Интеграция Orion soft StarVault со службой каталога ALD Pro

04/07/2026

StarVault - это комплексное решение для безопасного управления секретами и доступом к ним, обеспечивающее централизованное хранение и защиту конфиденциальной информации в организации.

Интеграция позволяет вести базу пользователей централизованно в ALD Pro, а также перенести функции аутентификации и авторизации на ALD Pro через LDAP. Это позволит пользователям аутентифицироваться в StarVault с использованием учетных записей из ALD Pro и получать доступы к приложениям Nova в соответствии с группами и ролями. Интеграция выполняется путем настройки LDAP-метода аутентификации в веб-интерфейсе StarVault, создания внешних групп и алиасов, а также привязки назначений к OIDC-приложениям для доступа к Nova Console и kubectl.

Инструкция по интеграции разработана компанией OrionSoft и размещена.

1. Создание сервисной учетной записи

Аутентификация и авторизация выполняются методом LDAP Bind, для чего необходимо создать в ALD Pro сервисную учётную запись, которая не является POSIX-пользователем, не имеет прав на вход в домен и не отображается в портале управления, а используется только для чтения LDAP.
Для этого нужно подключиться по SSH к контроллеру домена и выполнить следующие шаги:
1. Создать файл с именем ldap-bind.update.
2. Внести в файл следующее содержимое:

dn: uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: ldap-bind
add:userPassword: securePassword
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0

Разъяснения:

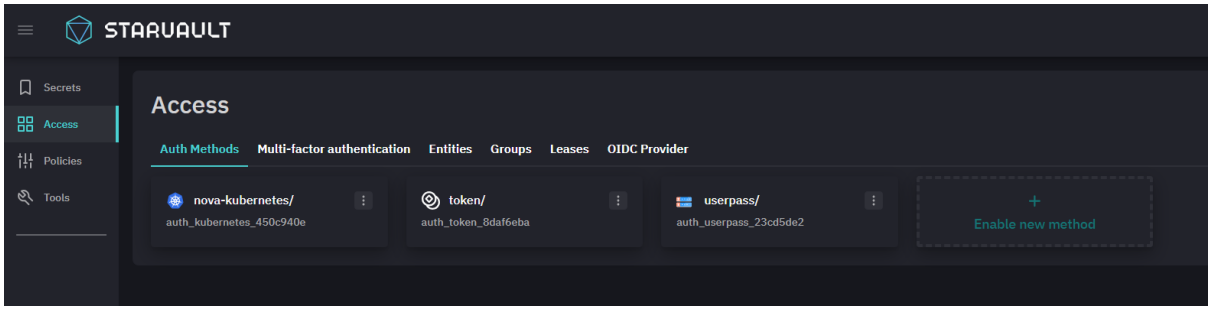
- ***dn*** *— уникальный идентификатор записи пользователя в LDAP*
- ***add:objectclass: account*** *— добавляет базовый класс для учётной записи*
- ***add:objectclass: simplesecurityobject*** *— добавляет класс для хранения пароля и других атрибутов безопасности*
- ***add:uid: ldap-bind*** *— уникальный идентификатор пользователя*
- ***add:userPassword: securePassword*** *— пароль для учётной записи, заменить на желаемый*
- ***add:passwordExpirationTime: 20380119031407Z*** *— время истечения пароля (можно адаптировать под политики безопасности)*
- ***add:nsIdleTimeout: 0*** *— отключает таймаут простоя для этой учетной записи*

3. Выполнить добавление пользователя следующей командой:

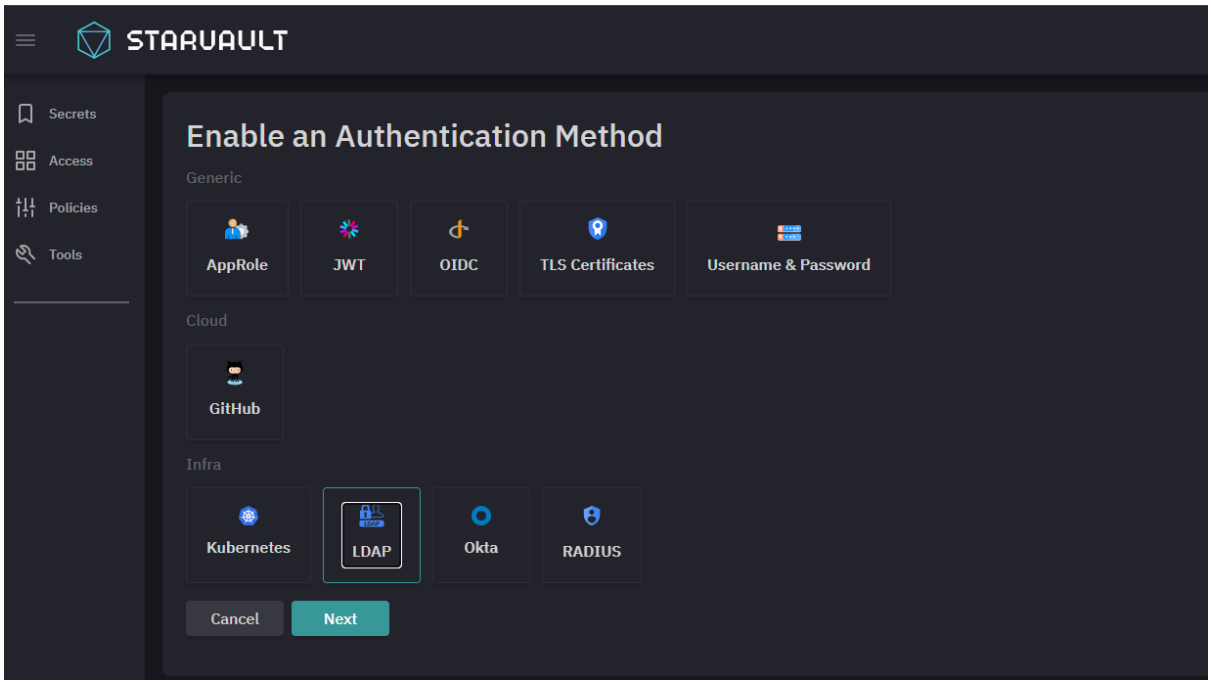
kinit admin && ipa-ldap-updater ldap-bind.update

2. Настройка метода аутентификации LDAP

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



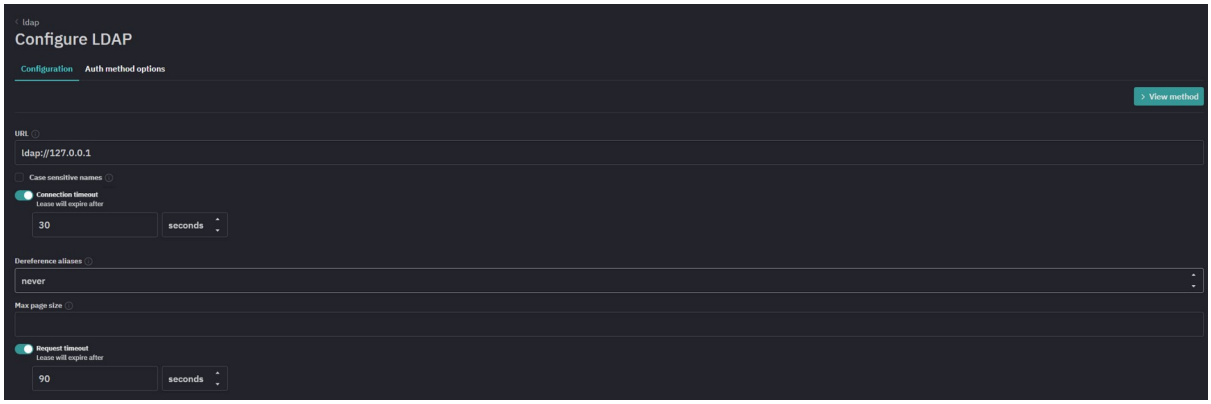
2. Выберите опцию Enable new method, далее - LDAP и нажмите Next.



