

第 3 节

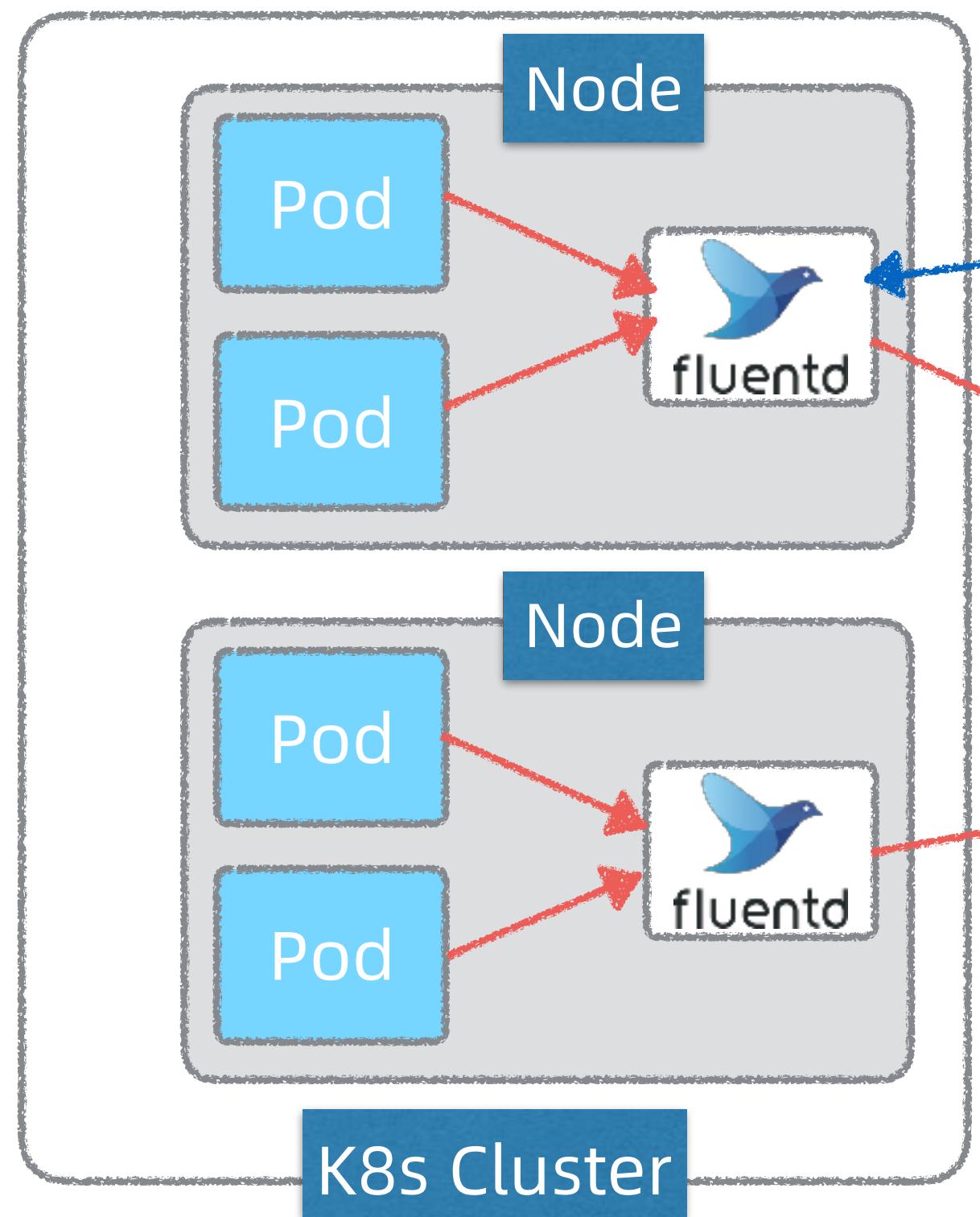
EFK日志监控平台搭建

本课内容

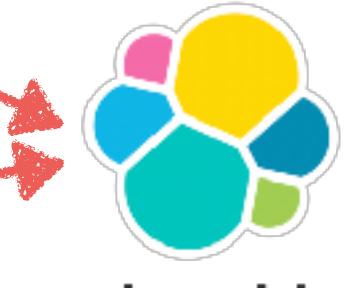
- EFK日志监控平台部署架构
- 演示本地搭建K8s EFK日志监控平台



