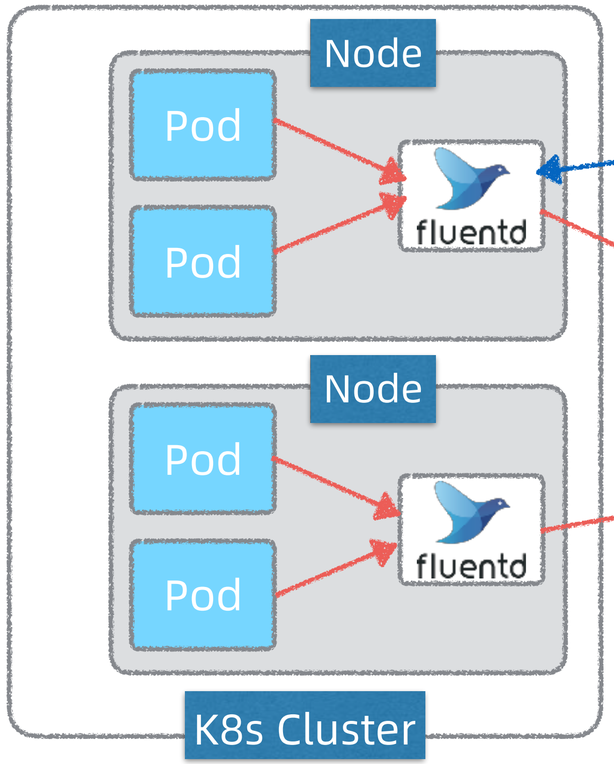
第 3 节

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

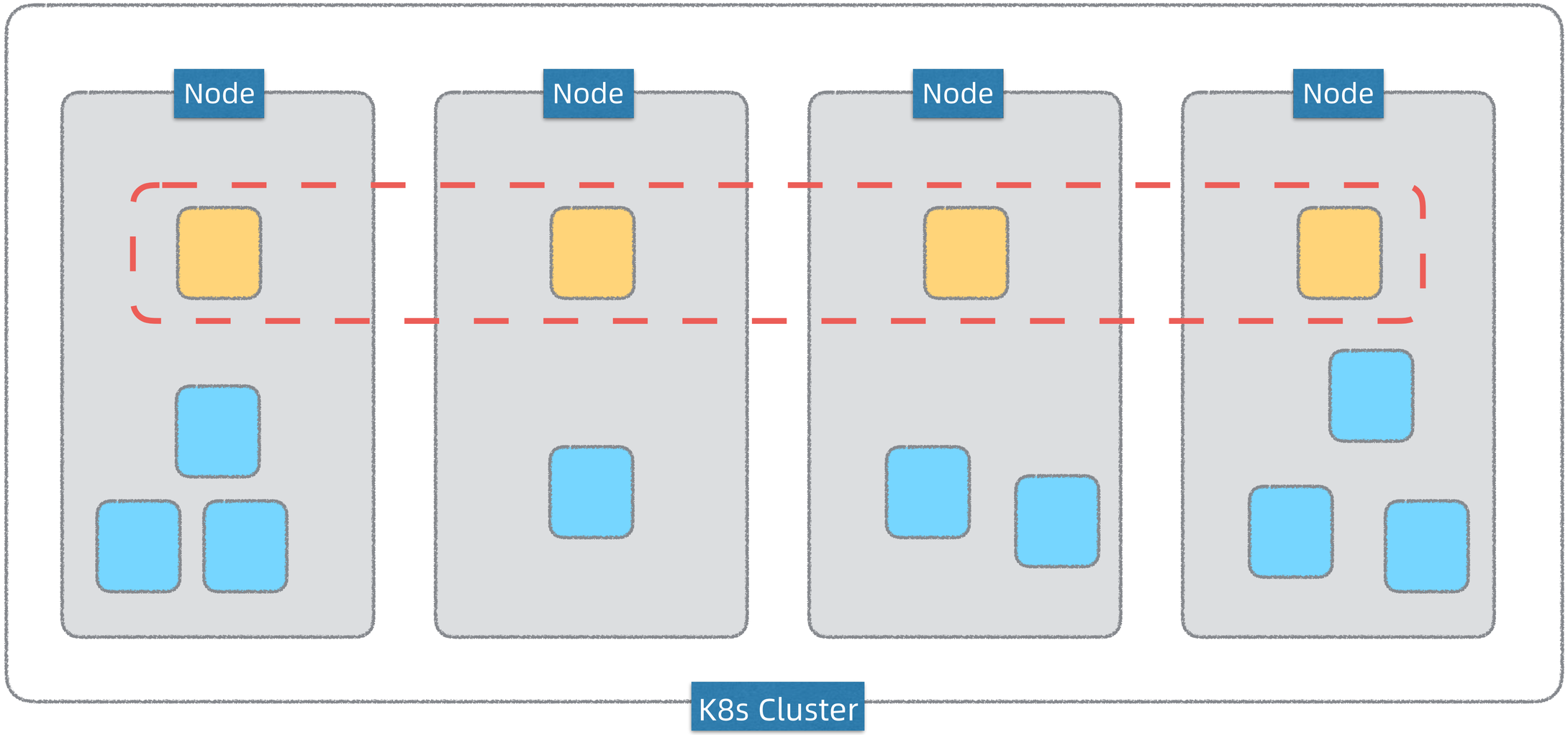
EFK部署架构



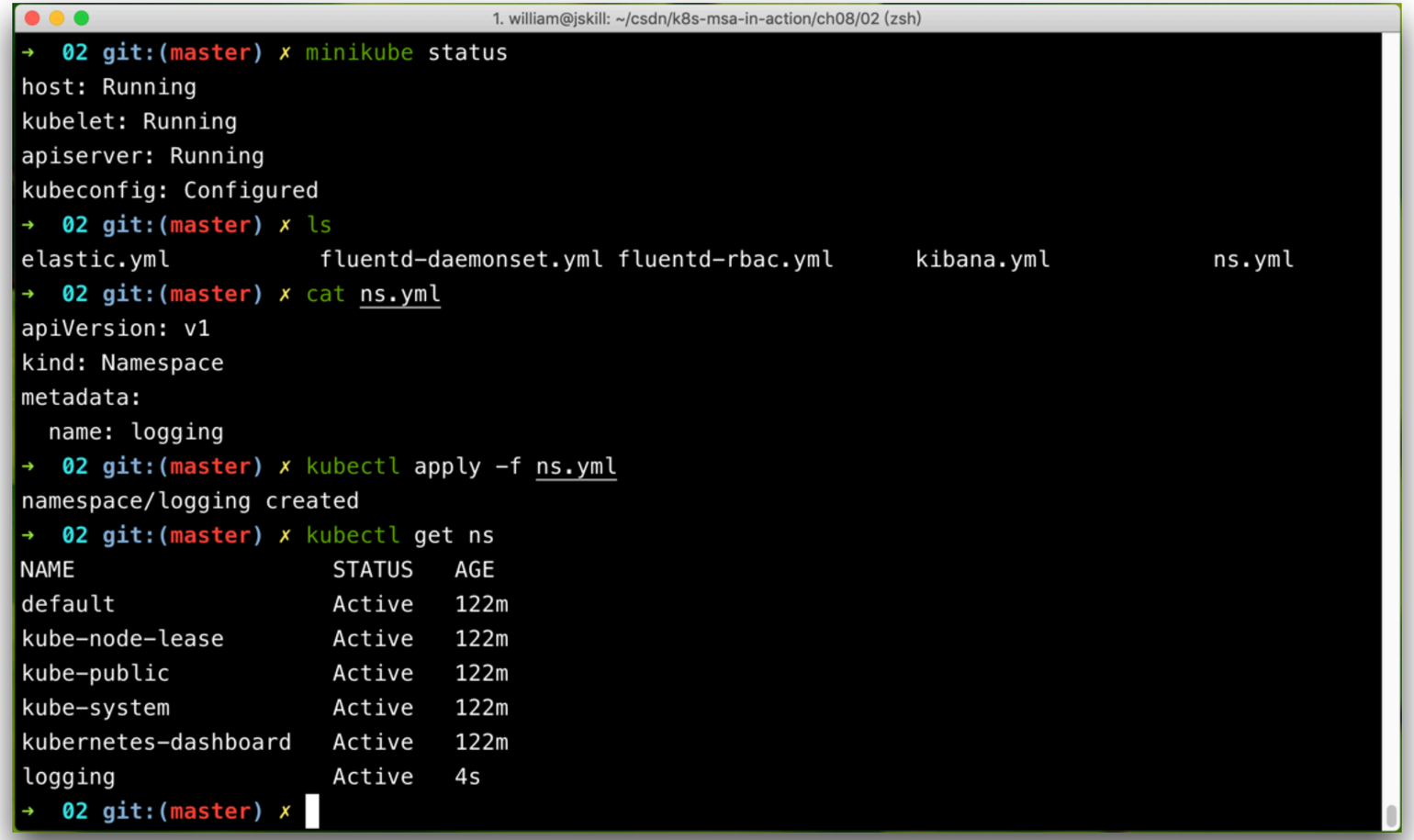

```yaml
kind: ConfigMap
apiVersion: v1
metadata:
  name: fluentd-es-config-v0.2.0
