splunk>

Deploying Splunk on OpenShift – Part2 : Getting Data In

Eric Gardner (Splunk) – Sr. Solutions Engineer
Matthew Bach (RedHat) – Sr. Specialist Solutions Architect
Public Sector - DoD

splunk> turn data into doing™

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

#whoami

Eric Gardner ericg@splunk.com

- 20+ years in IT (ITOPS focus)
- Worked with DoD/INTEL since leaving the Army in 1999.
- Spend my time traveling and usually planning travel when not actually doing it. Lately spending lots of time fighting bamboo.
- Based out of Bridgton, ME (that's about 1 hour north-west of Portland and Stephen King's stomping grounds)

#whoami

Matthew Bach: mbach@redhat.com

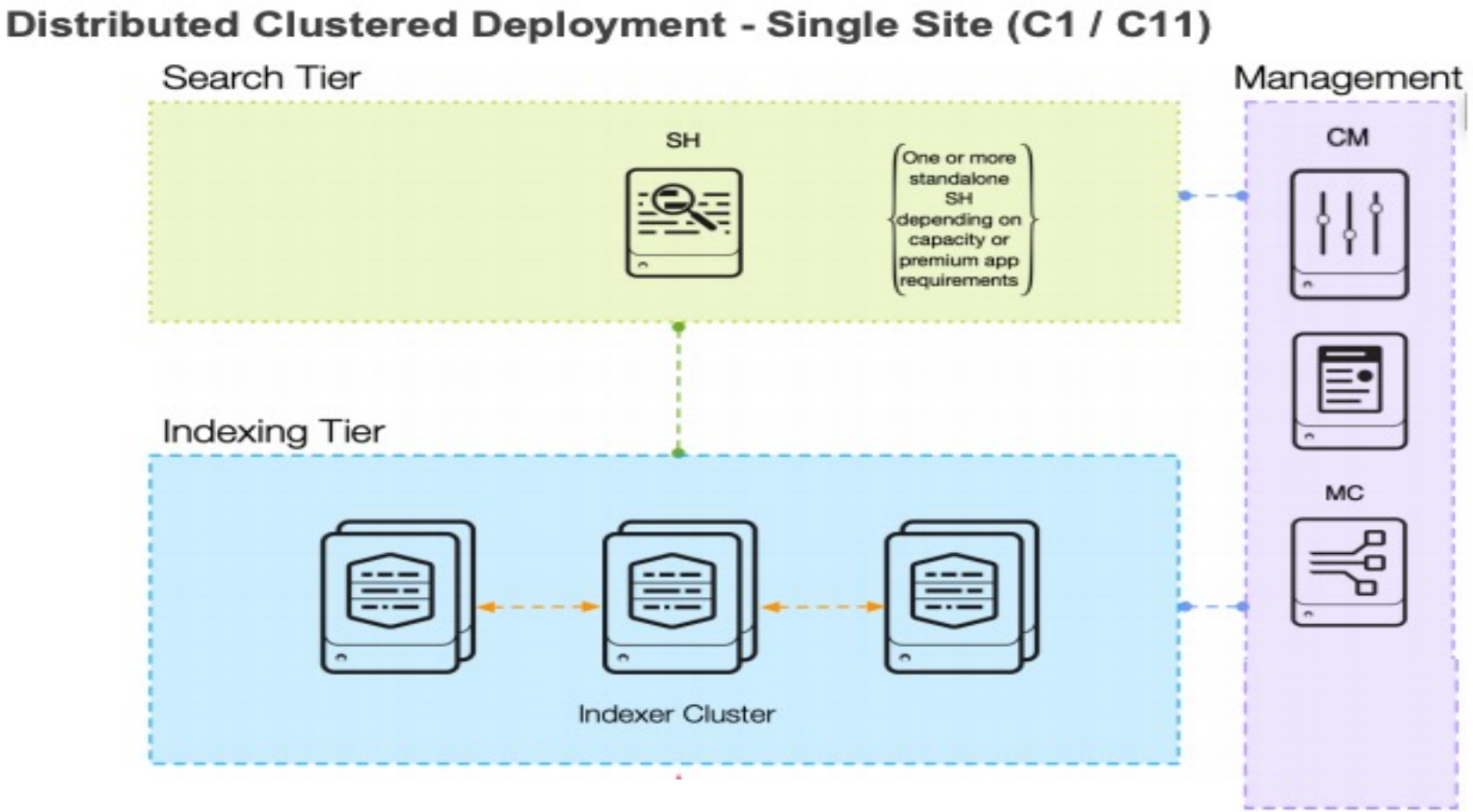
uid=1000(mbach) gid=1000(mbach) groups=1000(mbach),10(wheel)

