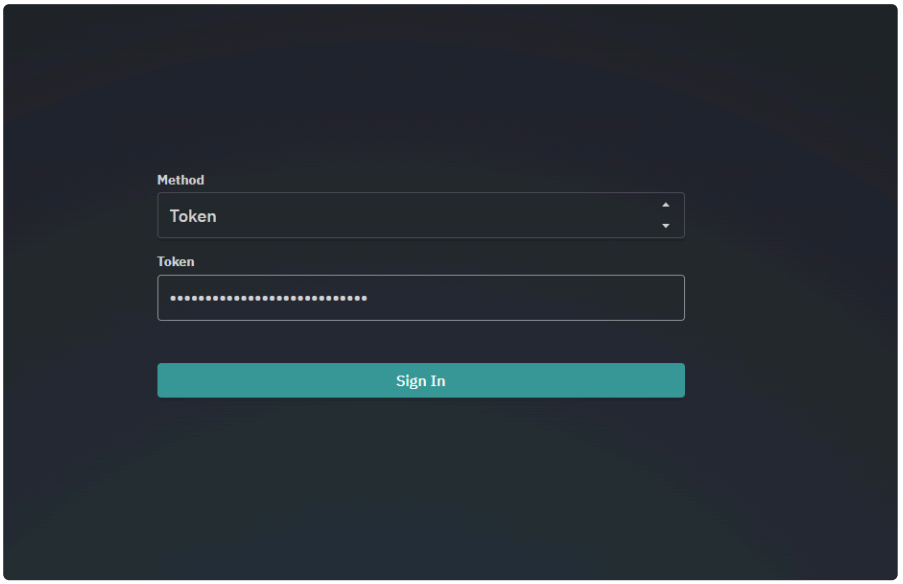
Доступ к компонентам платформы по OIDC

1. В данной инструкции описаны следующие процессы

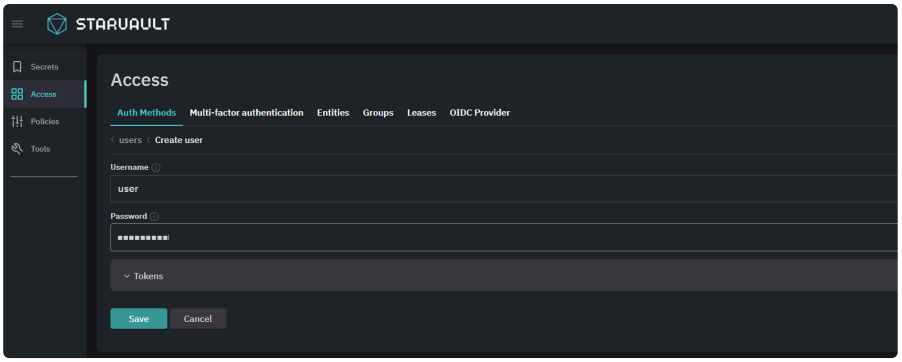
- создание пользователя во внутреннем провайдере идентификации Vault
- создание группы пользователей
- настройка для группы пользователей аутентификации по протоколу OIDC в компонентах платформы

2. Порядок действий

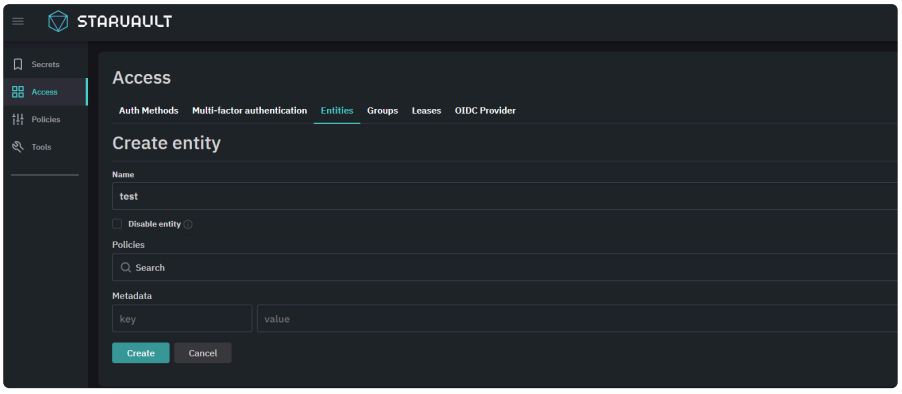
1. Откройте в браузере веб-интерфейс StarVault и авторизуйтесь, используя учетную запись с правом создания пользователей (по умолчанию это только root-токен).



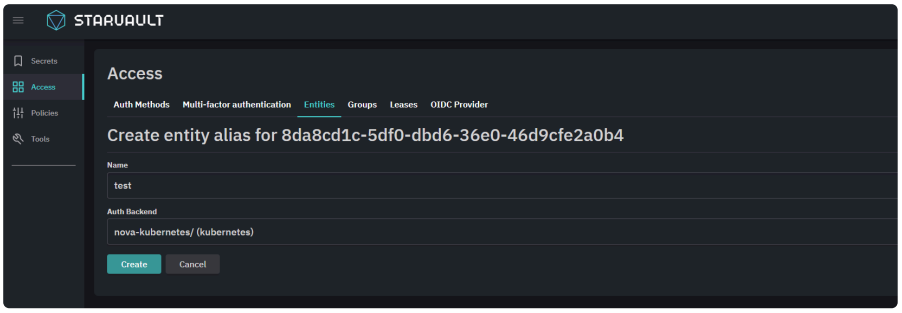
2. Следующим шагом нужно создать саму сущность пользователя. Перейдите в раздел **Auth Methods** в метод **userpass** и нажмите *«Create User +»*. В открывшемся окне задайте имя, пароль и нажмите *«Save»*.



