Обновление сертификатов платформы

1. Обновление сертификатов, выпущенных в StarVault

Обновление сертификатов Nova Container Platform, выпущенных в StarVault, выполняется администратором кластера с помощью утилиты `nova-ctl`.

Процесс обновления затрагивает только серверные и клиентские сертификаты узлов платформы. Обновление сертификатов корневых центров в настоящий момент не поддерживается и находится в разработке.

В процессе обновления сертификатов на мастер-узлах платформы выполняется перезапуск следующих сервисов:

- Сервер Kubernetes API
- Сервер Kubernetes Controller Manager
- Сервер Kubernetes Scheduler
- Компоненты CNI
- Kubelet

На инфраструктурных и рабочих узлах выполняется перезапуск следующих сервисов:

- Компоненты CNI
- Kubelet

В ходе перезапуска данных сервисов может наблюдаться кратковременная недоступность компонентов Nova Container Platform.

Необходимые условия

- ✓ У вас есть закрытый ключ SSH на вашем локальном компьютере, который нужно предоставить утилите `nova-ctl`.
- ✓ У вас есть токен доступа к хранилищу секретов StarVault с привилегиями `root`.

Процедура

Для обновления сертификатов выполните следующую команду:

```bash
nova-ctl certs renew --ssh-user ec2-user --ssh-key key.pem
```

В качестве аргументов `--ssh-key` и `--ssh-user` укажите информацию, использованную на этапе конфигурации ключевой пары SSH.

Пример

```bash
$ nova-ctl certs renew --ssh-user ec2-user --ssh-key key.pem
Are you sure you want to renew all the certificates in the cluster? (yes/no)
[no] yes

Enter Vault root token: ******************

 ■ Setting up secrets store access... done
 ■ Renewing certificates on master-nova-internal... done
 ■ Renewing certificates on infra-nova-internal... done
 ■ Renewing certificates on worker-nova-internal... done
 ■ Downloading new Kubernetes configuration..... done

All certificates are renewed.
New Kubernetes client configuration is saved to kubeadmin.conf.
```

2. Обновление сертификатов, выпущенных в Cert-Manager

Обновление сертификатов Nova Container Platform, выпущенных в Cert-Manager, может быть выполнено принудительно администратором кластера с помощью утилиты `kubectl`.

Для принудительного обновления любого сертификата необходимо удалить секрет, в котором сохранены данные сертификата. Cert-Manager автоматически перевыпустит сертификат и сохранит его в секрет с прежним именем.

Процедура

Для принудительного обновления сертификата выполните следующую команду:

```bash
kubectl get certificate custom-dynamic-cert -n custom-namespace -
o=jsonpath='{.spec.secretName}' | xargs kubectl delete secret -n custom-
namespace
```

где `custom-dynamic-cert` - имя вашего сертификата, `custom-namespace` - имя пространства имен (namespace), в котором находится ваш сертификат.

Пользовательские сертификаты для Ingress-ресурсов

При установке Nova Container Platform вы можете указать цепочку сертификатов собственного центра сертификации, которая будет использована в ходе установки Nova Container Platform для инициализации центра сертификации `nova-kubernetes-pki-ingress`. Данный центр сертификации используется по умолчанию в платформе для всех Ingress-ресурсов.

1. Предварительные условия

- ✓ Вы ознакомились с блоком конфигурации параметров собственного CA-сертификата.
- ✓ Вы подготовили сертификат корневого центра сертификации в формате `pem`.
- ✓ Вы подготовили сертификат промежуточного центра сертификации в формате `pem` со сроком действия не менее двух лет с текущей даты.
- ✓ Вы подготовили зашифрованный приватный ключ промежуточного центра сертификации.

При подготовке сертификата промежуточного центра сертификации, рекомендуется ограничить возможность подписи этим сертификатом других промежуточных центров сертификации параметром `pathlen` с помощью стандартных расширений `basicConstraints = critical, CA:true, pathlen:0`.

