Интеграция Боцман со службой каталога ALD Pro

12/15/2025

Содержание

1 ВВЕДЕНИЕ

Платформа Боцман (Bootsman) – это контейнерная платформа управления и оркестрации, предоставляющая инструменты для развертывания и управления приложениями в многокластерной инфраструктуре. Интеграция ALD Pro с Платформой Боцман позволяет централизованно управлять пользователями и их правами доступа, обеспечивает единую аутентификацию через LDAP и упрощает соблюдение корпоративных стандартов безопасности.

2 НАСТРОЙКА НА КОНТРОЛЛЕРЕ ДОМЕНА ALD PRO

2.1 Создание сервисной учетной записи LDAP

Для подключения к ALD Pro из Платформы Боцман необходимо создать специальную сервисную учетную запись, которая будет использоваться для аутентификации через LDAP. Эта учетная запись не является POSIX-пользователем, не имеет прав на вход в домен и используется только для чтения LDAP.

Подключитесь по SSH к контроллеру домена и создайте файл для добавления сервисной учетной записи:

```
sudo nano /tmp/ldap-bind.update
```

Добавьте следующее содержимое в файл:

```
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: <SECURE_PASSWORD>
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

Замените `<SECURE_PASSWORD>` на безопасный пароль в соответствии с политиками безопасности вашей организации. Параметр `passwordExpirationTime` установлен на 2038 год для учетных записей сервисов. При необходимости адаптируйте его под политики безопасности.

Примените изменения:

```
kinit admin
sudo ipa-ldap-updater /tmp/ldap-bind.update
```

Система запросит пароль администратора ALD Pro. Убедитесь, что команда выполнена без ошибок.

Проверьте создание учетной записи:

```
ldapsearch -x -H ldap://dc-1.ald.company.lan \
  -D "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" \
  -W -b "uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan" uid
```

Убедитесь, что вывод содержит информацию о созданной учетной записи.

2.2 Создание группы пользователей

После установки и первичной настройки контроллера необходимо создать группу пользователей для управления доступом к Платформе Боцман. Подключитесь по SSH к контроллеру домена или используйте веб-интерфейс управления ALD Pro.

Создайте группу с помощью команды IPA:

```
sudo ipa group-add bootsman --desc="Bootsman Platform Users"
```

Или через графический интерфейс ALD Pro, перейдя в раздел `Пользователи и компьютеры → Группы пользователей`:

1. Нажмите кнопку для создания новой группы
2. В поле "Название группы" введите: `bootsman`
3. В поле "Подразделение" выберите организационную структуру, например: `bootsman.host`
4. В поле "Описание" введите: `Bootsman Platform Users`
5. Нажмите "Сохранить"

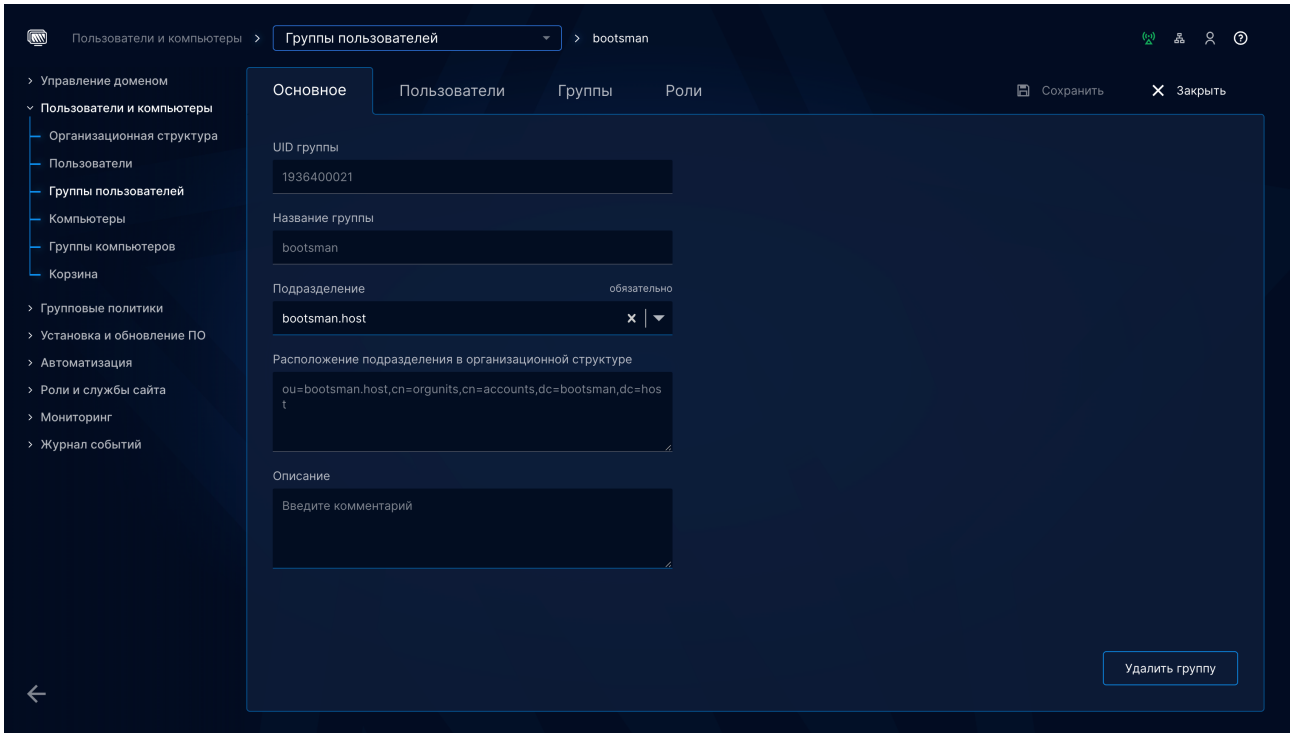

Рис.1 Окно настроек группы пользователей.

Добавьте пользователей в группу (эта операция может быть выполнена позже, когда пользователи будут созданы):