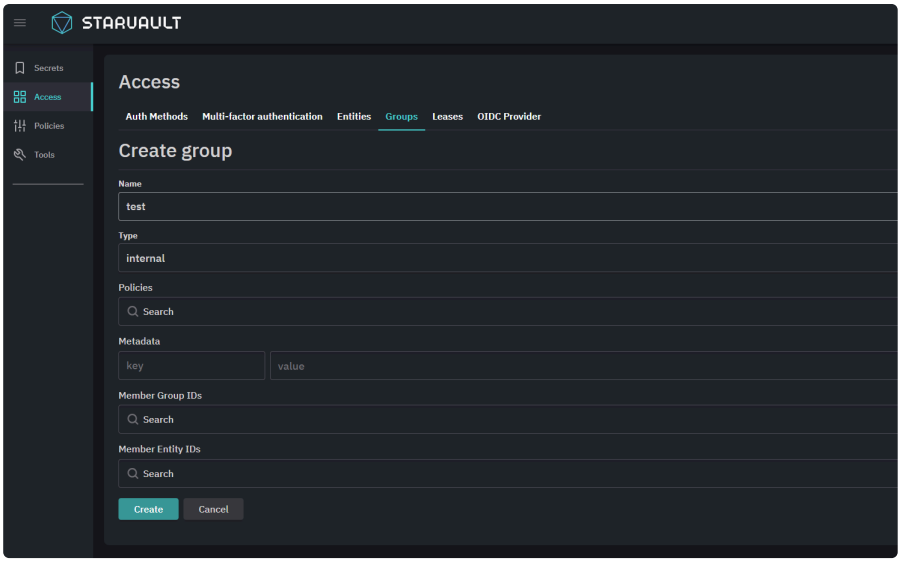
3. Следующим шагом нужно создать саму сущность пользователя. Перейдите в раздел *Entities* и нажмите *«Create entity +»*. В открывшемся окне задайте имя (как в п.2) и нажмите *«Create»*.



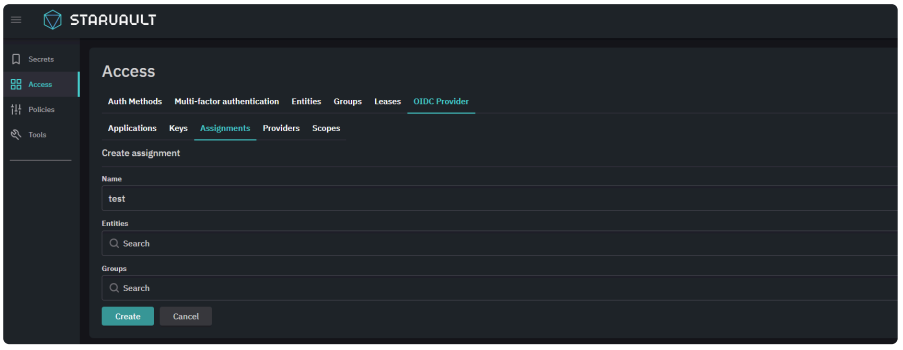
4. Теперь необходимо связать сущность пользователя с методом аутентификации. На открывшейся странице созданной *Entity* нажмите *«Add alias +»* в правом верхнем углу. В открывшемся окне введите имя (как в п.2), выберите *userpass* в качестве *Auth Backend* и нажмите *«Create»*.



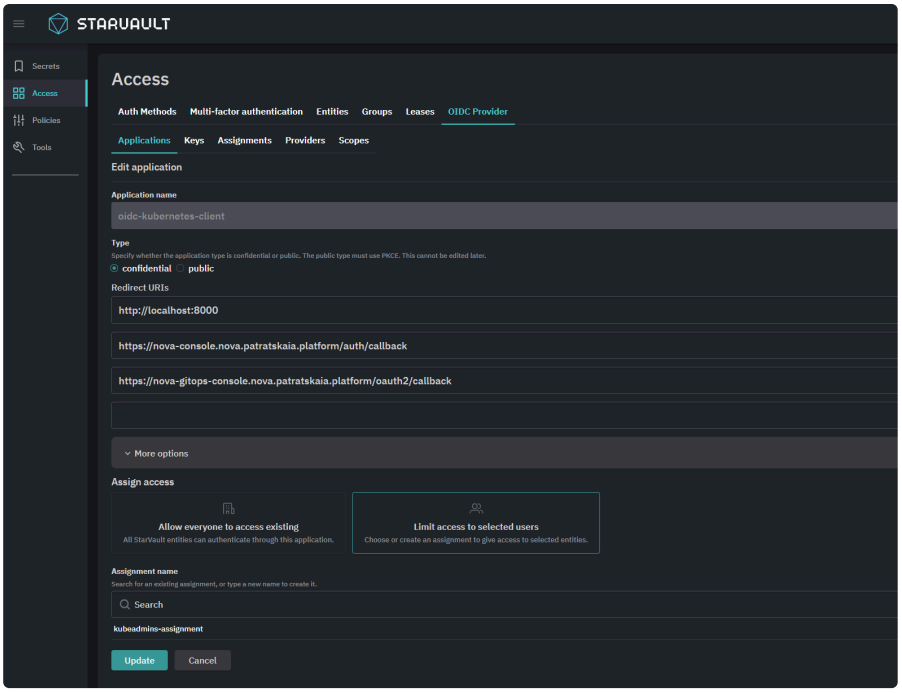
5. На следующем шаге создадим группу, которой будут выдаваться права (можно выдать права напрямую пользователю, но корректнее делать это с помощью групп). Перейдите на вкладку *Groups* и нажмите *«Create group +»*. В открывшемся окне введите имя группы, в качестве *type* выберите *internal*, а в *Member Entity IDs* добавляем *Entity* из п.3, после чего нажмите *«Create»*.



6. Далее нам нужно связать созданного пользователя с OIDC провайдером. Для этого перейдите в раздел *OIDC Provider* → *Assignment* и нажмите *«Create Assignment +»*. В открывшемся окне введите имя и выберите пользователя из п.3 или группу из п.5 (можно добавлять как пользователей, так и группы) и нажмите *«Create»*.



7. Теперь нам необходимо связать этот Assignment с OIDC-клиентами. Для этого перейдите в раздел *OIDC Provider* → *Applications* и выберите `oidc-kubernetes-client`. В открывшемся окне нажмите *«Edit application»*, в самом низу в секции *Assignment name* добавьте *Assignment* из п.6 и нажмите *«Update»*. Тем самым мы разрешили пользователям из группы, созданной в п.5 аутентификацию в Nova Console и kubernetes-api (`kubectl`) посредством протокола OIDC.