2. Подготовительные действия

Если приватный ключ промежуточного центра сертификации не зашифрован, то необходимо выполнить его шифрование.

Пример

BASH

```
openssl rsa -in intermediateCA/private/intermediate.key.pem -aes256 -out
intermediateCA/private/intermediate.key.pem.crypted

writing RSA key
Enter pass phrase:
```

На запрос `Enter pass phrase:` введите парольную фразу.

На этапе запуска установки Nova Container Platform вам будет необходимо указать парольную фразу для продолжения установки.

Пример

```bash
nova-ctl bootstrap --ssh-key key.pem --ssh-user nova-installer
Enter ingress CA key passphrase:
```

Сертификаты корневого и промежуточного центров сертификации, а также приватный ключ промежуточного центра сертификации передаются в виде строки с данными, закодированными в base64.

Закодируйте сертификаты и приватный ключ промежуточного центра сертификации в base64.

Пример

```bash
cat rootCA/certs/ca.cert.pem | base64 -w0
cat intermediateCA/certs/intermediate.cert.pem | base64 -w0
cat intermediateCA/private/intermediate.key.pem.crypted | base64 -w0
```

3. Пример файла конфигурации установки

Ниже представлен пример файла конфигурации установки Nova Container Platform с использованием собственного центра сертификации для выпуска сертификатов Ingress-ресурсов.

Пример

```yaml
apiVersion: "config.nova-platform.io/v1alpha4"
kind: "Infrastructure"
metadata:
  name: "cluster"
spec:
  customerID: "5d4a2c84b6e22323"
  licenseKey: "a098f0aefdc022b643c2eb76c1cad0a8"
  version: "v6.0.1"
  infrastructureProvider:
    none: {}
  clusterNodes:
    master:
      - networkSpec:
          ip: "172.31.101.24"
          hostname: "master.mycompany.local"
        state: "present"
    worker:
```

```
      - networkSpec:
          ip: "172.31.101.25"
          hostname: "worker.mycompany.local"
        state: "present"
    infra:
      - networkSpec:
          ip: "172.31.101.26"
          hostname: "infra.mycompany.local"
        state: "present"
    ingress:
      - networkSpec:
          ip: "172.31.101.27"
          hostname: "ingress.mycompany.local"
        state: "present"
  clusterConfiguration:
    dnsBaseDomain: "nova.mycompany.local"
    extraOptions:
      ingressTLSConfig:
        externalCA:
          tlsConfig:
            ca: "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tC.." ①
            cert: "LS0tLS1CRUdJTiBDRVJdGbUSUdmMyTnZkek.." ②
            key: "LS0tLS1CRUdJTiBFTkNSWVBURUQgUFJJVkFU.." ③
```

① Сертификат корневого центра сертификации, закодированный в base64.

② Сертификат промежуточного центра сертификации, закодированный в base64.

③ Зашифрованный приватный ключ промежуточного центра сертификации, закодированный в base64.

4. Следующие шаги

Вы можете перейти к установке платформы Nova Container Platform.

- Универсальная установка Nova Container Platform для различных сред
- Установка Nova Container Platform в среде zVirt
- Установка Nova Container Platform в среде VMware vSphere

История изменений

История изменений отражает хронологию развития платформы Nova Container Platform: расширение функциональности, изменения, исправления ошибок и другие обновления.

v3.1.10

▶ Описание обновления

v3.1.9

▶ Описание обновления

v3.1.8

▶ Описание обновления

v3.1.7

▶ Описание обновления

v3.1.6

▶ Описание обновления

v3.1.5

▶ Описание обновления

v3.1.4

▶ Описание обновления

v3.1.3

▶ Описание обновления

v3.1.2

▶ Описание обновления

v3.1.1

▶ Описание обновления

v3.1.0

▶ Описание обновления

v3.0.1

▶ Описание обновления

v3.0.0

▶ Описание обновления