

# 第 11 节

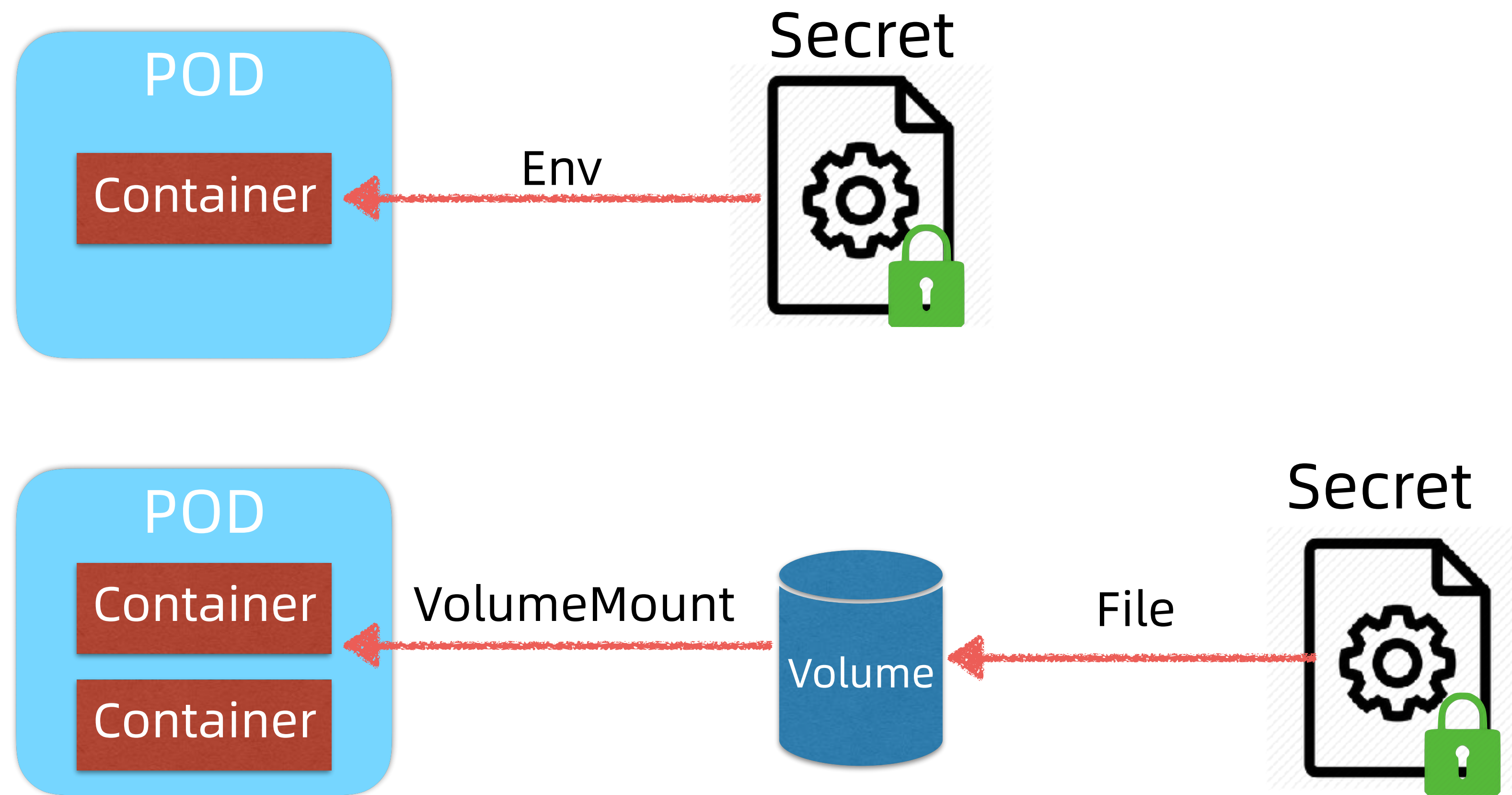
## K8s机密配置抽象Secret

# 本课内容

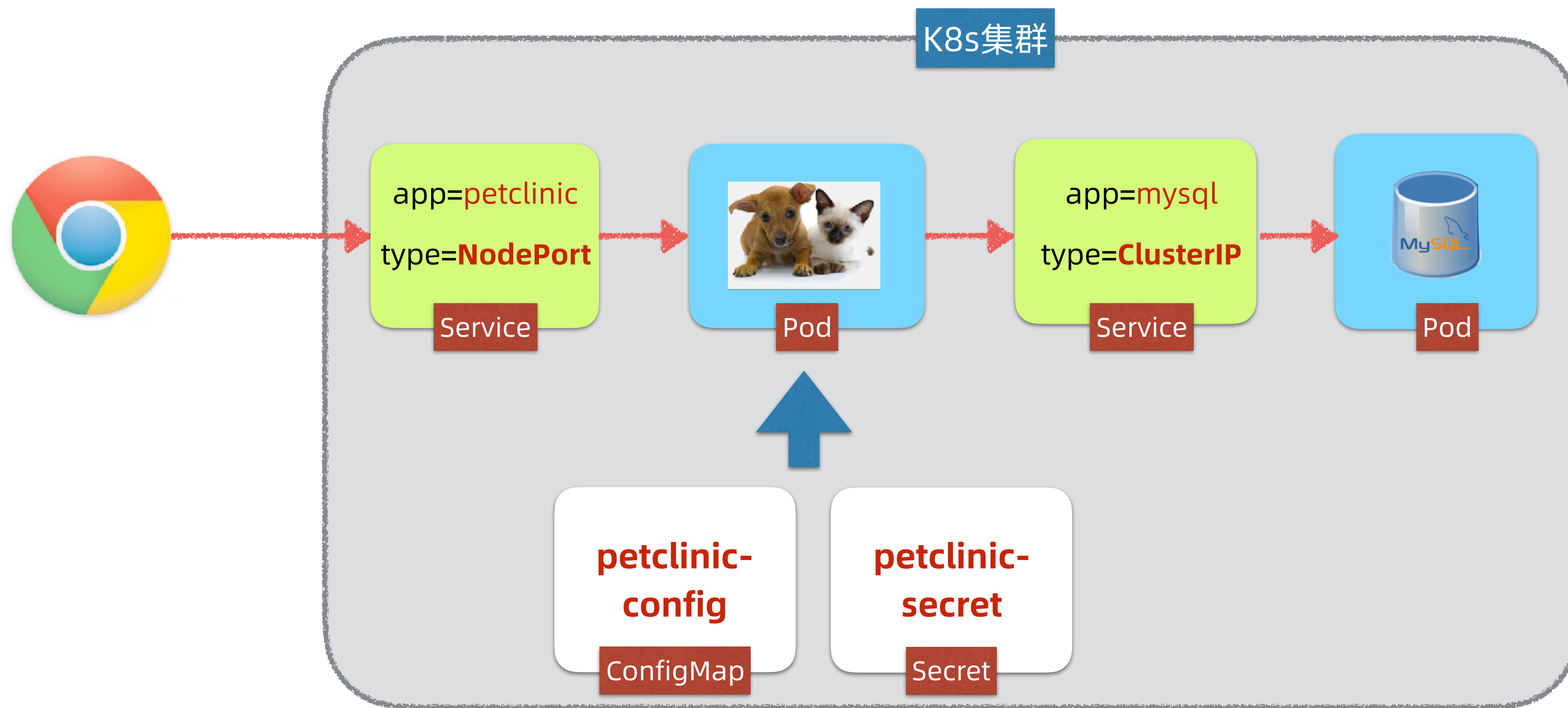
- K8s机密配置抽象Secret的原理和演示
- 解释Secret的安全性



# K8s机密配置抽象Secret



# 演示部署架构



# Petclinic Config & Secret

echo -n petclinic | base64

<https://www.base64encode.org>

```
1  apiVersion: v1
2  kind: ConfigMap
3  metadata:
4    name: petclinic-config-v2
5  data:
6    SPRING_PROFILES_ACTIVE: mysql
7    DATASOURCE_URL: jdbc:mysql://mysql/petclinic
8    DATASOURCE_INIT_MODE: always
9    TEST_CONFIG: test_config_v2
```

```
1  apiVersion: v1
2  kind: Secret
3  metadata:
4    name: petclinic-secret
5  type: Opaque
6  #data:
7  #  DATASOURCE_USERNAME: cm9vdA==
8  #  DATASOURCE_PASSWORD: cGV0Y2xpbmlj
9  stringData:
10    DATASOURCE_USERNAME: root
11    DATASOURCE_PASSWORD: petclinic
```