8. По аналогии вы можете разрешить аутентификацию для других компонентов платформы (OpenSearch, Neuvector, Prometheus, AlertManager, Hubble), добавляя assignment в соответствующие Applications.
9. Теперь вы можете аутентифицироваться в Nova Console используя учетные данные пользователя из п.2. Стоит учитывать, что на данном этапе была настроена только аутентификация, поэтому данный пользователь не увидит никакой информации в Nova Console. Выдача прав доступа настраивается для каждого компонента отдельно.

Настройка провайдера идентификации LDAP

В данном разделе описывается процедура подключения провайдера идентификации в *StarVault* по протоколу LDAP.

Необходимые условия

- ✓ У вас есть токен доступа к хранилищу секретов StarVault с привилегиями `root`.
- ✓ У вас есть доступ к Kubernetes API с привилегиями администратора кластера.
- ✓ (Опционально) У вас есть CA-сертификат в формате `x509 PEM` для валидации подключения в случае использования защищенного протокола LDAPS (LDAP over SSL).
- ✓ У вас есть сервисная учетная запись для выполнения операций поиска в каталоге LDAP-сервера.
- ✓ Сервер LDAP доступен для *StarVault*.

StarVault размещается на мастер-узлах Kubernetes и запущен в качестве службы Systemd. *StarVault* должен корректно разрешать DNS-имя LDAP-сервера или иметь доступ к его IP-адресу и портам `tcp/389`, `udp/389`, `tcp/636`, `udp/636`.

Рекомендуется использовать защищённую версию протокола LDAPS (LDAP over SSL), которая использует безопасное TLS/SSL-соединение для передачи данных. Протокол LDAPS по умолчанию использует порт `tcp/636`.

1. Об аутентификации по протоколу LDAP

В ходе аутентификации по протоколу LDAP в каталоге сервера (провайдера идентификации) выполняется поиск записи, соответствующей указанному имени пользователя. Если обнаружено одно уникальное совпадение, предпринимается попытка аутентификации с использованием уникального имени (DN) записи и предоставленного пароля.

В StarVault вы можете определить фильтры для поиска пользователей и групп в каталоге LDAP-сервера.

В процессе аутентификации можно выделить следующие особенности:

1. Если в процессе поиска записи с учетом пользовательских фильтров не будет найдена ровно одна запись, соответствующая указанному имени пользователя, то доступ будет

запрещен.

2. Если ровно одна запись, соответствующая указанному имени пользователя, будет найдена, но попытка подключения к LDAP-серверу с предоставленным паролем будет неудачна, то доступ будет запрещен.
3. Если учетная запись найдена, и подключение к LDAP-серверу с предоставленным паролем выполнено успешно, то аутентификация также будет считаться успешной. После этого в StarVault автоматически будет создана сущность *Entity* как уникальный идентификатор пользователя.

> **Экранирование специальных символов**
>
> Обратите внимание, что конфигурация DN в StarVault должна выполняться с учетом экранирования специальных символов, следуя правилам RFC 4514. При настройке провайдера идентификации Microsoft Active Directory следует учесть дополнительные требования к экранированию символов `#` и `=`.

2. Подключение к StarVault

Подключитесь к StarVault следуя процедуре, описанной в разделе Подключение к StarVault.

3. Настройка с помощью графического интерфейса

3.1. Настройка метода аутентификации

Провайдер идентификации подключается к StarVault путем настройки соответствующего метода аутентификации.

1. В веб-интерфейсе StarVault выберите вкладку **Access**, далее **Auth Methods**.

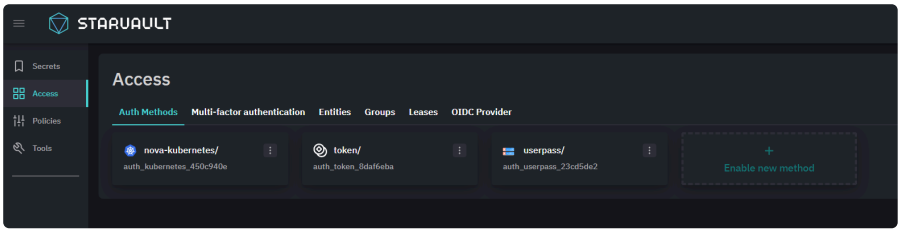


Рисунок 1. Методы аутентификации StarVault

2. Выберите опцию **Enable new method**, далее - **LDAP** и нажмите **Next**.

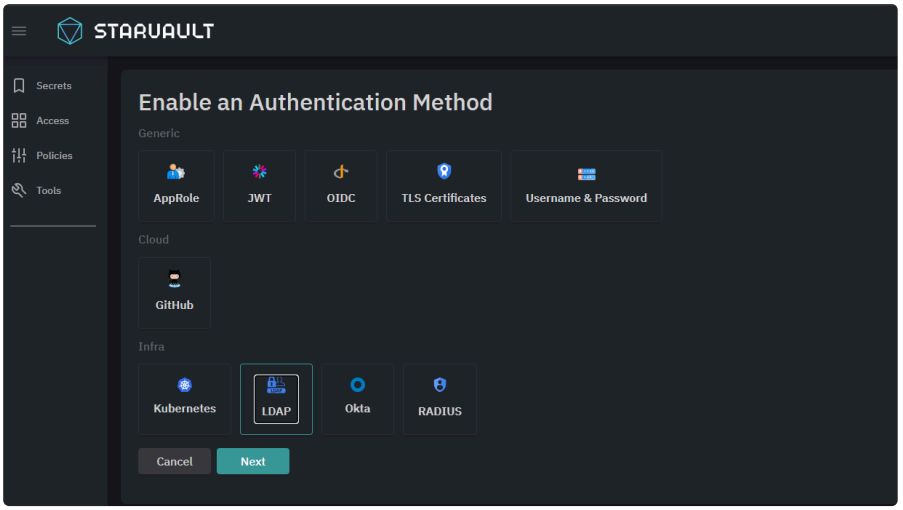


Рисунок 2. Выбор метода аутентификации LDAP в StarVault

3. Определите значение параметра **path** и настройте дополнительные параметры в меню **Method Options** при необходимости, далее нажмите **Enable Method**.