  namespace: kube-system
  labels:
    addonmanager.kubernetes.io/mode: Reconcile
data:
  system.conf: |-
    <system>
      root_dir /tmp/fluentd-buffers/
    </system>

  containers.input.conf: |-
    # This configuration file for Fluentd / td-agent is used
    # to watch changes to Docker log files. The kubelet creates symlinks that
    # capture the pod name, namespace, container name & Docker container ID
    # to the docker logs for pods in the /var/log/containers directory on the host.
    # If running this fluentd configuration in a Docker container, the /var/log
    # directory should be mounted in the container.
    #
```

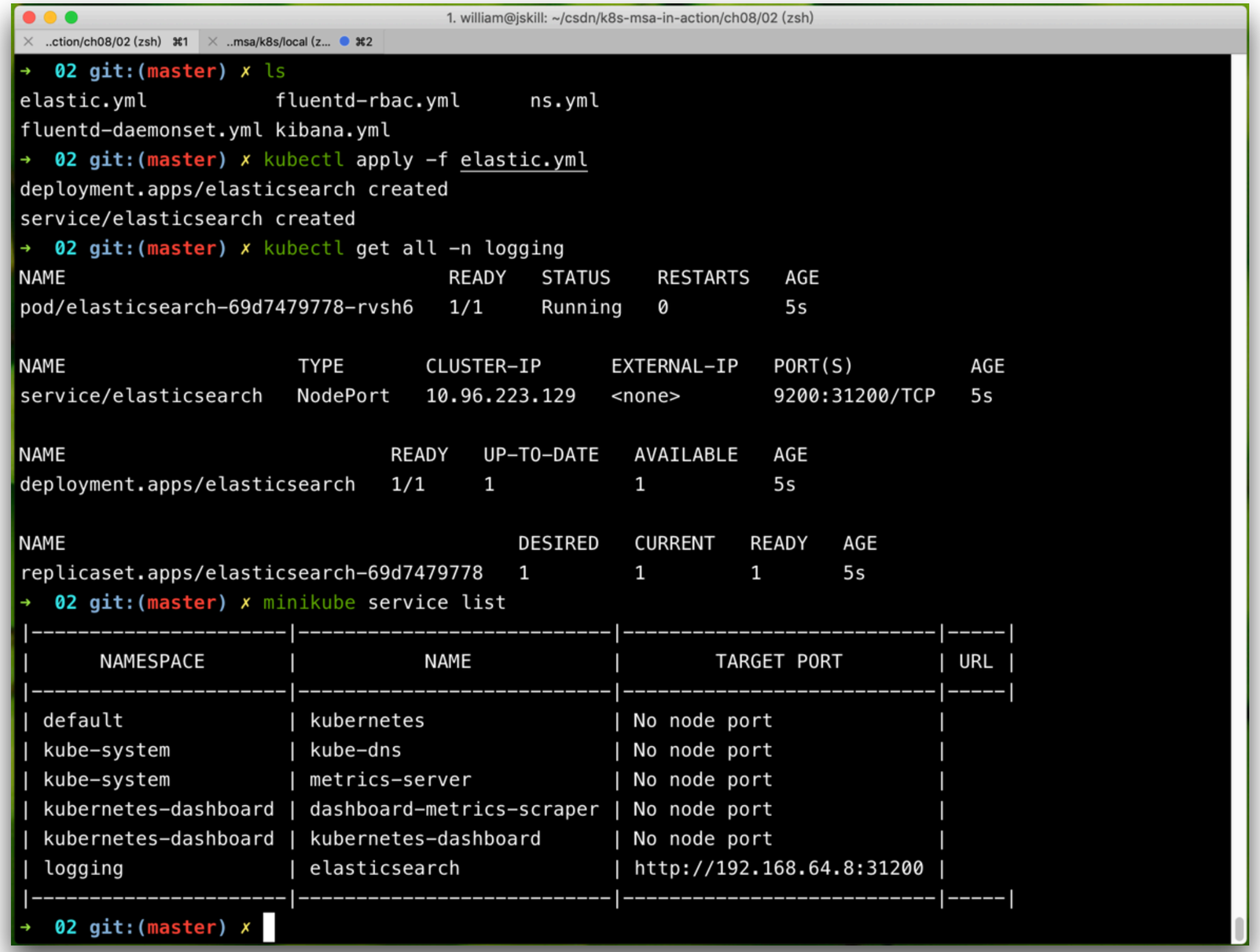
DaemonSet



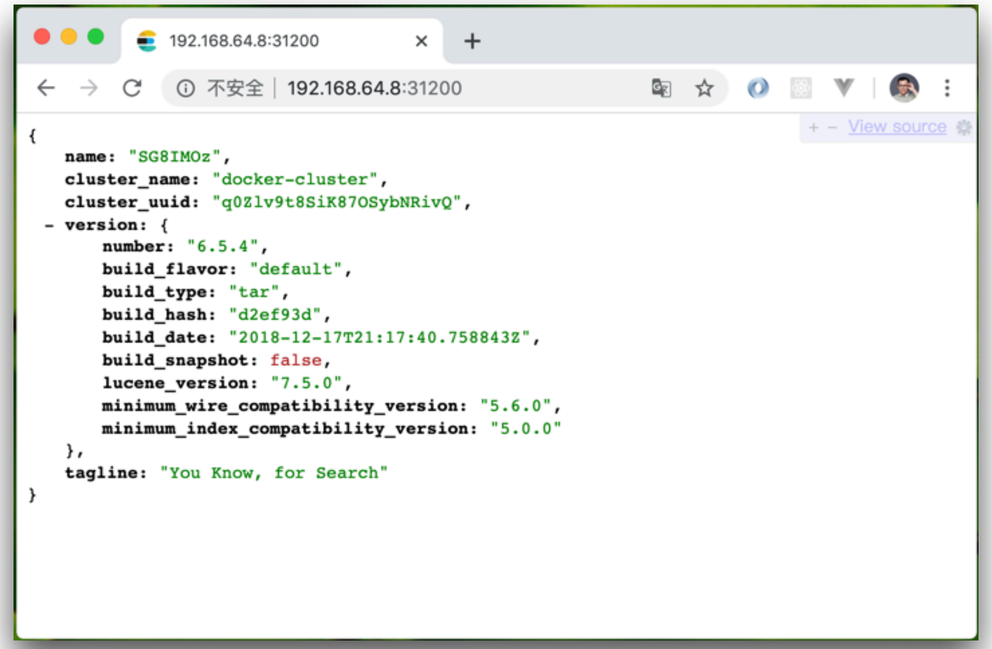
发布logging名字空间



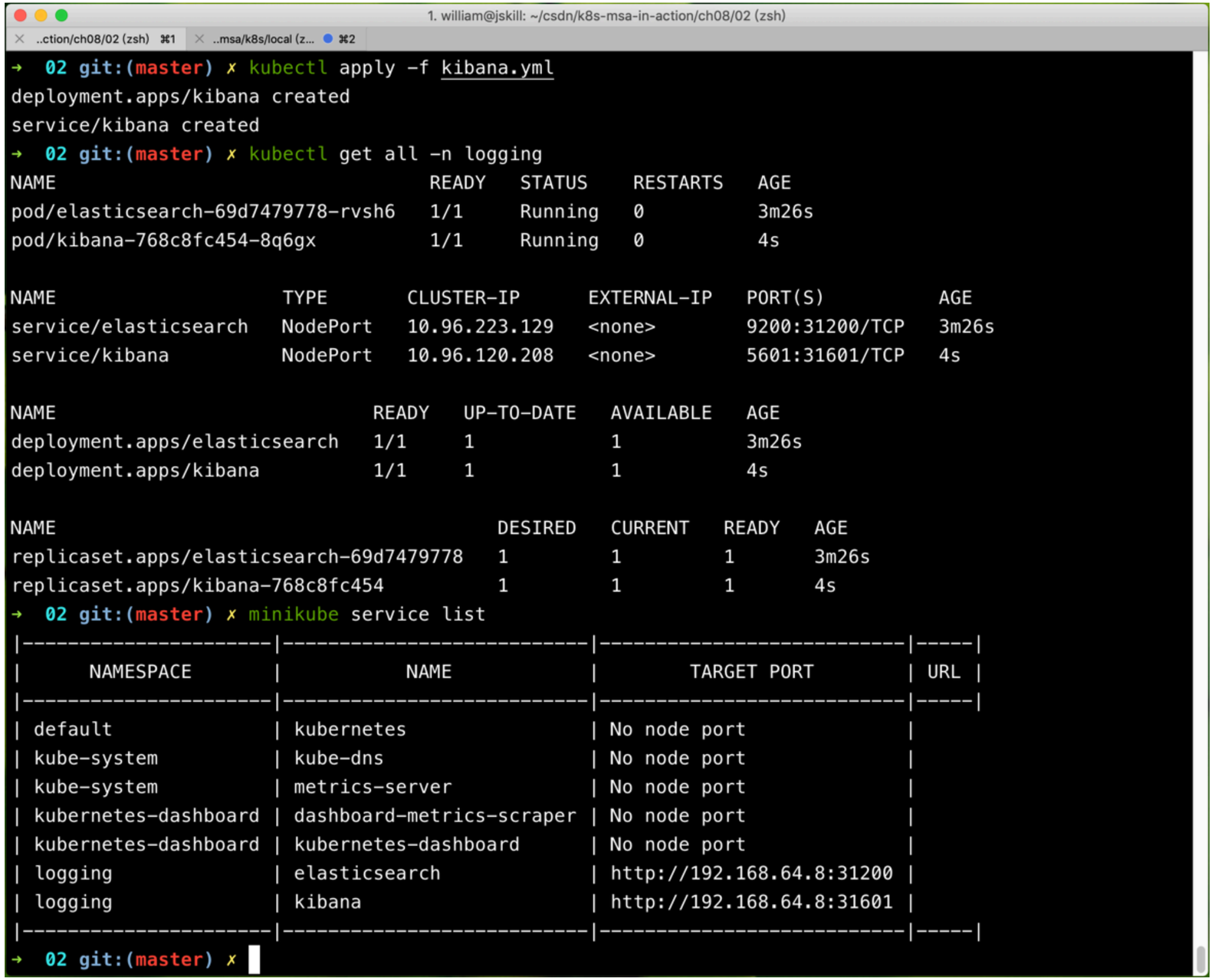
发布 ElasticSearch



