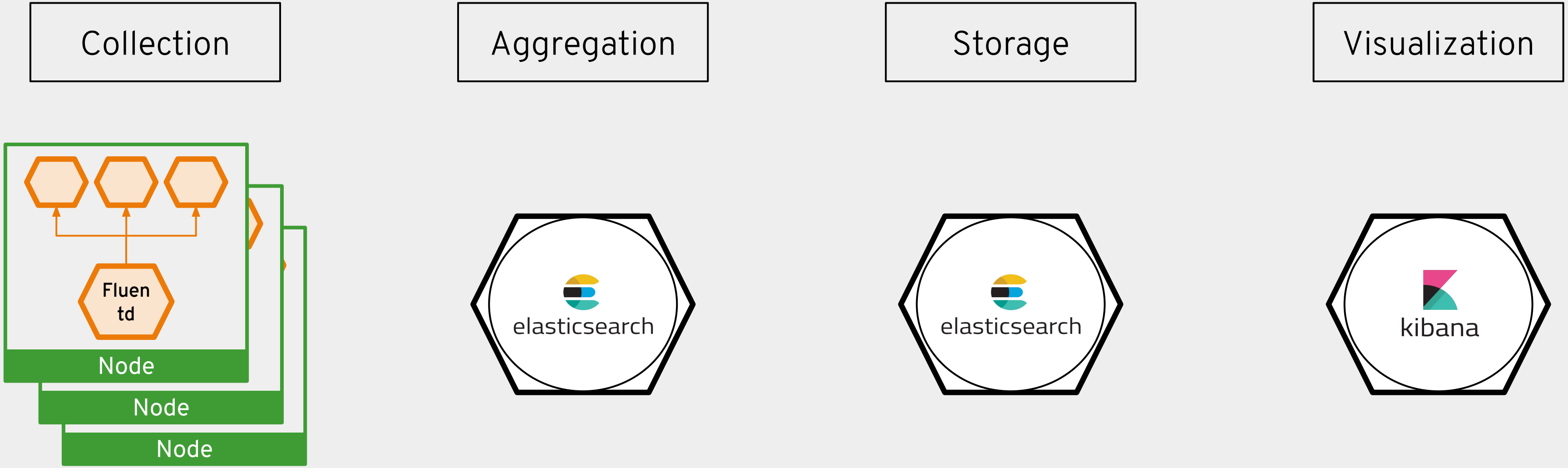
A deep dive on the OpenShift Logging-Stack

Gabriel Ferraz Stein
Technical Account Manager, OpenShift, Red Hat

Basic definitions

The Logging Stack



Collection

Aggregation

Storage

Visualization

Elasticsearch

- Object Store for Logs
- Receive logs from Fluentd
- Create Indices
- “Deliver” to Kibana
- Needs resources:
    - Plenty of RAM / CPU
    - Discs with good I/O

Fluentd

- Gather logs from nodes and send to Elasticsearch

Kibana

- Web UI for Elasticsearch

Deployment considerations

Considerations

- Plan first, deploy after
- Basic calculation
- Fluentd Configuration
- Elasticsearch, 3 nodes
- ES Storage: 50% and below 70%

More Considerations

- Docker: Use json-file as Log-Driver
- Replicas(1 | 3)
- MERGE_JSON_LOG = False

Performance improvement

Performance

- Don’t use NFS
- Fast disks are a must
- I/O really matters
- Enough RAM
- Use curator / delete indices NN days(7 days is the recommended)
- Shards and Replicas

Common errors and how to fix them

Common errors and fixes

- Fluentd stopped working / does not send logs to Elasticsearch (not enough resources)

- Error: “Exit Code 60” on some files from logging-dump (not enough resources)

- https://access.redhat.com/articles/3136551

What should I expect on OpenShift Container Platform 4

OpenShift Container Platform 4

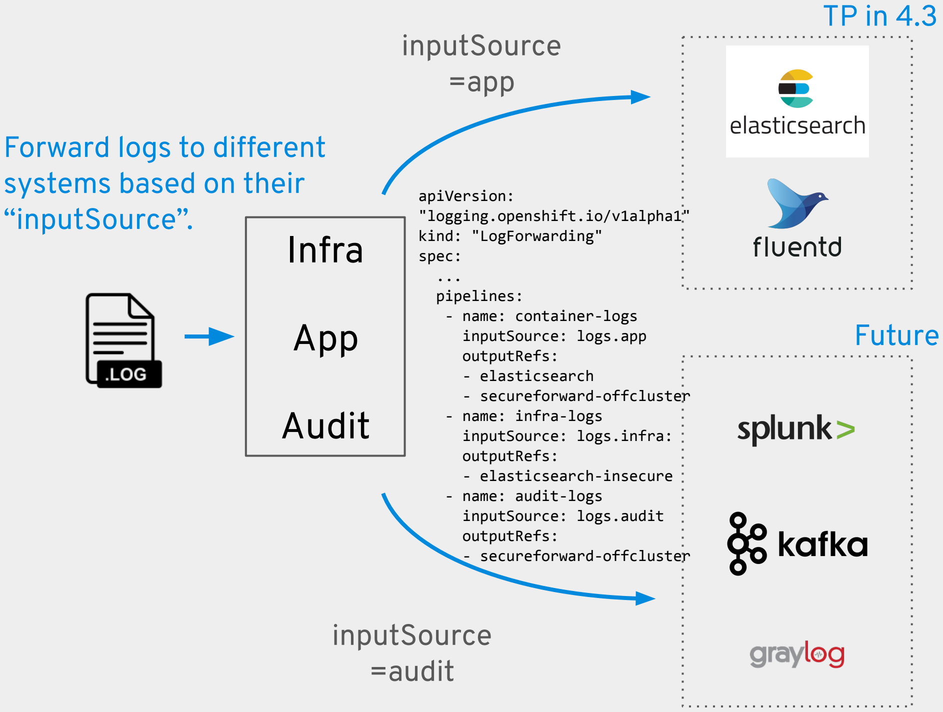
New ability to configure forwarding logs to various remote logging systems.

