

Сервис-аккаунты



Сергей
Андрюнин



Сергей Андрюнин

DevOps-инженер

RTLabs




Сергей Андрюнин



План занятия

1. [Общие сведения о сервис-аккаунтах](#)
2. [Использование](#)
3. [Итоги](#)
4. [Домашнее задание](#)



Общие сведения о сервис-аккаунтах

Общие сведения о сервис-аккаунтах

- предназначены для предоставления токена контейнеру, который сможет получить доступ к API kubernetes;
- в каждом неймспейсе есть свой сервис-аккаунт default, который создаётся с самим неймспейсом;
- у каждого сервис-аккаунта есть токен;
- токен сервис-аккаунта хранится в объекте secrets.

Общие сведения о сервис-аккаунтах

Предназначены для предоставления токена контейнеру, который сможет получить доступ к API kubernetes:

- пользовательский аккаунт отличается от сервис-аккаунта тем, что сервис-аккаунт используется непосредственно сервисами;
- монтируется внутри контейнера в подкаталог `/var/run/secrets/kubernetes.io/serviceaccount`.



Использование

Создание, просмотр и удаление

Создание:

```
kubectl create serviceaccount netology
```

Просмотр:

```
kubectl get serviceaccount netology
```

Удаление:

```
kubectl delete serviceaccount netology
```


Переменные среды

```
# env | grep KUBE
KUBERNETES_SERVICE_PORT_HTTPS=443
KUBERNETES_SERVICE_PORT=443
KUBERNETES_PORT_443_TCP=tcp://10.96.0.1:443
KUBERNETES_PORT_443_TCP_PROTO=tcp
KUBERNETES_PORT_443_TCP_ADDR=10.96.0.1
KUBERNETES_SERVICE_HOST=10.96.0.1
KUBERNETES_PORT=tcp://10.96.0.1:443
KUBERNETES_PORT_443_TCP_PORT=443
```

Переменные для удобства

Доступ к API осуществляется через протокол HTTPS. Это накладывает требование обязательной сертификации и наличия корневого сертификата.

Т.к. в большинстве случаев сертификат является самоподписанным, то kubernetes великодушно предоставляет нам корневой сертификат в виде файла ca.crt

```
K8S=https://$KUBERNETES_SERVICE_HOST:$KUBERNETES_SERVICE_PORT  
SADIR=/var/run/secrets/kubernetes.io/serviceaccount  
TOKEN=$(cat $SADIR/token)  
CACERT=$SADIR/ca.crt  
NAMESPACE=$(cat $SADIR/namespace)
```

Пример запроса

```
curl -H "Authorization: Bearer $TOKEN" \  
--cacert $CACERT $K8S/api/v1/
```

CRUD

- CREATE – создание;
- READ – чтение;
- UPDATE – обновление;
- DELETE – удаление.

HTTP API REST

- CREATE – POST;
- READ – GET;
- UPDATE – PATCH/PUT;
- DELETE – DELETE.

YAML ServiceAccount

```
---
apiVersion: v1
kind: ServiceAccount
metadata:
  creationTimestamp: "2021-06-15T10:14:29Z"
  name: netology
  namespace: default
  resourceVersion: "20692"
  selfLink:
    /api/v1/namespaces/default/serviceaccounts/netology
  uid: ff39cc45-7c2d-4933-a992-915735bcb64a
secrets:
- name: netology-token-rpthf
```

YAML Pod

```
---
apiVersion: v1
kind: Pod
metadata:
  name: netology-14.4
spec:
  containers:
  - name: myapp
    image: fedora:latest
    command: ['ls', '-la',
'/var/run/secrets/kubernetes.io/serviceaccount']
    serviceAccountName: netology
```

Итоги

Сегодня мы изучили:

- что такое сервис аккаунты;
- как их создавать и использовать в kubernetes.

Домашнее задание

Давайте посмотрим ваше [домашнее задание](#).

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

**Задавайте вопросы и
пишите отзыв о лекции!**

Сергей Андрюнин