EFK部署架构



kubernetes



elastic

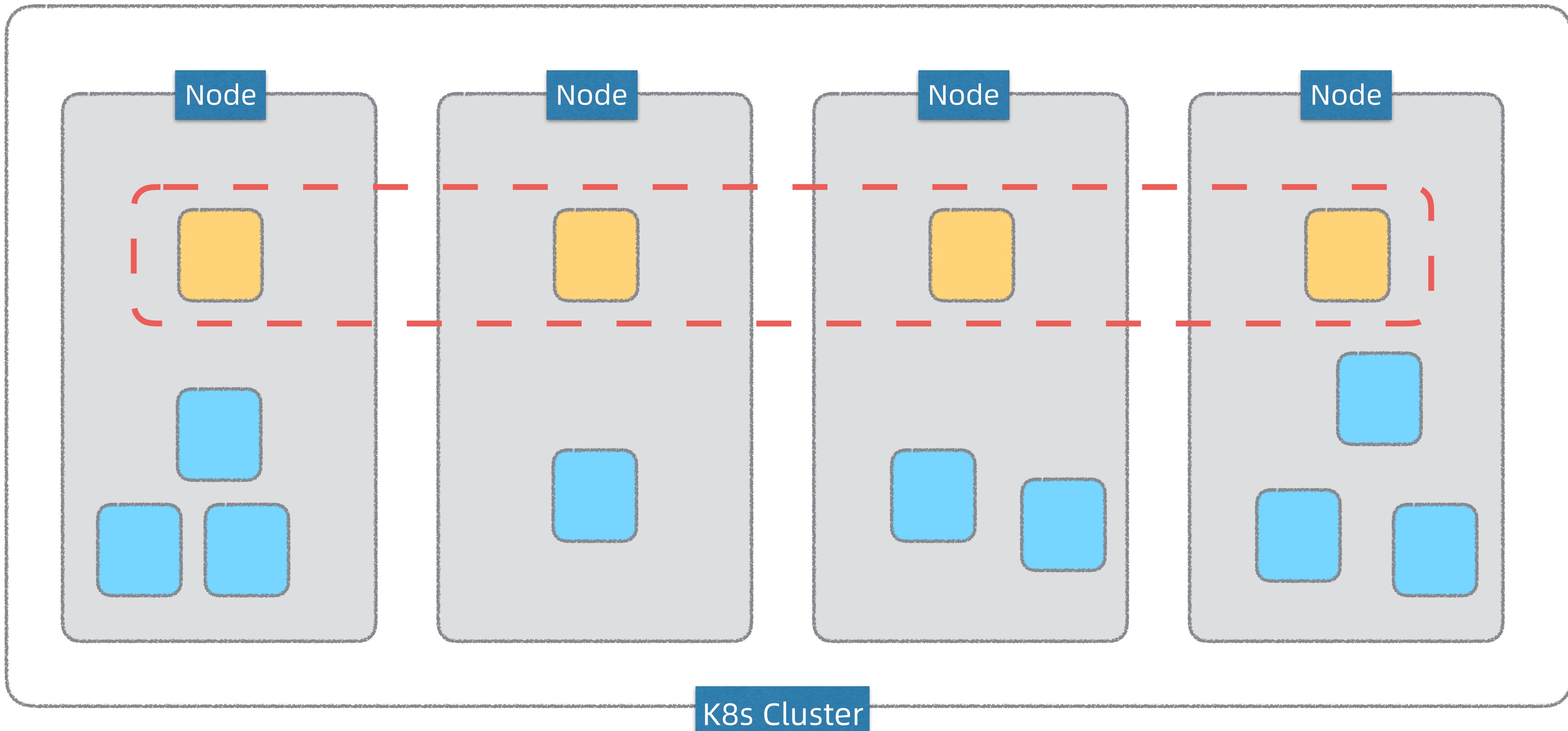
The screenshot shows the Kibana interface with the following details:

- Discover View:** Histogram showing event counts over time.
- Log View:** Log search results for May 13th, 2016, from 08:47:52 to 08:50:00. The logs include entries related to Fluentd configuration and Elasticsearch registration.
- Left Panel:** Includes sections for Discover, Visualize, Dashboards, Firewall, Dev Tools, and Management. A sidebar lists fields such as @version, @source, @type, _id, _index, _score, _type, and _version.



```
1 kind: ConfigMap
2 apiVersion: v1
3 metadata:
4   name: fluentd-es-config-v0.2.0
5   namespace: kube-system
6   labels:
7     addonmanager.kubernetes.io/mode: Recconcile
8 data:
9   system.conf: |-
10     <system>
11       root_dir /tmp/Fluentd-buffers/
12     </system>
13
14   containers.input.conf: |-
15     # This configuration file for Fluentd / td-agent is used
16     # to watch changes to Docker log files. The kubelet creates symlinks that
17     # capture the pod name, namespaces, container name & Docker container ID
18     # to the docker logs for pods in the /var/log/containers directory on the host.
19     # If running this fluentd configuration in a Docker container, the /var/log
20     # directory should be mounted in the container.
21     #
```

DaemonSet



发布logging名字空间

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch08/02 (zsh)
→ 02 git:(master) ✘ minikube status
host: Running
kubelet: Running
apiserver: Running
kubeconfig: Configured
→ 02 git:(master) ✘ ls
elastic.yml          fluentd-daemonset.yml  fluentd-rbac.yml    kibana.yml      ns.yml
→ 02 git:(master) ✘ cat ns.yml
apiVersion: v1
kind: Namespace
metadata:
  name: logging
→ 02 git:(master) ✘ kubectl apply -f ns.yml
namespace/logging created
→ 02 git:(master) ✘ kubectl get ns
NAME        STATUS   AGE
default     Active   122m
kube-node-lease  Active   122m
kube-public    Active   122m
kube-system    Active   122m
