

МЕГА
СЛЭРМ

+



Southbridge

Хранение секретов

Секреты

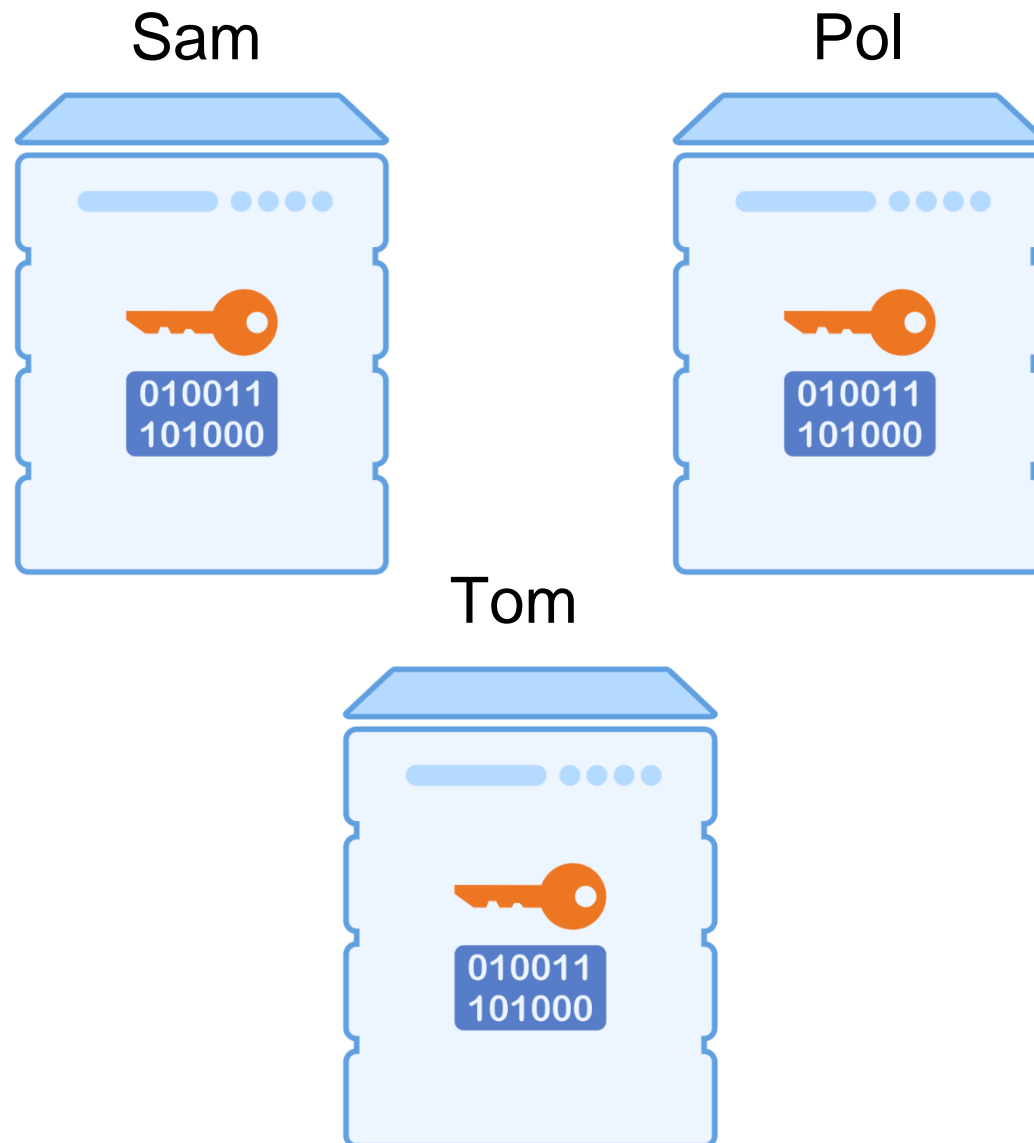
Логины и пароли

Токены

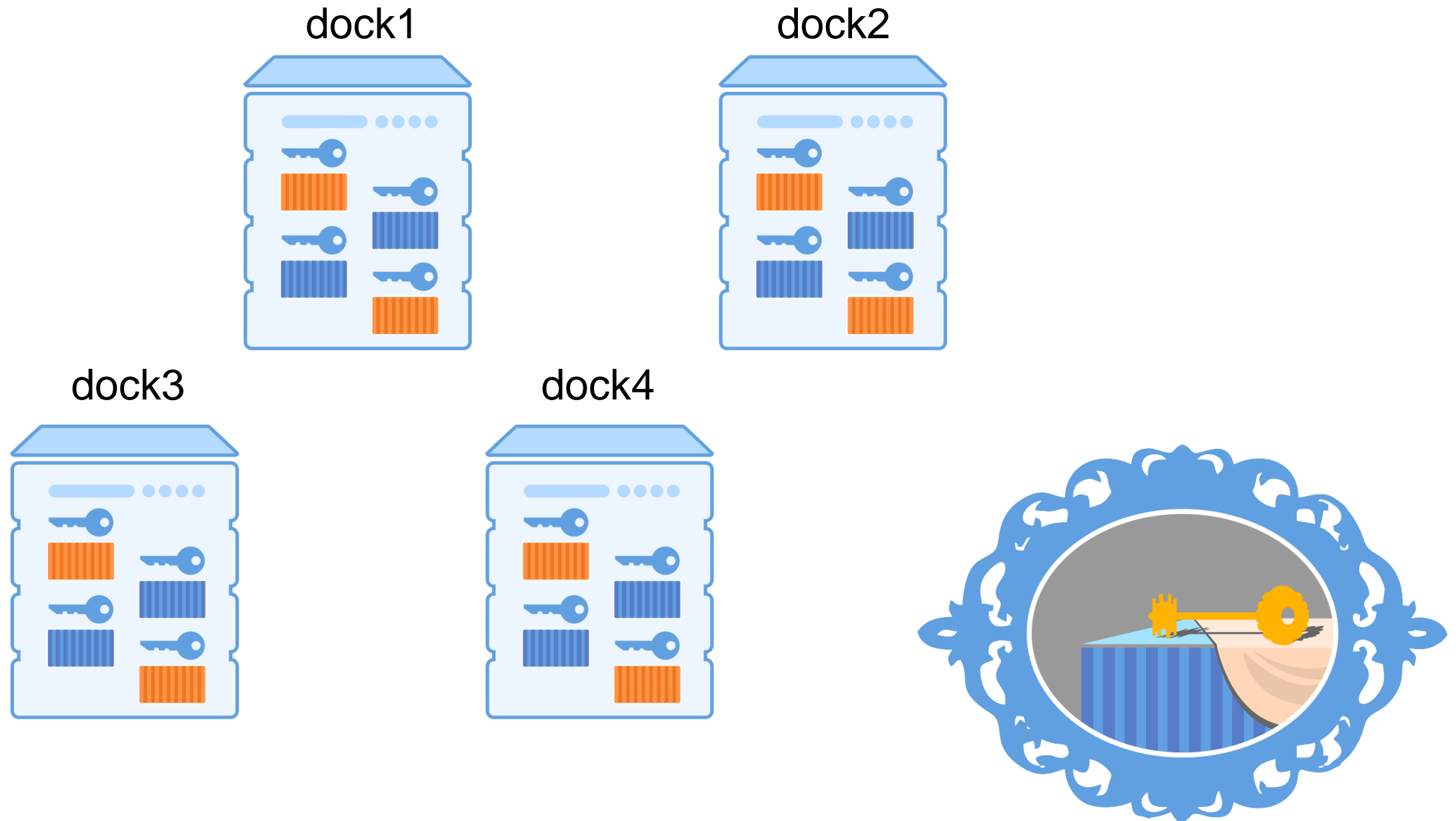
Ключи сертификатов



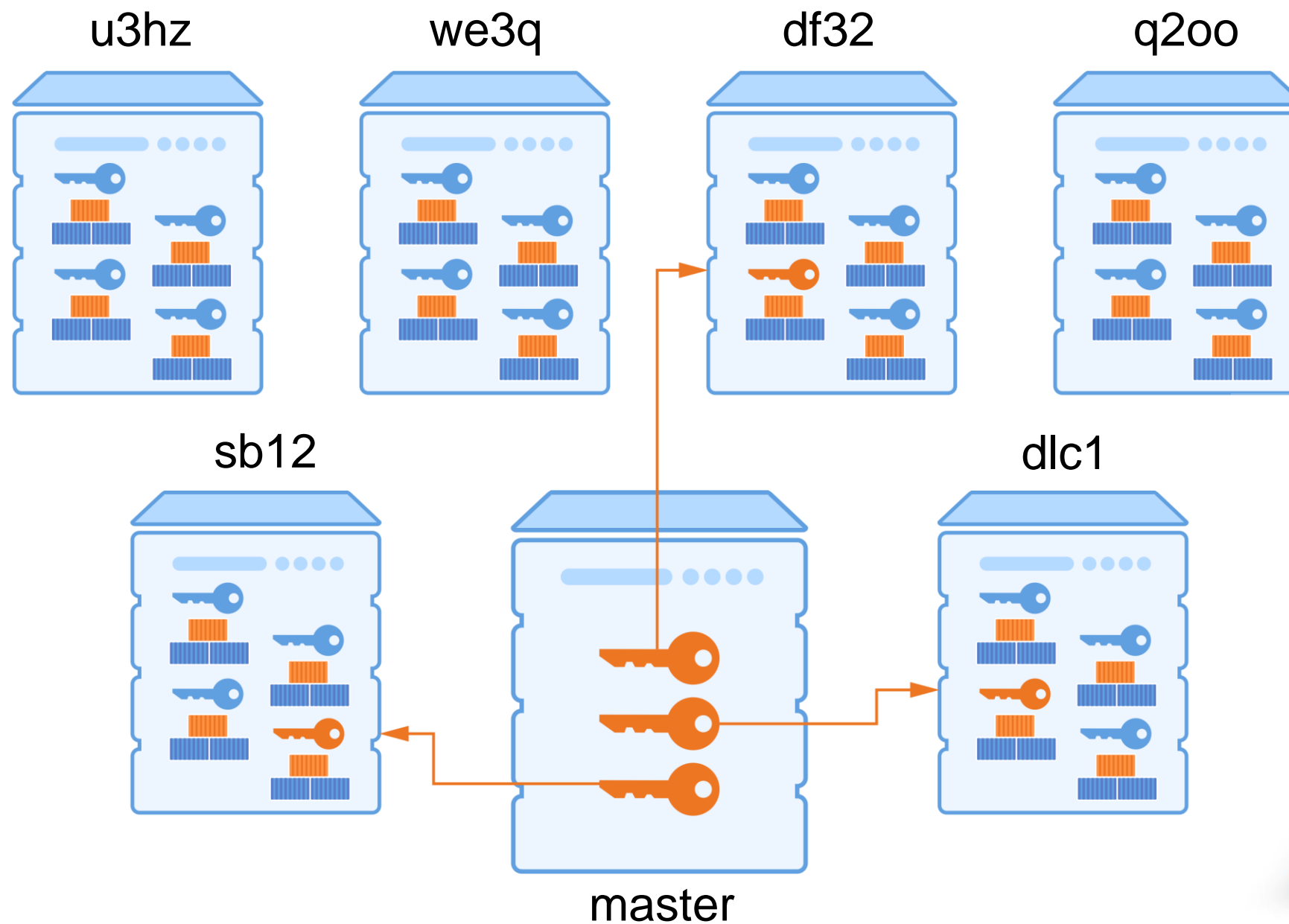
Античность – секреты на серверах



Новое время – секреты у контейнеров



Современность – копии секретов у подов



Секреты в Kubernetes

```
apiVersion: v1
kind: Secret
metadata:
  name: mysecret
type: Opaque
data:
  username: YWRtaW4=
stringData:
  apiUrl: "https://my.api.com/api/v1"
  username: username
  password: password
```



Секреты в Kubernetes

```
kubectl create secret generic mygreatsecret \  
  --from-file=username.txt \  
  --from-file=key=username.txt \  
  --from-literal=dbpass=rootpassword \  
  --from-env-file=file.env
```



Подключение секретов

```
containers:
- name: mypod
  image: redis
  volumeMounts:
  - name: foo
    mountPath: "/etc/foo"
    readOnly: true
volumes:
- name: foo
  secret:
    secretName: mysecret
```

