нетология

Синхронизация секретов с внешними сервисами. Vault

Сергей
Андрюнин

Сергей Андрюнин

DevOps-инженер

RTLabs

Сергей Андрюнин

План занятия

1. Общие сведения
2. Использование
3. Итоги
4. Домашнее задание

Общие сведения

Общие сведения

- Vault может управлять секретами независимо от кластера Kubernetes;
- к Vault можно обращаться с любого модуля, с которым есть сетевая связность;
- приложение аутентифицируется на сервере Vault через токен и возвращает секрет;
- Vault имеет API, который доступен через протокол HTTP. Кроме использования утилит типа curl для разных языков имеются готовые библиотеки.

Причины: Почему? Зачем?

- нельзя хранить секрет внутри конфига сервиса;
- нельзя хранить секреты в рабочем хранилище сервиса;
- секрет доступен только во время работы контейнера;
- можно хранить некую хеш-сумму, по которой можно сверять пришедший секрет, но это проблема для исходящих подключений;
- секреты меняются и нужна история;
- секрет может быть составным;

Причины: Почему? Зачем?

- к хранилищу секретов нужен раздельный доступ пользователей, права и ключи доступа;
- централизованность: хранение, управление, доступ;
- унифицированные протоколы доступа, в том числе шифрование при передаче;
- зашифрованное хранилище секретов;
- время аренды.

Особенности

- Vault является важным сервисом;
- для Vault лучше использовать конкретный статический адрес;
- необходимо обеспечить требования безопасности.

Рекомендации

- использовать шифрованные каналы связи. Например TLS;
- уменьшить количество слоёв абстракции. Другими словами хранилище Vault по возможности должно быть единственным запущенным процессом на машине. Т.е. “«голое» железо предпочтительнее виртуальной машины, а виртуальная машина предпочтительнее контейнера;
- использовать межсетевой экран для защиты;

Рекомендации:

- после настройки отключить или ограничить доступ к машине с Vault через SSH, RDP и т.п.;
- отключить swap;
- не запускать как root, использовать непривилегированного пользователя;
- отключить дампы. Например, отключить дамп ядра;
- не использовать корневой токен. Только для первоначальной настройки, а далее отозвать;
- включить аудит. Внутренние механизмы обеспечивают историю всех операций, при этом хешируют секреты.

Предназначены для хранения конфиденциальной информации:

- пароли;
- ключи;
- токены;
- сертификаты.

Требования безопасности:

- общие требования;
- руководящие документы;
- локальные правила и распоряжения.

Использование

Запуск сервиса Vault

Базово необходимо:

- примонтировать рабочие тома;
- указать порт для прослушивания и открыть его;
- указать токен.

Пример описания модуля Vault

```
---
apiVersion: v1
kind: Pod
metadata:
  name: 14.2-netology-vault
spec:
  containers:
  - name: vault
    image: vault
    ports:
    - containerPort: 8200
      protocol: TCP
    env:
    - name: VAULT_DEV_ROOT_TOKEN_ID
      value: "TOKEN"
    - name: VAULT_DEV_LISTEN_ADDRESS
      value: 0.0.0.0:8200
```

Сервис Vault

Проверяем состояние запущенного модуля:

```
kubectl get pod 14.2-netology-vault

kubectl describe pod 14.2-netology-vault
```

Нас интересует внутренний IP, по которому мы будем подключаться.

Тестовый модуль – клиент Vault

Запускаем тестовый модуль

```
kubectl run -i --tty fedora --image=fedora --restart=Never -- sh
```

Fedora весьма интересный для работы дистрибутив и имеет свежее и стабильное программное обеспечение.

Далее нужно его немного подготовить к работе.

```
dnf -y install pip

pip install hvac
```

После установки можем запустить интерпретатор Python и перейти к проверке.

Пример доступа из Python

```
import hvac

# Подключение и проверка
client = hvac.Client(
    url='http://10.10.133.71:8200',
    token='TOKEN'
)
client.is_authenticated()

# Пишем секрет
client.secrets.kv.v2.create_or_update_secret(
    path='hvac',
    secret=dict(netology='Big secret!!!'),
)

# Читаем секрет
client.secrets.kv.v2.read_secret_version(
    path='hvac',
)
```

Итоги

Сегодня мы изучили:

- что такое сервис Vault и как его запустить;
- как подключиться к сервису Vault;
- как работать с секретами из модуля 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**.

нетология

Задавайте вопросы и пишите отзыв о лекции!

Сергей Андрюнин

Сергей Андрюнин