<td>2005</td>
</tr>
</tbody>
</table>

http://zigispacenet/m/839
Playbook

- Playbooks are Ansible’s configuration, deployment, and orchestration language. They can describe a policy that you want your remote systems to enforce, or a set of steps in a general IT process.

- At a basic level, playbooks can be used to manage configurations and deployments to remote machines. At a more advanced level, they can sequence multi-tier rollouts involving rolling updates, and can delegate actions to other hosts, interacting with monitoring servers and load balancers along the way.
Ansible Structure

Host File

# Every IPs

[spl_all]
172.16.199.10  ansible_connection=ssh  ansible_user=rss
172.16.199.20  ansible_connection=ssh  ansible_user=rss
172.16.199.30  ansible_connection=ssh  ansible_user=rss
172.16.199.40  ansible_connection=ssh  ansible_user=rss
172.16.199.50  ansible_connection=ssh  ansible_user=rss
172.16.199.60  ansible_connection=ssh  ansible_user=rss

# Search Head Ips

[sh]
172.16.199.10  ansible_connection=ssh  ansible_user=rss
172.16.199.20  ansible_connection=ssh  ansible_user=rss
172.16.199.30  ansible_connection=ssh  ansible_user=rss

# Indexer Cluster Master

[master_idx]
172.16.199.60  ansible_connection=ssh  ansible_user=rss
# Install the basic on every OS
- hosts: spl_all
  become: yes
  become_user: root
  roles:
  - basic

# Configure Master Index Cluster
- hosts: master_idx
  become: yes
  become_user: splunk
  roles:
  - master_idx_cluster

# Configure Peers Index Cluster
- hosts: idx
  become: yes
  become_user: splunk
  roles:
  - peers_idx_cluster

# Configure Deploer
- hosts: deployer
  become: yes
  become_user: splunk
  roles:
  - deployer

# Bring Up the Search Head Cluster Captain
- hosts: captain
  become: yes
  become_user: splunk
  roles:
  - captain

# Bond Search Head Cluster and Indexer Cluster
- hosts: sh
  become: yes
  become_user: splunk
  roles:
  - bondshidx
# Clear firewall configuration

- name: Basic Role => Flush Iptables
tables:
  flush: yes

# tasks file for basic

- name: Basic Role => Copy Splunk Binary
copy:
  src: '{{ binary }}'
  dest: /tmp
  owner: root
  group: root

# Binary installation

- name: Basic Role => Install Splunk
  yum:
    name: '{{ binarydir }}/{{ binary }}'
    state: present
  notify:
    - Basic Role (Handler) => Starting Splunk for the First Time
DEMO Lab

Search Head Cluster

Indexer Cluster

Deployer

License Server

Master Node

Sources
DEMO Walkthrough

- Deploy Splunk binary
- Install Splunk on every node
- Configure Index cluster
- Configure Search Head cluster
- Configure Deployer and Master Node
- Connect everything!! (:
Splunk Cluster Implementation Demo

Ansible Playbooks
1. Using an automation tool reduces the efforts of implementation and support while deploying a Splunk Cluster environment.

2. Anyone could be able to execute advanced task, even without the right knowledge.

3. Every task will be executed using always the same steps.
All playbooks used in this talk will be available at the link below:

https://github.com/rodsansil/ansible_splunk_cluster
References

- https://github.com/divious1/splunk-ansible-advance/blob/master/README.md
- “Ansible for DevOps”, Jeff Geerling
- https://docs.ansible.com
- https://www.splunk.com
- http://www.devopsbookmarks.com/orchestration
- http://zigispace.net/m/839
Thank You

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