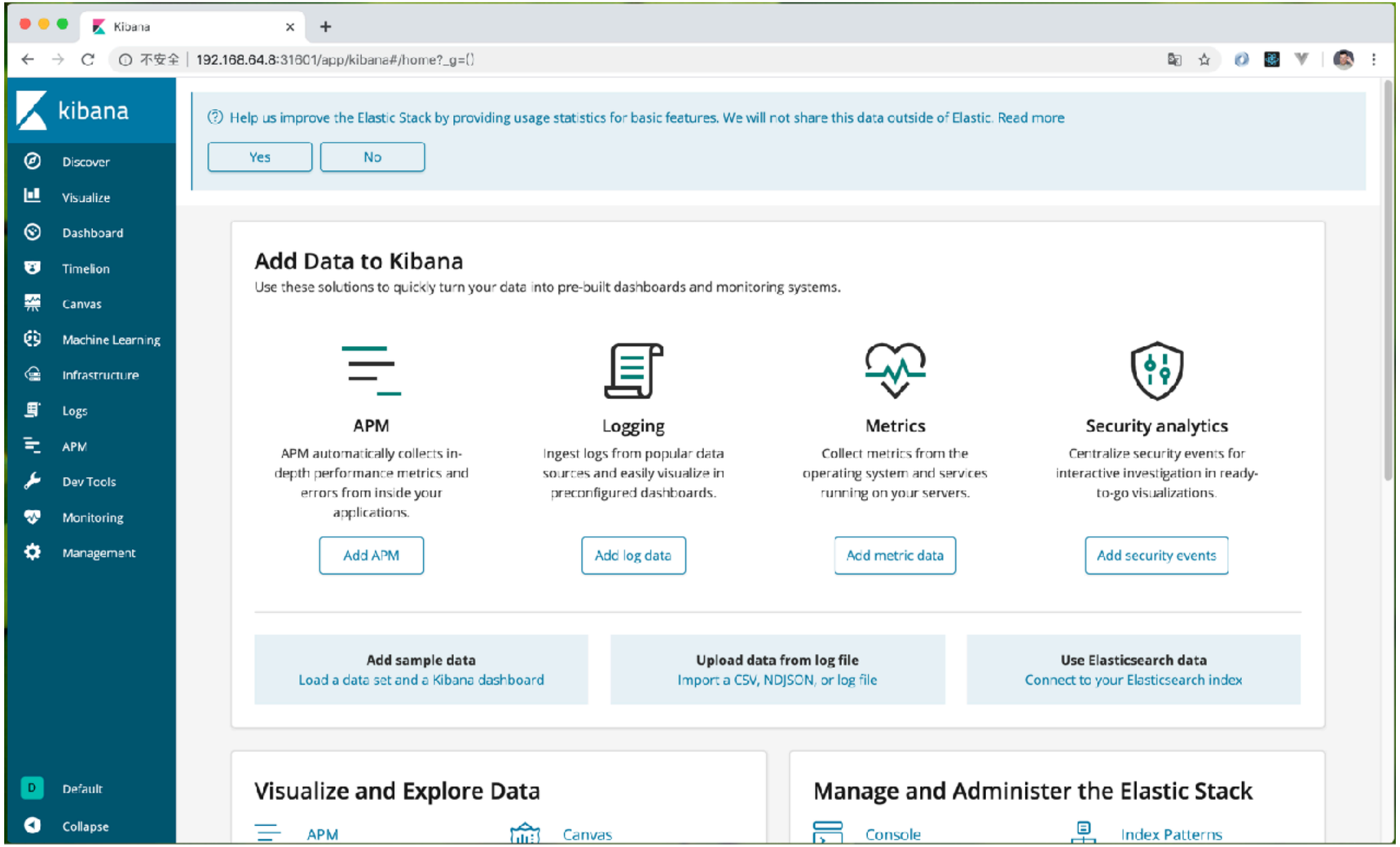
校验ElasticSearch



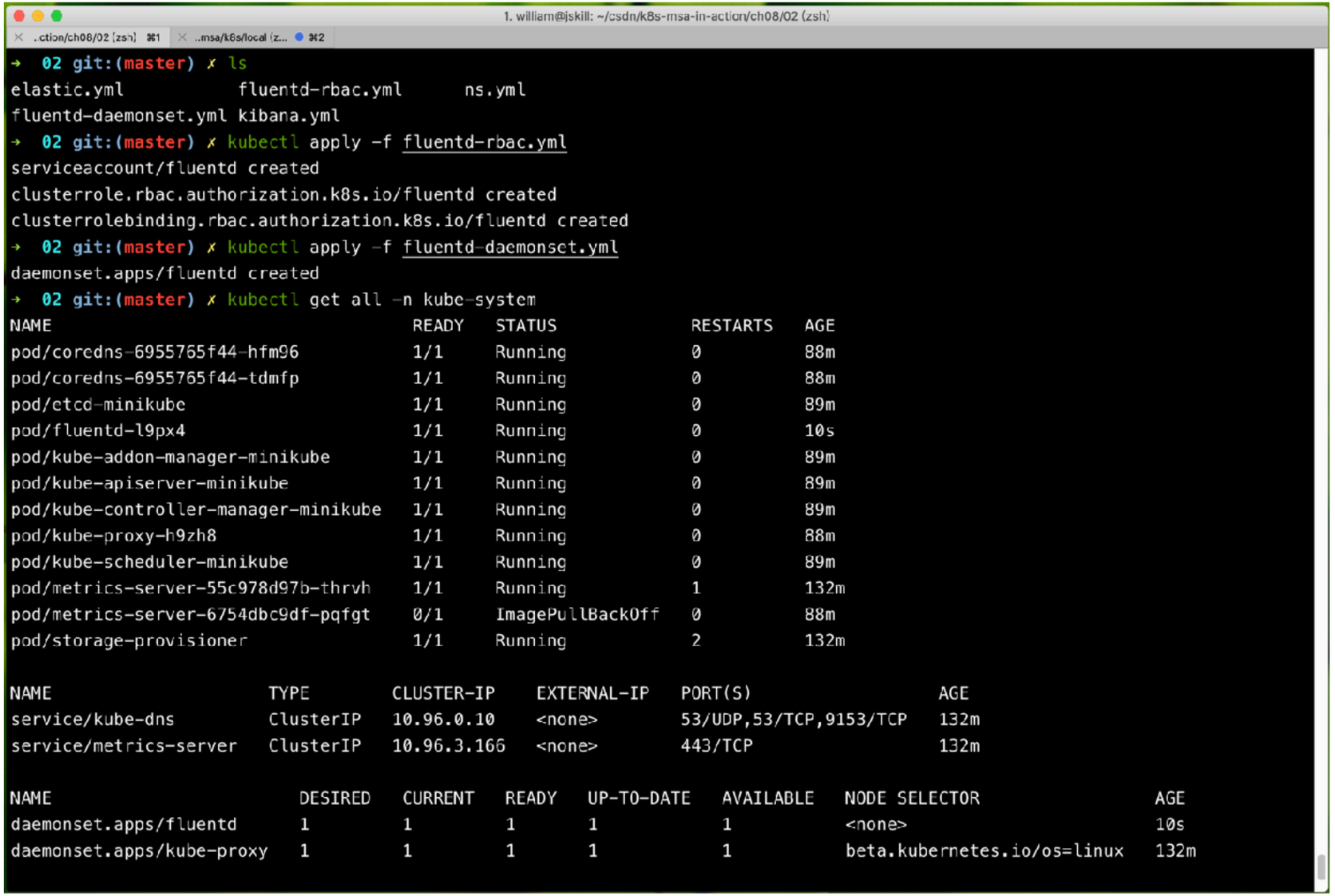
发布 Kibana


1. william@jskill: ~/csdn/k8s-msa-in-action/ch08/02 (zsh)
..ction/ch08/02 (zsh) ⌘1
..msa/k8s/local (z... ⌘2
→ 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) ✗

