拉勾教育
—互联网人实战大学—

《Kubernetes 原理剖析与实战应用》

正范

— 拉勾教育出品 —

14｜日志采集：如何在 Kubernetes 中做日志收集与管理？

前言

日志中不仅记录了代码运行的实时轨迹

往往还包含着一些关键的数据、错误信息，等等

方便我们进行分析统计及监控告警

Kubernetes 中的日志收集 VS 传统日志收集

对于传统的应用来说，大都都是直接运行在宿主机上的

会将日志直接写入本地的文件中或者由 systemd-journald 直接管理

在做日志收集的时候，只需要访问这些日志所在的目录即可

Kubernetes 中的日志收集 VS 传统日志收集

- 系统各组件的日志

  比如 Kubernetes 自身各大组件的日志（包括 kubelet、kube-proxy 等），容器运行时的日志（比如 Docker）

- 以容器化方式运行的应用程序自身的日志

  比如 Nginx、Tomcat 的运行日志

- Kubernetes 内部各种 Event（事件）

  比如通过kubebctl create创建一个 Pod 后，可以通过kubectl describe pod pod-xxx命令查看到的这个 Pod 的 Event 信息

前言

Pod “用完即焚”，Pod 销毁后日志也会一同被删除

Kubernetes 的日志系统在设计时

必须得**独立于节点和 Pod 的生命周期**，且**保证日志数据可以实时采集到服务端**

前言

很多人在 Kubernetes 中喜欢使用 hostpath 来保存 Pod 的日志

并且不做**日志轮转**（可以配置 Docker 的log-opts来设置容器的日志轮转）

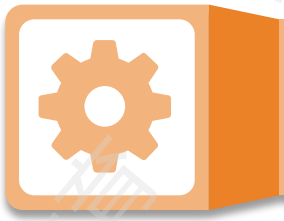
这很容易将宿主机的磁盘**“打爆”**

前言

配置了**日志轮转**，会让你丢失很多重要的上下文信息

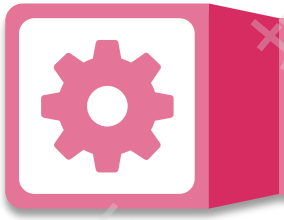
如果没有配置日志轮转，这些日志很快就会将磁盘打爆

几种常见的 Kubernetes 日志收集架构



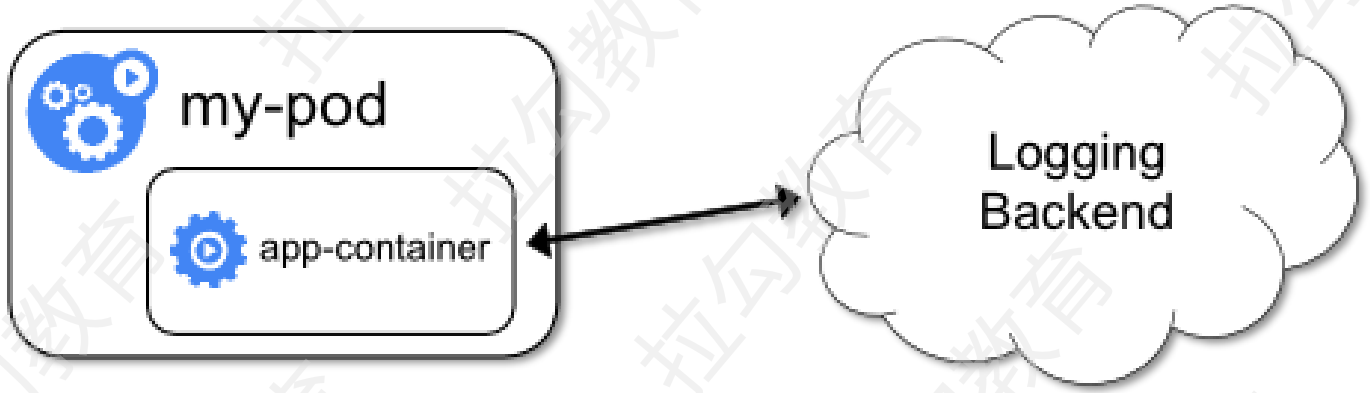
直接在应用程序中将日志信息推送到采集后端

在节点上运行一个 Agent 来采集节点级别的日志



在应用的 Pod 内使用一个 Sidecar 容器来收集应用日志

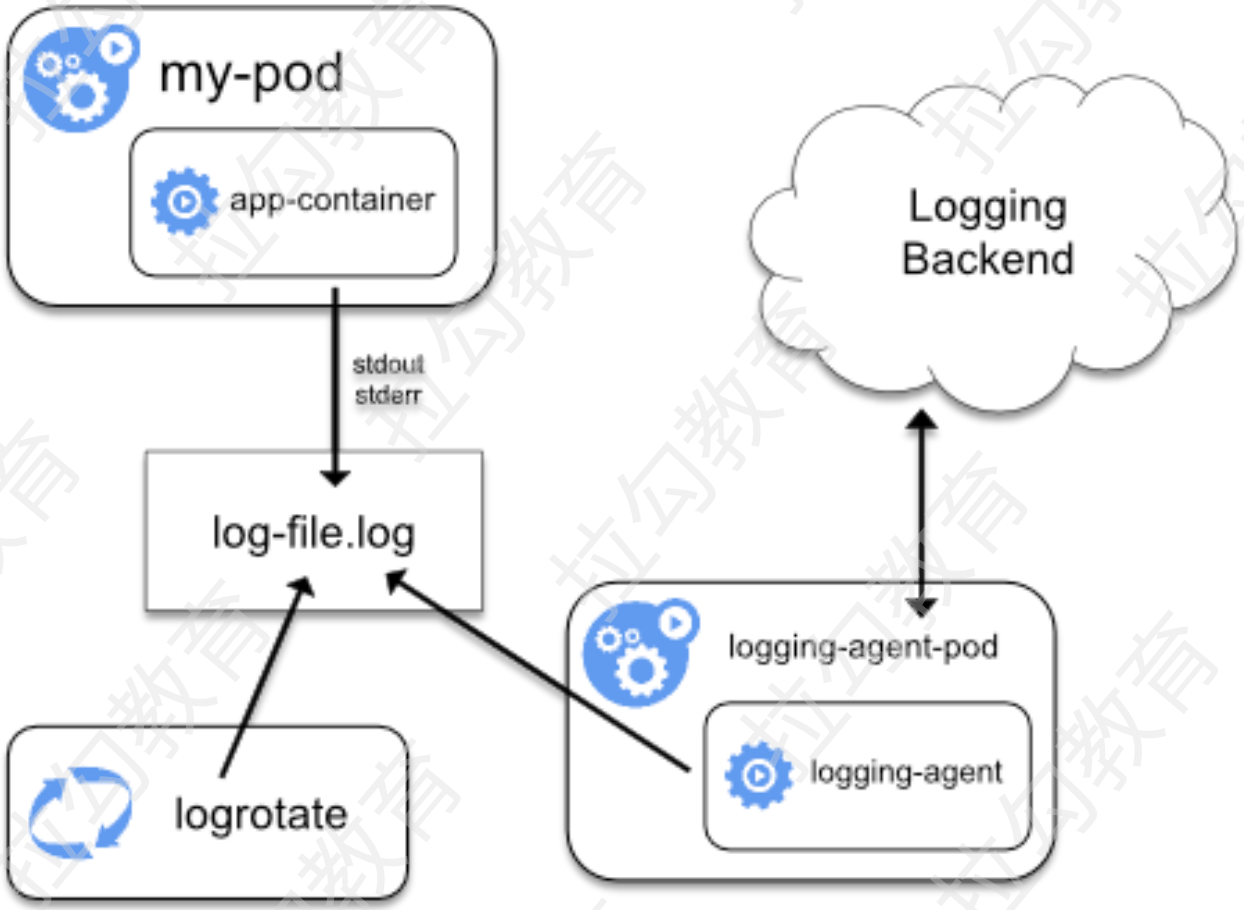
几种常见的 Kubernetes 日志收集架构



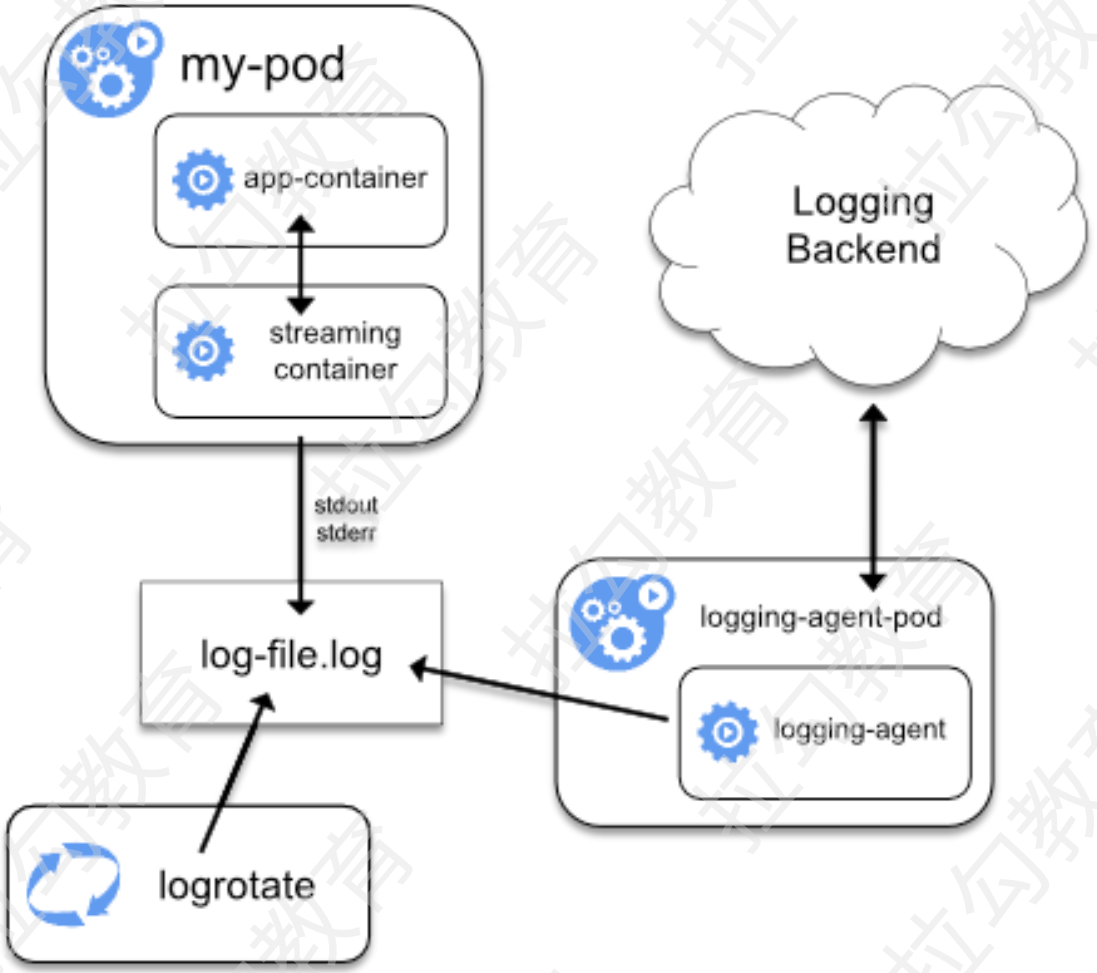
几种常见的 Kubernetes 日志收集架构


```
$ docker info |grep 'Logging Driver'
Logging Driver: json-file
```

几种常见的 Kubernetes 日志收集架构

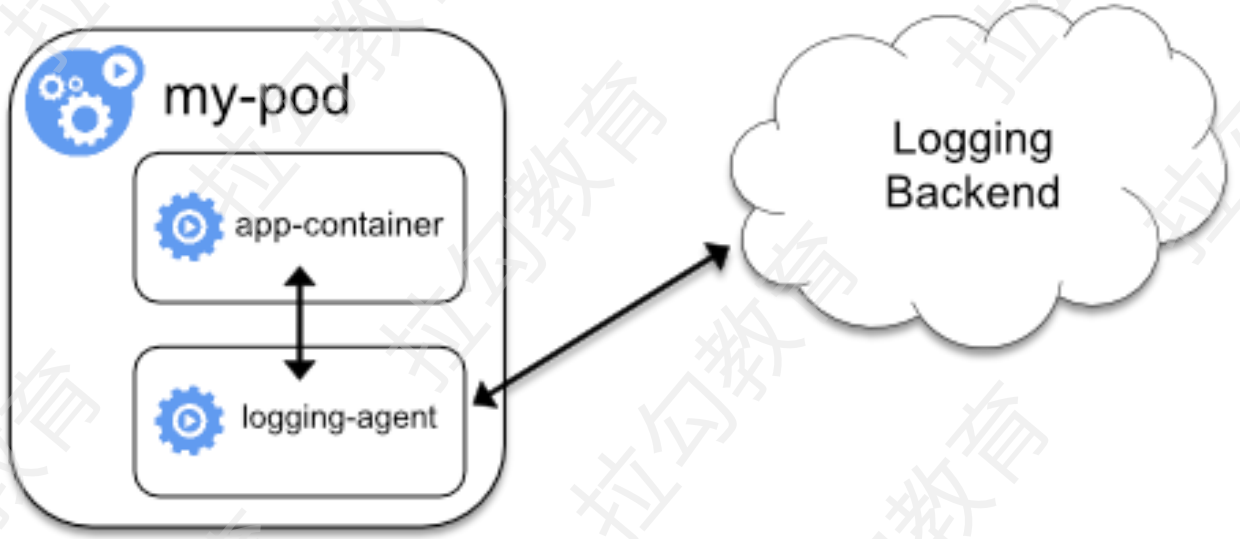


几种常见的 Kubernetes 日志收集架构



https://github.com/kubernetes/website/blob/master/content/en/examples/admin/logging/two-files-counter-pod-streaming-sidecar.yaml

几种常见的 Kubernetes 日志收集架构

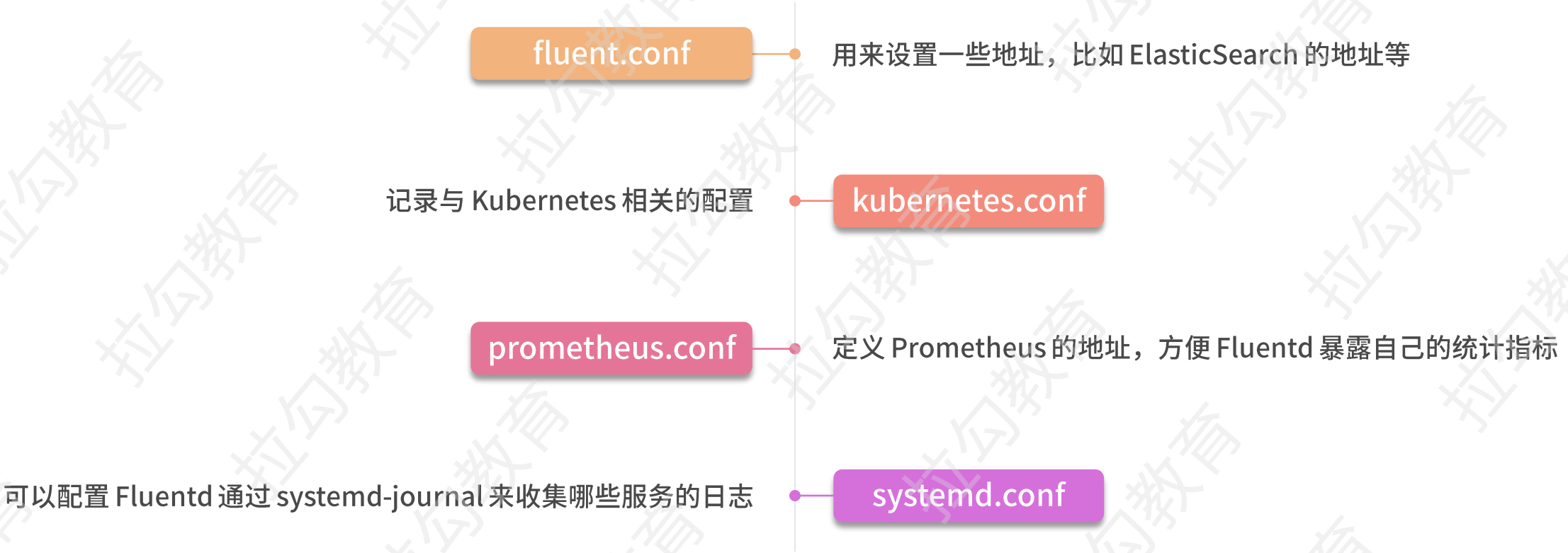


https://github.com/kubernetes/website/blob/master/content/en/examples/admin/logging/two-files-counter-pod-agent-sidecar.yaml

基于 Fluentd + ElasticSearch 的日志收集方案

使用 Fluentd+ElasticSearch+Kibana 进行日志的收集和管理

基于 Fluentd + ElasticSearch 的日志收集方案



基于 Fluentd + ElasticSearch 的日志收集方案

以上都默认内置到 **fluent/fluentd-kubernetes-daemonset** 的镜像中

默认示例配置

https://github.com/fluent/fluentd-kubernetes-daemonset/tree/master/docker-image/v1.11/debian-elasticsearch7/conf

基于 Fluentd + ElasticSearch 的日志收集方案


```yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
 name: fluentd
 namespace: kube-system
 labels:
  k8s-app: fluentd-logging
  version: v1
 spec:
  selector:
   matchLabels:
    k8s-app: fluentd-logging
    version: v1
  template:
   metadata:
    labels:
     k8s-app: fluentd-logging
     version: v1
   spec:
    tolerations:
```

基于 Fluentd + ElasticSearch 的日志收集方案


```
spec:
 tolerations:
 - key: node-role.kubernetes.io/master
   effect: NoSchedule
 containers:
 - name: fluentd
   image: fluent/fluentd-kubernetes-daemonset:v1-debian-elasticsearch
   env:
    - name:  FLUENT_ELASTICSEARCH_HOST
      value: "elasticsearch-logging"
    - name: FLUENT_ELASTICSEARCH_PORT
      value: "9200"
    - name: FLUENT_ELASTICSEARCH_SCHEME
      value: "http"
    # Option to configure elasticsearch plugin with self signed certs
    # ================================================================
    - name: FLUENT_ELASTICSEARCH_SSL_VERIFY
      value: "true"
    # Option to configure elasticsearch plugin with tls
    # ================================================================
```

基于 Fluentd + ElasticSearch 的日志收集方案


```
    # ================================================================
    - name: FLUENT_ELASTICSEARCH_SSL_VERSION
      value: "TLSv1_2"
    # X-Pack Authentication
    # =====================
    - name: FLUENT_ELASTICSEARCH_USER
      value: "elastic"
    - name: FLUENT_ELASTICSEARCH_PASSWORD
      value: "changeme"
    # Logz.io Authentication
    # ======================
    - name: LOGZIO_TOKEN
      value: "ThisIsASuperLongToken"
    - name: LOGZIO_LOGTYPE
      value: "kubernetes"
  resources:
    limits:
      memory: 200Mi
    requests:
      cpu: 100m
```

基于 Fluentd + ElasticSearch 的日志收集方案


```
  resources:
    limits:
      memory: 200Mi
    requests:
      cpu: 100m
      memory: 200Mi
  volumeMounts:
    - name: varlog
      mountPath: /var/log
    - name: varlibdockercontainers
      mountPath: /var/lib/docker/containers
      readOnly: true
terminationGracePeriodSeconds: 30
volumes:
- name: varlog
  hostPath:
    path: /var/log
- name: varlibdockercontainers
  hostPath:
    path: /var/lib/docker/containers
```

Next：《15 | Prometheus：Kubernetes 怎样实现自动化服务监控告警？》

拉勾教育

—互联网人实战大学—

关注拉勾「教育公众号」
获取更多课程信息

L / A / G / O / U