kubernetes-dashboard  Active   122m
logging       Active   4s
→ 02 git:(master) ✘
```

发布 ElasticSearch

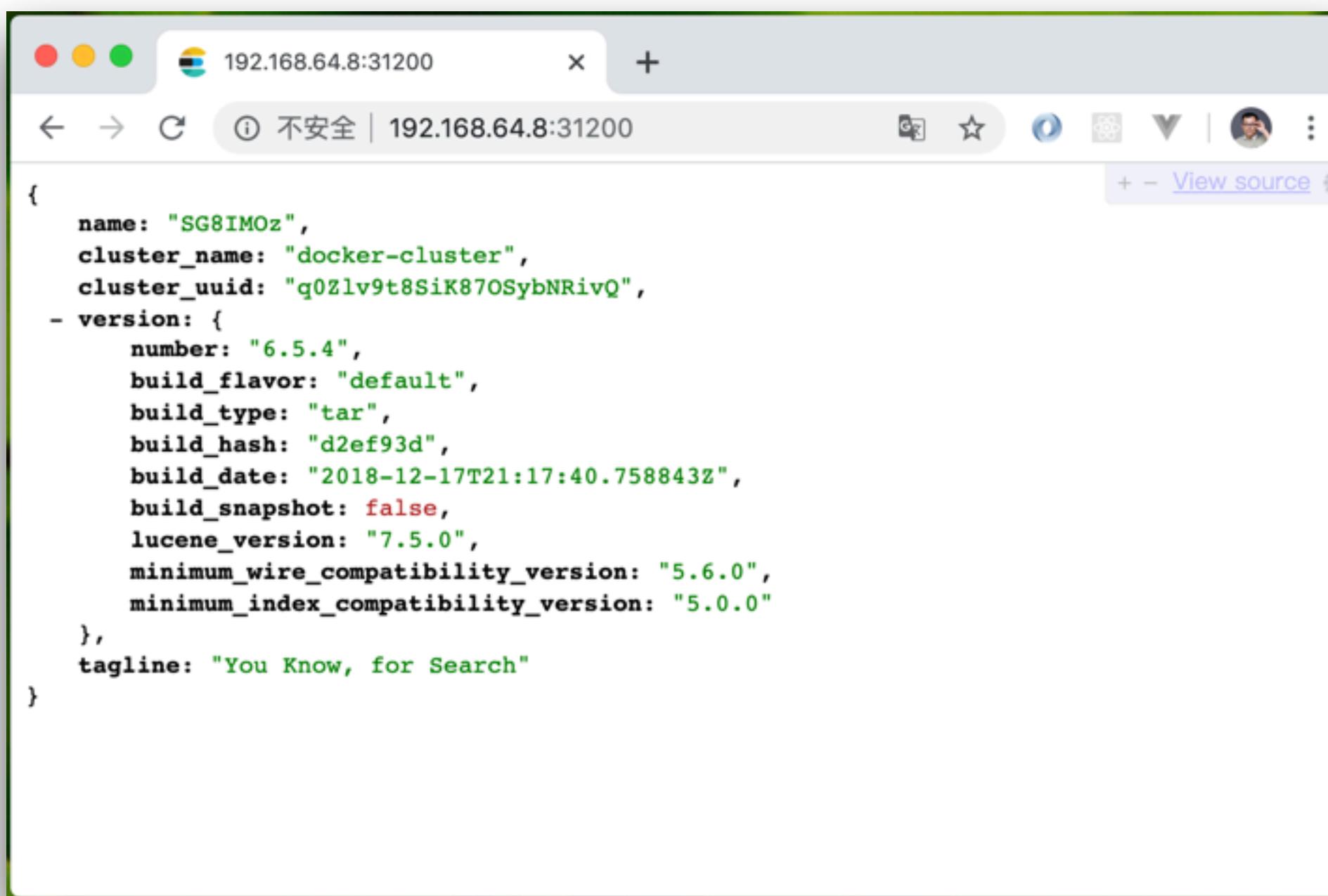
```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch08/02 (zsh)
  x ..ction/ch08/02 (zsh)  #1  x ..msa/k8s/local (z...  #2
→ 02 git:(master) x ls
elastic.yml          fluentd-rbac.yml      ns.yml
fluentd-daemonset.yml kibana.yml
→ 02 git:(master) x kubectl apply -f elastic.yml
deployment.apps/elasticsearch created
service/elasticsearch created
→ 02 git:(master) x kubectl get all -n logging
NAME                           READY   STATUS    RESTARTS   AGE
pod/elasticsearch-69d7479778-rvsh6  1/1     Running   0          5s

NAME                  TYPE       CLUSTER-IP      EXTERNAL-IP      PORT(S)        AGE
service/elasticsearch  NodePort  10.96.223.129 <none>           9200:31200/TCP  5s

NAME                           READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/elasticsearch  1/1     1           1          5s

NAME                           DESIRED  CURRENT  READY   AGE
replicaset.apps/elasticsearch-69d7479778  1        1        1      5s
→ 02 git:(master) x minikube service list
|-----|-----|-----|-----|
|     NAMESPACE     |     NAME      |     TARGET PORT    | URL |
|-----|-----|-----|-----|
| default          | kubernetes  | No node port    |
| kube-system      | kube-dns    | No node port    |
| kube-system      | metrics-server | No node port    |
| kubernetes-dashboard | dashboard-metrics-scraper | No node port    |
| kubernetes-dashboard | kubernetes-dashboard | No node port    |
| logging           | elasticsearch | http://192.168.64.8:31200 |
|-----|-----|-----|-----|
→ 02 git:(master) x
```

校验ElasticSearch



A screenshot of a web browser window titled "192.168.64.8:31200". The address bar shows the URL "192.168.64.8:31200". The page content displays the following JSON response:

```
{  
  "name": "SG8IM0z",  
  "cluster_name": "docker-cluster",  
  "cluster_uuid": "q0Zlv9t8SiK870SybNRivQ",  
  "version": {  
    "number": "6.5.4",  
    "build_flavor": "default",  
    "build_type": "tar",  
    "build_hash": "d2ef93d",  
    "build_date": "2018-12-17T21:17:40.758843Z",  
    "build_snapshot": false,  
    "lucene_version": "7.5.0",  
    "minimum_wire_compatibility_version": "5.6.0",  
    "minimum_index_compatibility_version": "5.0.0"  
  },  
  "tagline": "You Know, for Search"  
}
```

发布 Kibana

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch08/02 (zsh)
→ 02 git:(master) ✘ kubectl apply -f kibana.yml
deployment.apps/kibana created
service/kibana created
→ 02 git:(master) ✘ kubectl get all -n logging
NAME                               READY   STATUS    RESTARTS   AGE
pod/elasticsearch-69d7479778-rvsh6  1/1     Running   0          3m26s
pod/kibana-768c8fc454-8q6gx       1/1     Running   0          4s

NAME           TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE
service/elasticsearch  NodePort  10.96.223.129  <none>        9200:31200/TCP  3m26s
service/kibana    NodePort  10.96.120.208  <none>        5601:31601/TCP  4s

NAME           READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/elasticsearch  1/1     1           1           3m26s
deployment.apps/kibana        1/1     1           1           4s

NAME           DESIRED  CURRENT  READY   AGE
replicaset.apps/elasticsearch-69d7479778  1        1        1        3m26s
replicaset.apps/kibana-768c8fc454        1        1        1        4s
→ 02 git:(master) ✘ minikube service list
|-----|-----|-----|-----|
|   NAMESPACE   |     NAME     | TARGET PORT | URL |
|-----|-----|-----|-----|
| default      | kubernetes | No node port |      |
| kube-system  | kube-dns   | No node port |      |
| kube-system  | metrics-server | No node port |      |
| kubernetes-dashboard | dashboard-metrics-scraper | No node port |      |
| kubernetes-dashboard | kubernetes-dashboard | No node port |      |
| logging       | elasticsearch | http://192.168.64.8:31200 |      |
| logging       | kibana      | http://192.168.64.8:31601 |      |
|-----|-----|-----|-----|
→ 02 git:(master) ✘
```

校验Kibana

The screenshot shows the Kibana home page in a web browser. The URL in the address bar is `192.168.64.8:31601/app/kibana#/home?_g=()`. A modal dialog at the top asks for user consent to share usage statistics, with "Yes" and "No" buttons. The main content area is titled "Add Data to Kibana" and includes sections for APM, Logging, Metrics, and Security analytics, each with an "Add" button. Below these are three data loading options: "Add sample data", "Upload data from log file", and "Use Elasticsearch data". At the bottom, there are links for "Visualize and Explore Data" (with APM and Canvas sub-links), "Manage and Administer the Elastic Stack" (with Console and Index Patterns sub-links), and navigation buttons for "Default" and "Collapse".

② Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

Yes No

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
[Add APM](#)

Logging
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
[Add log data](#)

Metrics
Collect metrics from the operating system and services running on your servers.
[Add metric data](#)

Security analytics
Centralize security events for interactive investigation in ready-to-go visualizations.
[Add security events](#)

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

Manage and Administer the Elastic Stack

Default

Collapse

APM

Canvas

Console

Index Patterns

发布Fluentd

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch08/02 (zsh)
  ⌘ .action/ch08/02 [zsh]  861  ✘ ..msa/k8s/local (z...  ● 862
→ 02 git:(master) ✘ ls
elastic.yml          fluentd-rbac.yml      ns.yml
fluentd-daemonset.yml kibana.yml
→ 02 git:(master) ✘ kubectl apply -f fluentd-rbac.yml
serviceaccount/fluentd created
clusterrole.rbac.authorization.k8s.io/fluentd created
clusterrolebinding.rbac.authorization.k8s.io/fluentd created
→ 02 git:(master) ✘ kubectl apply -f fluentd-daemonset.yml
daemonset.apps/fluentd created
→ 02 git:(master) ✘ kubectl get all -n kube-system
NAME                           READY   STATUS    RESTARTS   AGE
pod/coredns-6955765f44-hfm96   1/1     Running   0          88m
pod/coredns-6955765f44-tdmfp   1/1     Running   0          88m
pod/etcd-minikube              1/1     Running   0          89m
pod/fluentd-l9px4              1/1     Running   0          10s
pod/kube-addon-manager-minikube 1/1     Running   0          89m
pod/kube-apiserver-minikube    1/1     Running   0          89m
pod/kube-controller-manager-minikube 1/1     Running   0          89m
pod/kube-proxy-h9zh8            1/1     Running   0          88m
pod/kube-scheduler-minikube    1/1     Running   0          89m
pod/metrics-server-55c978d97b-thrvh 1/1     Running   1          132m
pod/metrics-server-6754dbc9df-pqfgt 0/1     ImagePullBackOff 0          88m
pod/storage-provisioner         1/1     Running   2          132m

NAME           TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)        AGE
service/kube-dns  ClusterIP  10.96.0.10  <none>        53/UDP,53/TCP,9153/TCP  132m
service/metrics-server  ClusterIP  10.96.3.166 <none>        443/TCP       132m

NAME           DESIRED  CURRENT  READY  UP-TO-DATE  AVAILABLE  NODE SELECTOR          AGE
daemonset.apps/fluentd  1        1        1      1          1          <none>               10s
daemonset.apps/kube-proxy  1        1        1      1          1          beta.kubernetes.io/os=linux  132m
```

校验Fluentd启动日志

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch08/02 (zsh)
→ 02 git:(master) ✘ kubectl logs pod/fluentd-l9px4 -n kube-system
2020-01-20 09:42:20 +0000 [info]: parsing config file is succeeded path="/fluentd/etc/fluent.conf"
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-concat' version '2.4.0'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-detect-exceptions' version '0.0.13'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-elasticsearch' version '3.7.1'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-grok-parser' version '2.6.1'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-json-in-json-2' version '1.0.2'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-kubernetes_metadata_filter' version '2.3.0'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-multi-format-parser' version '1.0.0'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-prometheus' version '1.6.1'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-record-modifier' version '2.0.1'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-rewrite-tag-filter' version '2.2.0'
2020-01-20 09:42:20 +0000 [info]: gem 'fluent-plugin-systemd' version '1.0.2'
2020-01-20 09:42:20 +0000 [info]: gem 'fluentd' version '1.8.1'
2020-01-20 09:42:20 +0000 [warn]: define <match fluent.**> to capture fluentd logs in top level is deprecated. Use <label @FLUENT_LOG> instead
2020-01-20 09:42:20 +0000 [info]: using configuration file: <ROOT>
<source>
  @type prometheus
  bind "0.0.0.0"
  port 24231
  metrics_path "/metrics"
</source>
<source>
  @type prometheus_output_monitor
</source>
<match fluent.**>
  @type null
</match>
<source>
  @type tail
  @id in_tail_container_logs
</source>
```

本课小结



- EFK日志监控平台部署架构
 - ElasticSearch ~ 日志存储+索引+搜索
 - Fluentd ~ 日志采集/装饰/转换和传输
 - Kibana ~ 日志查询展示
 - 生产环境+Kafka
- 本地minikube环境搭建EFK
 - Fluentd DaemonSet
 - 也可以采用minikube efk addon, 更简单