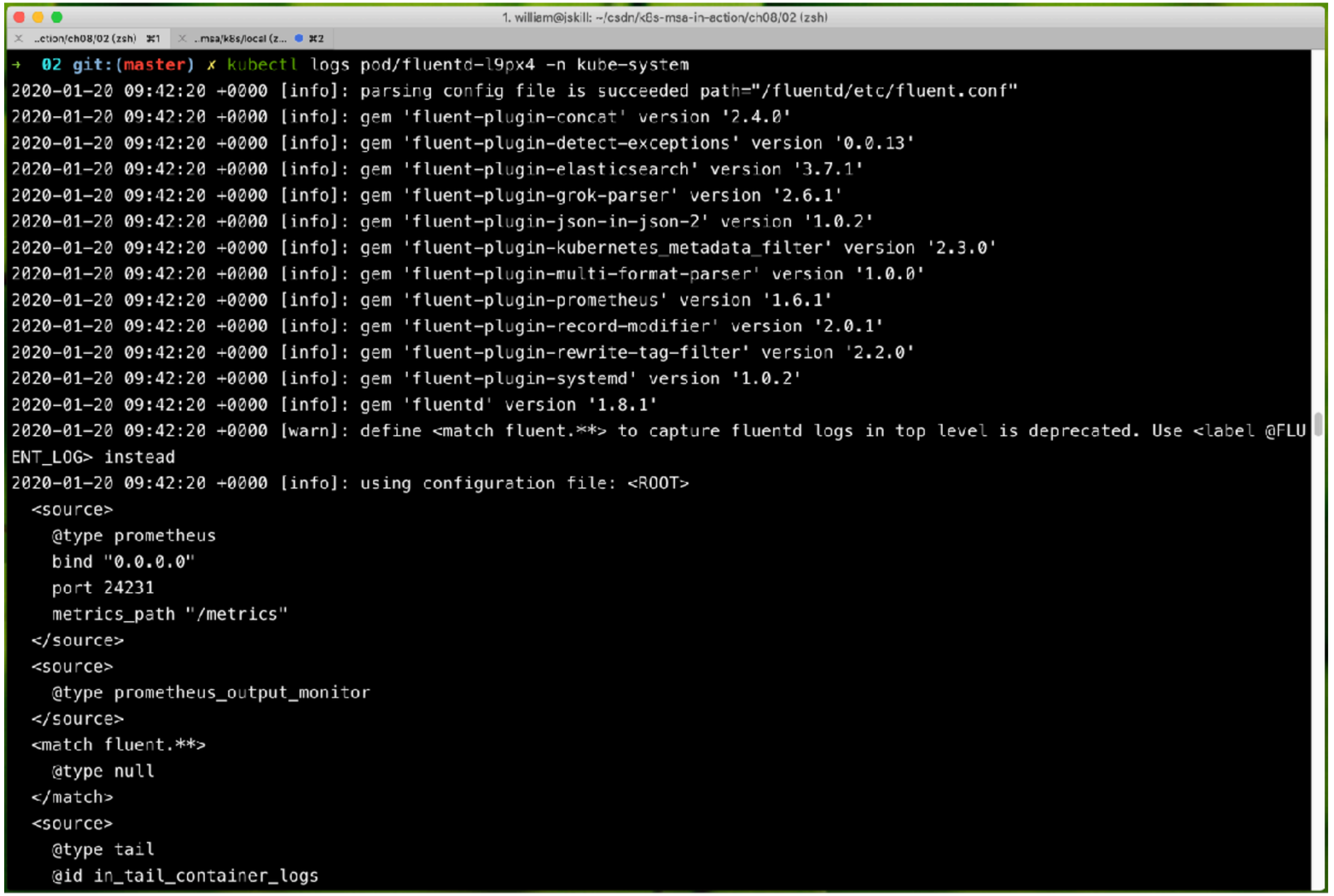
校验Kibana


Kibana
192.168.64.8:31601/app/kibana#/home?_g=()
kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Default
Collapse
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
APM
Canvas
Manage and Administer the Elastic Stack
Console
Index Patterns

发布Fluentd


1. william@jskill: ~/csdn/k8s-msa-in-action/ch08/02 (zsh)
.ction/ch08/02 (zsh) ⌘1
..msa/k8s/local (z... ⌘2
→ 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-daemonsct.yml
daemonset.apps/fluentd created
→ 02 git:(master) ✗ kubectl get all -n kube-system
NAME READY STATUS RESTARTS AGE
pod/corcdns-6955765f44-hfm96 1/1 Running 0 88m
pod/coredns-6955765f44-tdmfp 1/1 Running 0 88m
pod/ctcd-minikubc 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



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