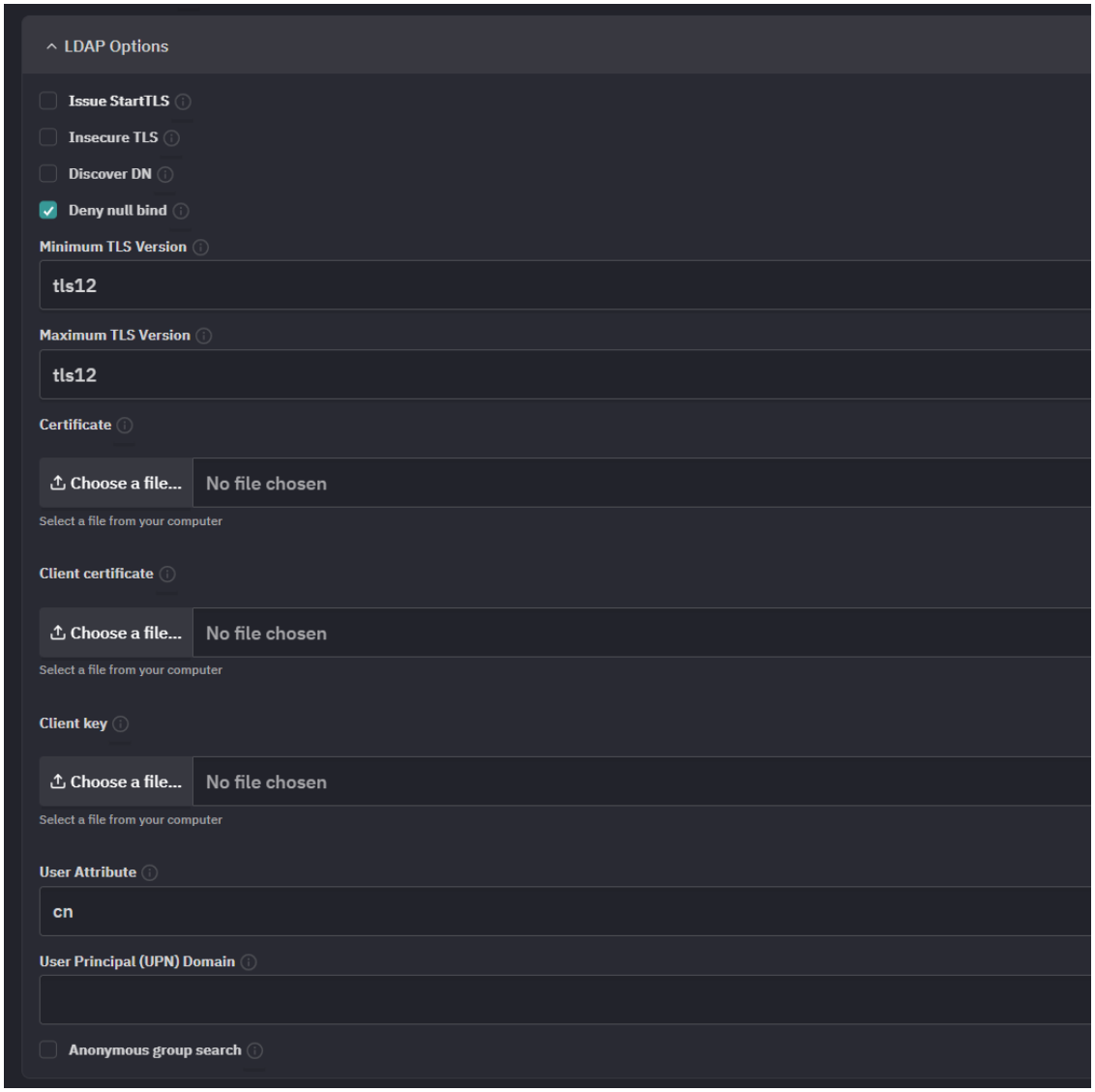
3. Определите значение параметра path и настройте дополнительные параметры в меню Method Options при необходимости, далее нажмите Enable Method.

4. Выполните настройку созданного метода аутентификации в окне Configure LDAP.