Goals:

- Configure forwarding logs based on the "class" of a log.
- Only support specific systems such as Splunk, Graylog, Kafka, etc.
- Allow deployment of OpenShift Logging without deploying the entirety infrastructure (e.g. Kibana, Elasticsearch)
- Support TLS between the collector and destination if so configured.

- **Tech Preview in 4.3**

GA in 4.5



```
apiVersion:
"logging.openshift.io/v1alpha1"
kind: "LogForwarding"
spec:
  ...
  pipelines:
   - name: container-logs
     inputSource: logs.app
     outputRefs:
     - elasticsearch
     - secureforward-offcluster
   - name: infra-logs
     inputSource: logs.infra:
     outputRefs:
     - elasticsearch-insecure
   - name: audit-logs
     inputSource: logs.audit
     outputRefs:
     - secureforward-offcluster
```

OpenShift Container Platform 4

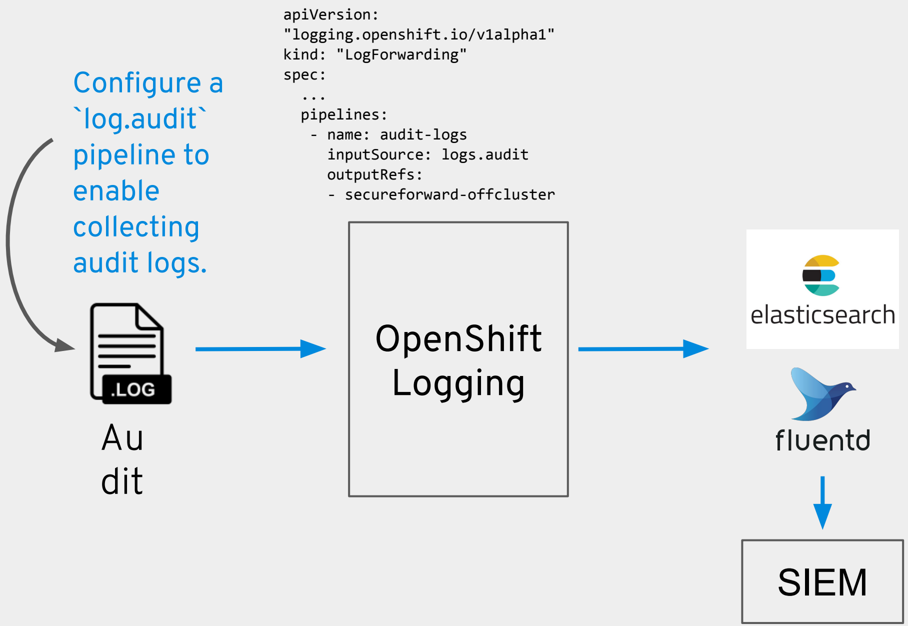
Collect and forward audit logs to external systems.

- Configure `logs.audit` pipeline to enable a new ability to collect audit logs and to setup and external system you’d like to forward them.
- Either use your own Elasticsearch or your own fluentd via secure-forward as in previous OCP releases; where you can send them to any SIEM system.

Tech Preview in 4.3

GA in 4.5

.



```
apiVersion:
"logging.openshift.io/v1alpha1"
kind: "LogForwarding"
spec:
  ...
  pipelines:
   - name: audit-logs
     inputSource: logs.audit
     outputRefs:
     - secureforward-offcluster
```

Configure a `log.audit` pipeline to enable collecting audit logs.

OpenShift Container Platform 4

Provide a more recent Elasticsearch version with several scalability improvements.

- Major upgrade from Elasticsearch & Kibana from 5 to 6.
- Moving from SearchGuard to OpenDistro for more open-source choices around Elasticsearch plugins.
- New data model for improved scalability.
- Clear separation between Cluster Logging Operator (collection & forwarding) and Elasticsearch (Elasticsearch & Kibana).

Planned for 4.5

.

Creating and troubleshooting a logging-dump

Logging Dump

- Use a script to run a openshift-logging project dump, which takes all details from the project including status and pods

Logging Dump

```
$ wget https://raw.githubusercontent.com/openshift/origin-aggregated-logging/release-<version>/hack/logging-dump.sh
$ chmod +x logging-dump.sh
$ oc login -u admin -p <password> https://openshift.example.com:8443
$ ./logging-dump.sh
```

Logging Dump

- File: logging-<date>

Directory	Description
curator	Exported details from the Pod running and logs
fluentd	Exported details from the pods running and logs
es	Exported details from the pods running and logs
kibana	Exported details from the Pod running and logs
project	Exported details from all resources from openshift-logging project

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

in linkedin.com/company/red-hat	f facebook.com/redhatinc
youtube.com/user/RedHatVideos	twitter.com/RedHat

Red Hat