title: Logagent input plugin for Kubernetes Audit logs description: Logagent features modular logging architecture framework where each input or output module is implemented as a plugin. Logagent can receive Kubernetes Audit logs via http.

Input Plugin: Kubernetes Audit Logs

Input plugin to receive Kubernetes Audit logs via HTTP.

Features:

- parse bulk messages

Applications:

- centralize Kubernetes Audit logs
- act as webhook to receive Kubernetes Audit logs
- index Kubernetes Audit logs in Elasticsearch or Sematext Cloud
- create alerts on Kubernetes Audit logs

Requirements:

- configure Kubernetes to send Audit logs via webhook

Configuration

```
# Receive Kubernetes Audit logs via HTTP server
input:
  kubernetesAudit:
    module: input-kubernetes-audit
    # server listens to a port
    port: 9091
    # dynamic index setting by posting Audit logs to /indexName/ URL
    useIndexFromUrlPath: true
    # number of extra processes to fork as web server workers
    worker: 0
    tags:
      receiver: logagent_kubernetes_audit

output:
  # view events on console during test setups
  stdout: yaml
  # ship Audit logs to Sematext Cloud
  elasticsearch:
    module: elasticsearch
    url: https://logsene-receiver.sematext.com
    index: YOUR_LOGS_TOKEN
```

Start Logagent

```
logagent --config kubernetes-audit.yml
```

Note: You can use the command line argument `--k8sAudit portNumber` to activate the plugin via the `logagent` command. The following command listens on TCP port 9091 for Kubernetes logs and dumps the logs in YAML format to the console.

```
logagent --k8sAudit 9091 --yaml
```