CLI

Данный раздел содержит информацию по консольным инструментам управления (CLI) в Nova Container Platform.

1. Перечень инструментов управления CLI

Следующий набор инструментов CLI доступен в Nova Container Platform:

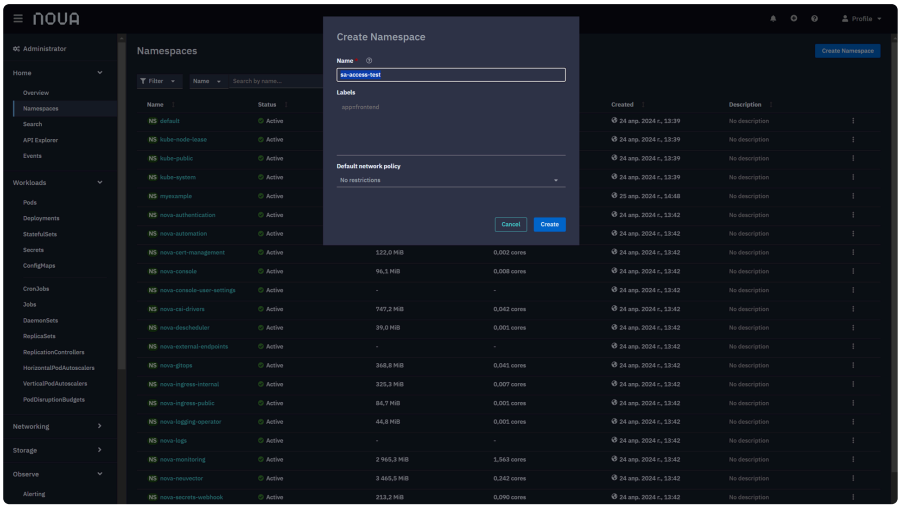
- Nova CLI (nova-ctl): Инструмент управления кластерами Nova Container Platform, с помощью которого администраторы платформы могут выполнять операции по созданию новых кластеров, а также масштабированию или обновлению существующих кластеров.
- Kubernetes CLI (kubectl): Наиболее часто используемый инструмент CLI в Nova Container Platform. Он помогает как администраторам кластеров, так и разработчикам выполнять операции от начала и до конца с помощью терминала.
- FluxCD CLI (flux): Инструмент автоматизированного и декларативного управления инфраструктурой. Он позволяет управлять объектами FluxCD - решения, используемого для непрерывной интеграции и непрерывного развертывания (CI/CD) в Nova Container Platform.

2. Содержание раздела

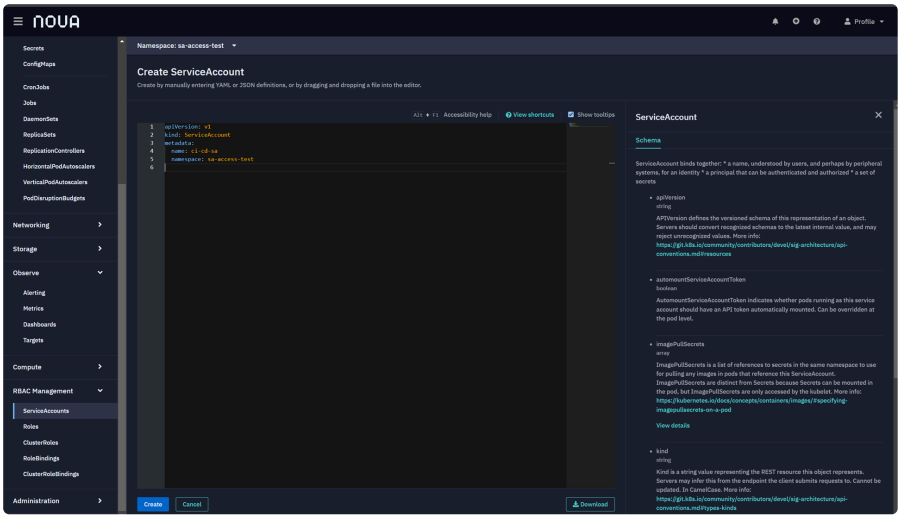
- nova-ctl
- kubectl
- velero

Создание учетной записи для не интерактивного доступа (CI\CD, автоматизация)

1. Если у вас уже есть *Namespace*, к которому будет выдаваться доступ, то переходите к следующему шагу. Если нет, то откройте страницу *Home* → *Namespaces* и нажмите *«Create Namespace»*.
   В открывшемся окне введите имя и по желанию добавьте метки\сетевую политику, после чего нажмите *«Create»*:

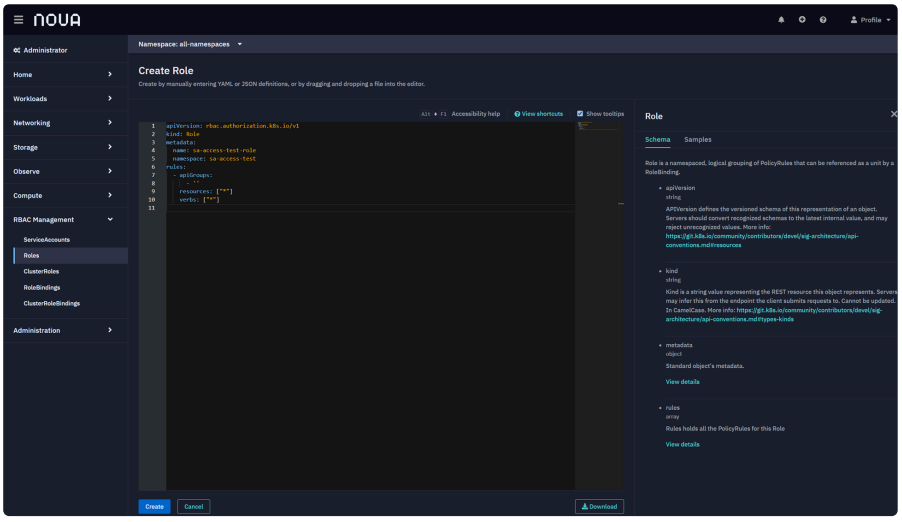


2. Необходимо создать сервисную учетную запись. Для этого, открываете страницу *RBAC Management* → *ServiceAccounts* и нажмите *«Create ServiceAccount»*.
   В открывшемся окне введите имя и namespace из п.1 и нажмите *«Create»*:

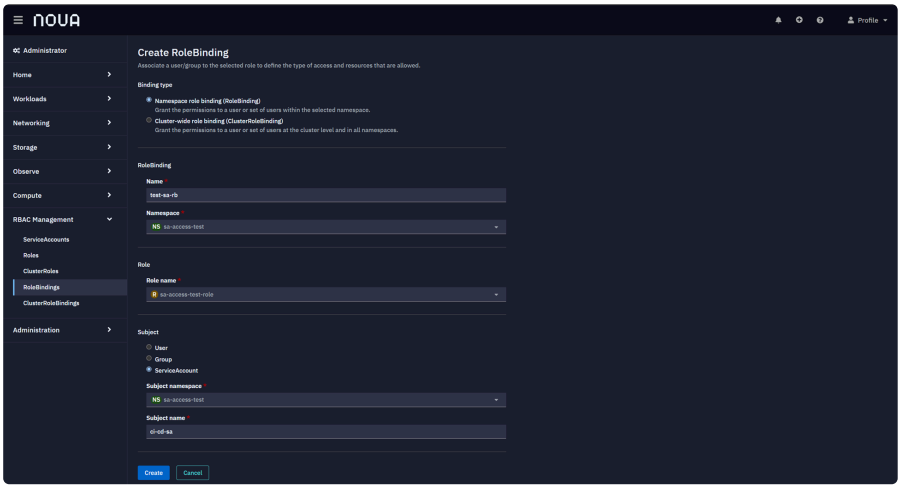


3. Далее необходимо создать роль, которой будет обладать сервисная учетная запись.
   Если у вас уже есть роль, то переходите к следующему шагу.
   Чтобы создать роль откройте страницу *RBAC Management* → *Roles* и нажмите *«Create*

Role». В открывшемся окне введите имя, *namespace* из п.1 и правила. Нажмите *«Create»*:



4. Далее необходимо связать роль с сервисной учетной записью. Для этого откройте страницу *RBAC Management* → *RoleBindings* и нажмите *«Create Binding»*.
   В открывшемся окне выберите *Binding type* (в данной демонстрации это *Namespace role binding*, но вы так же можете привязать роль для всего кластера), введите имя для *RoleBinding*, выберите namespace (из п.1) из выпадающего списка. Затем, выберите роль, созданную на предыдущем шаге, а в качестве *Subject* выберите *ServiceAccount*, namespace из п.1 и имя сервисной учетной записи из п.2. Нажмите *«Create»*:



5. Далее нам нужно создать токен для аутентификации. Для этого нажмите *“+”* в правом верхнем углу и в открывшемся окне вставьте следующий манифест, убедившись, что namespace и имя аккаунта в блоке `annotations` совпадают с вашими:

```yaml
apiVersion: v1
kind: Secret
type: kubernetes.io/service-account-token
metadata:
  name: ci-cd-sa-token
  namespace: sa-access-test
  annotations:
    kubernetes.io/service-account.name: ci-cd-sa
```

6. Теперь вы можете получить аутентификационную информацию для данного сервисного аккаунта. Для этого откройте страницу *Workloads* → *Secrets* и выберите секрет из п.5. Из раздела *data* скопируйте *ca.crt* и *token* и закодируйте значение сертификата в *base64* (вместо кодирования в *base64* можно перейти на вкладку *YAML* и скопировать уже закодированное значение. При этом, у значения *ca.crt* необходимо удалить последние 4 символа `«Cg==»`)

7. Для доступа к API с помощью HTTP-запроса сохраните *ca.crt* в файл, токен из п.6 в переменную *TOKEN* и неймспейс из п.1 в переменную *NAMESPACE*.
   Теперь выполните следующую команду подставив вместо `<адрес_мастер_узла>` IP или DNS вашего мастер-узла:
   `curl --cacert cert.crt -H "Authorization: Bearer $TOKEN" "https://<адрес_мастер_узла>:6443/api/v1/namespaes/$NAMESPACE/pods/"`

8. Для доступа к кластеру с помощью утилиты `kubectl` вам необходимо создать конфиг файл. Для этого в шаблоне замените значения `<ca.crt_из_секрета>` и `<токен_из_секрета>` на данные из п.6, `<имя_сервисного_аккаунта>` на имя из п.2, `<адрес_мастер_узла>` на IP или FQDN вашего мастер-узла

```yaml
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <ca.crt_из_секрета>
    server: https://<адрес_мастер_узла>:6443
  name: nova-kubernetes-cluster
contexts:
- context:
    cluster: nova-kubernetes-cluster
    user: <имя_сервисного_аккаунта>
  name: default
current-context: default
kind: Config
preferences: {}
users:
- name: <имя_сервисного_аккаунта>
  user:
    token: <токен_из_секрета>
```

Доступ к Nova Console и kubectl

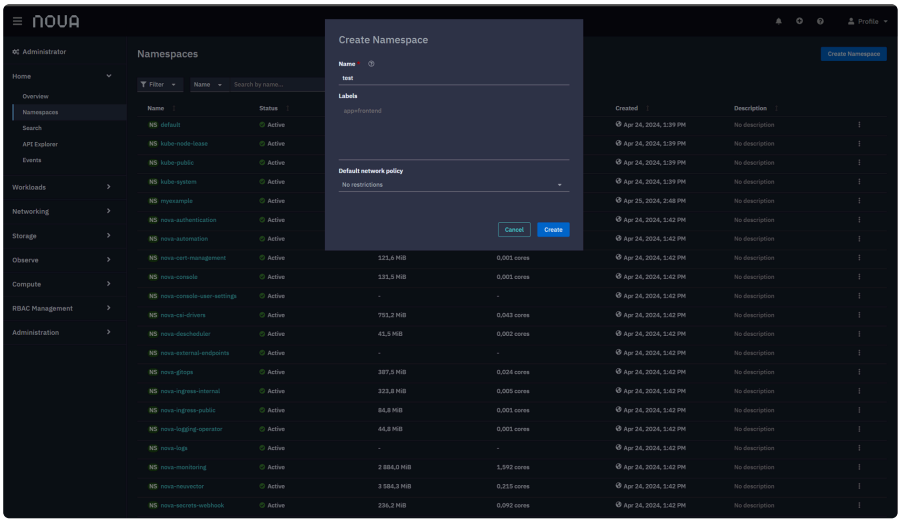
Доступ к Nova Console и API разграничивается при помощи *Roles* и *ClusterRoles*. Роли ассоциируются с пользователями и группами провайдера идентификации при помощи *RoleBindings* и *ClusterRoleBindings*. Управление данным функционалом осуществляется при помощи Nova Console или `kubectl`.

