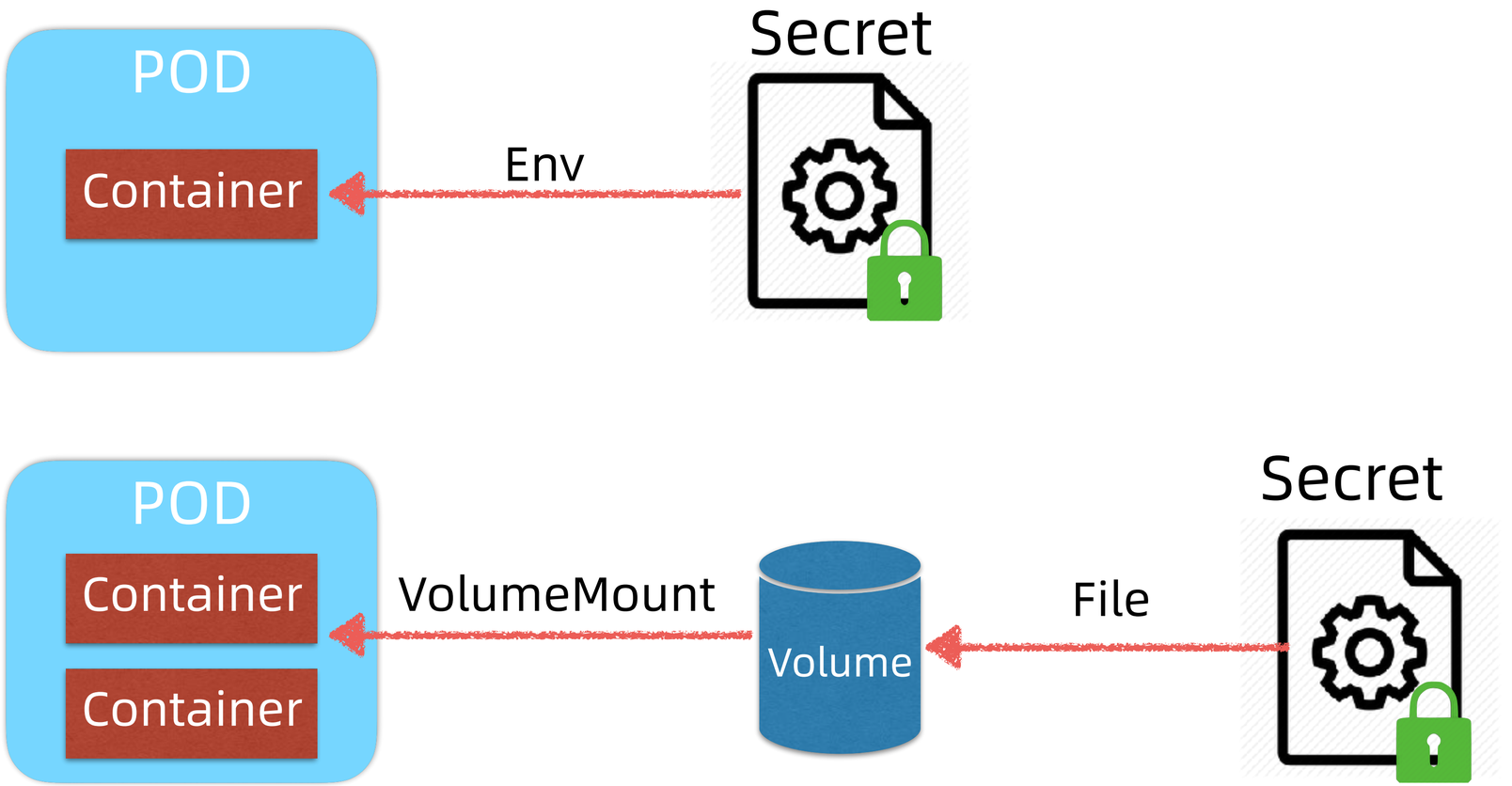
第 11 节

K8s机密配置抽象Secret

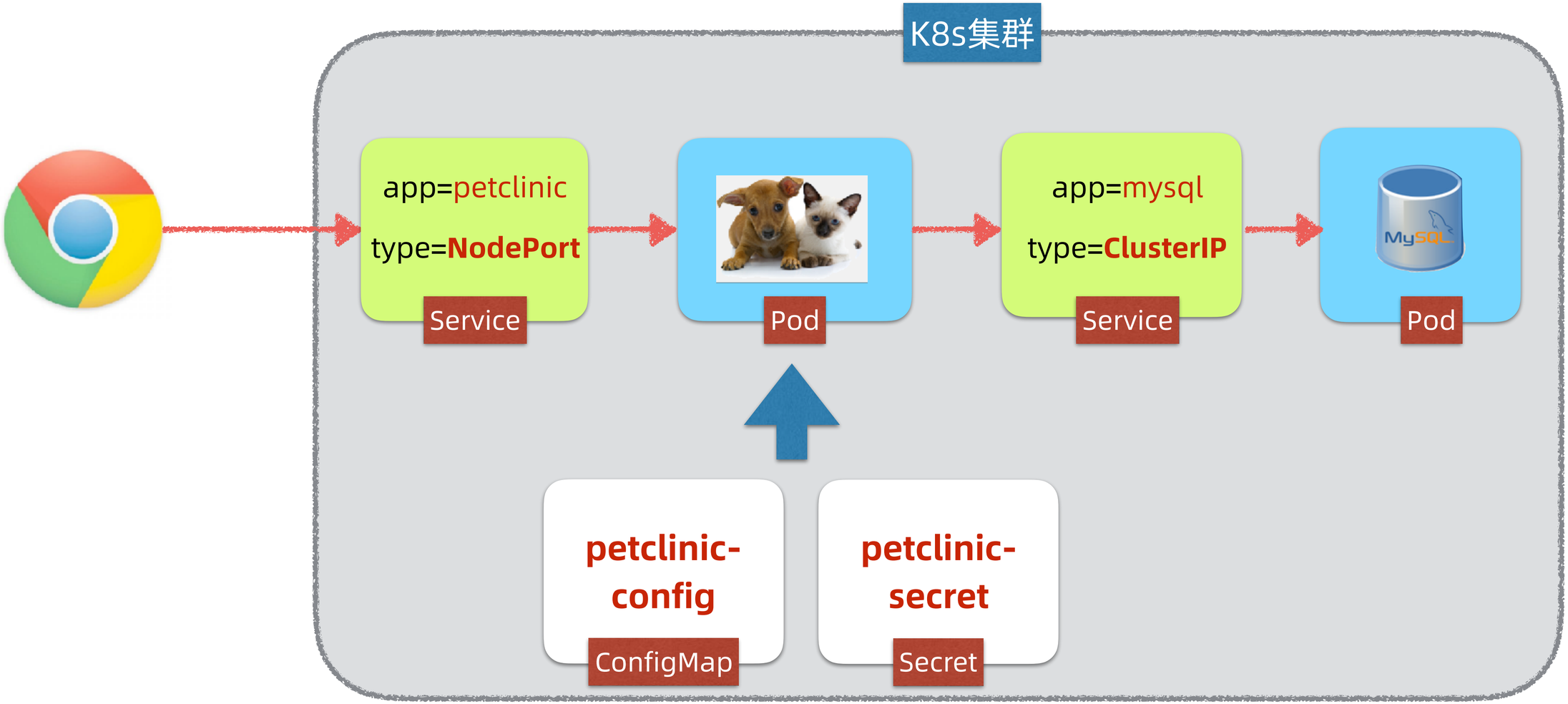
本课内容

- K8s机密配置抽象Secret的原理和演示
- 解释Secret的安全性

K8s机密配置抽象Secret



演示部署架构


K8s集群
app=petclinic
type=NodePort
Service
Pod
app=mysql
type=ClusterIP
Service
MySQL
Pod
petclinic-config
ConfigMap
petclinic-secret
Secret