> В данном примере используется параметр `path` со значением `site1`. Обычно, кастомизация параметра `path` требуется при использовании нескольких различных серверов `LDAP`. Вы можете оставить значение параметра `path` по умолчанию - `ldap` при настройке первого метода идентификации с типом LDAP и кастомизировать его в дальнейшем при настройке дополнительных методов аутентификации.

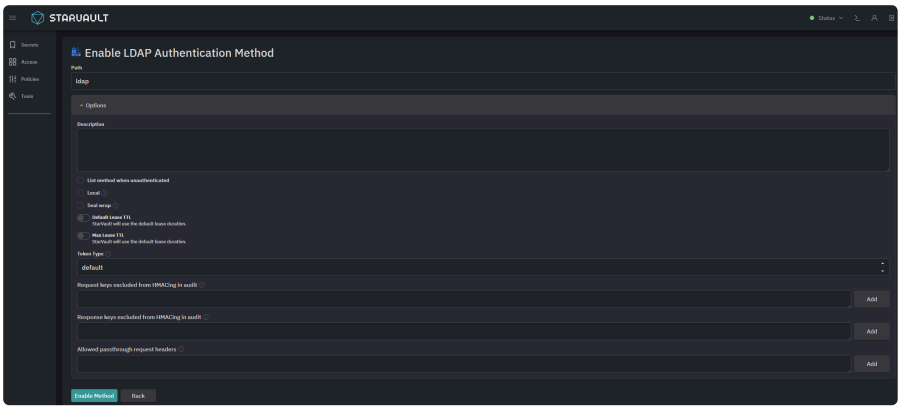


Рисунок 3. Настройка метода аутентификации LDAP в StarVault

4. Выполните настройку созданного метода аутентификации в окне **Configure LDAP**.
    - В поле **URL** укажите URL-адрес сервера(ов) LDAP. Вы можете оставить по умолчанию параметры токенов, полученных в результате аутентификации данным методом.

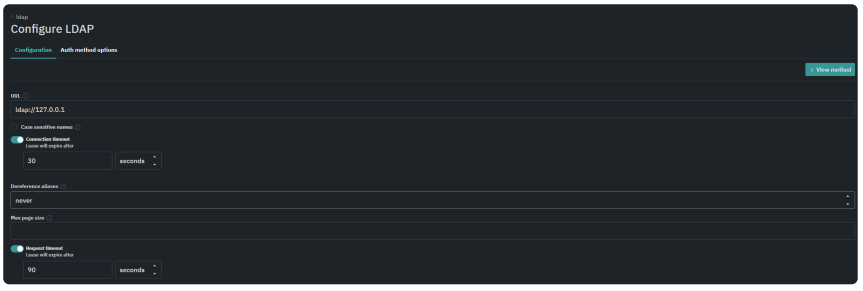


Рисунок 4. Настройка метода аутентификации LDAP в StarVault

В данном примере используется безопасное подключение по протоколу LDAPS. Для использования незащищенного соединения используйте параметр `URL` вида `ldap://server01.nova.external`.

- Перейдите ниже и разверните меню **LDAP Options**.
- Выберите параметры подключения к LDAP, загрузите CA-сертификат, который будет использован для проверки сертификата сервера LDAP (опционально).

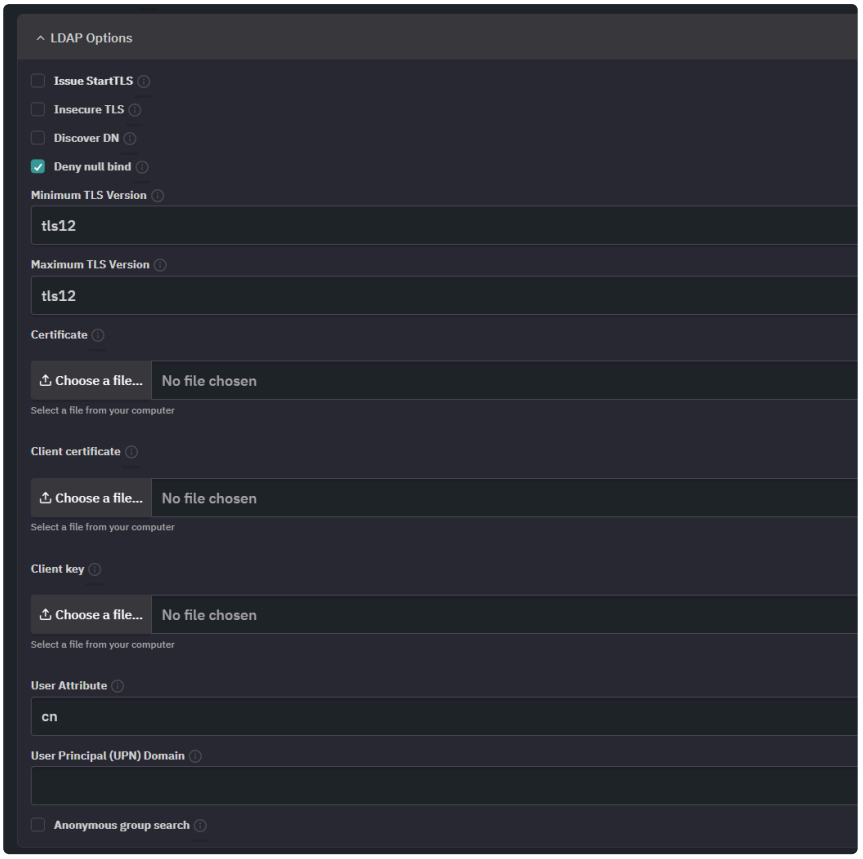


Рисунок 5. Настройка метода аутентификации LDAP в StarVault

- В поле **User Attribute** укажите имя атрибута пользовательского объекта, который соответствует имени пользователя. В зависимости от провайдера идентификации пользовательский атрибут может принимать такие значение, как `sAMAccountName`, `cn`, `uid` и другие.