# Petclinic Deployment

```
1  apiVersion: apps/v1
2  kind: Deployment
3  metadata:
4    name: petclinic
5  spec:
6    selector:
7      matchLabels:
8        app: petclinic
9    replicas: 1
10   template:
11     metadata:
12       labels:
13         app: petclinic
14     spec:
15       containers:
16         - name: petclinic
17           image: spring2go/spring-petclinic:1.0.1.RELEASE
18           envFrom:
19             - configMapRef:
20               name: petclinic-config-v2
21             - secretRef:
22               name: petclinic-secret
```



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

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch05/11 (zsh)
→ 11 git:(master) ✕ ls
mysql-svc.yml          petclinic-secret.yml
petclinic-config.yml   petclinic-svc.yml
→ 11 git:(master) ✕ kubectl get all
NAME                                TYPE                CLUSTER-IP    EXTERNAL-IP    PORT(S)    AGE
service/kubernetes              ClusterIP          10.96.0.1     <none>         443/TCP    20m
→ 11 git:(master) ✕ kubectl apply -f petclinic-config.yml
configmap/petclinic-config-v2 created
→ 11 git:(master) ✕ kubectl apply -f petclinic-secret.yml
secret/petclinic-secret created
→ 11 git:(master) ✕
```

# 查看petclinic-secret详情

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch05/11 (zsh)
→ 11 git:(master) x kubectl describe secret petclinic-secret
Name:          petclinic-secret
Namespace:     default
Labels:        <none>
Annotations:
Type:          Opaque

Data
====
DATASOURCE_PASSWORD:  9 bytes
DATASOURCE_USERNAME:  4 bytes
→ 11 git:(master) x
```

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch05/11 (zsh)
→ 11 git:(master) x kubectl get secret petclinic-secret -o yaml
apiVersion: v1
data:
  DATASOURCE_PASSWORD: cGV0Y2xpbmlj
  DATASOURCE_USERNAME: cm9vdA==
kind: Secret
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","kind":"Secret","metadata":{"annotations":{},"name":"petclinic-secret","namespace":"default"},"stringData":{"DATASOURCE_PASSWORD":"petclinic","DATASOURCE_USERNAME":"root"},"type":"Opaque"}
  creationTimestamp: "2019-12-18T03:25:44Z"
  name: petclinic-secret
  namespace: default
  resourceVersion: "5632155"
  selfLink: /api/v1/namespaces/default/secrets/petclinic-secret
  uid: 1330e798-2146-11ea-8d76-025000000001
type: Opaque
→ 11 git:(master) x
```



# 发布Mysql & PetClinic

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch05/11 (zsh)
→ 11 git:(master) ✕ clear
→ 11 git:(master) ✕ kubectl apply -f mysql-svc.yml
pod/mysql created
service/mysql created
→ 11 git:(master) ✕ kubectl apply -f petclinic-svc.yml
deployment.apps/petclinic created
service/petclinic created
→ 11 git:(master) ✕ kubectl get all
```

NAME	READY	STATUS	RESTARTS	AGE
pod/mysql	1/1	Running	0	12s
pod/petclinic-5bc4ccfb58-9r57s	1/1	Running	0	4s

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
service/kubernetes	ClusterIP	10.96.0.1	<none>	443/TCP	25m
service/mysql	ClusterIP	10.107.117.132	<none>	3306/TCP	12s
service/petclinic	NodePort	10.105.91.135	<none>	8080:31080/TCP	4s

