Introduction

This document shows how typically log collection is carried out on Linux and how it may be configured to send logs to Logpoint SIEM. This document is provided “as is”. It is highly recommended to practice before trying these instructions in production!

Enabling Kubernetes Audit logs for a K8s Cluster

Audit logs are not enabled by default. An audit policy should be defined to decide which events are to be captured. To do this:

- Move to the directory **/etc/kubernetes/** and create a file named **audit.yaml**
- Define basic audit rules as follows:

```
apiVersion: audit.k8s.io/v1
kind: Policy
rules:
 - level: Metadata
```

The above rule would capture all log request metadata and write all the requests into a file as defined in the configuration.

The APIServer should be configured to use the previously created audit rules and export all the logs to the audit log path. Edit the manifest file of the kube-api-server, typically located at **/etc/kubernetes/manifests/kube-apiserver.yml** and add the following lines:

```
spec:
 containers:
  - command:
    - --audit-policy-file=/etc/kubernetes/audit.yaml
    - --audit-log-path=/var/log/audit/audit.log
    - --audit-log-maxage=5 # No of days we want to retain the logs
```

Since these files need to be accessed by the kube-apiserver pod, they need to be made available within the pod by mounting the hostPath to the location of the policy and log file. This makes the audit records persistent.

```
volumes:
  - name: audit
    hostPath:
    path: /etc/kubernetes/audit-policy.yaml
    type: File
  - name: audit-log
    hostPath:
    path: /var/log/audit/audit.log
    type: FileOrCreate
```

```
volumeMounts:
    - mountPath: /etc/kubernetes/audit-policy.yaml
      name: audit
      readOnly: true
    - mountPath: /var/log/audit/audit.log
      name: audit-log
      readOnly: false
```

In case the kube-apiserver doesn't come up online, it is also necessary to look at the pod logs held in **/var/log/pods/kube-system_kube-master_xxx/kube-apiserver/x.log** for any misconfiguration and errors.

A sample of a Kubernetes audit log is shown below:


```
{
 "kind": "Event",
 "apiVersion": "audit.k8s.io/v1",
 "level": "Metadata",
 "auditID": "c762ad6d-9994-4b03-8e6b-eee5e19d3d98",
 "stage": "ResponseComplete",
 "requestURI": "/api/v1/namespaces/default/pods/test",
 "verb": "get",
 "user": {
 "username": "kubernetes-admin",
 "groups": [
 "system:masters",
 "system:authenticated"
    ]
  },
 "sourceIPs": [
 "192.168.56.11"
  ],
 "userAgent": "kubectl/v1.26.0 (linux/amd64) kubernetes/b46a3f8",
 "objectRef": {
 "resource": "pods",
 "namespace": "default",
 "name": "test",
 "apiVersion": "v1"
  },
 "responseStatus": {
 "metadata": {},
 "code": 200
  },
 "requestReceivedTimestamp": "2023-03-29T15:33:20.131662Z",
 "stageTimestamp": "2023-03-29T15:33:20.133724Z",
 "annotations": {
 "authorization.k8s.io/decision": "allow",
 "authorization.k8s.io/reason": ""
  }
}
```

Forwarding Audit Logs to Logpoint

It is possible to leverage different formats to forward Kubernetes API Audit Logs to Logpoint. An rsylog sample is shown below:

Using rsyslog

Create a file named **00-k8s-audit.conf** in the **/etc/rsyslog.d/** directory and add the following configuration, where `LP-IP-ADDRESS:PORT` is the address and port of the Logpoint SIEM.

```
$ModLoad imfile
$InputFileName /var/log/kubernetes/audit.log
$InputFileTag kubernetes-audit
$InputFileStateFile state-kubernetes
$InputFileSeverity debug
$InputFileFacility local3
$InputRunFileMonitor
local3.* @@LP-IP-ADDRESS:PORT
```