# Организация инфраструктуры PKI в Nova Container Platform

В Kubernetes SSL/TLS сертификаты используются в различных сценариях для решения следующих задач:

- защита веб-трафика внутри кластера и за его пределами.
- дополнительная TLS-аутентификация между компонентами Kubernetes.

Следующие операции в среде Kubernetes требуют наличия инфраструктуры PKI:

- Клиентские сертификаты *Kubelet* необходимы для взаимодействия с *Kubernetes API*.
- Серверные сертификаты *Kubelet* необходимы *Kubernetes API* для взаимодействиями с *Kubelet* на узлах кластера.
- Серверные сертификаты необходимы для взаимодействия с *Kubernetes API*.
- Клиентские сертификаты администраторов кластера необходимы для взаимодействия с *Kubernetes API*.
- Клиентские сертификаты *Kubernetes API* необходимы для взаимодействиями с *Kubelet* на узлах кластера.
- Клиентские сертификаты *Kubernetes API* необходимы для взаимодействиями с хранилищем *Etcd*.
- Клиентские сертификаты *Controller Manager* необходимы для взаимодействиями с *Kubernetes API*.
- Клиентские сертификаты *Scheduler* необходимы для взаимодействиями с *Kubernetes API*.
- Клиентские сертификаты необходимы для компонента Kubernetes *Front Proxy*.
- Клиентские и серверные сертификаты ресурсов *Ingress* необходимы для взаимодействия пользователей платформы с опубликованными веб-ресурсами.

В хранилище *Etcd* также используется механизм взаимной TLS-аутентификации (mTLS) для клиентов и участников кластера.

В Nova Container Platform все необходимые для Kubernetes и компонентов платформы сертификаты создаются автоматически в StarVault и впоследствии могут быть автоматически или принудительно обновлены.

## 1. Архитектура PKI

Выпуск и управление требуемыми сертификатами осуществляется в *StarVault* с использованием движка *PKI Secrets Engine*. Данный движок позволяет не только динамически генерировать X.509 сертификаты, но также и организовывать центры сертификации (CA), обслуживать базы данных сертификатов, управлять процессами отзыва, а также применять политики сертификатов.

## 1.1. Центры сертификации

Центры сертификации в StarVault делятся на корневые и промежуточные:

- Корневые CA создаются по принципу Single root CA для каждого глобального блока платформы (Kubernetes, Etcd, Kubernetes Front Proxy и т.п.).
- Промежуточные CA используются в платформе более гранулярно, разделяя взаимодействие компонентов глобального блока платформы (Kubernetes API, Kubelet, Controller Manager и т.п.).

### 1.1.1. Корневые центры сертификации

В Nova Container Platform используется следующие корневые центры сертификации:

| Имя | Default CN | TTL | Описание |
|---|---|---|---|
| `nova-etcd-pki-root` | `etcd-ca-root` | 10 лет | Корневой CA для хранилища Etcd. |
| `nova-kubernetes-pki-root` | `kubernetes-ca-root` | 10 лет | Корневой CA для инфраструктуры Kubernetes. |

### 1.1.2. Промежуточные центры сертификации

В Nova Container Platform используется следующие промежуточные центры сертификации:

| Имя | Default CN | Родительский CA | TTL | Описание |
|---|---|---|---|---|
| `nova-etcd-pki-int` | `etcd-ca-int` | `nova-etcd-pki-root` | 5 лет | Промежуточный CA для хранилища Etcd. Применяется для выпуска сертификатов (Etcd Client). |

| Имя | Default CN | Родительский CA | TTL | Описание |
| --- | --- | --- | --- | --- |
| `nova-etcd-pki-peer` | `etcd-ca-peer` | `nova-etcd-pki-root` | 5 лет | Промежуточный CA для хранилища Etcd. Применяется для выпуска сертификатов (Etcd Peer). |
| `nova-kubernetes-pki-int` | `kubernetes-ca` | `nova-kubernetes-pki-root` | 5 лет | Промежуточный CA для инфраструктуры Kubernetes. Применяется для выпуска сертификатов компонентов Kubernetes Control Plane. |
| `nova-kubernetes-pki-kubelet` | `kubernetes-kubelet-ca` | `nova-kubernetes-pki-root` | 5 лет | Промежуточный CA для инфраструктуры Kubernetes. Применяется для выпуска сертификатов компонента Kubelet. |
| `nova-kubernetes-pki-ingress` | `kubernetes-ingress` | `nova-kubernetes-pki-root` | 5 лет | Промежуточный CA для инфраструктуры Kubernetes. Применяется для выпуска сертификатов для ресурсов Ingress. Интегрирован с компонентом CertManager через ресурс *ClusterIssuer* `nova-oauth-internal-cluster-issuer`, а также может быть инициализирован с помощью пользовательского промежуточного сертификата. |

| Имя | Default CN | Родительский CA | TTL | Описание |
| --- | --- | --- | --- | --- |
| `nova-kubernetes-pki-signer` | `kubernetes-signer-ca` | `nova-kubernetes-pki-root` | 5 лет | Промежуточный CA для инфраструктуры Kubernetes. Применяется для выпуска сертификатов компонентом Controller Manager при использовании Certificates API. Интегрирован с компонентом CertManager через ресурс *ClusterIssuer* `nova-dynamic-internal-cluster-issuer` для автоматизированного выпуска сертификатов компонентов Kubernetes Admission Webhook. |
| `nova-kubernetes-pki-front-proxy` | `kubernetes-front-proxy-ca` | `nova-kubernetes-pki-root` | 5 лет | Промежуточный CA для инфраструктуры Kubernetes. Используется в Kubernetes Front Proxy, применяется для выпуска сертификатов компонентов, расширяющих возможности Kubernetes API. |

## 1.2. Политики выпуска сертификатов

Для обеспечения дополнительной безопасности процесса выпуска сертификатов в StarVault для каждого PKI автоматически настраиваются определенные политики выпуска (роли) сертификатов. Данные роли контролируют различные параметры выпускаемых сертификатов, например:

- Тип используемого криптографического алгоритма для ключей шифрования
- Разрешение на выпуск wildcard-сертификатов

- Правила проверки Common Name
- TTL
- Разрешенные домены
- Разрешение на добавление в сертификаты IP и DNS Sans и их перечень.
- Правила расширенного использования ключа (Extended Key Usage)

Каждая роль содержит только те параметры, которые требуются тому или иному компоненту согласно лучшим практикам Kubernetes. Таким образом, выпуск сертификата без строгого соответствия данным параметрам невозможен.

Некоторые параметры сертификатов в ролях являются динамическими и различаются в кластерах Nova Container Platform. При установке платформы `nova-ctl` генерирует данные параметры, используя данные конфигурационного манифеста, а затем выполняет инициализацию StarVault.

## 1.3. Расположение сертификатов

Корневые и промежуточные центры сертификации, создаваемые в StarVault, не являются экспортируемыми. Это означает, что сгенерированные приватные ключи CA сохраняются в StarVault в зашифрованном виде и впоследствии не могут быть получены.

На узлах кластера Kubernetes находятся выпущенные сертификаты и приватные ключи для компонентов Kubernetes в следующих директориях и файлах:

- `/opt/nova/conf.d/pki/`
- `/opt/nova/conf.d/pki/etcd/`

# 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 Nova API
- Сервер Nova Controller Manager
- Сервер Nova 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.