Petclinic Config & Secret

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: petclinic-config-v2
data:
  SPRING_PROFILES_ACTIVE: mysql
  DATASOURCE_URL: jdbc:mysql://mysql/petclinic
  DATASOURCE_INIT_MODE: always
  TEST_CONFIG: test_config_v2
```

echo -n petclinic | base64

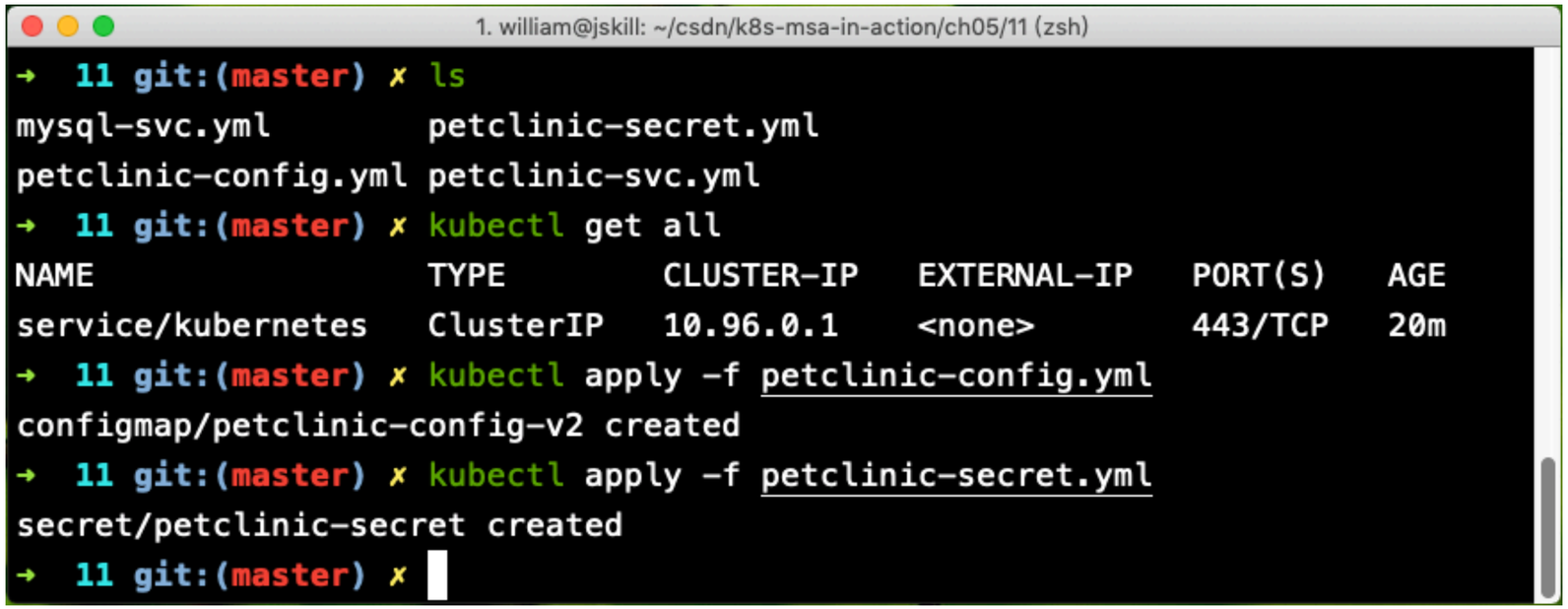
https://www.base64encode.org

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: petclinic-secret
type: Opaque
#data:
#  DATASOURCE_USERNAME: cm9vdA==
#  DATASOURCE_PASSWORD: cGV0Y2xpbmlj
stringData:
  DATASOURCE_USERNAME: root
  DATASOURCE_PASSWORD: petclinic
```