Как правило, в *Active Directory* в качестве атрибута имени пользователя используется параметр `sAMAccountName`, а в решениях на базе Linux - `cn` или `uid`.

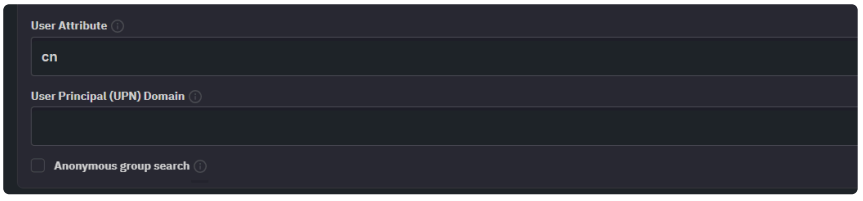


Рисунок 6. Настройка метода аутентификации LDAP в StarVault

- Перейдите ниже и разверните меню **Customize User Search**.

- В поле **Name of Object to bind (binddn)** укажите уникальное имя (DN) сервисной учетной записи для выполнения операций поиска в каталоге LDAP-сервера.
- В поле **Bindpass** укажите пароль пользователя для подключения к LDAP.
- В поле **User DN** укажите DN, в котором будет производится поиск пользователей.
- В поле **User Search Filter** определите шаблон, который используется как фильтр при поиске пользователей в LDAP. Фильтр может использоваться для ограничения пользователей, которым необходимо разрешить доступ.

> Параметры `{{.UserAttr}}` и `{{.Username}}` являются переменными Go-шаблона, который применяется в StarVault при конструировании запросов к LDAP-серверу. В переменную `{{.UserAttr}}` передается установленное значение в поле `User Attribute`, а переменная `{{.Username}}` является именением, которое пользователь вводит при входе в StarVault.

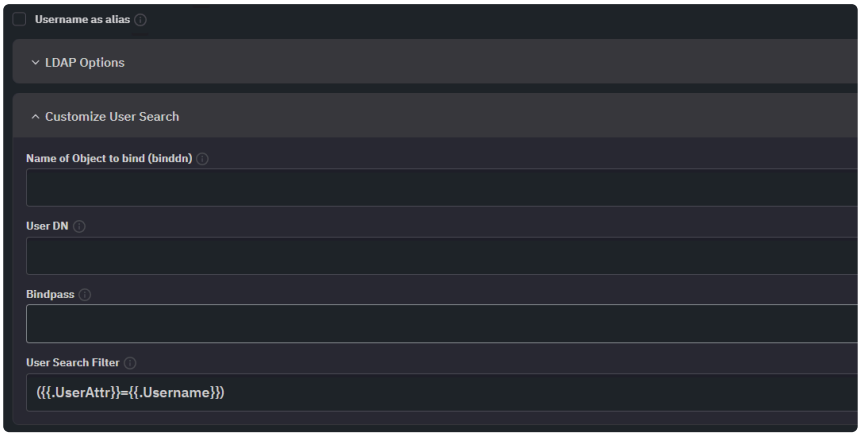


Рисунок 7. Настройка метода аутентификации LDAP в StarVault

- Перейдите ниже и разверните меню **Customize Group Membership Search**.
- В поле **Group Filter** определите шаблон, который используется как фильтр при поиске групп, в которых состоит пользователь.

> Для получения групп пользователя, включая вложенные, в *Active Directory* используется оператор `LDAP_MATCHING_RULE_IN_CHAIN` - `1.2.840.113556.1.4.1941`.

- В поле **Group Attribute** укажите LDAP-атрибут, который следует использовать для объектов, возвращаемых фильтром **Group Filter**, для перечисления членства в группах пользователей.
- В поле **Group DN** укажите DN, в котором будет производится поиск групп.
- При включении параметра **Use token groups**, другие настройки параметров поиска групп (**Group Filter**, **Group Attribute** и **Group DN**) перестают иметь эффект. Поиск членства в группах в данном случае будет работать следующим образом:

  1. На LDAP-сервер отправляется запрос параметра `tokenGroups` для пользователя. При этом в качестве базы для поиска будет использован **User**

DN;

2. Из полученного токена берется SID каждой группы и запрашивается ее имя.

> Если LDAP-сервер является **GlobalCatalog**, то рекомендуется выключить параметр **Use token groups** и использовать фильтр.

- Чтобы сохранить, установленные настройки, нажмите **Save**.

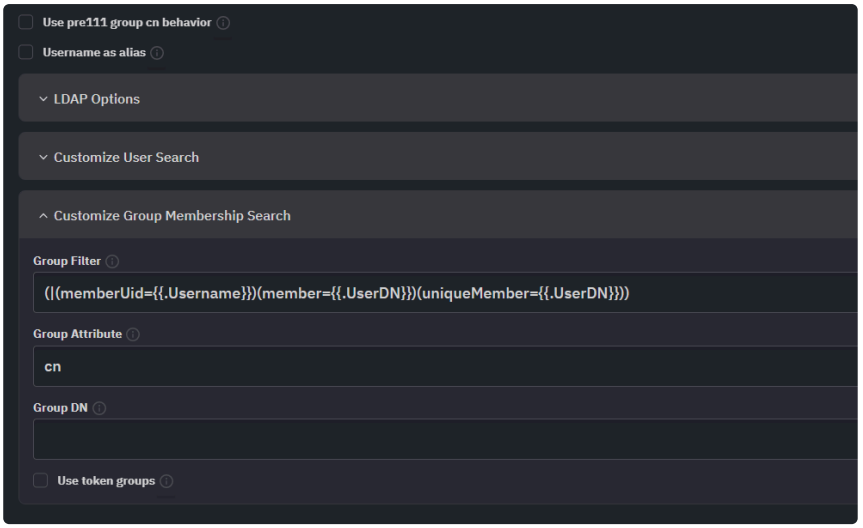


Рисунок 8. Настройка метода аутентификации LDAP в StarVault

> В данном примере используется фильтр проверки членства в группе `nova-users`. Группа `nova-users` может содержать в себе множество других групп, на уровне которых можно создавать политики StarVault и правила RBAC в Kubernetes.