```
sudo ipa group-add-member bootsman --users=test_user1
sudo ipa group-add-member bootsman --users=test_user2
```

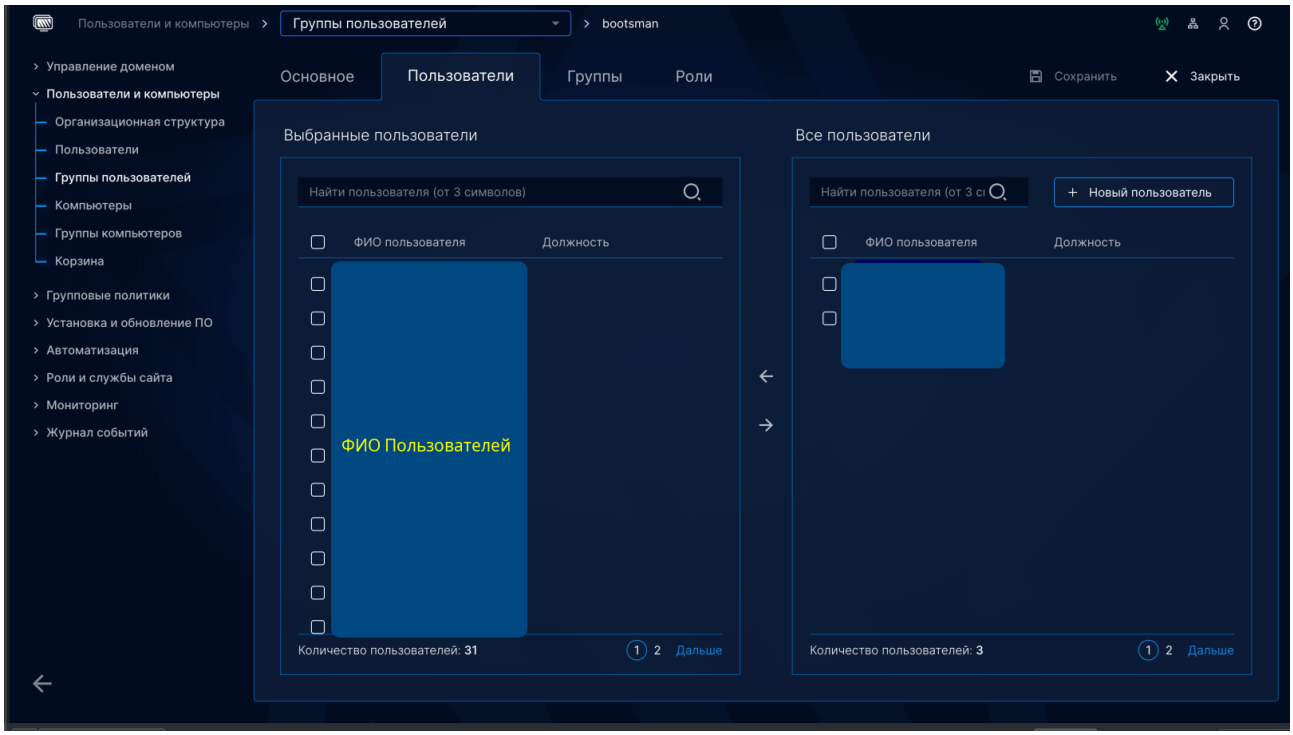

Рис. 2 Окно настроек Пользователей.

Проверьте членство в группе:

```
sudo ipa group-show bootsman
```

Вывод должен содержать список всех членов группы и информацию о группе.

3 НАСТРОЙКА ИНТЕГРАЦИИ В ПЛАТФОРМЕ БОЦМАН

3.1 Подключение провайдера аутентификации ALD Pro

Необходимо авторизоваться в веб-интерфейсе Платформы Боцман под ролью "Администратор" и подключить ALD Pro в качестве внешнего провайдера аутентификации.

Выполните следующие шаги:

1. Авторизуйтесь в Платформе Боцман с учетной записью администратора
2. Перейдите в левом меню в раздел `Users & Authentication`

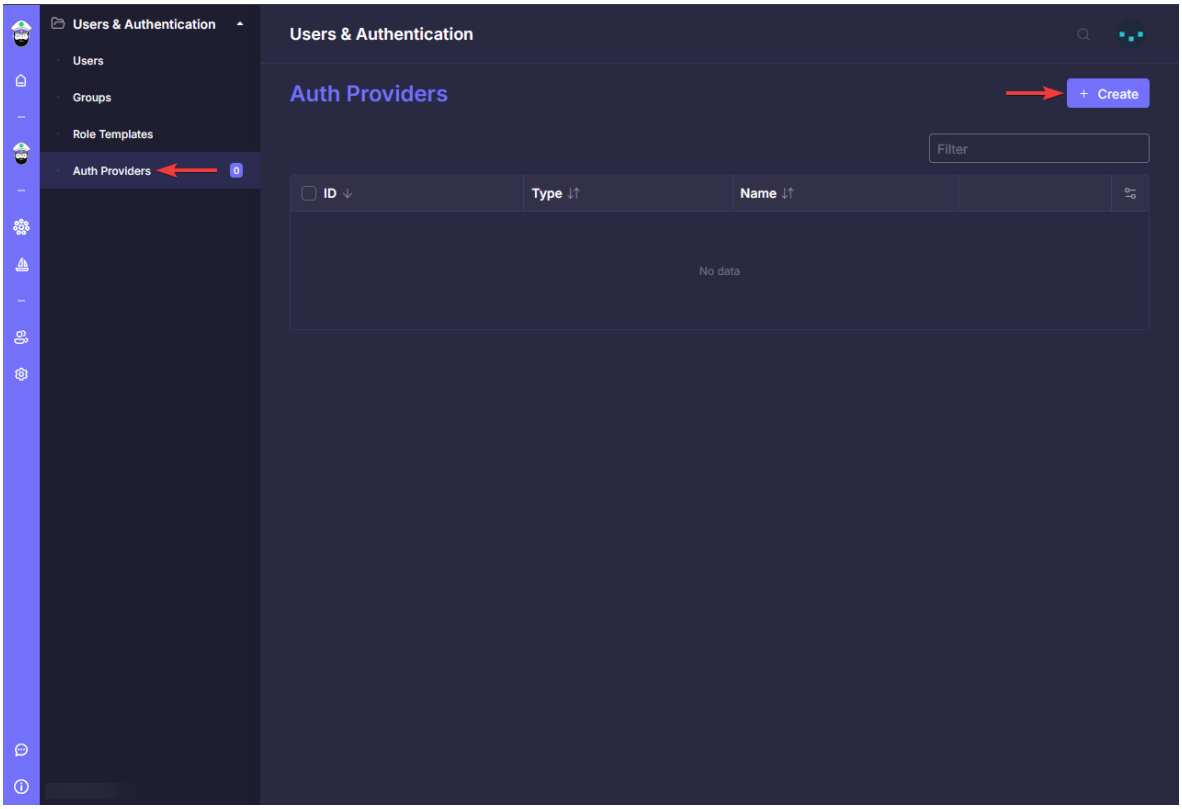

Рис. 3 Окно управления сторонними провайдерами аутентификации.

На открывшейся странице нажмите кнопку "`+ Create`" в окне "`Auth Providers`":

3. В поле "`ID`" задайте уникальное имя (например, `aldpro-bootsman`)
4. В выпадающем списке "`Type`" выберите `ALD Pro`
5. В поле "`Name`" введите описательное имя (например, `ALD Pro Bootsman`)

3.2 Заполнение конфигурации подключения LDAP

В поле "`Data`" заполните конфигурацию в JSON-формате:

```
{
```

```
  "host": "dc-1.ald.company.lan:389",
  "insecureNoSSL": false,
  "bindDN": "uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan",
  "bindPW": "<SECURE_PASSWORD>",
  "usernamePrompt": "ALD Pro Username",
  "userSearch": {
    "baseDN": "cn=users,cn=accounts,dc=ald,dc=company,dc=lan",
    "filter": "(objectClass=person)",
    "idAttr": "uid",
    "emailAttr": "mail",
    "nameAttr": "cn"
  },
  "groupSearch": {
    "baseDN": "cn=groups,cn=accounts,dc=ald,dc=company,dc=lan",
    "filter": "(objectClass=groupOfNames)",
    "userMatchers": [
      {
        "userAttr": "entrydn",
        "groupAttr": "member"
      }
    ],
    "nameAttr": "cn"
  }
}
```

Замените `<SECURE_PASSWORD>` на пароль сервисной учетной записи `ldap-bind`, созданной на контроллере домена.

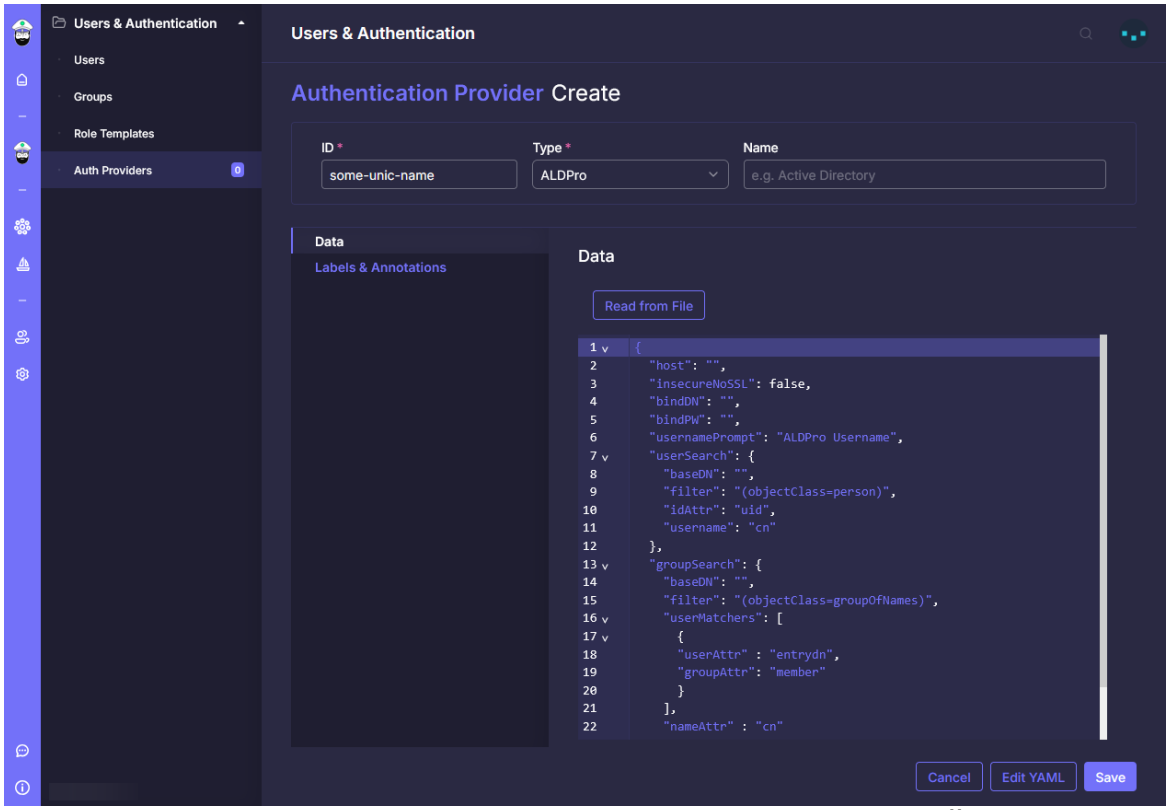

Рис. 4 Заполнение необходимых для подключения полей.

3.3 Описание полей конфигурации

Параметр	Описание	Пример значения
`host`	Адрес и порт контроллера домена ALD Pro. Стандартный порт LDAP: 389 (незащищенный), 636 (защищенный TLS)	`dc-1.` ald.company.lan `:636`
`insecureNoSSL`	Игнорировать ошибки сертификата TLS. `false` — проверять сертификат, `true` — игнорировать	`false`
`bindDN`	Distinguished Name сервисной учетной записи для аутентификации и чтения LDAP	`uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan`
`bindPW`	Пароль сервисной учетной записи	`<SECURE_PASSWORD>`
`usernamePrompt`	Текст подсказки для поля ввода имени пользователя в форме авторизации	`ALD Pro Username`
`userSearch.baseDN`	DN структуры в директории, в которой ищутся пользователи	`cn=users,cn=accounts,dc=ald,dc=company,dc=lan`
