УДК 004

Шифрование данных в Kubernetes

Еровлева Регина Викторовна
Приамурский государственный университет имени Шолом-Алейхема
Студент

Еровлев Павел Андреевич
Приамурский государственный университет имени Шолом-Алейхема
Студент

Аннотация
В данной статье будут рассмотрены работы по выполнению шифрования данных в Kubernetes. Будет произведена настройка компонентов для шифрования. Итоговым результатом будет являться настроенное приложение с шифрацией данных.
Ключевые слова: Kubernetes, Java, Шифрование

Data Encryption in Kubernetes

Erovleva Regina Viktorovna
Sholom-Aleichem Priamursky State University
Student

Erovlev Pavel Andreevich
Sholom-Aleichem Priamursky State University
Student

Abstract
This article will cover the work on performing data encryption in Kubernetes. The components for encryption will be configured. The final result will be a customized application with data encryption.
Keywords: Kubernetes, Java, Encryption

В современных реалиях шифрование играет немаловажную роль. Ведь переданные данные не должны попасть в руки злоумышленников. Для этого во многих приложениях используется метод шифрования данных перед отправкой, передача данных и декодирование с использованием специального ключа, который злоумышленник не способен подобрать в случае кражи данных.

Kubernetes – это открытое ПО для автоматического развертывания контейнеризированных приложений.

Цель данной статьи – настроить Kubernetes для шифрования данных.

В своей работе А.А. Артамонова провела сравнительный анализ систем для автоматической контейнеризации приложений: Kubernetes и Docker [1]. Так же Д.П. Белов и И.А. Пелевин разработали методику для обеспечения отказоустойчивости микросервисных архитектур на базе Kubernetes и Docker [2]. С.П. Хиков разработал модель эффективного выбора средств сканирования изображений в Kubernetes [3]. М.С. Ивченко, В.Г. Тарасов рассмотрели Kubernetes для построения облачной платформы для запуска удаленных учебных сервисов [4]. О.О. Сергеева и А.Р. Белозерова провели сравнительный анализ потребительский сведений об аппаратной виртуализации на основе Kubernetes и Docker [5].

Для начала создадим конфигурационные файлы на компьютере куда спрячем необходимые данные (рис.1).

```
echo -n "myusername" > ./username.txt
echo -n "mypassword" > ./password.txt
```

Рисунок 1 – Создание файлов

Теперь добавим данный файлы в структуру Kubernetes (рис.2).

```
kubectl create secret generic mysecrets-file --from-
file=./username.txt --from-file=./password.txt
```

Рисунок 2 – Добавление файлов

После данных процедур проведенный выше, в окне логов будет надпись: «secret/mysecrets-file created».

Далее добавим литерал данных файлов командой (рис.3).

```
kubectl create secret generic mysecrets-literal --from-
literal=username=myusername --from-literal=password=mypassword
```

Рисунок 3 – Добавление литерала

Теперь в иерархии фалов появится файл «secret.yaml» (рис.4).

```
apiVersion: v1
kind: Secret
metadata:
  name: mysecrets
data:
  mysecret: bXl1cmw=
```

Рисунок 4 – secret.yaml

Теперь создадим ресурс, который будет производить проверку с данным файлом (рис.5).

```
kubectl apply -f secret.yaml
```

Рисунок 5 – Создание ресурса

Осталось проверить список командой «kubectl get secrets». После данной команды появится список (рис.6).

```
NAME                  TYPE                                  DATA   AGE
default-token-c5fql   kubernetes.io/service-account-token   3
5m21s
mysecrets             Opaque                                1      16s
mysecrets-file        Opaque                                2      64s
mysecrets-literal     Opaque                                2      50s
```

Рисунок 6 – Список данных

Шифр, который начинается с «default-token» — это специальный ключ, сгенерированный Kubernetes, чтобы разрешить внутренним службам доступ к серверу API.

Теперь проверим настройки файла «mysecrets-file» и убедимся, что сообщение зашифровано в base64 (рис.7).

```
apiVersion: v1
data:
  mysecret: bXl1cmw=
kind: Secret
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","data":
{"mysecret":"bXl1cmw="},"kind":"Secret","metadata":{"annotations":
{},"name":"mysecrets","namespace":"default"}}
  creationTimestamp: "2022-02-22T20:30:07Z"
  managedFields:
  - apiVersion: v1
    fieldsType: FieldsV1
    fieldsV1:
      f:data:
        .: {}
        f:mysecret: {}
      f:metadata:
        f:annotations:
          .: {}
          f:kubectl.kubernetes.io/last-applied-configuration: {}
      f:type: {}
    manager: kubectl-client-side-apply
    operation: Update
    time: "2022-02-22T20:30:07Z"
  name: mysecrets
  namespace: default
  resourceVersion: "958"
  uid: 08ed4643-470c-46f9-8a60-b174eddf0b1e
type: Opaque
```

Рисунок 7 – Настройки файла

Теперь все данные, поступающие в Kubernetes будут так же шифроваться.

В данной статье был рассмотрен процесс реализации шифрования, данный в k8s.

Библиографический список

1. Артамонова А.А. Сравнительный анализ двух систем управления контейнерами: docker swarm и kubernetes // Синергия наук. 2018. №23. С. 1173-1182.
2. Белов Д.П., Пелевин И.А. Реализация отказоустойчивости в системе оркестрации микросервисной архитектуры kubernetes // Вестник УРФО. безопасность в информационной сфере. 2019. №2(32). С. 5-11.
3. Хиков С.П. Модель выбора эффективного средства сканирования изображений контейнеров в инфраструктуре kubernetes // Инновационные технологии: теория, инструменты, практика. 2019. №1. С. 249-253.
4. Ивченко М.С., Тарасов В.Г. Использование kubernetes для построения

облачной платформы для удаленного запуска учебных сервисов // Информационные технологии в науке, промышленности и образовании. 2020. С.107-109.

5. Сергеева О.О., Белозерова А.Р. Kubernetes с docker на локальной машине // Вестник димитровградского инженерно-технологического института. 2020. №1(21). С. 44-53.