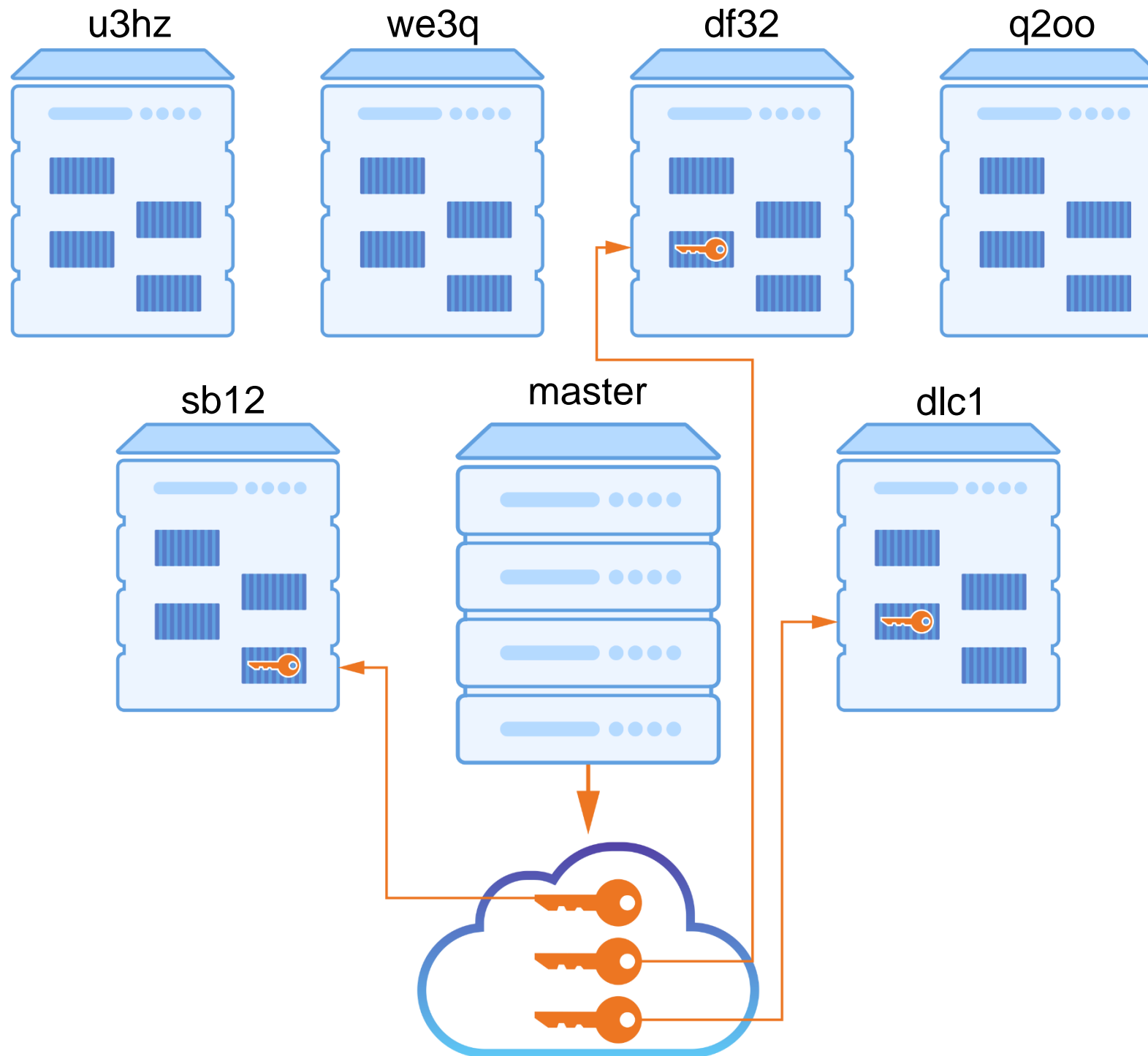
```
containers:
- name: mypod
  image: redis
  env:
  - name: SECRET_TOKEN
    valueFrom:
      secretKeyRef:
        name: mysecret
        key: token
```



