KUB 25: Сетевая безопасность в Kubernetes

Описание:

Kubernetes разрешает вам создавать, по сути, правила firewall, которые будут разрешать или запрещать доступ подов к подам в зависимости от условий. Прошу обратить внимание, что эта опция должна быть включена в настройках облачного кластера. Давайте обсудим простой пример:

```
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:
        - 172.17.1.1/32
    - 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
```

Мы создали сетевую политику test-network-policy, которая применяет ко всем подам с label role=db. Для этих подов будут действовать правила на исходящий и входящий трафик (ingress & egress). Для входящего трафика мы одобряем доступ с:

- 172.17.0.0/16, за исключением 172.17.0.1;
- с namespaces, у которых стоит label myproject;
- с подов, у которых есть label role: frontend;

на порт 6379.
Для исходящего трафика мы одобряем доступ до 10.0.0.0/24 на порт 5978.

Полезные ссылки:

- Официальная документация
- Примеры сетевых политик
- Онлайн-редактор для сетевых политик
- Примеры политик при подготовке к CKS

Задание. Правила:

1. Окружение: После нажатия кнопки «Начать выполнение» для вас будет подготовлен Kubernetes кластер. Kubeconfig находится на первой ноде (node1) у пользователя root (/root/.kube/config). Вы так же можете использовать уже установленный kubectl на первой ноде (node1). Приведенное ниже задание следует выполнять на данном кластере.
2. Время создания: Время создания окружения составляет порядка 10 минут.
3. На выполнение задания вам будет отведено определенное время (вы увидите таймер после начала выполнения). По истечении этого времени окружение будет сброшено и вам придется повторить попытку. Количество пересдач не ограничено.
4. Также вам будут выданы переменные (если они будут нужны), которые в задании указаны в фигурных скобках, — их надо будет подставить при выполнении задания. Переменные могут отсутствовать, если они не требуются по заданию.
5. После выполнения всех пунктов задания нажмите кнопку «Отправить на проверку», и в течение ближайших 3-5 минут скрипт проверит выполнение всех условий и выставит вам оценку.
6. В случае, если вы что-то забыли, можно исправить ошибки и отправить на проверку повторно.

7. Также, если вы успешно сдали задание, но у вас остались вопросы — вы всегда сможете задать их куратору после проверки или в чате в любое удобное для вас время.

Задание:

1. Создайте Network Policy local-http в namespace default, которая будет разрешать подам из namespace default обращаться к подам из этого же namespace по порту 8080.
2. Отправьте задание на проверку.