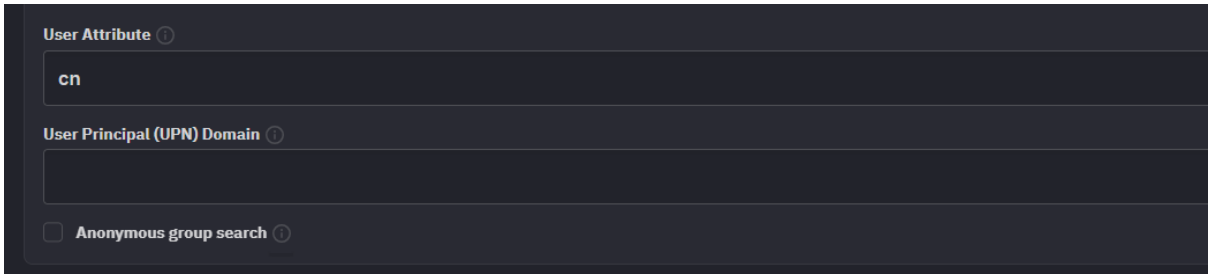
В поле URL укажите URL-адрес сервера(ов) LDAP. Вы можете оставить по умолчанию параметры токенов, полученных в результате аутентификации данным методом



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

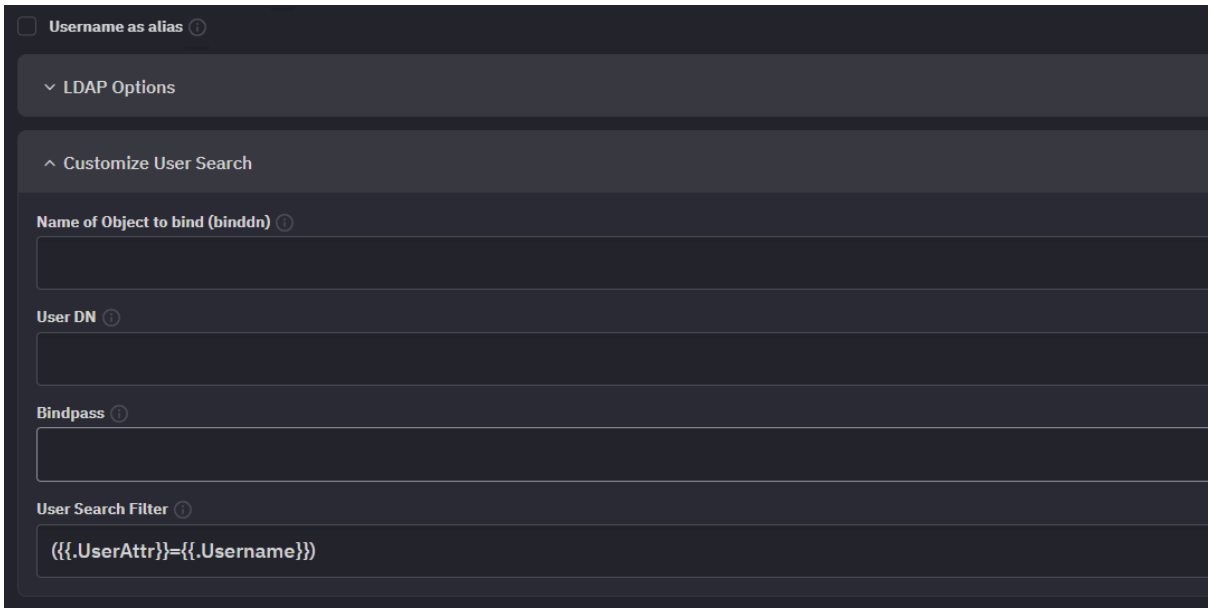


В поле User Attribute укажите имя атрибута пользовательского объекта, который соответствует имени пользователя. В зависимости от провайдера идентификации пользовательский атрибут может принимать такие значение, как `sAMAccountName`, `cn`, `uid` и другие.