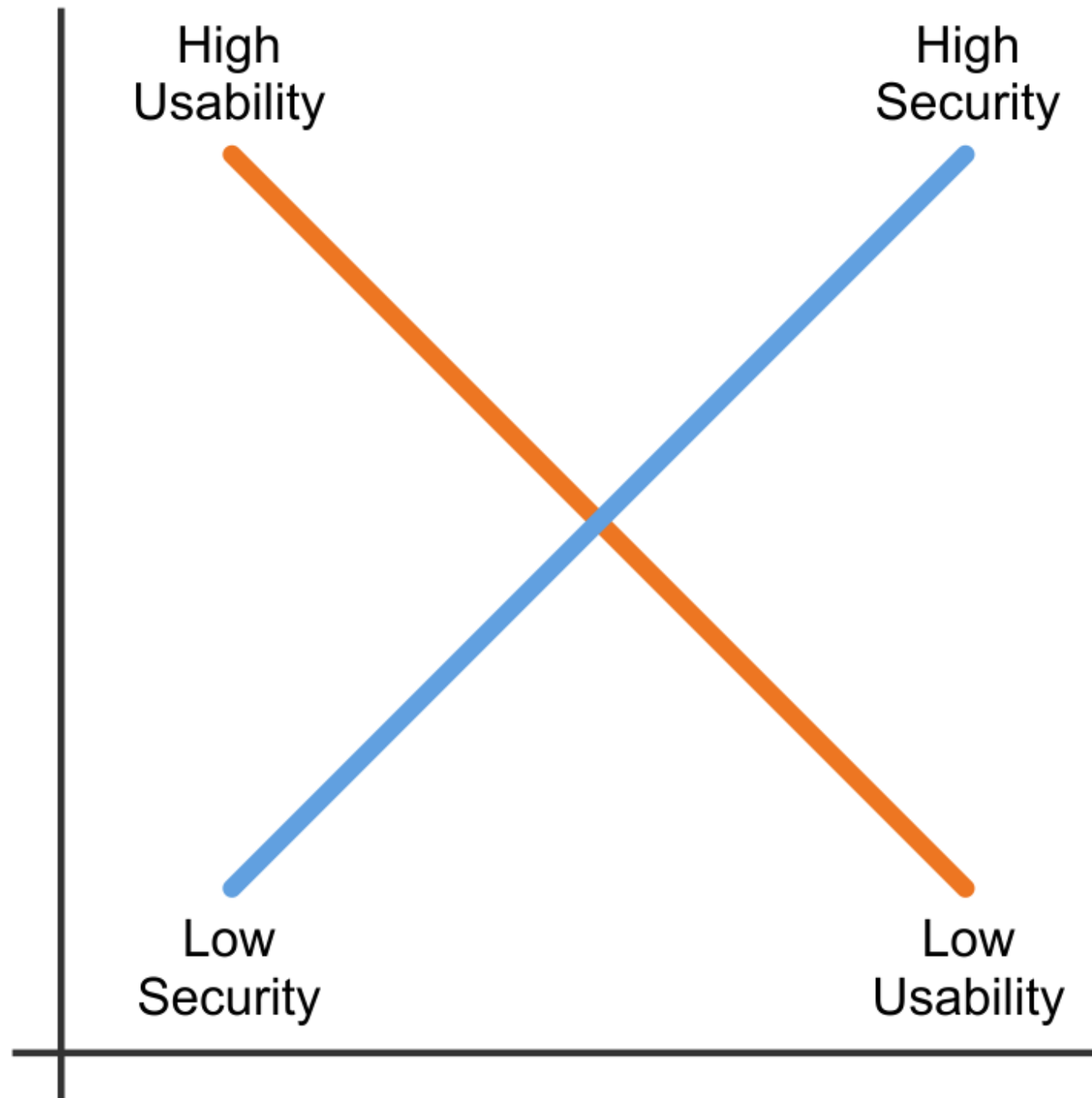
Возможности и опасности



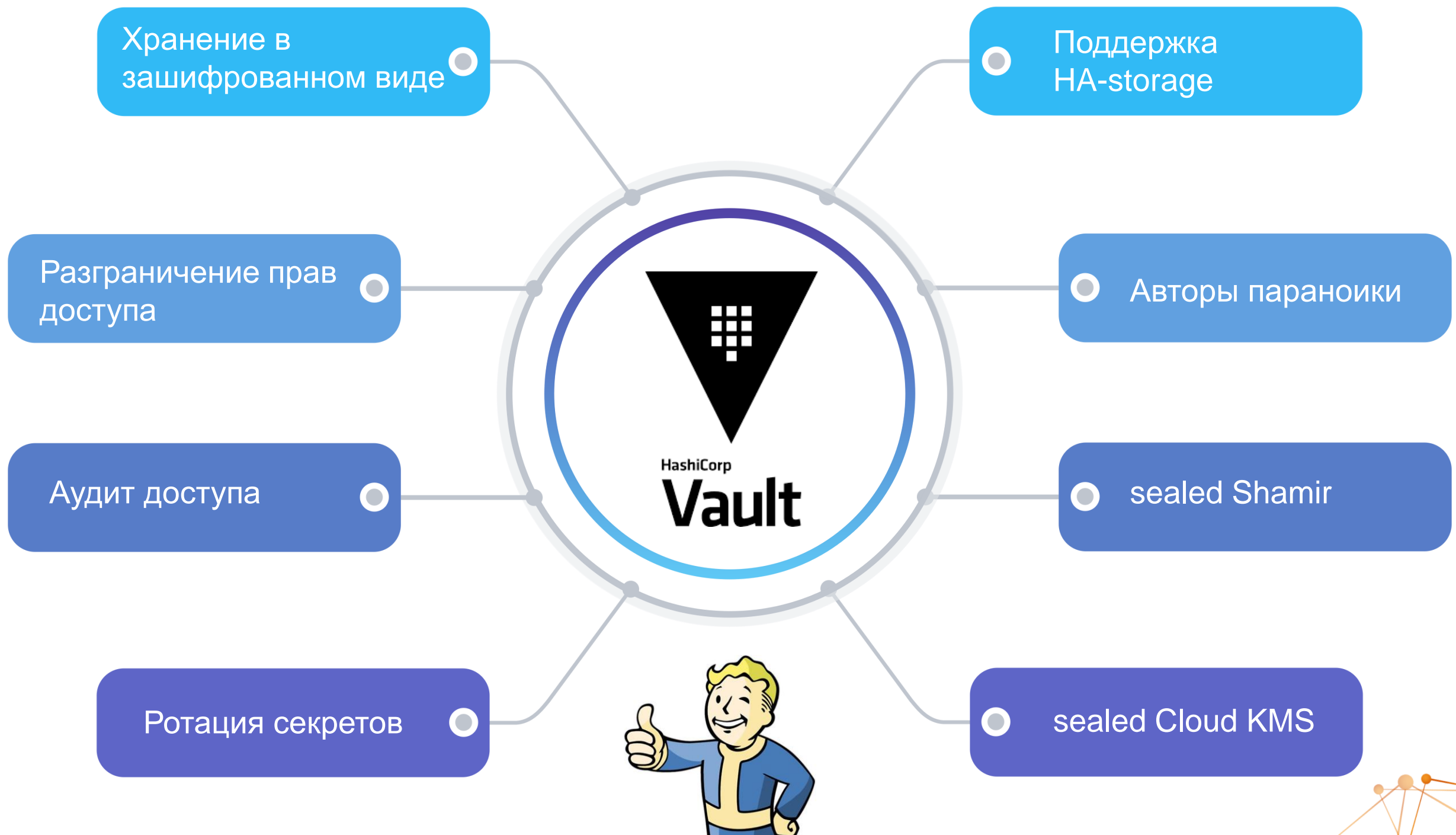
Светлое будущее – секреты внутри пода