Настройка фильтров и атрибутов групп необходима для того, чтобы определить, членом каких групп является пользователь. Конфигурация для этого может различаться в зависимости от вашего LDAP-сервера (провайдера идентификации) и схемы его каталога.

Существует две основные стратегии определения членства в группах:

- поиск пользователя и отслеживание атрибута групп, членом которых он является.
- поиск групповых объектов, членом которых является пользователь.

Например, для `Group Filter`, возвращающего групповые объекты, используйте `Group Attribute` со значением `cn`. Для запросов, возвращающих пользовательские объекты, используйте `Group Attribute` со значением `memberOf`.

3.2. Проверка метода аутентификации

После настройки метода аутентификации вы можете проверить его. Попробуйте выполнить вход в StarVault с помощью учетной записи, отвечающей ранее настроенным в методе аутентификации фильтрам.

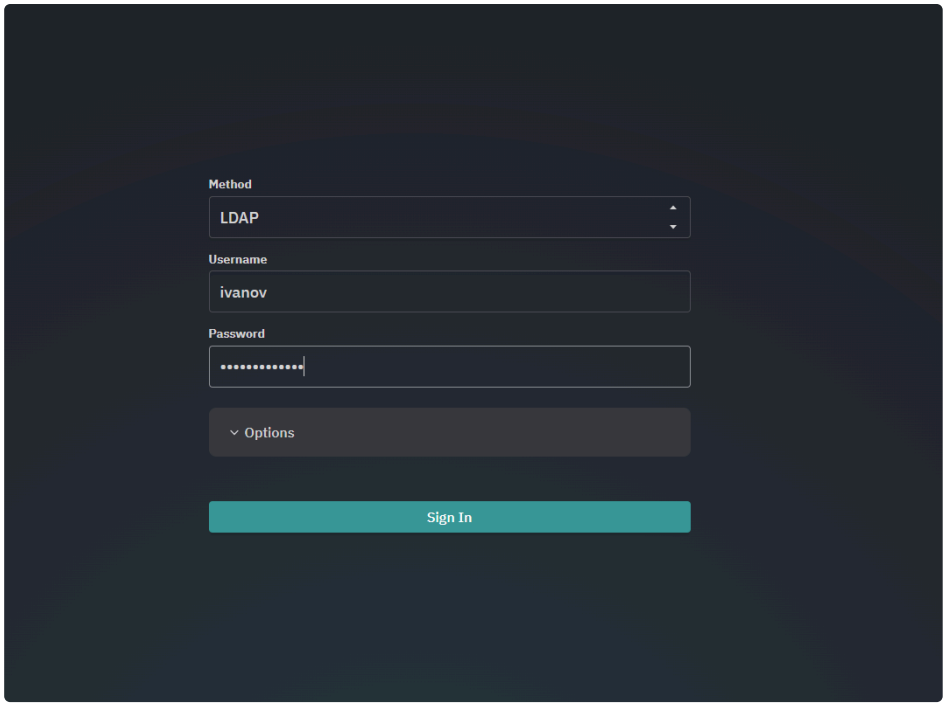


Рисунок 9. Проверка входа с использованием метода аутентификации LDAP в StarVault

Если при настройке метода аутентификации вы не меняли параметр `path`, то при входе опцию **Mount path** можно не указывать.

3.3. Настройка политик доступа к ресурсам StarVault для пользователей и групп

Если пользователям из каталога LDAP-сервера требуется доступ к ресурсам в StarVault, вы можете назначить определенным пользователям или группам специальные политики. Это может быть полезно в следующих сценариях:

- Пользователи должны иметь доступ к какому-либо общему или приватному хранилищу секретов.
- Существует необходимость настройки учетной записи администратора StarVault для пользователя из каталога LDAP-сервера.

> Если пользователям из каталога LDAP-сервера требуется только возможность входа в Kubernetes и его приложения, вы можете пропустить этот шаг.

Для того, чтобы добавить политики пользователям или группам пользователей следуйте процедуре ниже.

1. Перейдите в раздел **Access**, далее **Auth Methods**.
2. Выберите ранее созданный метод аутентификации, например, **site1**.
3. Для назначения политик конкретному пользователю из каталога LDAP-сервера перейдите на вкладку **Users** и нажмите **Create user**.

- В поле **Name** укажите имя пользователя.
- В поле **Policies** укажите необходимую политику.
- Сохраните настройки нажав на **Save**.

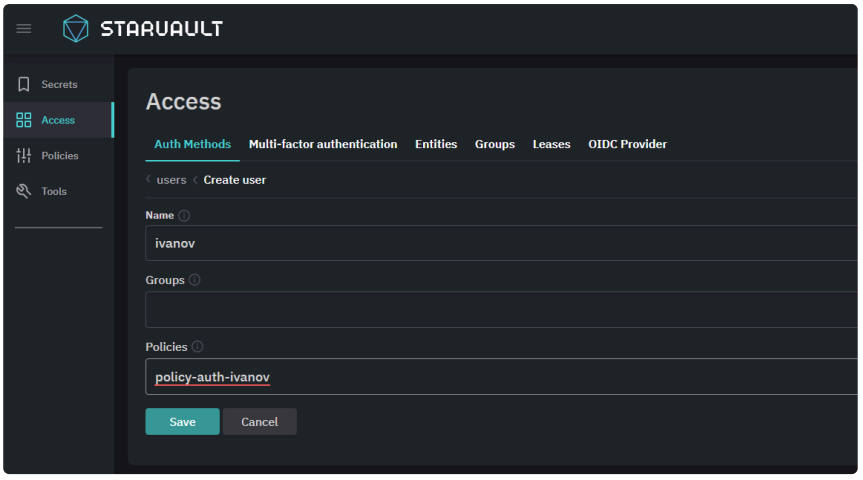


Рисунок 10. Установка политик пользователям в StarVault

4. Для назначения политик группе пользователей из каталога LDAP-сервера перейдите на вкладку **Groups** и нажмите **Create group**.
   - В поле **Name** укажите имя группы.
   - В поле **Policies** укажите необходимую политику.
   - Сохраните настройки нажав на **Save**.