1. Предварительные условия

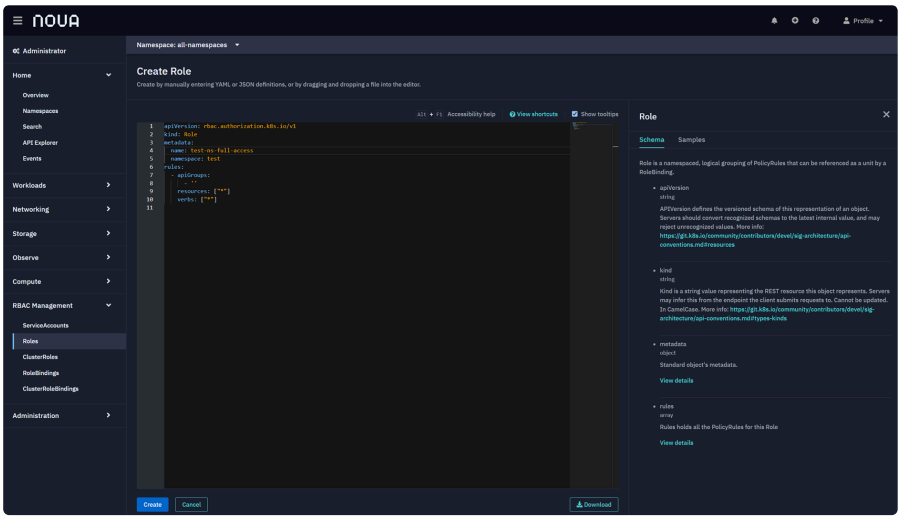
- создан пользователь в провайдере идентификации (StarVault), данный пользователь добавлен в группу и для группы создан Assignment, который добавлен в приложение `oidc-kubernetes-client` (процесс описан в Доступ к компонентам платформы по OIDC)

2. Сценарий 1 – выдача прав для конкретного пространства имен (подходит для команды проекта или отдельных разработчиков)

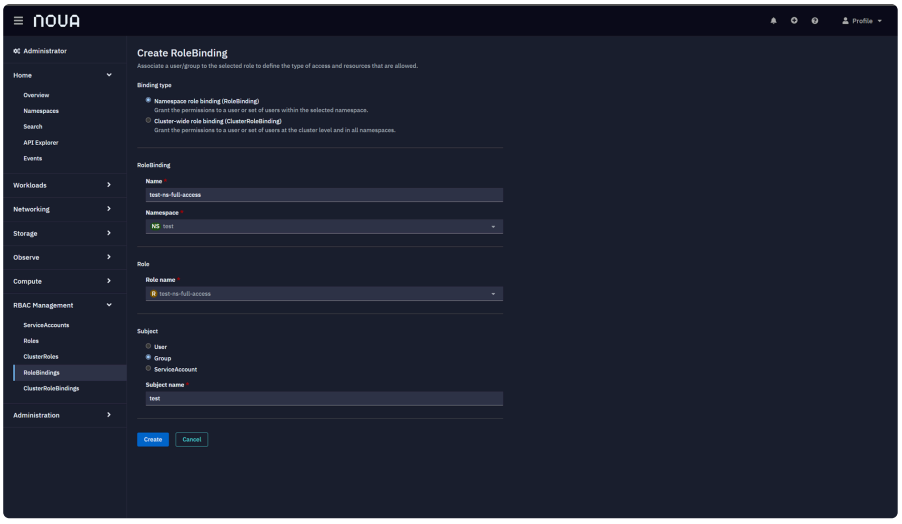
1. Откройте в браузере веб-интерфейс консоли управления (GUI Nova Console) и авторизоваться с использованием учетной записи администратора
2. Если у вас уже есть *Namespace*, к которому будет выдаваться доступ, то переходите к следующему шагу. Если нет, то откройте страницу *Home* → *Namespaces* и нажмите *«Create Namespace»*.
   В открывшемся окне введите имя и по желанию добавьте метки\сетевую политику, после чего нажмите *«Create»*:



3. Далее необходимо создать роль, которой будет обладать пользователь\группа. Если у вас уже есть роль, то переходите к следующему шагу.
   Чтобы создать роль откройте страницу *RBAC Management* → *Roles* и нажмите *«Create Role»*. В открывшемся окне введите имя, namespace из п.2 и правила. Нажмите *«Create»*. В данном примере мы создаем роль с полным доступом ко всем ресурсам пространства имен `test`. Подробнее про разграничение доступа K8S.



4. Далее необходимо связать роль с пользователем или группой пользователей. Для этого откройте страницу *RBAC Management* → *RoleBindings* и нажмите *«Create Binding»*. В открывшемся окне выберите Namespace *role binding* в качестве *Binding type*, введите имя для *RoleBinding*, выберите *namespace* (из п.2) из выпадающего списка. Затем, выберите роль, созданную на предыдущем шаге, а в качестве *Subject* выберите *Group* и введите имя группы, созданной на подготовительном этапе. Нажмите *«Create»*:

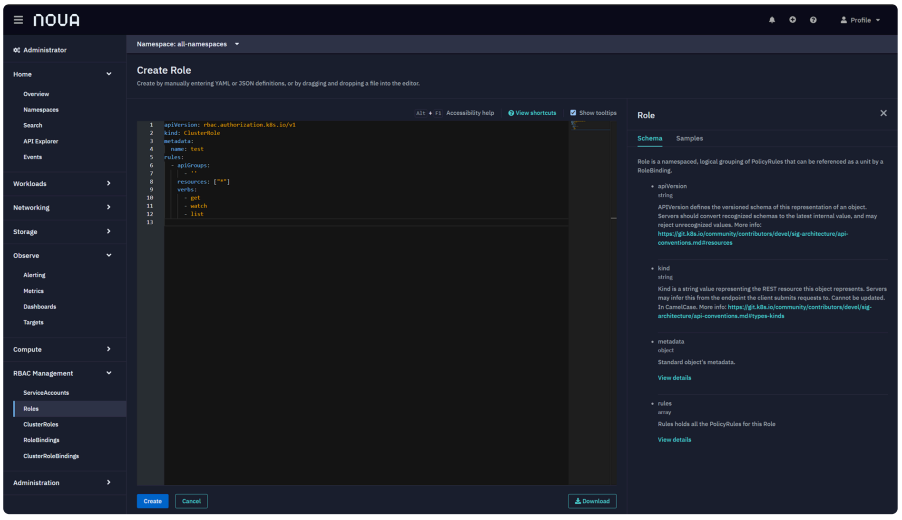


5. Теперь все члены группы имеют полный доступ к пространству имен из п.2 через Nova Console и `kubectl`. Для доступа с помощью утилиты `kubectl` произведите настройку согласно инструкции.

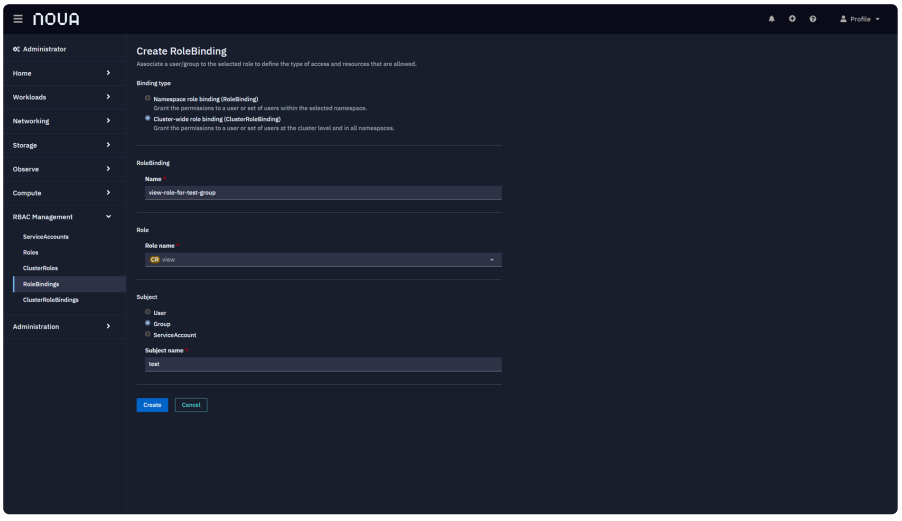
3. Сценарий 2 – выдача прав для всего кластера (подходит для учетных записей администраторов

или пользователей с правом только просмотра)

1. Сначала, необходимо создать роль, которой будет обладать пользователь/ группа или использовать уже имеющуюся.
   Чтобы создать роль откройте страницу *RBAC Management* → *Roles* и нажмите *«Create Role»*. В открывшемся окне введите имя и необходимые правила. Нажмите *«Create»*. По умолчанию уже созданы роли администратора (*admin*) и пользователя с правами просмотра (*view*). Далее мы будем использовать роль *view*, которая наделяет пользователя правами на просмотр всех ресурсов кластера. Подробнее про разграничение доступа K8S.



2. Далее необходимо связать роль с пользователем или группой пользователей. Для этого откройте страницу *RBAC Management* → *ClusterRoleBindings* и нажмите «Create Binding». В открывшемся окне выберите *Cluster-wide role binding (ClusterRoleBinding)* в качестве *Binding type*, введите имя для *RoleBinding*, выберите роль, созданную на предыдущем шаге или одну из преднастроенных, а в качестве *Subject* выберите *Group* и введите имя группы, созданной на подготовительном этапе. Нажмите *«Create»*:



3. Теперь все члены группы имеют доступ на чтение ко всем ресурсам кластера через Nova Console и `kubectl`. Для доступа с помощью утилиты `kubectl` произведите настройку согласно инструкции.