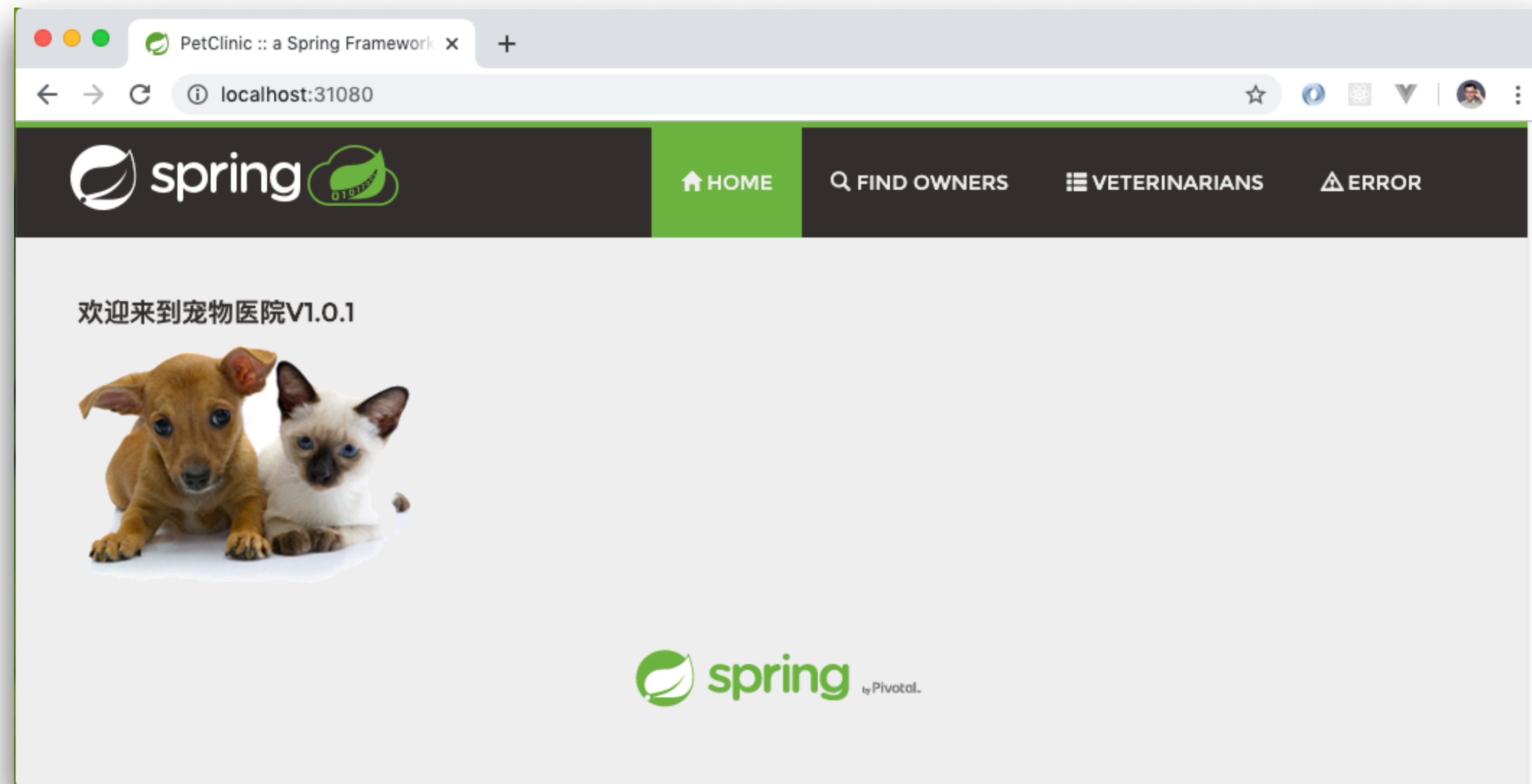
NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/petclinic	1/1	1	1	4s

NAME	DESIRED	CURRENT	READY	AGE
replicaset.apps/petclinic-5bc4ccfb58	1	1	1	4s

```
→ 11 git:(master) ✕
```

# 校验PetClinic应用



# 查询Petclinic Pod环境变量

```
1. william@jskill: ~/csdn/k8s-msa-in-action/ch05/11 (zsh)
replicaset.apps/petclinic-5bc4ccfb58 1 1 1 4s
→ 11 git:(master) x kubectl exec petclinic-5bc4ccfb58-9r57s printenv
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/lib/jvm/java-1.8-o
penjdk/jre/bin:/usr/lib/jvm/java-1.8-openjdk/bin
HOSTNAME=petclinic-5bc4ccfb58-9r57s
DATASOURCE_INIT_MODE=always
DATASOURCE_URL=jdbc:mysql://mysql/petclinic
SPRING_PROFILES_ACTIVE=mysql
TEST_CONFIG=test_config_v2
DATASOURCE_PASSWORD=petclinic
DATASOURCE_USERNAME=root
KUBERNETES_PORT_443_TCP_PROTO=tcp
KUBERNETES_PORT_443_TCP_PORT=443
MYSQL_PORT_3306_TCP_PORT=3306
PETCLINIC_PORT_8080_TCP_PORT=8080
PETCLINIC_PORT_8080_TCP_ADDR=10.105.91.135
MYSQL_SERVICE_PORT=3306
PETCLINIC_SERVICE_HOST=10.105.91.135
PETCLINIC_PORT_8080_TCP=tcp://10.105.91.135:8080
PETCLINIC_PORT_8080_TCP_PROTO=tcp
PETCLINIC_PORT=tcp://10.105.91.135:8080
KUBERNETES_PORT_443_TCP=tcp://10.96.0.1:443
KUBERNETES_PORT_443_TCP_ADDR=10.96.0.1
```

# 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)