Управление сертификатами

Данный раздел содержит статьи описывающие управление сертификатами в Nova Container Platform.

1. Содержание раздела

Управление секретами платформы

Данный раздел содержит статьи полезные для управления секретами в Nova Container Platform.

1. Подключение к StarVault

Для выполнения различных задач по администрированию аутентификации и авторизации в Nova Container Platform требуется подключение к StarVault с привилегиями администратора.

Вы можете получить адрес и подключиться к StarVault, используя процедуру ниже.

Необходимые условия

- ✓ У вас есть токен доступа к хранилищу секретов StarVault или учетная запись с привилегиями `root`.
- ✓ У вас есть доступ к Kubernetes API с привилегиями администратора кластера.

Процедура

1. Получите адрес StarVault:

   ▸ **Web UI**

   ▸ **CLI**

2. Перейдите по полученному адресу и авторизуйтесь в StarVault, указав токен доступа к хранилищу секретов StarVault или параметры собственной учетной записи с привилегиями `root`.

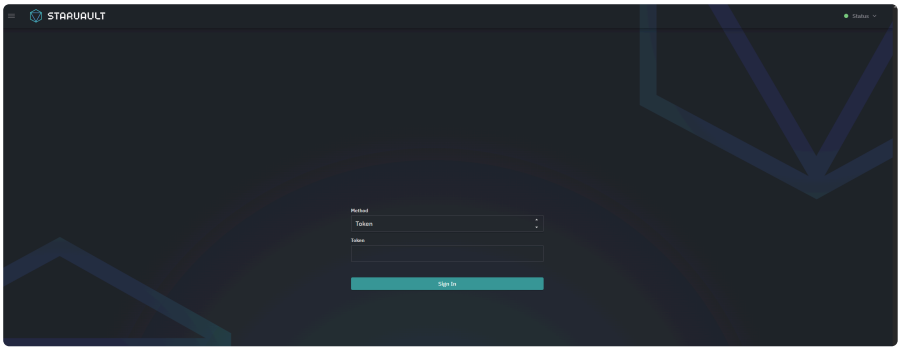

Рисунок 1. Страница входа в StarVault

2. Приложения OAuth

Данный раздел содержит статьи полезные для управления OAuth приложениями в Nova Container Platform.

2.1. Настройка доступа к приложениям OAuth

Доступ к каком-либо компоненту Nova Container Platform для конечного пользователя выполняется по протоколу OpenID Connect (OIDC). Поскольку StarVault является основным OIDC-провайдером в платформе, то для доступа к приложениями, зарегистрированным в StarVault, необходимо выполнить процедуру назначения приложения определенной группе пользователей или конкретным пользователям.

2.1.1. Настройка назначений

Для настройки назначения приложений воспользуйтесь процедурой ниже.

1. Откройте веб консоль Vault.
2. Перейдите в раздел **Access**, далее **OIDC Provider**.
3. Перейдите в список **Assignments** и нажмите **Create assignment**.
    - В поле **Name** укажите имя назначения. Это может быть, например, имя группы пользователей в каталоге LDAP-сервера.
    - В поле **Entities** укажите ранее созданные сущности пользователей.
    - В поле **Groups** укажите ранее созданную группу.
    - Нажмите **Create**, чтобы создать назначение.

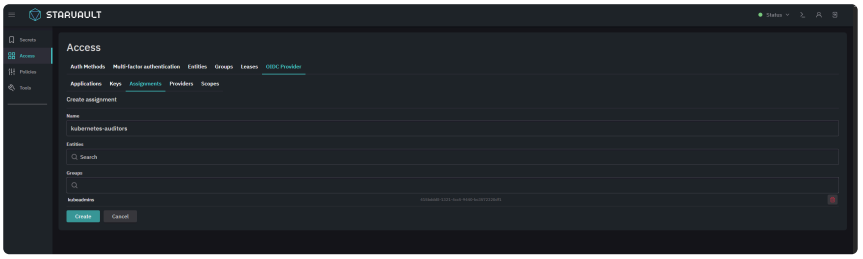

Рисунок 2. Настройка назначений в StarVault

2.1.2. Привязка назначений к приложениям

Для привязки назначения к приложению воспользуйтесь процедурой ниже.

1. Откройте веб консоль Vault.
2. Перейдите в раздел **Access**, далее **OIDC Provider**.
3. Перейдите в список **Applications** и выберете необходимое приложение. Например, для добавления пользователям возможности выполнять аутентификацию в утилите kubectl

или веб-интерфейсе Nova Console, выберете приложение `oidc-kubernetes-client`.

- Нажмите **Edit application**.
- В разделе **Assign access** добавьте ранее настроенное назначение в список разрешенных.
- Нажмите **Update**, чтобы обновить параметры назначения.