`userSearch.filter`	LDAP-фильтр для поиска объектов типа "пользователь"	`(objectClass=person)`
`userSearch.idAttr`	Атрибут LDAP, который будет использоваться как username для входа в Боцман	`uid`
`userSearch.emailAttr`	Атрибут LDAP для получения email адреса пользователя	`mail`
`userSearch.nameAttr`	Атрибут LDAP для отображения полного имени пользователя в интерфейсе	`cn`

`groupSearch.baseDN`	DN структуры в директории, в которой ищутся группы	`cn=groups,cn=accounts,dc=ald,dc=company,dc=lan`
`groupSearch.filter`	LDAP-фильтр для поиска объектов типа "группа"	`(objectClass=groupOfNames)`
`groupSearch.userMatchers`	Правило для сопоставления пользователя с группой. userAttr указывает атрибут пользователя (DN), groupAttr указывает атрибут группы, в котором хранятся члены группы	`{"userAttr": "entrydn", "groupAttr": "member"}`
`groupSearch.nameAttr`	Атрибут LDAP для получения имени группы	`cn`

После заполнения всех полей нажмите кнопку "`Save`" для сохранения конфигурации.

3.4 Проверка подключения

После сохранения конфигурации провайдер аутентификации будет отображаться в списке подключенных. Система автоматически проверит подключение к контроллеру домена. Если подключение успешно, провайдер будет готов к использованию.

Теперь группы пользователей и отдельные пользователи, имеющие необходимые разрешения и выданные в контроллере домена ALD Pro, будут присутствовать в списке доступных групп и пользователей при назначении ролей.

4 НАСТРОЙКА ПРАВ И НАЗНАЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

4.1 Управление ролями группы пользователей

