AGENDA

We have about 20 minutes

- OpenShift Cluster Logging
- Challenges of running Elasticsearch in OpenShift
- Prometheus & Grafana
- Elasticsearch Operator
- Questions
OPENSHEET CLUSTER LOGGING
OPENSHIFT CLUSTER LOGGING

A container log message flow on a node

Container -> stdout

Container -> stderr

cri-o

Files on disk

/kvar/log/containers/*.log

Collector

kubectl logs <pod>

kubectl logs <pod>

Kubernetes master

send off the node
OPENSHIFT CLUSTER LOGGING

Per Project (Namespace) isolation
OPENSHIFT CLUSTER LOGGING
Openshift-logging Project
ELASTICSEARCH IN OPENSHIFT
WHAT ARE THE CHALLENGES

Scaling Elasticsearch with limited resources is hard

THE DATA MODEL

OPERATIONAL & PERFORMANCE TUNING

SKILLED PEOPLE
DATA MODEL
How we store logs into individual indices.

- One index per namespace
- One index per day
Scaling issues:
- Number of indices/shards
- Number of index fields

Reduce number of indices/shards:
- Rollover API
- Commercial (requires license)
- Spread the load to more clusters
PERFORMANCE & OPERATIONAL TUNING
CH#2 - OPS & PERF TUNING

Topology of Elasticsearch cluster and underlying HW is important

Physical and functional layout:
- Fast local storage
- Dedicated node roles
- Hot-Warm

Monitoring and Alerting:
- Commercial (requires license)
- DIY/3rd party solutions
SKILLED PEOPLE
There is *always* someone who takes care of your cluster and typically performs the following tasks:

- Maintenance
- Upgrades
- Troubleshooting
PROMETHEUS
PROMETHEUS

https://prometheus.io/

100% open-source and community driven

- Prometheus is systems monitoring and alerting toolkit
- Pull-based metrics gathering system, simple text format for metrics exposition
- PromQL: powerful query language
- CNCF member project
ELASTICSEARCH ➔ PROMETHEUS

Elasticsearch *does not* support metric exposition in Prometheus format

Prometheus exporter

- Requires additional container(s)
- More configuration (security)
- “High level” REST client
- Complex integration testing
- Independent upgrades

Elasticsearch native plugin

- Adding new HTTP endpoint
- Seamless integration with security existing model (SearchGuard)
- “Low level” Java
- Simple integration testing
- Upgrade require node restart
- [https://github.com/vvanholl/elastic search-prometheus-exporter](https://github.com/vvanholl/elastic search-prometheus-exporter)
GRAFANA
Dashboard to visualize Elasticsearch metrics stored in Prometheus.

- Cluster
- Shrads
- OS & JVM
- Indexing
- Searching
- Caches
- Throttling
- Indices (WIP)
- ...
ELASTICSEARCH-MIXIN
Magic of Kubernetes-mixin and Jsonnet templates

Bundle of:
- Prometheus recording rules, alerting rules
- Grafana dashboard

Build on top of [Jsonnet](https://github.com/jsonnet/jsonnet) and [Kubernetes-mixin](https://github.com/kubernetes-mixin).
Currently at [https://github.com/lukas-vlcek/elasticsearch-mixin](https://github.com/lukas-vlcek/elasticsearch-mixin). This location is likely to change in the future (community mixins).
ELASTICSEARCH OPERATOR
ELASTICSEARCH OPERATOR
Operator pattern for Cluster Logging and Elasticsearch

openshift-operators Namespace
- cluster-logging-operator
- elasticsearch-operator

openshift-logging Namespace
- ClusterLogging CR
- Fluentd
- Elasticsearch CR
- Elasticsearch (Cluster)
- Kibana
OPENSIFT MONITORING INTEGRATION

Prometheus and Grafana artifacts get loaded

- openshift-monitoring
  - Prometheus
  - Grafana
  - Alert Manager

- openshift-logging
  - Elasticsearch-mixin artifacts

- openshift-operators
  - openshift-monitoring Namespace
WHAT THE FUTURE HOLDS
Cluster Logging Operator and Elasticsearch Operator are opening new horizons

Operator pattern makes deployment and maintenance of complex components simpler

- Where the logs are routed
- Diversified Elasticsearch Topologies
- Modify cluster based on OpenShift Platform Metrics
TIME FOR YOUR QUESTIONS!
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHat