Настройка регистрации и управления доступом

1. Настройка регистрации событий безопасности

Функция регистрации событий безопасности реализована в компонентах Neuvector и Opensearch, их настройка описана в статье Настройка контроля целостности настоящего руководства.

Регистрация событий безопасности в средстве контейнеризации осуществляется с учетом требований разделов 5-6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

Оповещением администратора безопасности о событиях безопасности Платформы является регистрация и вывод информации о событиях безопасности подсистемой Opensearch.

Регистрации подлежат следующие события безопасности:

- неуспешные попытки аутентификации;
- получение доступа к образам контейнеров;
- запуск и остановка контейнеров с причиной остановки;
- изменение ролевой модели;
- модификация запускаемых контейнеров;
- выявление известных уязвимостей в образах контейнеров и некорректности конфигурации.

Типы событий безопасности описаны в Руководстве пользователя. Для каждого события безопасности регистрируются:

- время;
- идентификатор пользователя;
- описание события;
- критичность события (**Info**/**Warning**/**Critical**/**Error**).

Журналы событий безопасности Изделия доступны только для чтения. При исчерпании области памяти, отведенной под журнал событий безопасности средства контейнеризации, изделие осуществляет архивирование журнала с последующей очисткой указанного журнала.

2. Настройка управления доступом

Ролевая модель ПО Nova Container Platform Special Edition.

Применение прав пользователя при изменении или смене роли происходит только при следующей авторизации.

Объекты RBAC (Role-based access control) в Kubernetes определяют, разрешена ли пользователю определенная операция в контексте всего кластера или в контексте пространства имен (Namespace).

Администраторы кластера Kubernetes могут использовать кластерные роли (ClusterRoles) и их привязки (ClusterRoleBindings) к пользовательским объектам, чтобы контролировать тот или иной доступ к ресурсам Kubernetes, пространствам имен и другим сущностям в контексте всего кластера.

Регулярные пользователи кластера могут использовать локальные роли (Roles) и их локальные привязки (RoleBindings), чтобы контролировать доступ к собственным пространствам имен (Namespaces).

Авторизация в Kubernetes управляется с помощью следующих объектов:

- **Правила** (Rules) – перечень разрешенных методов работы с объектами Kubernetes.
- **Роли** (Roles) – набор правил, определяющий разрешенные действия с объектами Kubernetes.
- **Привязки** (Bindings) – ассоциация между пользователями или группами с какой-либо ролью.

В Kubernetes предусмотрено два уровня ролей RBAC и их привязок:

- **Кластерный RBAC** – кластерные роли и привязки, которые могут применяться на уровне всего кластера.
- **Локальный RBAC** – локальные роли и привязки, которые могут применяться на уровне пространства имен. При этом, в привязке может указываться также и кластерная роль, описывающая какие-либо действия в Kubernetes.

Для удобства администрирования используйте кластерные роли (ClusterRoles) в локальных привязках (RoleBindings) и создавайте локальные роли (Roles) только при необходимости.

Данная двухуровневая иерархия позволяет переиспользовать одни и те же кластерные роли (ClusterRoles) в пределах пространств имен, а также сохраняет возможность установки дополнительных локальных ролей.

В результате какого-либо действия пользователя в Kubernetes предварительно оцениваются правила в ролях (Roles), назначенных ему с помощью привязок (Bindings):

- Выполняется проверка разрешений по кластерным ролям (ClusterRoles);
- Выполняется проверка разрешений по локальным ролям (Roles);
- Запрещается все, что явно не разрешено.

Роли по умолчанию

ПО Nova Container Platform Special Edition включает базовый набор кластерных ролей (ClusterRoles), которые можно использовать для назначения пользователям и группам в контекстах кластера и пространств имен (таблица ниже).

Описание кластерных ролей

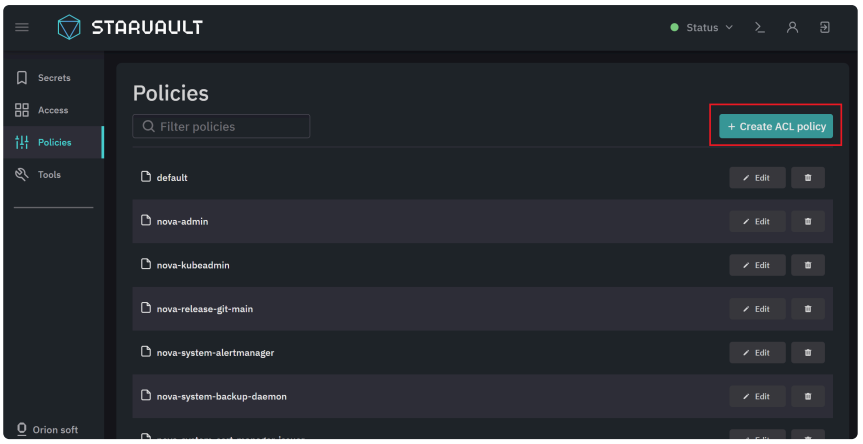
Кластерная роль	Описание
`cluster-admin`	Роль, определяющая права супер-пользователя. Данный пользователь может выполнить любое действие с любым объектом в кластере, если роль привязана с помощью ClusterRoleBinding. Если роль привязана с помощью RoleBinding, то пользователь сможет управлять всеми ресурсами пространства имен, в том числе квотами.
`admin`	Роль администратора пространства имен. Пользователь может управлять всеми ресурсами пространства имен кроме квот.
`edit`	Роль пользователя в пространстве имен, позволяющая выполнять операции с большинством объектов в пространстве имен за исключением ролей и их привязок.
`view`	Роль пользователя, который не может производить какие-либо изменения в Kubernetes, но может просматривать большинство объектов кроме ролей, их привязок, некоторых CR и секретов.

В ПО Nova Container Platform Special Edition возможно создание собственных ролей. Для управления ролями можно использовать использовать утилиту kubectl или веб-интерфейс Nova Console. С помощью возможностей ПО Nova Container Platform Special Edition возможно создание ролей со следующими правами:

1. **Администратор ИС**, имеющий возможность:
    - Менять установленный администратором безопасности СК для администратора ИС пароль;
    - Запускать и останавливать контейнеры.

Для создания роли **Администратор ИС** необходимо:

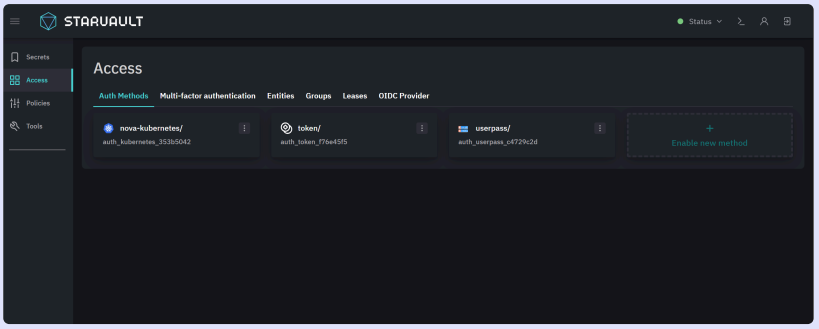
1. Открыть в браузере веб-интерфейс StarVault и авторизоваться, используя учетную запись с правом создания пользователей (по умолчанию это только root-токен).
2. Перейти на вкладку **Policies** и нажать **[Create ACL policy +]**.

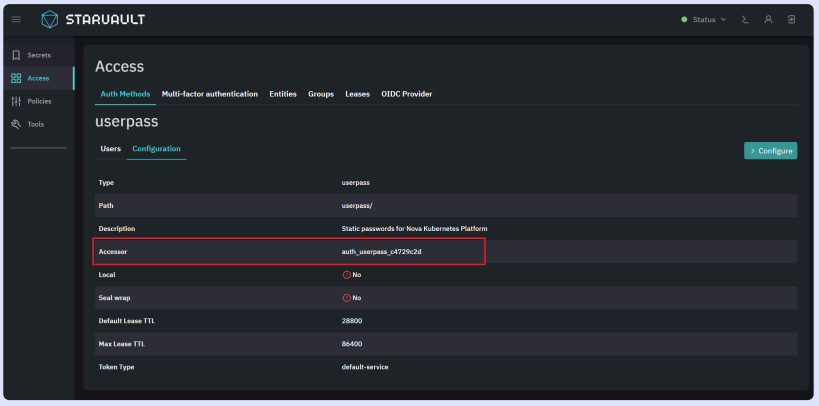


3. В поле **Name** указать понятное имя политики, например `pwd_change`.
4. В поле **Policy** добавить следующее:

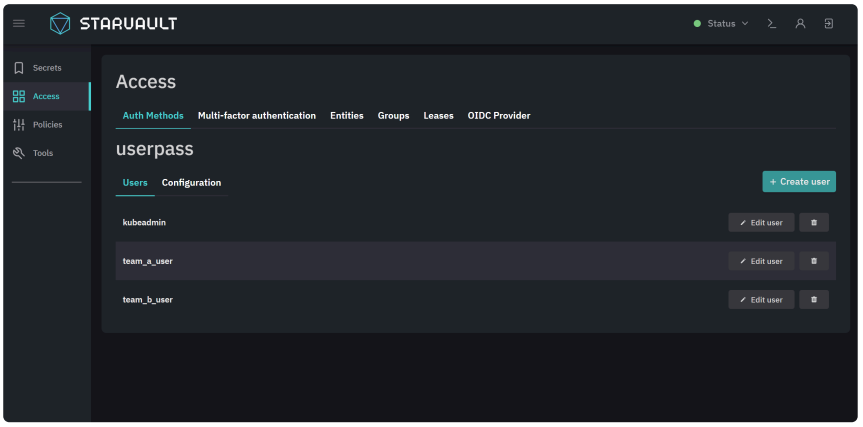
```yaml
path "sys/auth" { capabilities = ["read", "list"]}
path "auth/userpass/users" { capabilities = ["read", "list"]}
path "auth/userpass/users/{{identity.entity.aliases.
<userpass_accessor>.name}}" {
capabilities = ["read", "update"]
}
```

Замените часть `<userpass_accessor>` на свойство `Accessor`, которое можно найти по пути **Access → Auth Methods → userpass/**.

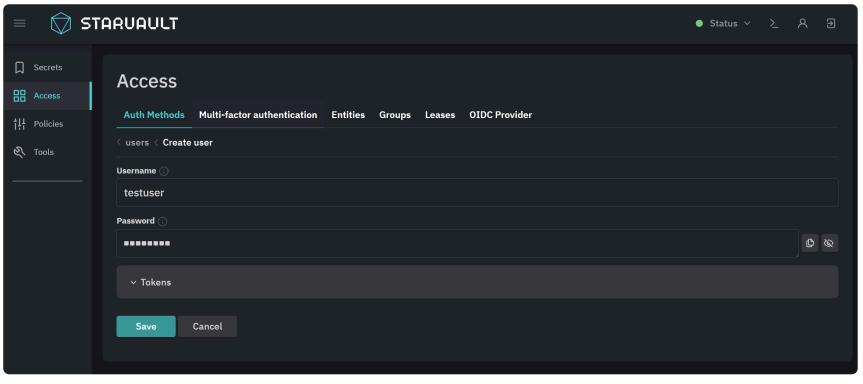




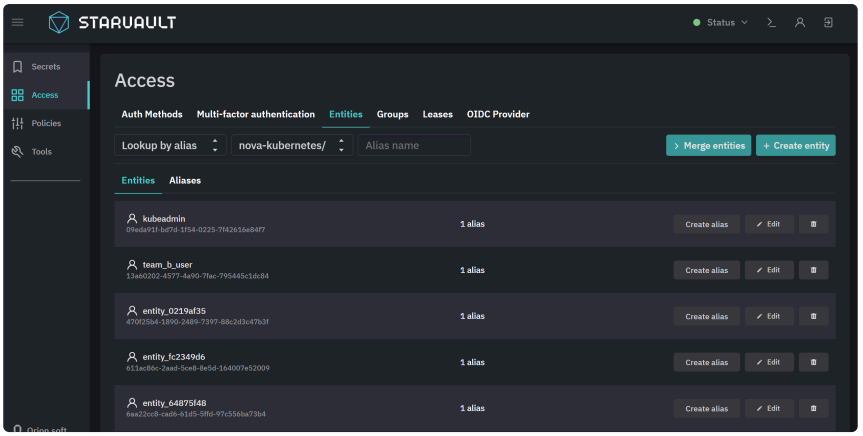
5. В случае, если необходимо создать нового пользователя перейдите к **Access → Auth Methods → userpass/** и нажмите **[Creatt user +]**.



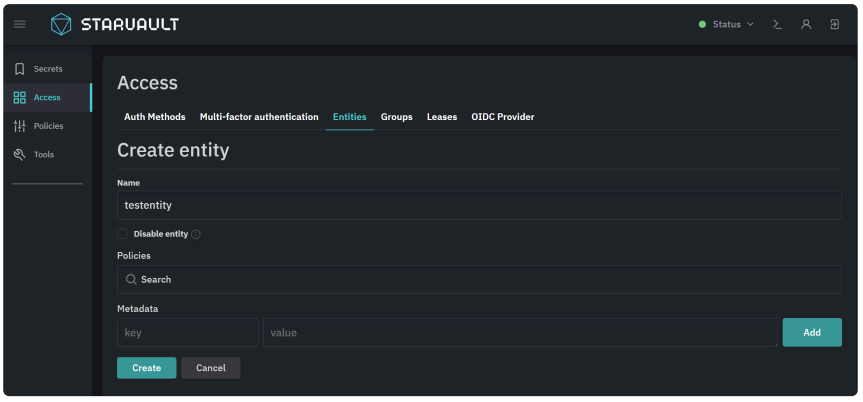
В открывшемся окне задайте имя (в нашем случае - `testuser`), пароль и нажмите **Save**.



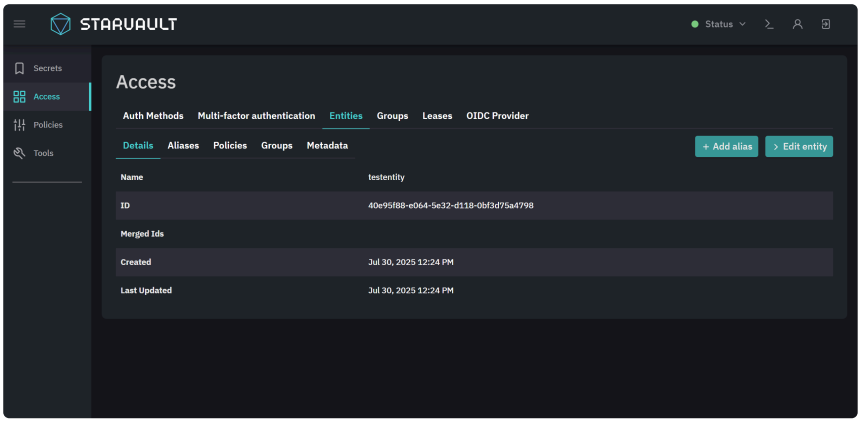
6. Создайте сущность пользователя. Перейдите в раздел **Entities** и нажмите **Create entity**.



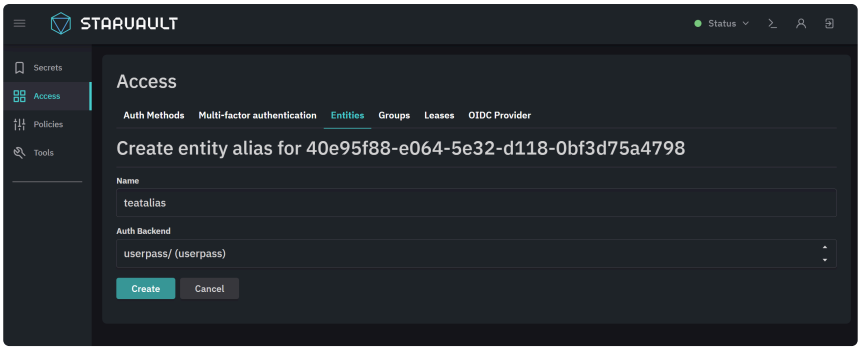
7. В открывшемся окне задайте имя (как в п.5) и нажмите **[Create]**.



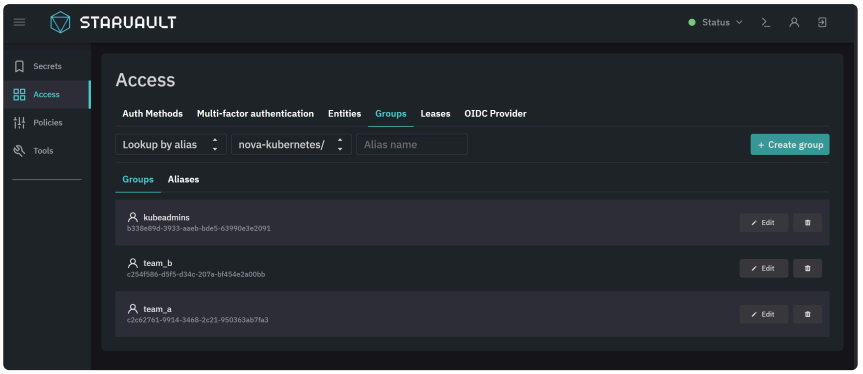
8. Свяжите сущность пользователя с методом аутентификации. На открывшейся странице созданной **Entity** нажмите **[Add alias +]** в правом верхнем углу.



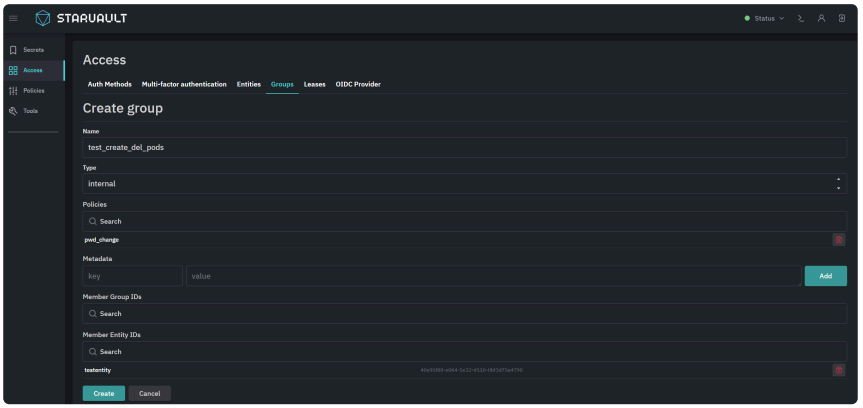
В открывшемся окне введите имя (как в п.5), выберите **userpass** в качестве **Auth Backend** и нажмите **[Create]**.



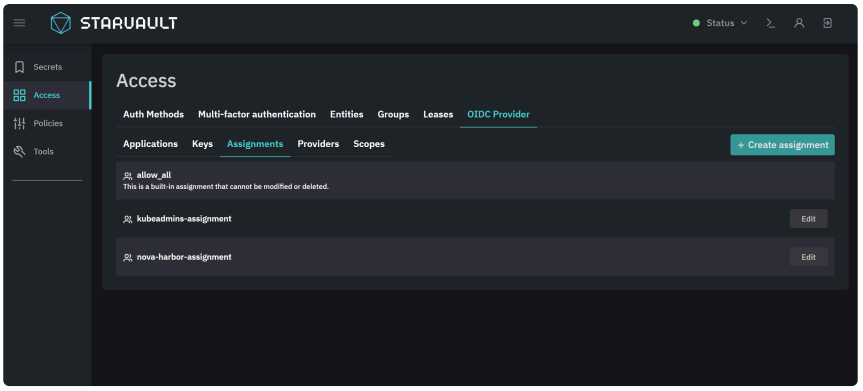
9. Создайте группу, которой будут выдаваться права (можно выдать права напрямую пользователю, но корректнее делать это с помощью групп). Перейдите на вкладку **Groups** и нажмите **[Create group +]**.



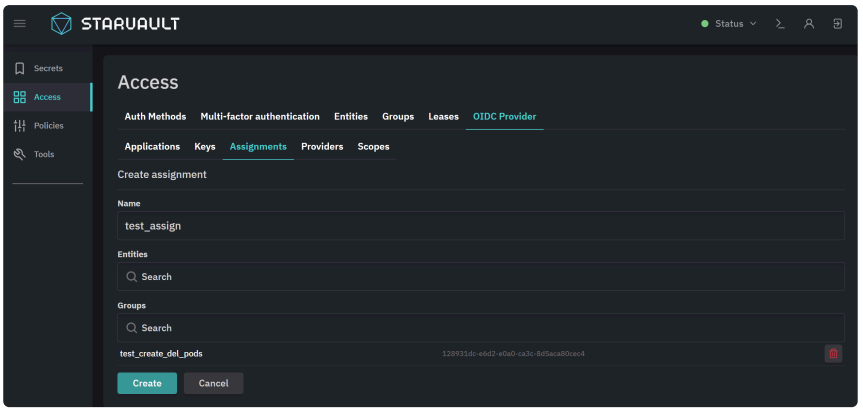
В открывшемся окне введите имя группы (в нашем случае - `test_create_del_pods`), в качестве **type** выберите **internal**. В **Member Entity IDs** добавляем **Entity** из п.6. В поле **Policy** выберите политику из п.2, после чего нажмите **[Create]**.



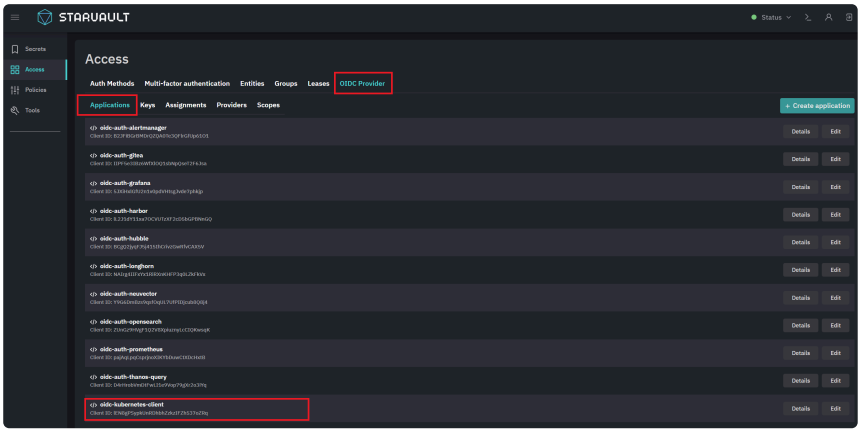
10. Свяжите созданного пользователя с OIDC провайдером. Для этого перейдите в раздел **OIDC Provider → Assignment** и нажмите **[Create Assignment +]**.



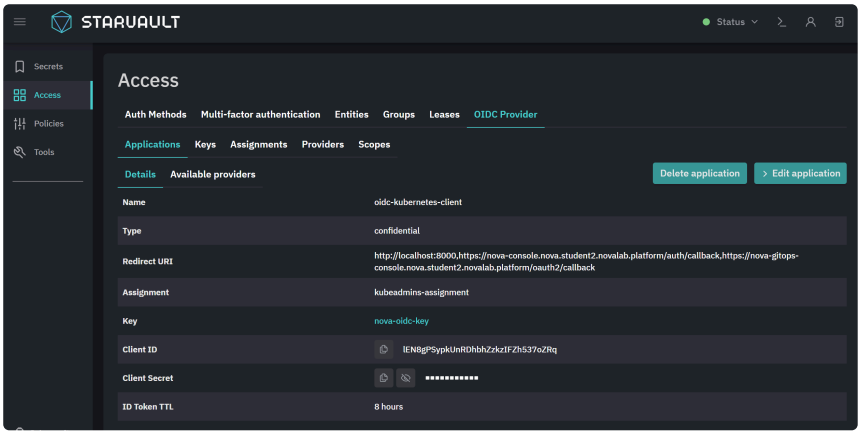
В открывшемся окне введите имя группы из п.8 (можно добавлять как пользователей, так и группы) и нажмите **[Create]**.



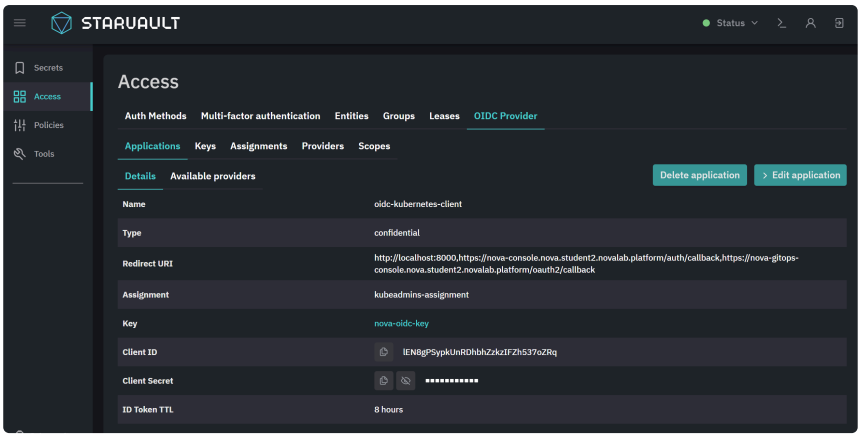
11. Свяжите созданный **Assignment** с OIDC-клиентами. Для этого перейдите в раздел **OIDC Provider → Applications** и выберите `oidc-kubernetes-client`.



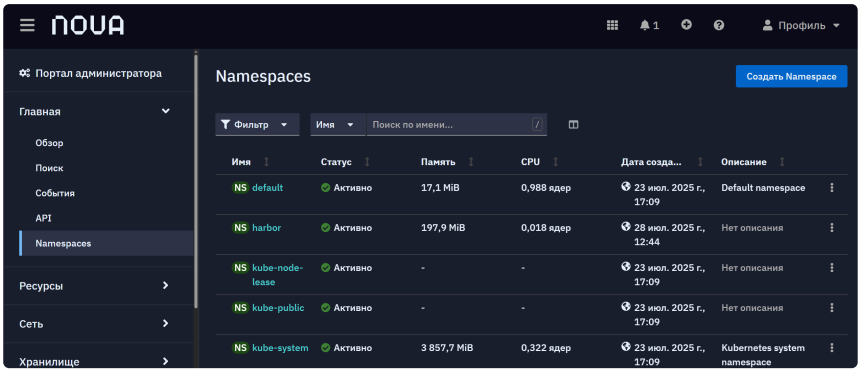
В открывшемся окне нажмите **[Edit application]**.

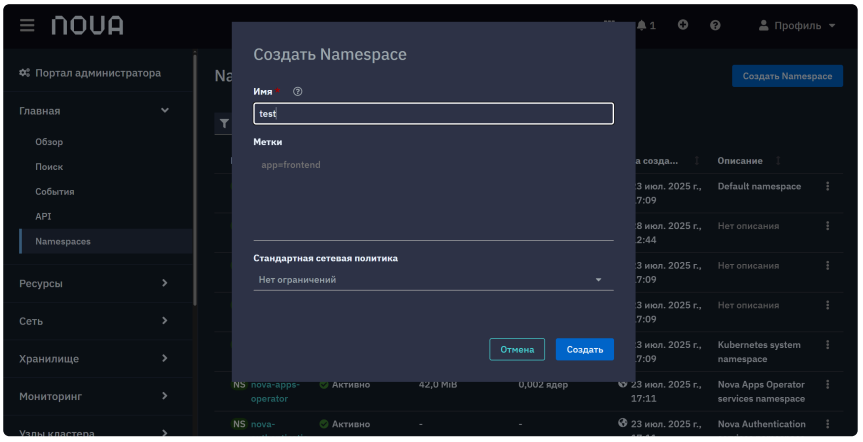


В секции Assignment name добавьте Assignment из п.9 и нажмите **[Update]**. Тем самым мы разрешили пользователям из группы, созданной в п.8 аутентификацию в Nova Console и kubernetes-api (kubectl) посредством протокола OIDC.

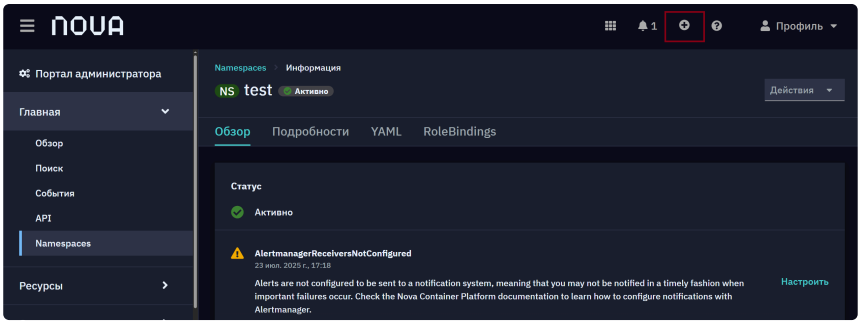


12. Зайдите в Nova Console и создайте пространство имен с именем `test`.Перейдите на вкладку **Home → Namespaces** и нажмите на **[Создать Namespace]**.





13. Создать роль в новом пространстве имен с правами на просмотр, создание и удаление подов. Роль можно создать с помощью манифеста, нажав в правом верхнем углу консоли на `+`.



Далее представлен манифест для создания роли:

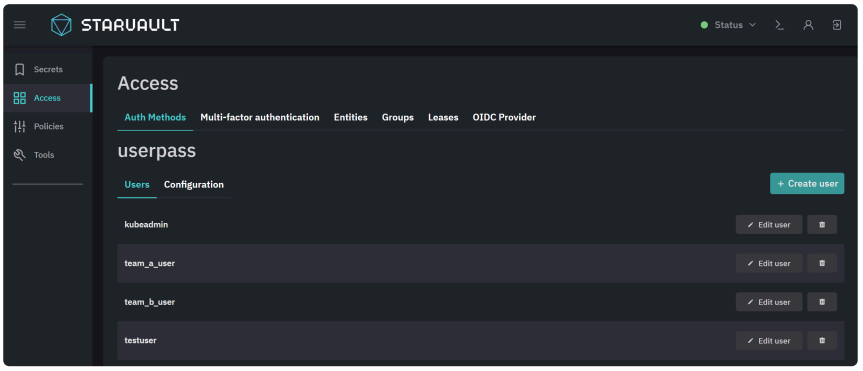
<details>
<summary>Манифест</summary>
</details>

В свойстве `subject.name` указывается имя группы созданное в StarVault.

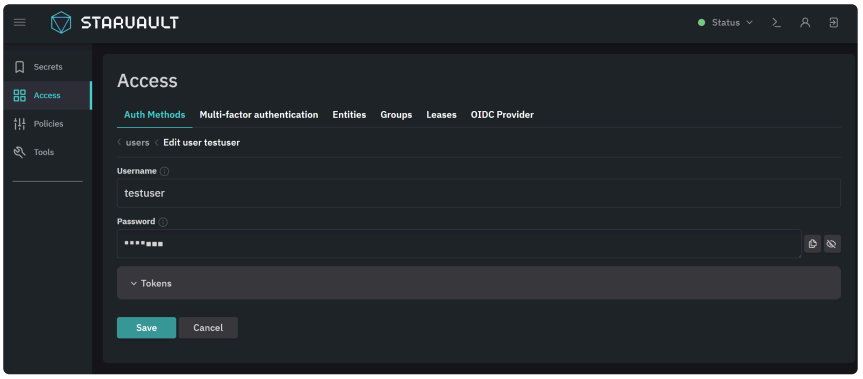
Проверка корректной настройки:

Проверьте, что можете зайти в Nova Console с новым пользователем и что права есть только на секцию **Workloads → Pods**. Для этого следуйте по шагам:

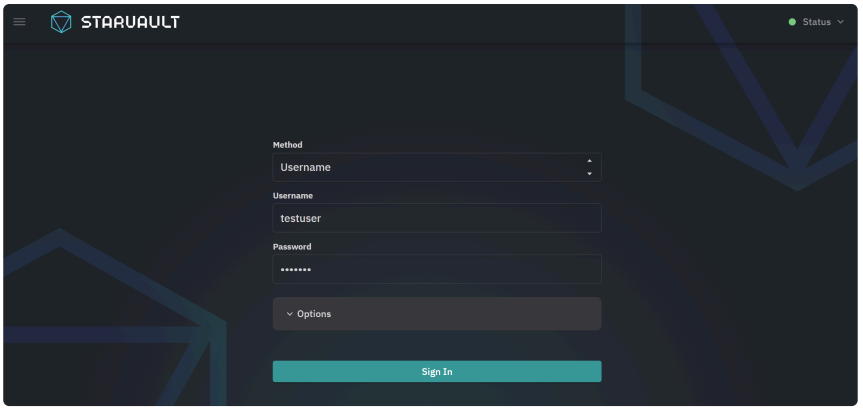
1. Авторизируйтесь в StarVault с новым пользователем и поменяйте пароль своему аккаунту. **Access → Auth Methods → userpass →** нажмите на пользователя `testuser`.



Нажмите на **[Edit user]**. Введите новый пароль и сохраните.



2. Проверьте, что можете зайти с новым паролем в Nova Console.

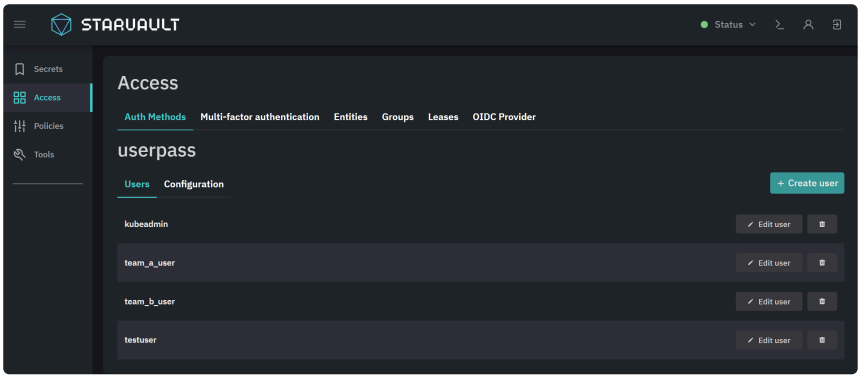


3. Зайдите в StarVault с новым пользователем и проверьте, что не можете поменять пароль другим пользователям. **Access → Auth Methods → userpass →** выберете любого пользователя и убедитесь, что нет прав на просмотр и редактирование.

2. **Администратор безопасности средства контейнеризации** должен иметь возможность:
   - Назначать права доступа пользователям средства к образам контейнеров;
   - Создавать учетные записи пользователей средства контейнеризации;
   - Управлять учетными записями пользователей средства контейнеризации;
   - Иметь доступ на чтение к журналу событий безопасности СК;
   - Формировать отчеты с учетом заданных критериев отбора, выгрузку данных из журнала событий безопасности средства контейнеризации.

   Для создания роли **Администратор безопасности средства контейнеризации** необходимо следовать шагам:

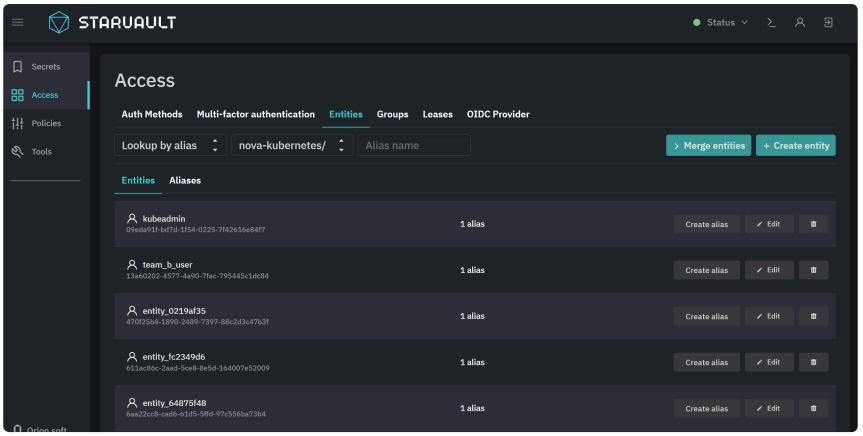
   1. Откройте в браузере веб-интерфейс StarVault и авторизуйтесь, используя учетную запись с правом создания пользователей (по умолчанию это только root-токен).
   2. Создайте пару `логин` `пароль` для авторизации пользователя. Перейдите на вкладку **Access** в раздел **Auth Methods** в метод **userpass** и нажмите **[Create User +]**.



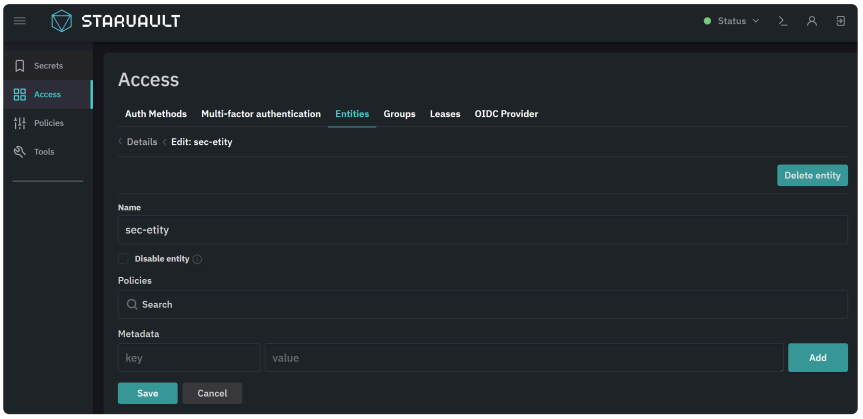
В открывшемся окне задайте имя (в данном случае - `security_admin1`), пароль и нажмите **[Save]**.

+ image::sec-admin.png[sec-admin]

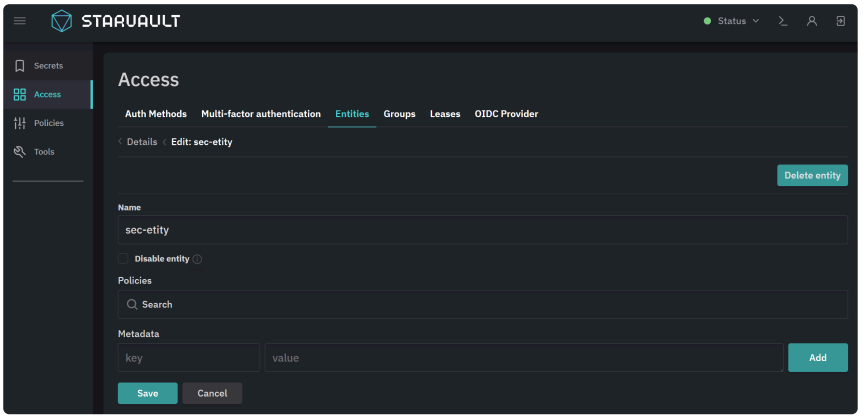
1. Создайте сущность пользователя. Перейдите в раздел **Entities** и нажмите **[Create entity +]**.



В открывшемся окне задайте имя (как в п.2) и нажмите **[Create]**.

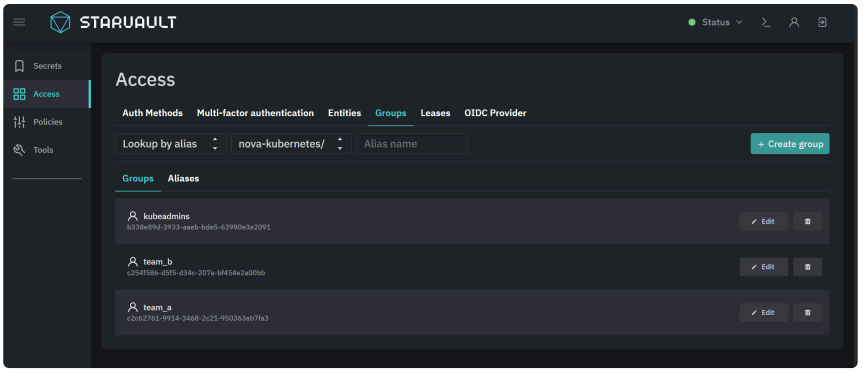


2. Свяжите сущность пользователя с парой `логин` `пароль`. На открывшейся странице созданной **Entity** нажмите **[Add alias +]** в правом верхнем углу.



В открывшемся окне введите имя (как в п.2), выберите **userpass** в качестве Auth Backend и нажмите **[Create]**.

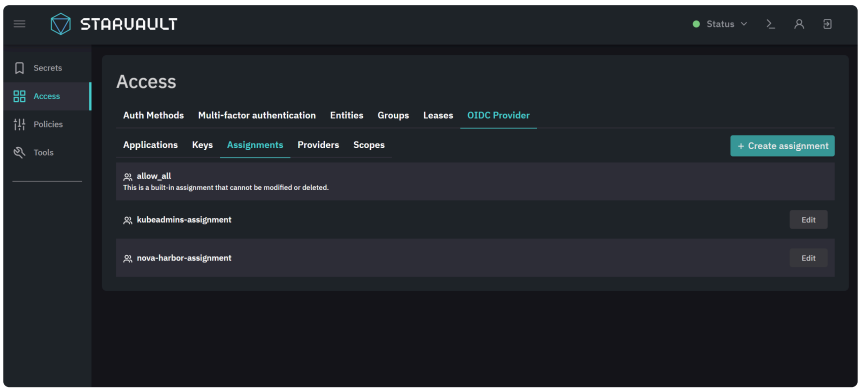
3. Создайте группу, в которой будут выдаваться права (можно выдать права напрямую пользователю, но корректнее делать это с помощью групп). Перейдите на вкладку **Groups** и нажмите **[Create group +]**.



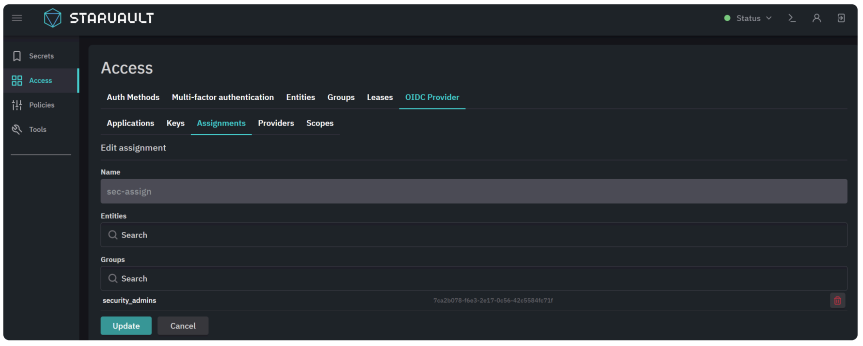
В открывшемся окне введите имя группы (в нашем случае - `security_admins`), в качестве **type** выберите **internal**. В **Member Entity IDs** добавьте **Entity** из п.3, после чего нажмите **[Create]**.

+ image::create-sec-group.png[create-sec-group]

1. Свяжите созданного пользователя с OIDC провайдером. Для этого перейдите в раздел **OIDC Provider → Assignment** и нажмите **[Create Assignment +]**.



   В открывшемся окне введите имя группы из п.5 и нажмите **[Create]**.

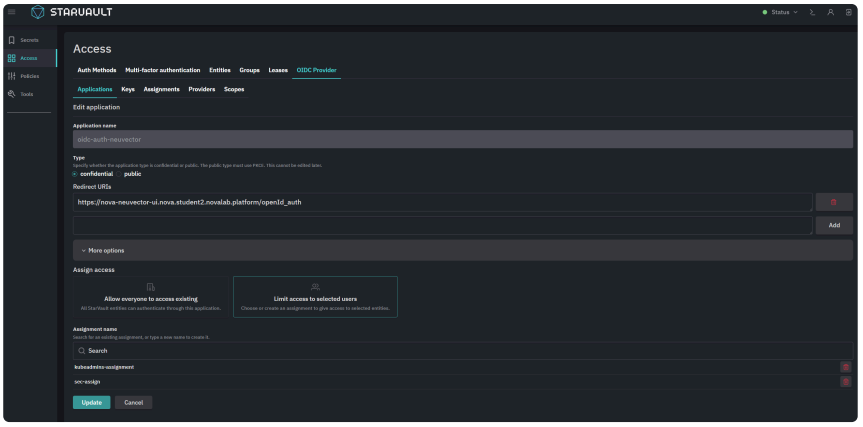


2. Свяжите **Assignment** с OIDC-клиентами. Для этого перейдите в раздел **OIDC Provider → Applications**.

   Для доступа к Neuvector выберите `oidc-auth-neuvector`.

   Для доступа к Opensearch выберите `oidc-auth-opensearch`.

   Для каждого из этих приложений в открывшемся окне нажмите **[Edit application]**, в самом низу в секции Assignment **name** добавьте **Assignment** из п.6 и нажмите **[Update]**.



3. Для доступа в Neuvector у псевдонима пользователя в атрибуте `custom_metadata` должно был ключ-значение с почтовым адресом. Этот атрибут можно добавить только через командную строку. Открыть командную строку можно двумя способами:
    - В веб-консоли нажать справа-вверху на иконку терминала.
    - Войти на мастер нод кластера и выполнить команду `starvault login`.
4. Для работы в веб-консоли выполните следующие действия:
    - Найлите ID псевдонима пользователя. Для этого перейдите на вкладку **Access** → **Entities** → **Aliases**. Найдите `security_user` и зайдите в его свойства. Запишите значение ID.
    - Выполните команду предварительно заменив `<entity_alias_id>` на значение из предыдущего пункта: `starvault read identity/entity-alias/id/<entity_alias_id>`.
    - Теперь выполните команду предварительно заменив `<userpass_accessor>` на значение `mount_accessor` из предыдущего пункта:

```bash
starvault write identity/entity-alias name="security_admin1"
mount_accessor="<userpass_accessor>"
"custom_metadata=contact_email=security_admin1@cluster.local"
```

5. Пользователи могут аутентифицироваться в указанных в предыдущем пункте приложениях используя учетные данные пользователя из п.2. Стоит учитывать, что на данном этапе была настроена только аутентификация, выдача прав доступа настраивается для каждого компонента отдельно.

Настройка доступа в StarVault

1. Откройте в браузере веб-интерфейс StarVault и авторизуйтесь. Используя учетную запись с правом создания пользователей (по умолчанию это только root-токен).
2. Перейдите на вкладку **Policies** и нажмите на **[Create ACL policy +]**.
3. Укажите имя и политику доступа:

```yaml
path "sys/auth" { capabilities = ["read", "list"]}
       path "auth/userpass/users/*" {
         capabilities = ["create", "update", "delete", "read", "list"]
       }
       path "identity/entity/*" {
         capabilities = ["create", "update", "delete", "read", "list"]
       }
       path "identity/entity" {
         capabilities = ["create", "update", "delete", "read", "list"]
       }
       path "identity/entity-alias/*" {
         capabilities = ["create", "update", "delete", "read", "list"]
       }
       path "identity/entity-alias" {
         capabilities = ["create", "update", "delete", "read", "list"]
       }
       path "identity/group" {
         capabilities = ["read", "list"]
       }
       path "identity/group/*" {
         capabilities = ["update", "read", "list"]
       }
```

4. Перейдите на вкладку **Access → Groups** и нажмите на **[Create group +]**.
5. Укажите имя группы, новую политику и пользователей.

Настройка доступа в Neuvector

1. Зайдите в консоль Neuvector используя стандартный логин - `kubeadmin`.
2. Настройте нестандартную роль. Перейдите на вкладку **Settings → Users**, **API Keys & Roles → Roles →** нажмите **[Add] →** выбирите **Modify** доступ для Admission Control.
3. Соотнесите новую роль и группу, что была создана в StarVault. Для этого перейдите на вкладку **Settings → OpenID Connect Settings →** внизу страницы нажмите на **[+]** (если навести курсор, то высветится Add Group Role Map).
4. Укажите имя группы `security_admins`, выберите созданную роль, соответствующий Namespace из предложенных вариантов и нажмите **[Add]** и затем **[Submit]**.

Настройка доступа в Opensearch

1. Зайдите в консоль Opensearch используя стандартный логин - `kubeadmin`.
2. В Opensearch уже есть преднастроенные роли и группы доступа, которые можно сразу использовать, однако мы создадим свои.
3. Перейдите на вкладку **Management → Security → Permissions**.

4. Создайте свою группу доступа. Нажмите на **Create action group → Create from blank** → укажите имя группы и доступы:
   - `read`;
   - `get`;
   - `search`;
   - `indices_monitor`;
   - `cluster_monitor`.

   1. Данные группы являются преднастроенными. Их можно добавить в другую группу или указать в роли.
   2. При изменении доступа необходимо обновить страницу, чтобы при редактировании группы отобразилась актуальная информация.

5. Перейдите на вкладку **Management → Security → Roles**.
6. Нажмите на **Create Role** и укажите созданную группу прав в полях **Cluster permissions** и **Index permissions**. Учтите, что в поле Index выбираются индексы к которым будет предоставлен доступ. Поставьте знак `*`, чтобы предоставить доступ ко всем индексам.
7. После создания роли - зайдите в неё, перейдите на вкладку **Mapped users** и нажмите **Manage mapping**.
8. Добавьте имя группы из StarVault в блок **Backend roles**.
9. Зайдите в Opensearch с учётной записью `security_admin1`.
10. Перейдите на вкладку **Management → Index Management → Indexes**. Убедитесь, что системные индексы отображаются.
11. Перейдите на вкладку **OpenSearch Plugins → Query Workbench**. Убедитесь, что выбраны SQL запросы и выполните скрипт:

```bash
select * from nova-k8s-audit-apiserver-*
order by stageTimestamp desc
```

12. Убедитесь, что отобразились логи индексов nova-k8s-audit-apiserver.

3. Рекомендуется к ознакомлению

- Настройка идентификации и аутентификации

Безопасность среды функционирования

Nova Container Platform Special Edition может быть установлена на следующую операционную систему:

- РЕД ОС версия 7.3 (Сертифицированная редакция (сертификат ФСТЭК России № 4060), дата сборки образа 19.12.2023 г. и новее).

1. Реализация функций безопасности среды функционирования

Для реализации функций безопасности среды функционирования Nova Container Platform Special Edition должны выполняться следующие действия:

- ПО Nova Container Platform Special Edition должно использоваться только на рекомендуемых аппаратных мощностях и средствах;
- должна обеспечиваться физическая сохранность аппаратной платформы с установленным ПО Nova Container Platform Special Edition и контроль доступа к ней.

Для всех компонентов среды функционирования ПО Nova Container Platform Special Edition должны быть установлены все актуальные обновления, либо приняты организационно-технические меры, направленные на исключение возможности эксплуатации уязвимостей.

Каналы передачи данных (включая каналы управления), используемые ПО Nova Container Platform Special Edition должны быть либо расположены в пределах контролируемой зоны и защищены с использованием организационно-технических мер.

Если каналы передачи данных выходят за пределы контролируемой зоны, то в целях обеспечения удаленного доступа пользователей с использованием сетей связи общего пользования к средству виртуализации должны применяться средства криптографической защиты информации, прошедшие процедуру оценки соответствия в соответствии с законодательством Российской Федерации.

2. Рекомендуется к ознакомлению

- Безопасность установки