- Information Systems Technician in the US Navy from 2004 - 2017
- Have been a Red Hatter ever since ~4.5 years
- RH OpenShift & Ansible Specialist
- Cover DoD customers (SOF, Missile Defense, 4th Estate)
- Based in VA Beach, VA
- Spend my time raising kids, tinkering with tech, video games, and mountain biking

Red Hat OpenShift

Previously …

•Deployed Splunk Enterprise (Core) in OpenShift using the Splunk Operator for Kubernetes



Splunk Connect for Kubernetes

https://github.com/splunk/splunk-connect-for-kubernetes

Splunk Connect for Kubernetes provides a way to import and search your Kubernetes logging, object, and metrics data in your Splunk platform deployment. Splunk Connect for Kubernetes supports importing and searching your container logs on the following technologies:

- Amazon Web Services (AWS) Elastic Container Service (ECS) and AWS Fargate, using Firelens.
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- RedHat OpenShift

Splunk Inc. is a proud contributor to the Cloud Native Computing Foundation (CNCF). Splunk Connect for Kubernetes utilizes and supports multiple CNCF components in the development of these tools to get data into Splunk.

Prerequisites

- Splunk Enterprise 7.0 or later
- A HEC token. See the following topics for more information:
  - http://docs.splunk.com/Documentation/Splunk/8.2.2/Data/UsetheHTTPEventCollector
  - http://docs.splunk.com/Documentation/Splunk/8.2.2/Data/ScaleHTTPEventCollector
- You should be familiar with your Kubernetes configuration and know where your log information is collected in your Kubernetes deployment.
- Administrator access to your Kubernetes cluster.
- To install using Helm (best practice), verify you are running Helm in your Kubernetes configuration. See https://github.com/kubernetes/helm for more information.
- A minimum of two Splunk platform indexes ready to collect the log data. One for both logs and Kubernetes objects, and one for metrics. You can also create separate indexes for logs and objects, but you will need three Splunk platform indexes.

Before we begin

- ✓ HEC Token has already been installed
- ✓ Three indexes created (minimum of two):
  - ✓ em_metrics (metrics)
  - ✓ em_meta (objects)
  - ✓ em_events (logs)
- ✓ Helm is installed
- ✓ Helm repo added
  - ✓ helm repo add splunk https://splunk.github.io/splunk-connect-for-kubernetes/
- ✓ Installed Splunk App for Infrastructure
- ✓ Installed IT Essentials Work (SAI will be going away in 2022)

Let's talk about SAI

There's more than one way to skin a cat …

- SAI is going away, and its functionality will be rolled into IT Essentials Work
- The OpenShift Configuration script installs an old version of Splunk Connect for Kubernetes (SCK) – version 1.3.0
- Today we are going to walk through that script to understand what it does and how you can hack it for the latest version (Just be aware today doing this works but the next version may require more effort)
- Key Take-Aways:
  - You can break-down exactly what this script does and do it for yourself manually
  - You should know your environment well enough to override default settings with values that are appropriate for your environment
  - Some of the things you're being shown today are probably not best practice when it comes to OpenShift, but for lab/demo purposes it's OK. Just be sure to "DO THE RIGHT THING IN PRODUCTION".