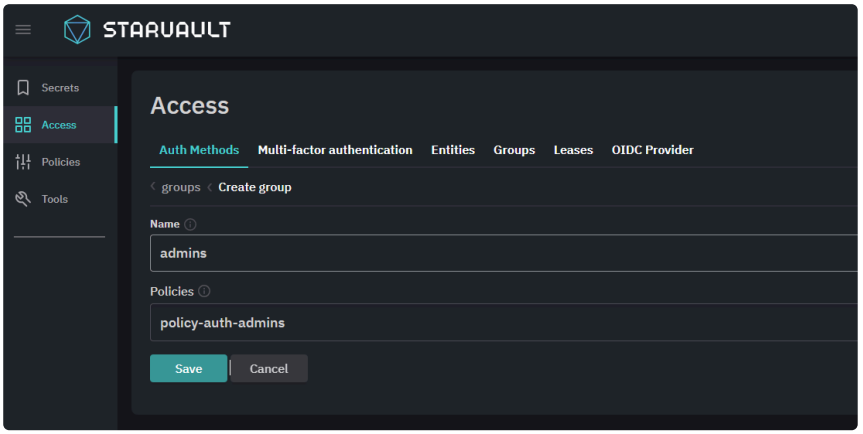


Рисунок 11. Установка политик пользователям в StarVault

3.4. Настройка групп пользователей

Каждая новая группа из каталога LDAP-сервера должна быть явно создана и настроена в StarVault. Автоматическая синхронизация (импорт) доступных групп не поддерживается.

Например, в сценарии настройки выше использовалась общая группа `nova-users` для фильтрации пользователей, которым разрешена аутентификация.

Аналогичная группа в каталоге вашего LDAP-сервера может включать множество дополнительных групп. Для того, чтобы добавить дополнительные группы в StarVault, следуйте процедуре ниже.

1. Перейдите в раздел **Access**, далее **Groups**.
2. Нажмите **Create group**.
    - В поле **Name** укажите имя группы так же, как группа названа в каталоге LDAP-сервера.
    - В поле **Type** укажите **External**.
    - (Опционально) В поле **Policies** можно указать политику доступа к ресурсам StarVault.
    - Нажмите **Create**, чтобы создать группу. Откроется страница с параметрами созданной группы.

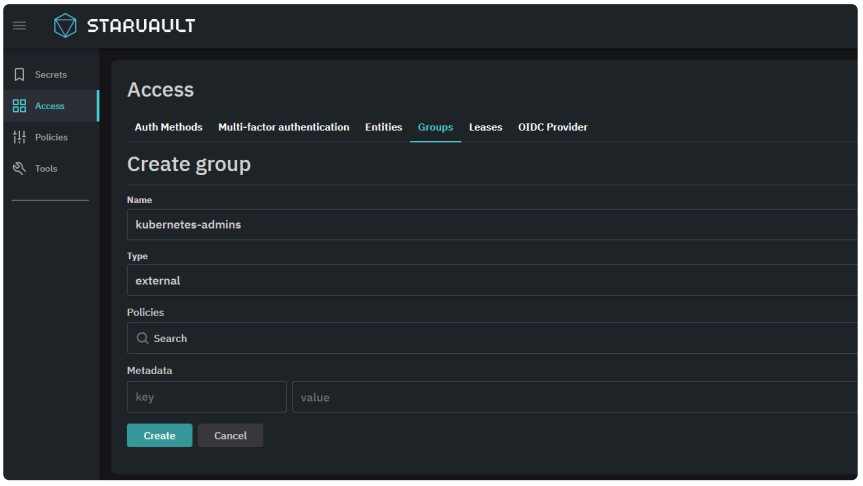


Рисунок 12. Настройка внешних групп в StarVault

Вы создали сущность внешней группы в StarVault, которую далее необходимо привязать к действительной группе в каталоге LDAP-сервера, то есть создать алиас (Alias). Для этого выполните действия ниже.

- 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.

Вы выполнили привязку группы в StarVault к действительной группе в каталоге LDAP-сервера. Аналогичным способом вы можете создать все необходимые группы и алиасы

для других доступных групп в каталоге LDAP-сервера.

3.4.1. Настройка доступа к приложениям OIDC

Для возможности использования приложений Nova Container Platform пользователи должны быть явно назначены каким-либо приложениям.

> **Информация**
>
> Получить подробную информацию о преднастроенных приложениях вы можете в разделе Приложения OAuth.

Выполните настройку доступа к необходимым приложениям OIDC в Nova Container Platform согласно процедуре, описанной в разделе документации Настройка доступа к приложениям OAuth

3.5. Настройка авторизации в Kubernetes

После того, как все необходимые назначения настроены для пользователя или группы пользователей, вы можете настроить необходимые правила RBAC в среде Kubernetes. Это может быть необходимо в случаях, когда вам необходимо добавить в Kubernetes пользователей в качестве администратора кластера, администратора пространства имен (namespace) и других.

Выполните настройку RBAC согласно процедуре, описанной в разделе документации Использование RBAC для разграничения доступа в Kubernetes.

4. Решение проблем

При некорректной настройке сущностей StarVault, а также фильтров LDAP, необходимых для поиска пользователей и групп в структуре службы каталогов, вы можете получить различные ошибки. Далее приведены примеры ошибок и способы их устранения.

4.1. Типовые ошибки

Ошибка при входе в StarVault `Authentication failed: ldap operation failed: failed to bind as user` может возникать в следующих ситуациях:

- Ошибка в учетных данных сервисной учетной записи, с помощью которой выполняется подключение к службе каталогов и поиск пользователя в каталоге LDAP-сервера. Проверьте, что параметры сервисной учетной записи указаны верно, а в логах LDAP-сервера фиксируется успешный вход данной учетной записи.

- Ошибка в учетных данных учетной записи, с помощью которой вы выполняете вход. Проверьте, что учетная запись активна, пароль установлен, не просрочен и не требует замены.
- Ошибка в настроенных фильтрах, по которым выполняется поиск пользователя. Проверьте настроенные фильтры. Для локализации проблемы с фильтром рекомендуется использовать в тестовых целях как можно более простой фильтр без комплексных условий.