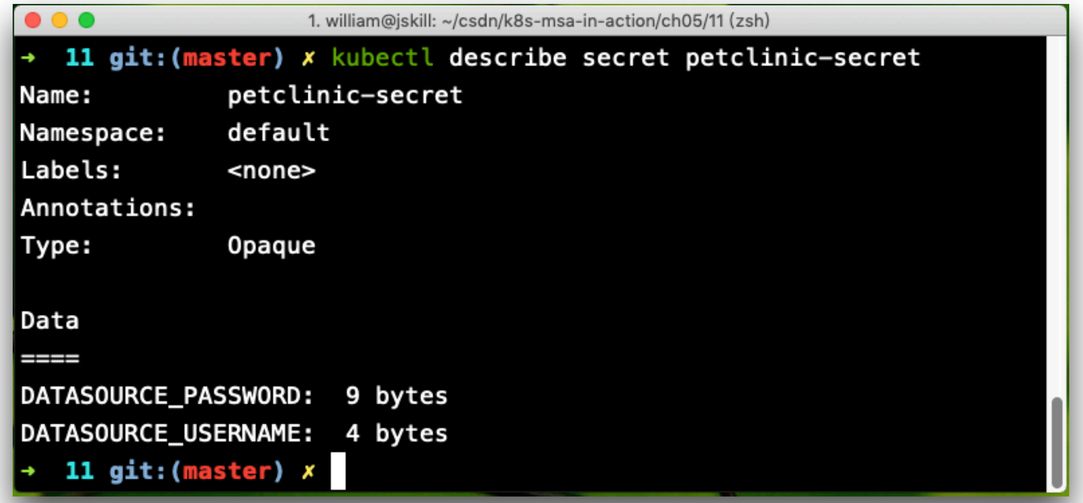
Petclinic Deployment

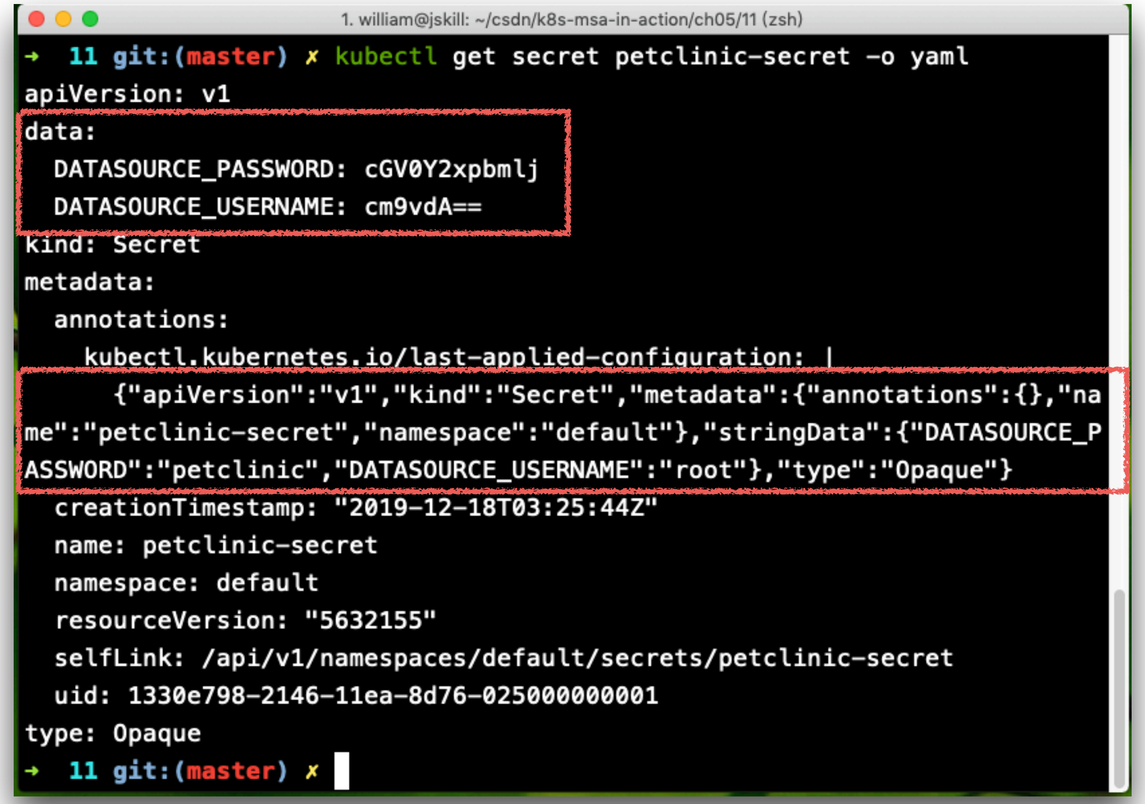
```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: petclinic
spec:
  selector:
    matchLabels:
      app: petclinic
  replicas: 1
  template:
    metadata:
      labels:
        app: petclinic
    spec:
      containers:
        - name: petclinic
          image: spring2go/spring-petclinic:1.0.1.RELEASE
          envFrom:
            - configMapRef:
                name: petclinic-config-v2
            - secretRef:
                name: petclinic-secret
```

