Network & Authentification

Plan

I. Namespace

II. Cluster networking

III. Network policy

IV. Authentification

V. RBAC

VI. TP

ynov CAMPUS

Namespace

Namespace

- Cluster virtuel présent sur un cluster physique
- Permet d'isoler des applications les unes des autres en les regroupant dans un même cluster virtuel
- Permet d'ajouter des restrictions / quotas de ressources

Ne permet pas de gérer les objets de type cluster, nœud, volumes, ...

Namespaces initiaux:
- default
- kube-system
- kube-public
- kube-node-lease

ynov CAMPUS

Cluster networking

Cluster networking

Brique central de Kubernetes
Attribue une adresse IP et définit les entrées DNS

Désactiver par défault au lancement de minikube

Nécessite d’ajouter les paramètres --network-plugin=cni --cni=calico

ynov CAMPUS

Network policy

ynov CAMPUS

Network policy

Pod accepte tous le trafic réseaux par défault

La ressource NetworkPolicy permet d'affiner le trafic entrant et sortant ou de l'élargir

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - ipBlock:
        cidr: 172.17.0.0/16
        except:
        - 172.17.1.0/24
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
    ports:
    - protocol: TCP
      port: 6379
  egress:
  - to:
    - ipBlock:
        cidr: 10.0.0.0/24
    ports:
    - protocol: TCP
      port: 5978
```

ynov CAMPUS

Authentification

Authentification

UserAccount :
- Lié à un secret
- Contient un token
- Non lié à un namespace
- Associé aux utilisateurs se connectant
- Permet de donner des autorisations spécifiques

ServiceAccount :
- Lié à un secret
- Contient un token
- Créé par l'api
- Associé aux pods
- Permet de donner des autorisations spécifiques

Permet de sécuriser l'accès au cluster avec un certificat ssl
Permet de restreindre les actions possible par un user

ynov CAMPUS

RBAC

RBAC

RBAC : Role-based access control

Type :
- Role
- ClusterRole
- RoleBinding
- ClusterRoleBinding

Role :
- Ensemble de permissions
- Lié à un namespace

RoleBinding :
- Lie un rôle à un ensemble de sujet (service account, ...)
- Lié à un namespace

ClusterRole :
- Ensemble de permissions
- Non lié à un namespace

ClusterRoleBinding:
- Lie un rôle à un ensemble de sujet (user, ...)
- Non lié à un namespace

TP

TP

- Monter 2 pods dans un même namespace (pod1 et pod2)
- Monter un pod dans un 2eme namespace (pod3)
- Discuter entre les pods (pod1 et pod2)
- Écrire les règles de réseau pour autoriser pod1 à discuter avec pod3
- Écrire les règles de réseau pour interdire pod1 à discuter avec pod2

TP

- Créer un certificat avec openssl (csr / crt)
- Ajouter un utilisateur via kubeconfig
- Changer de contexte et essayer d’ajouter une ressource
- Ajouter un rôle et essayer d’ajouter une ressource

TP

- Restreindre l’accès au dashboard de minikube via un token

Résumé

I. Namespace

II. Cluster networking

III. Network policy

IV. Authentification

V. RBAC

VI. TP

Prochaine étape

Allez plus loin