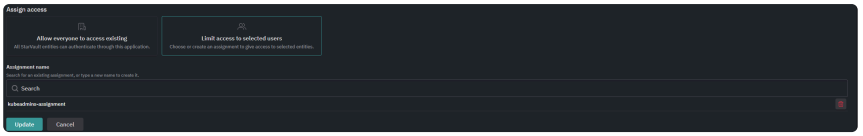

Рисунок 3. Настройка назначений в StarVault

2.2. Настройка доступа до OAuth приложений с использованием LDAP

В данном разделе описывается процедура использования провайдера идентификации в *StarVault* по протоколу LDAP для доступа к OAuth приложениям на примере **NeuVector**.

2.2.1. Необходимые условия

- ✓ У вас есть токен доступа к хранилищу секретов *StarVault* с привилегиями `root`.
- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Модуль NeuVector установлен в вашем кластере.
- ✓ Провайдер идентификации LDAP подключен в *StarVault*.

2.2.2. Настройка доступа в StarVault

1. В веб-интерфейсе StarVault выберите вкладку **Access**, далее **Groups**.
2. Создайте группу и алиас.
   - Нажмите **Create group**.
     - В поле **Name** укажите имя группы так же, как группа названа в каталоге LDAP-сервера.
     - В поле **Type** укажите **External**.
     - Нажмите **Create**, чтобы создать группу. Откроется страница с параметрами созданной группы.
   - Нажмите **Add alias**.
     - В поле **Name** укажите имя алиаса так же, как группа названа в каталоге LDAP-сервера.
     - В поле **Auth Backend** выберете имя метода аутентификации LDAP.

- Нажмите **Create**, чтобы создать алиас.

Для удобства и простоты администрирования рекомендуется использовать один алиас на одну сущность StarVault.

3. В веб-интерфейсе StarVault перейдите на вкладку **Access → OIDC Provider → Assignments**.
4. Нажмите **Create assignment**
   - В поле **Name** укажите любое имя, например название приложения к которому предоставляется доступ.
   - В поле **Groups** выберите группу созданную ранее.
   - Нажмите **Create**.
5. Перейдите на вкладку **Access → OIDC Provider → Applications**.
   - Выберите нужное приложение. В нашем случае `oidc-auth-neuvector`.
   - Нажмите **Edit application**
   - В поле **Assignment name** выберите ранее созданный Assignment.
   - Нажмите **Update**.
6. Перейдите на вкладку **Access → OIDC Provider → Scopes**.
   - Нажмите на **Edit** у параметра `email`.
   - Измените значение на `{ "email": {{identity.entity.name}} }`
   - Нажмите **Update**

2.2.3. Настройка доступа в NeuVector

1. В веб-интерфейсе Nova Container Platform выберите вкладку **Ресурсы**, далее **Secrets**.
2. Скопируйте значение `oidcinitcfg.ctmpl` из секрета `neuvector-init-template`.
3. Перейдите на вкладку **Администрирование → CustomResourceDefinitions** и выберите **Kustomization**
4. Перейдите на вкладку **Инстансы** и выберите `nova-release-neuvector-main`
5. На вкладке **YAML** добавьте патч в блок **spec**. Значение файла `oidcinitcfg.ctmpl` должно быть аналогичным значению из пункта 2.
   В блок **group_mapped_roles** добавьте соответствие нужной группы и роли.

Всего в NeuVector есть 3 группы по умолчанию.

- admin
- reader
- ciops

Пример

```yaml
patches:
  - patch: |-
      kind: Secret
      apiVersion: v1
      metadata:
        name: neuvector-init-template
        namespace: nova-neuvector
      stringData:
        oidcinitcfg.ctmpl: |
          {{- with secret "identity/oidc/provider/nova" }}
          always_reload: false
          Issuer: {{ .Data.issuer }}
          {{- end -}}
          {{ with secret "identity/oidc/client/oidc-auth-neuvector" }}
          Client_ID: {{ .Data.client_id }}
          Client_Secret: {{ .Data.client_secret }}
          {{ end -}}
          GroupClaim: groups
          Scopes:
            - openid
            - profile
            - email
            - groups
          Enable: true
          Default_Role:
          group_mapped_roles:
            - group: kubeadmins ①
              global_role: admin
            - group: global-admins ②
              global_role: admin
          group_claim: groups
    target:
      kind: Secret
      name: neuvector-init-template
      namespace: nova-neuvector
```

1. Настройка доступа для kubeadmins. Изменять не нужно.
2. Пример добавления группы с определённой ролью.

2.2.4. Проверка

1. Убедитесь, что под `neuvector-controller-pod-0` работает.
2. Зайдите в веб-интерфейс NeuVector с использованием LDAP подключения.