发布petclinic-config.yml & petclinic-secret.yml

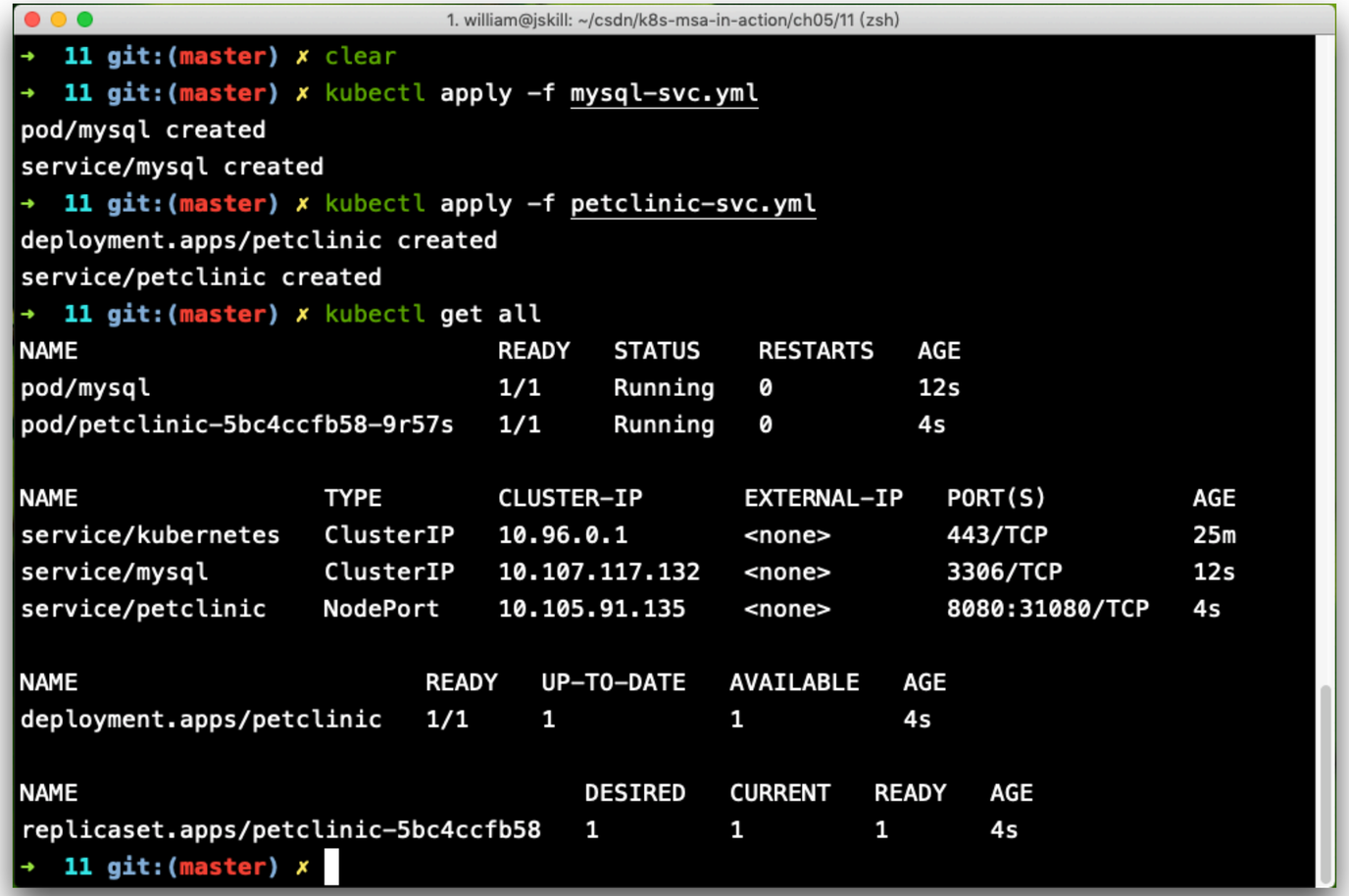


查看petclinic-secret详情

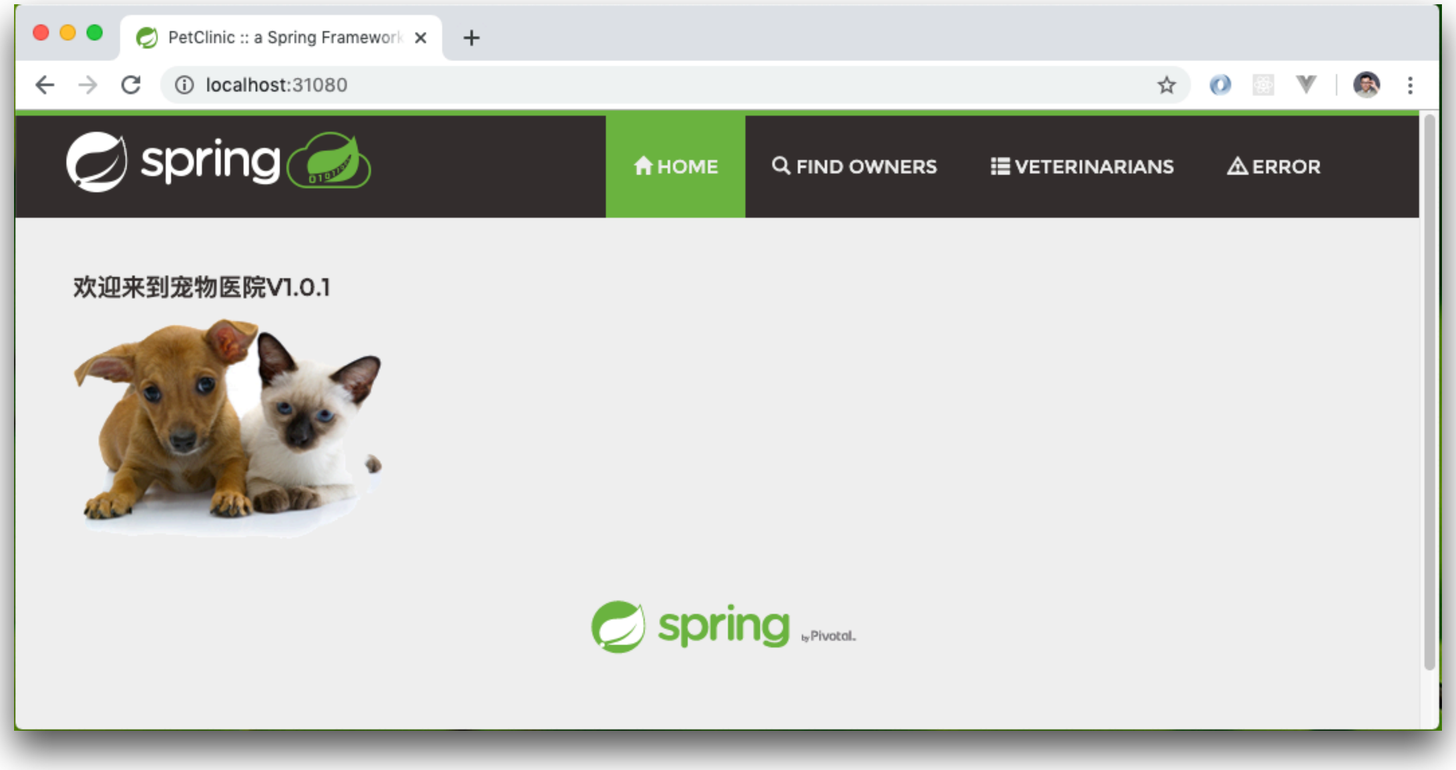




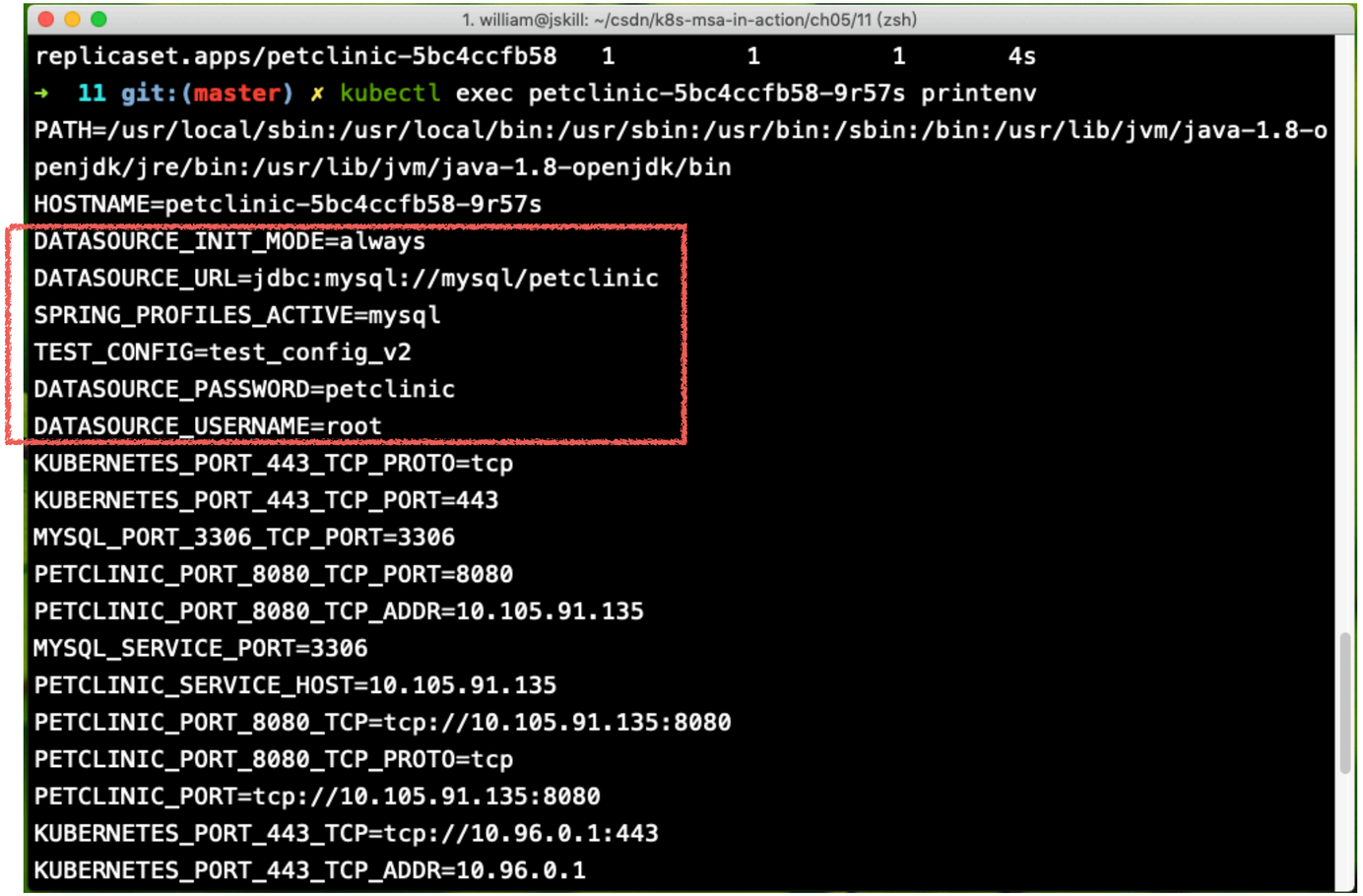
发布Mysql & PetClinic



校验PetClinic应用



查询Petclinic Pod环境变量



环境清理

```
kubectl delete cm petclinic-config-v2

kubectl delete secret petclinic-secret

kubectl delete deploy — all

kubectl delete svc — all

kubectl delete po —al
```

本课小结

- Secret是K8s提供的一种机密配置抽象，便于在微服务间共享机密配置
- Secret仅提供有限安全
  - 协作时防止机密数据泄露
  - 为Secret资源设置单独安全访问策略
- Secret和Pod绑定
  - 环境变量(Env)
  - 持久卷(Volume)