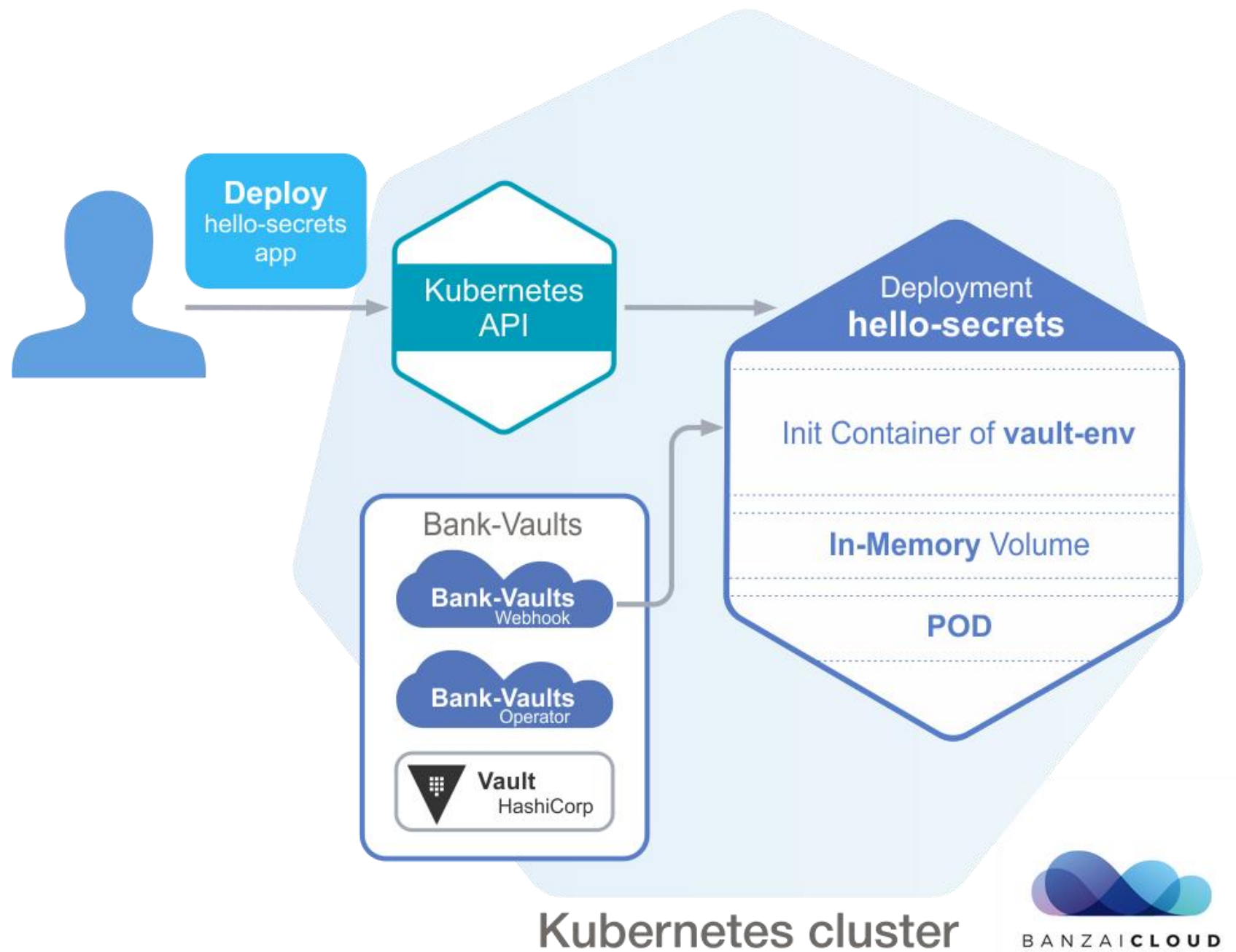
Security vs Usability



Hashicorp Vault

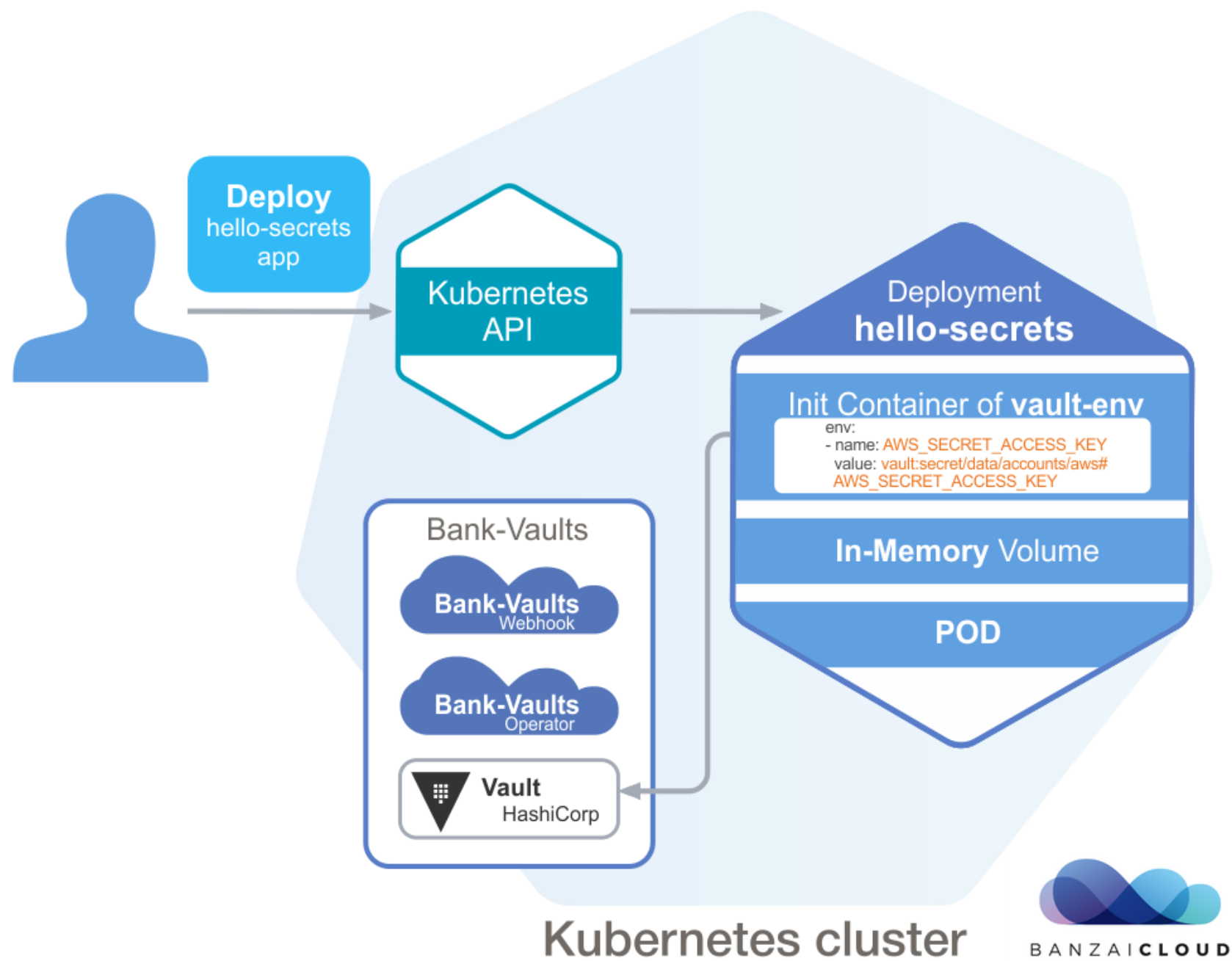