Configure & Manually deploy the manifests

https://docs.splunk.com/Documentation/InfraApp/2.2.3/Admin/AddDataOpenShift

SAI – Add Data > Configure Integrations > OpenShift

1. Prepare for deployment
   a. Select Download Config Only – since we are manually deploying the manifests

2. Specify Configuration Options
   a. Customize Objects – for the demo we are selecting all
   b. Monitoring Machine = indexer service (e.g. splunk-cl01-indexer-service.splunk.svc.cluster.local)
   c. HEC Token (will be the token you already deployed)
   d. HEC Port (recommended 8088)
   e. Cluster Name (unique name that makes sense (e.g. cluster-5752)
   f. Openshift Project Name (e.g. splunk-connect, sc4k, etc)

Configure & Manually deploy the manifests

https://docs.splunk.com/Documentation/InfraApp/2.2.3/Admin/AddDataOpenShift

3. Configure OpenShift Options
   a. Enable Insecure SSL
   b. Journald Path = /var/log/journal

4. Index Options
   a. Metrics index = em_metrics
   b. Log index = em_events
   c. Metadata index = em_meta

5. Copy the script & Modify the command line script
   a. Copy the script to a text editor and replace “1.3.0” with “1.4.9”
   b. Run the script then follow the steps for Manually deploying the manifests for OpenShift

Configure & Manually deploy the manifests

https://docs.splunk.com/Documentation/InfraApp/2.2.3/Admin/AddDataOpenShift

What just happened?

That command sets up environment variables to be used in ”values.yaml” file that is applied to the helm charts downloaded from the SCK repository. The “deploy_sck_openshift.sh” script contains the command that modifies the charts. The modified charts can be found under a directory named “rendered-charts” in the same directory from where the command was run.

The script has a bug where it doesn’t correctly change a block of “yaml” code in this file:

./rendered-charts/splunk-connect-for-kubernetes/charts/splunk-kubernetes-logging/templates/daemonset.yaml

Edit the “securityContext” section to look like this:

```
securityContext:
    runAsUser: 0
    privileged: true
```

OpenShift Specific Things …

https://docs.splunk.com/Documentation/InfraApp/2.2.3/Admin/AddDataOpenShift

1. Create new project called “splunk-connect”
    1. oc new-project splunk-connect

2. Create service accounts for logging,objects, & metrics and configure initial permissions:
    1. oc create sa splunk-kubernetes-logging
    2. oc adm policy add-scc-to-user privileged ”system:serviceaccount:splunk-connect:splunk-kubernetes-logging”
    3. oc create sa splunk-kubernetes-objects
    4. oc adm policy add-scc-to-user privileged ”system:serviceaccount:splunk-connect:splunk-kubernetes-objects”
    5. oc create sa splunk-kubernetes-metrics
    6. oc adm policy add-scc-to-user privileged ”system:serviceaccount:splunk-connect:splunk-kubernetes-metrics”

Finally Deploy the Helm Charts

https://docs.splunk.com/Documentation/InfraApp/2.2.3/Admin/AddDataOpenShift

1. oc apply -f ./rendered-charts/splunk-connect-for-kubernetes/charts/splunk-kubernetes-metrics/templates/
2. oc apply -f ./rendered-charts/splunk-connect-for-kubernetes/charts/splunk-kubernetes-logging/templates/
3. oc apply -f ./rendered-charts/splunk-connect-for-kubernetes/charts/splunk-kubernetes-objects/templates/oc new-project splunk-connect

Let's talk …

The waiting is the hardest part – Tom Petty

It will take a few minutes for entities to show up in SAI or IT Essentials Work

What are your thoughts on Splunk on OpenShift?

What are your thoughts on OpenShift as a Kubernetes platform?

Questions?

splunk> turn data into doing™