Информационное сообщение после входа в StarVault `no LDAP groups found in groupDN; only policies from locally-defined groups available` может возникать в следующих ситуациях:

- Ошибка в настроенных фильтрах, по которым выполняется поиск групп и определение принадлежности пользователя к группам. Проверьте настроенные фильтры. Для локализации проблемы с фильтром рекомендуется использовать в тестовых целях как можно более простой фильтр без комплексных условий.

4.2. Проверка конфигурации фильтров LDAP

Для диагностики фильтров LDAP удобно использовать утилиту `ldapsearch`. С помощью данной утилиты вы можете конструировать и направлять запросы к LDAP-серверу. В ответе LDAP-сервера вы можете проверить, насколько возвращаемая информация соответствует используемым вами фильтрам.

Процедура

1. Проверьте, что в вашем каталоге пользователей (User DN) доступны все необходимые пользователи:

```bash
ldapsearch -x -LLL -h '<Имя или IP-адрес LDAP-сервера>' \
  -p '<Порт LDAP-сервера>' \
  -D '<имя сервисного аккаунта>' \
  -w '<пароль сервисного аккаунта (Bindpass)>' \
  -b "<Каталог пользователей (User DN)>" \
  '<Атрибут имени пользователя (User Attribute)>' \
  distinguishedName \
  -s sub "(objectClass=user)"
```

Пример

```bash
ldapsearch -x -LLL -h ldap.mycompany.local \
      -p 389 \
      -D sa \
      -w 'p@$sw0rd' \
      -b "OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal" \
```

```
      sAMAccountName \
      distinguishedName \
      -s sub "(objectClass=user)"

    dn: OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    distinguishedName: OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal

    dn: CN=user3,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    distinguishedName:
CN=user3,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    sAMAccountName: user3

    dn: CN=user1,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    distinguishedName:
CN=user1,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    sAMAccountName: user1

    dn: CN=kubeadmin1,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    distinguishedName:
CN=kubeadmin1,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    sAMAccountName: kubeadmin1

    dn: CN=kubeadmin2,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    distinguishedName:
CN=kubeadmin2,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    sAMAccountName: kubeadmin2

    dn: CN=user2,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    distinguishedName:
CN=user2,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    sAMAccountName: user2
```

2. Выберите из списка любого пользователя и используйте его атрибут `distinguishedName` для дальнейших проверок. Получите список групп, в которые входит данный пользователь:

```
BASH
ldapsearch -x -LLL -h '<Имя или IP-адрес LDAP-сервера>:<Порт LDAP-сервера>'
\
  -D '<имя сервисного аккаунта>' \
  -w '<пароль сервисного аккаунта (Bindpass)>' \
  -b "<Каталог групп (Group DN)>" \
  '<Фильтр групп (Group Filter)>'
```

Пример

```
BASH
ldapsearch -x -LLL -h ldap.mycompany.local\
      -D sa \
      -w 'p@$sw0rd' \
      -b "OU=Nova,OU=Groups,OU=Kubernetes,DC=nova,DC=internal" \
```

```
      '(&(objectClass=group)
(member:1.2.840.113556.1.4.1941:=CN=user2,OU=Nova,OU=Users,OU=Kubernetes,DC=
nova,DC=internal))'

    dn: CN=Nova-users,OU=Nova,OU=Groups,OU=Kubernetes,DC=nova,DC=internal
    objectClass: top
    objectClass: group
    cn: Nova-users
    member: CN=user2,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    member: CN=kubeadmin1,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    member: CN=user1,OU=Nova,OU=Users,OU=Kubernetes,DC=nova,DC=internal
    distinguishedName: CN=Nova-
users,OU=Nova,OU=Groups,OU=Kubernetes,DC=ms,DC=infra
```

В выводе команды видно, что в каталоге есть только одна группа `Nova-users`, в которой находится пользователь `user2`.

Провайдеры идентификации

Компонент *StarVault* в Nova Container Platform имеет встроенный OAuth-сервер, который отвечает за логику работы с провайдерами идентификации и выдачу новых токенов доступа.

После установки платформы администратор может выполнить настройку методов аутентификации в *StarVault*, подключив различные провайдеры аутентификации.

1. Провайдер идентификации по умолчанию

По умолчанию, после установки Nova Container Platform сконфигурирован внутренний провайдер идентификации `Username`.

Данный провайдер содержит одну учетную запись `kubeadmin`, находящуюся в группе `kubeadmins`.

В Kubernetes создан объект *ClusterRoleBinding* `nova:kubeadmins`, описывающий привязку кластерной роли `cluster-admin` к группе `kubeadmins`.

2. Поддерживаемые провайдеры идентификации

Вы можете использовать следующие провайдеры идентификации в Nova Container Platform:

Провайдер идентификации	**Описание**
`Username`	Настройка выполняется с помощью метода аутентификации `userpass` (Username & Password). Используется внутреннее хранилище учетных данных *StarVault*.
`Token`	Для аутентификации используется токен доступа к *StarVault*. Может быть создан администратором и использован в случаях, когда необходимо предоставить краткосрочный доступ к кластеру Kubernetes без создания дополнительных пользователей.
LDAP	Настройка выполняется с помощью метода аутентификации `ldap`. В качестве служб каталогов могут использования решения, поддерживающие LDAPv3, например, FreeIPA, Microsoft Active Directory, OpenLDAP и другие.

Провайдер идентификации	Описание
`OIDC`	В качестве провайдеров идентификации могут быть использованы решения, поддерживающие протокол OpenID Connect (OIDC), например, Keycloak, Dex, StarVault, Gitlab и другие.
`Okta`	Аутентификация через интеграцию с облачной службой идентификации Okta.
`RADIUS`	Аутентификация через провайдер идентификации по протоколу RADIUS.
`GitHub`	Аутентификация через интеграцию с сервисом GitHub.

После настройки провайдера идентификации вы можете перейти к настройке RBAC в Kubernetes.