Banzaicloud



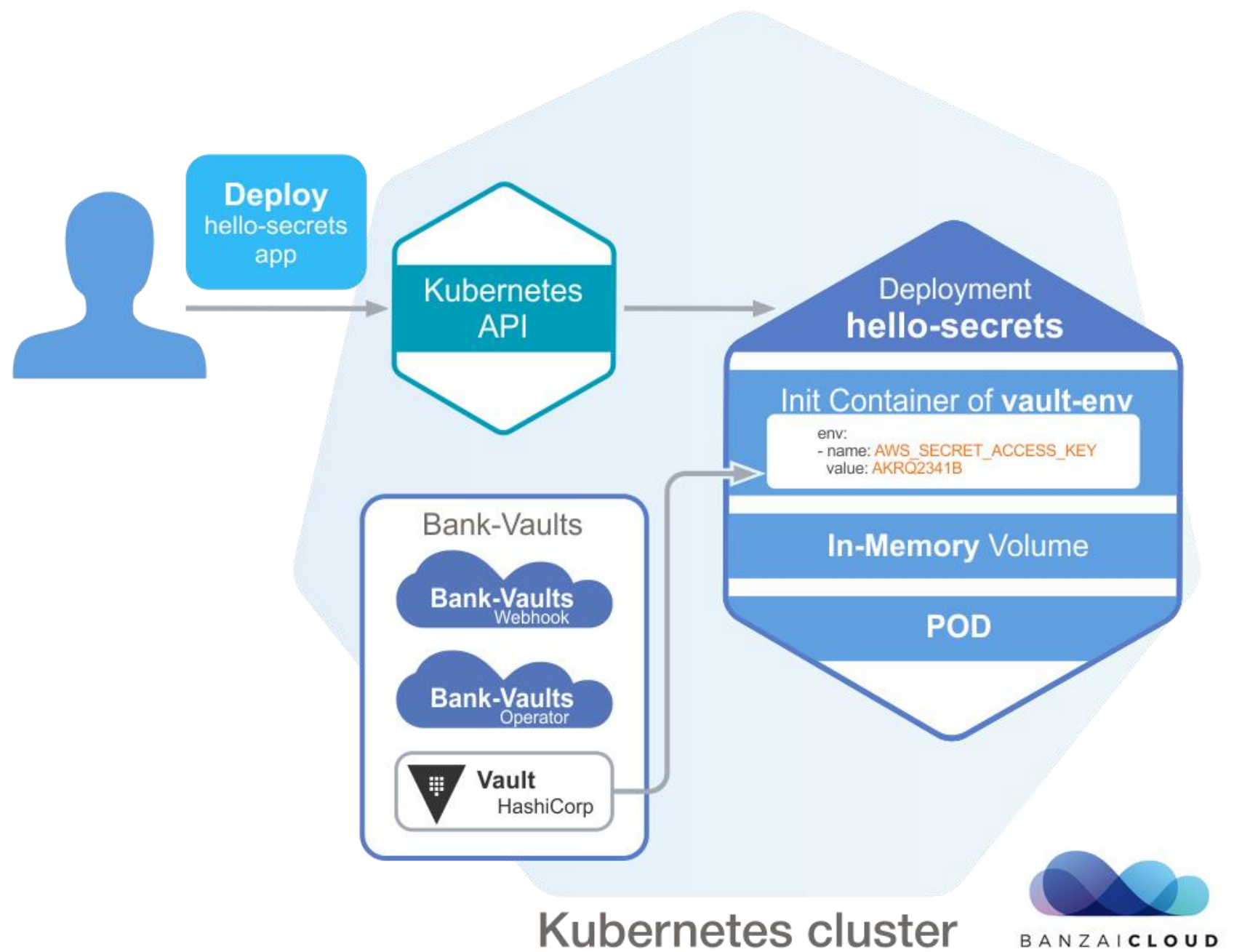
<https://github.com/banzaicloud/bank-vaults>

Banzaicloud



<https://github.com/banzaicloud/bank-vaults>

Banzaicloud



<https://github.com/banzaicloud/bank-vaults>

МЕГА
СЛЕРМ

+



Southbridge

slurm.io