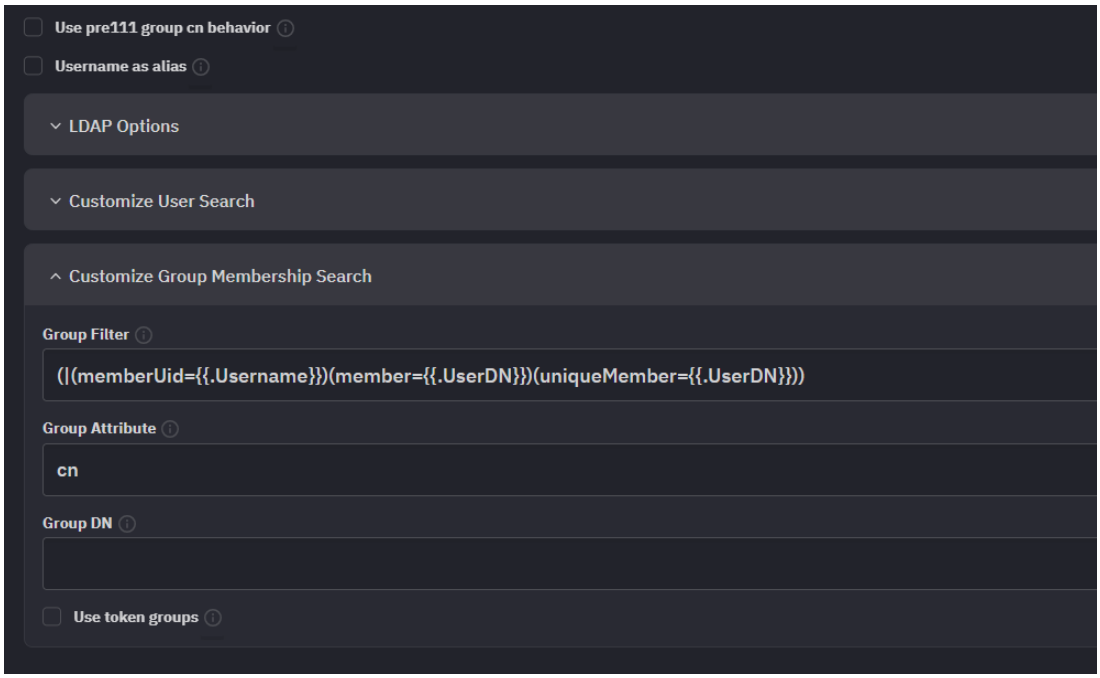
- Перейдите ниже и разверните меню Customize User Search.
- В поле Name of Object to bind (binddn) укажите уникальное имя (DN) сервисной учетной записи для выполнения операций поиска в каталоге LDAP-сервера.

- В поле Bindpass укажите пароль сервисной учетной записи 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.



- 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.
- 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:
    - На LDAP-сервер отправляется запрос параметра `tokenGroups` для пользователя. При этом в качестве базы для поиска будет использован User DN;
    - Из полученного токена берется SID каждой группы и запрашивается ее имя.

Чтобы сохранить, установленные настройки, нажмите Save.



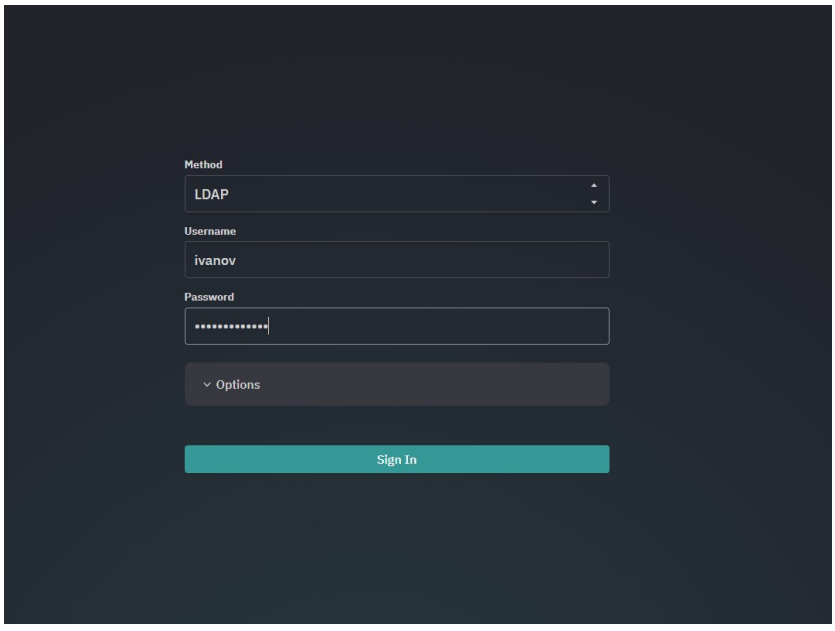
- Настройка фильтров и атрибутов групп необходима для того, чтобы определить, членом каких групп является пользователь. Конфигурация для этого может различаться в зависимости от вашего LDAP-сервера (провайдера идентификации) и схемы его каталога.

