Day13 容器进阶之Kubernetes 安全原理分析

1 打卡任务

作业：

使用kubectl为CCE集群创建一个pod只读用户，该用户只能查询指定namespace下的pod权限。本作业命令行操作较多，请按指导一步步执行

打卡：

使用只读用户测试读取、删除 pod 并将返回结果截图

2 准备工作

1、 已拥有可运行的CCE集群

3 使用 kubectl 为 CCE 集群创建一个只读用户

1、 登录day4已配置kubectl命令行的node节点

2、 创建一个新的namespace

通过kubectl创建一个namespace，后续只读用户只能在该namespace下操作

kubectl create namespace cce

3、 在cce namespace下创建一个serviceAccount(sa)并获取对应的secret下的token

kubectl create sa cce-service-account -ncce

获取sa对应的secret名字：

kubectl get sa cce-service-account -ncce –oyaml

```
[root@cce-21days-cluster-98379 ~]# kubectl get sa cce-service-account -ncce -oyaml
apiVersion: v1
kind: ServiceAccount
metadata:
  creationTimestamp: 2018-11-07T07:18:47Z
  name: cce-service-account
  namespace: cce
  resourceVersion: "196182"
  selfLink: /api/v1/namespaces/cce/serviceaccounts/cce-service-account
  uid: 5dec71df-e25d-11e8-a260-fa163efe9363
secrets:
- name: cce-service-account-token-g8dg5
[root@cce-21days-cluster-98379 ~]#
```

获取secret下的token，并base64解码获取token明文：

token=`kubectl get secret cce-service-account-token-g8dg5 -ncce -oyaml |grep token: | awk '{print $2}' | xargs echo -n | base64 -d`

4、 新增cce-user用户（绿色字体为自定义字段，可以不修改）：

kubectl config set-cluster cce-viewer --server=https://192.168.1.175:5443 --certificate-authority=/var/paas/srv/kubernetes/ca.crt

kubectl config set-context cce-viewer --cluster=cce-21days-cluster

kubectl config set-credentials cce-user --token=$token

kubectl config set-context cce-viewer --user=cce-user

红色server地址即master的访问地址可以在CCE界面上查询到：

通过如下命令可以看到已经有新建的context：

kubectl config get-contexts

```
[root@cce-21days-cluster-98379 ~]#
[root@cce-21days-cluster-98379 ~]# kubectl config get-contexts
CURRENT   NAME          CLUSTER             AUTHINFO   NAMESPACE
          cce-viewer    cce-21days-cluster
*         internal      internalCluster     user
[root@cce-21days-cluster-98379 ~]#
[root@cce-21days-cluster-98379 ~]#
```

5、 授予cce-user只读权限的role并通过rolebinding绑定对应的serviceAccount

role.yaml

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: cce
  name: pod-reader
rules:
- apiGroups: [""] # "" indicates the core API group
  resources: ["pods"]
  verbs: ["get", "watch", "list"]
```

rolebinding.yaml

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: pod-reader-binding
  namespace: cce
subjects:
- kind: ServiceAccount
  name: cce-service-account          #步骤2中创建的serviceAccount名称
  namespace: cce
roleRef:
  kind: Role
  name: pod-reader
```

apiGroup: rbac.authorization.k8s.io

执行以下命令创建role及rolebinding：

kubectl create -f role.yaml

kubectl create -f rolebinding.yaml

6、 切换context到cce-viewer用户下，验证权限设置结果：

kubectl config use-context cce-viewer

1） 查看default namespace下的pod，应该会返回403无权限的错误

kubectl get pods

```
[root@cce-21days-cluster-98379 .kube]#
[root@cce-21days-cluster-98379 .kube]# kubectl get pods
Error from server (Forbidden): pods is forbidden: User "system:serviceaccount:cce:cce-service-account" cannot list pods in the namespace "default"
[root@cce-21days-cluster-98379 .kube]#
```

若出现如下错误，请尝试设置环境变量后再执行命令

```
[root@cce-21days-cluster-98379 .kube]# kubectl get pods
The connection to the server localhost:8080 was refused - did you specify the right host or port?
```

export KUBERNETES_MASTER=*https://192.168.1.175:5443*

2） 查看cce namespace下的pod:

kubectl get pods -ncce

```
[root@cce-21days-cluster-98379 .kube]# kubectl get pods -ncce
No resources found.
[root@cce-21days-cluster-98379 .kube]#
[root@cce-21days-cluster-98379 .kube]#
```

“No resource found”表示请求返回200，只是该namespace下没有pod显示。可以通过CCE界面在该namespace下创建一个工作负载再次查看

7、 使用如下命令即可切换回admin管理员权限的context:

kubectl config use-context internal

4 打卡截图

只读用户权限下查看default和cce两个namespace下的pod结果：

```
[root@cce-21days-cluster-98379 .kube]# kubectl get pods
Error from server (Forbidden): pods is forbidden: User "system:serviceaccount:cce:cce-service-account" cannot list pods in the namespace "default"
[root@cce-21days-cluster-98379 .kube]#
[root@cce-21days-cluster-98379 .kube]#
[root@cce-21days-cluster-98379 .kube]# kubectl get pods -ncce
No resources found.
[root@cce-21days-cluster-98379 .kube]#
[root@cce-21days-cluster-98379 .kube]#
```