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`.

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

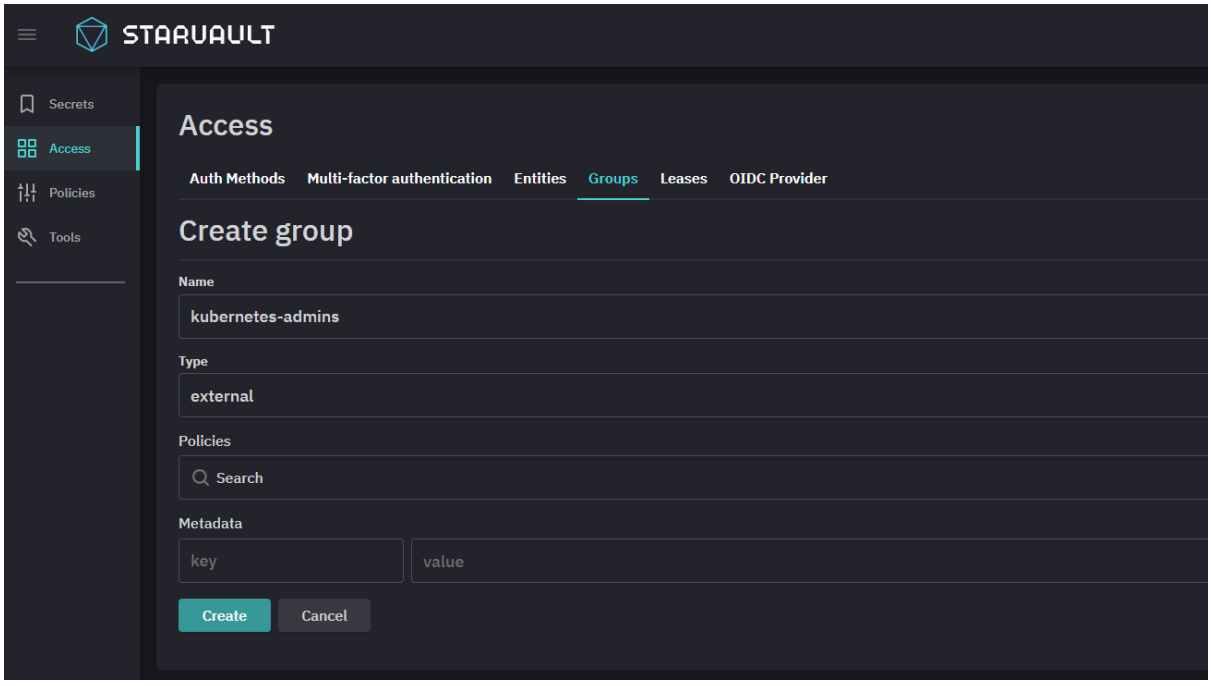


Если при настройке метода аутентификации вы не меняли параметр `path`, то при входе опцию Mount path можно не указывать.

3. Настройка группы пользователей для дальнейшей интеграции с Nova

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.



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.

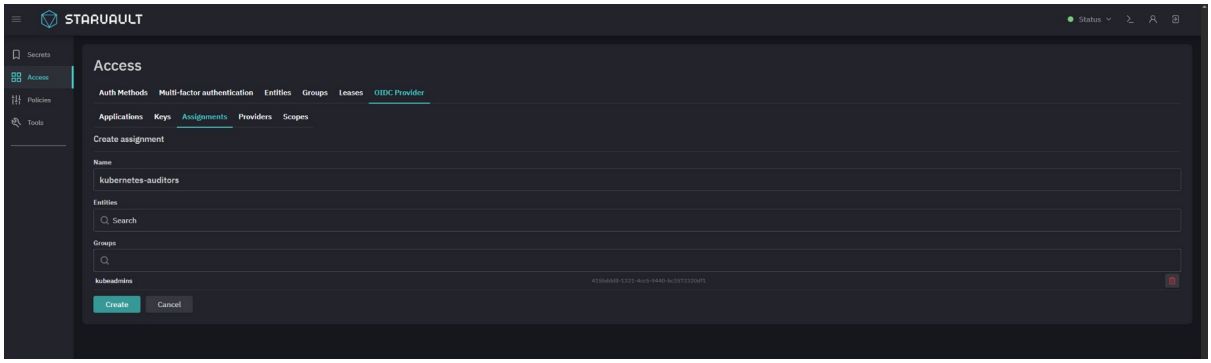
- В поле Name укажите имя алиаса так же, как группа названа в каталоге LDAP-сервера.
- В поле Auth Backend выберете имя метода аутентификации LDAP.
- Нажмите Create, чтобы создать алиас

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.

Настройка доступа к приложениям OIDC

Для возможности использования приложений Nova Container Platform пользователи должны быть явно назначены каким-либо приложениям. Для настройки назначения приложений воспользуйтесь процедурой ниже.

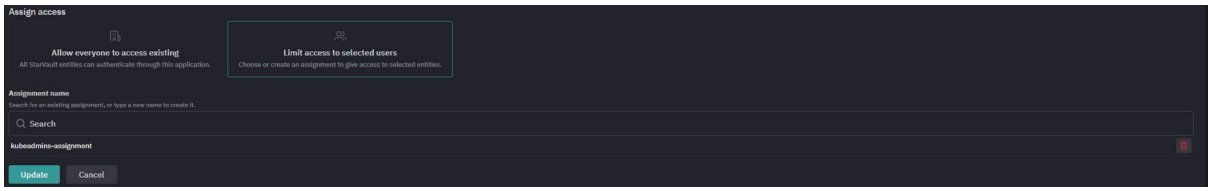
1. Откройте веб консоль StarVault.
2. Перейдите в раздел Access, далее OIDC Provider.
3. Перейдите в список Assignments и нажмите Create assignment.
    - В поле Name укажите имя назначения. Это может быть, например, имя группы пользователей в каталоге LDAP-сервера.
    - В поле Entities укажите ранее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



Привязка назначений к приложениям

Для привязки назначения к приложению воспользуйтесь процедурой ниже.

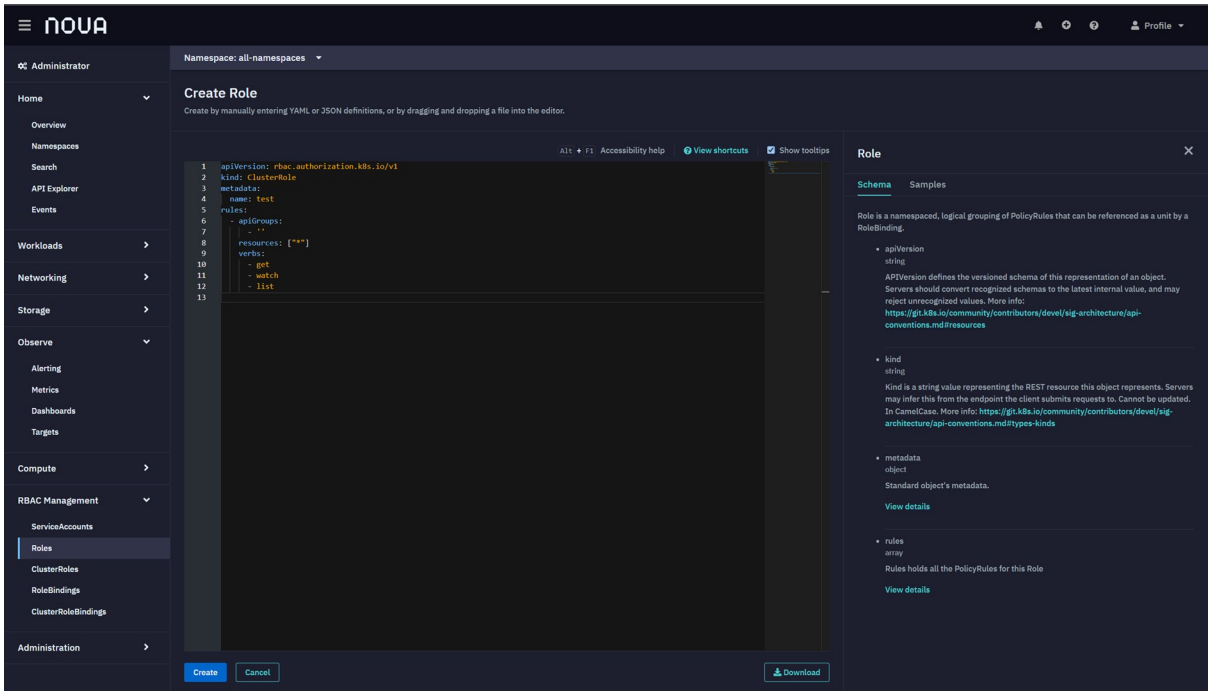
1. Откройте веб консоль StarVault.
2. Перейдите в раздел Access, далее OIDC Provider.
3. Перейдите в список Applications и выберете необходимое приложение. Например, для добавления пользователям возможности выполнять аутентификацию в утилите kubectl или веб-интерфейсе Nova Console, выберете приложение `oidc-kubernetes-client`.
    - Нажмите Edit application.
    - В разделе Assign access добавьте ранее настроенное назначение в список разрешенных.
    - Нажмите Update, чтобы обновить параметры назначения.



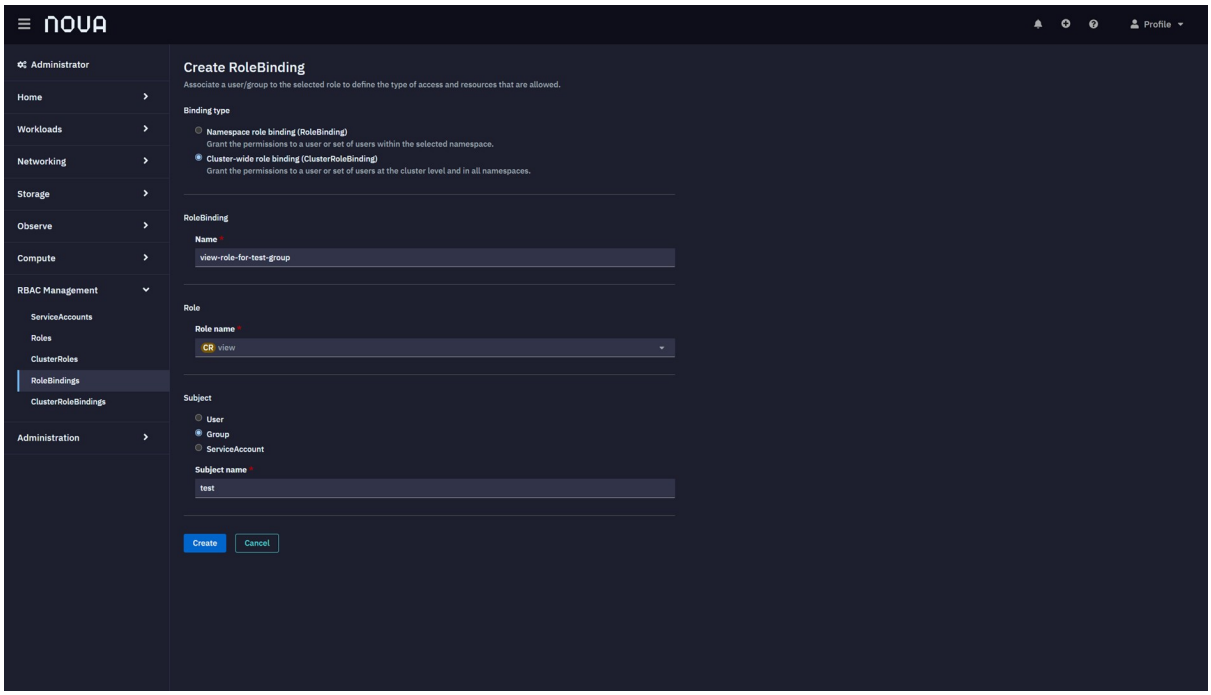
3. Доступ к Nova Console и kubectl

Сначала, необходимо создать роль, которой будет обладать пользователь/группа или использовать уже имеющуюся. Действия проводятся в веб-интерфейсе Nova.

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



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»*:



Теперь все члены группы имеют доступ на чтение ко всем ресурсам кластера через Nova Console.