Для работы с пользователями, включенными в группу контроллера домена, необходимо установить корректные права в Платформе Боцман. Перейдите в раздел "`Users & Authentication`" → "`Groups`":

1. На странице управления группами найдите группу `bootsman`, импортированную из ALD Pro
2. Откройте контекстное меню группы (три точки ⋮)
3. Выберите пункт "Редактировать конфигурацию"

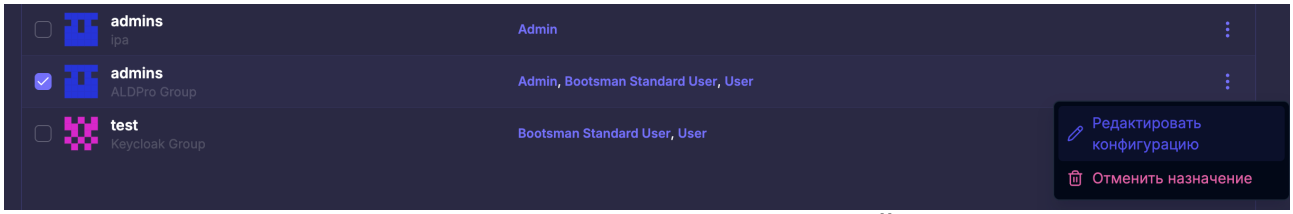

Рис.5 Переход в меню редактирования ролей группы.

На открывшейся странице редактирования установите необходимые роли и права:

4. Установите флаг "`Standard User`" для назначения базовых прав пользователя
5. Установите флаг "`Bootsman Standard User`" для доступа к функционалу платформы
6. При необходимости установите дополнительные флаги для специальных прав (администратор, управление кластерами и т.д.)

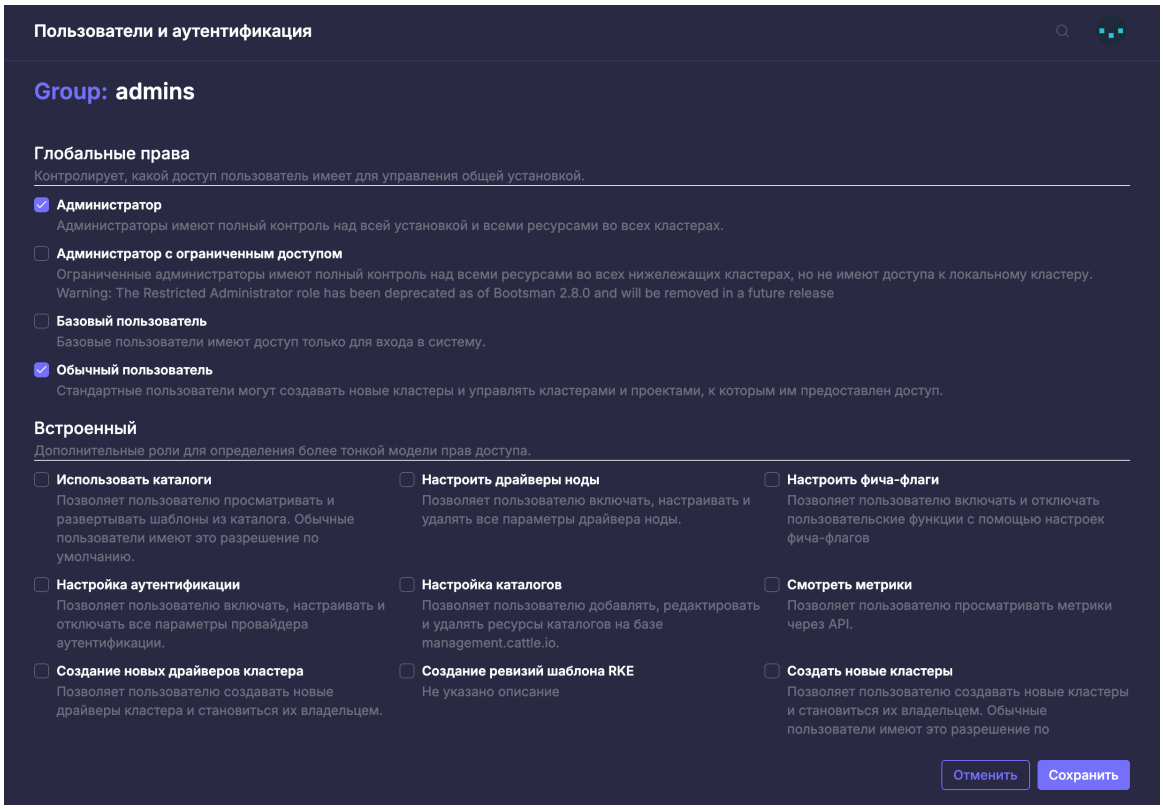

Рис. 6 Настройка прав группы через выбор необходимых ролей.

Роль	Описание
Глобальные права	
Администратор	Полный контроль над всей установкой и всеми ресурсами во всех кластерах
Администратор с ограниченным доступом	Полный контроль над всеми ресурсами во всех нижележащих кластерах, но без доступа к локальному кластеру
Обычный пользователь	Стандартные пользователи могут создавать новые кластеры и управлять кластерами и проектами, к которым им предоставлен доступ
Встроенные роли	
Использовать каталоги	Позволяет пользователю просматривать и развертывать шаблоны из каталога
Настройка аутентификации	Позволяет пользователю включать, настраивать и отключать параметры провайдера аутентификации

Создание новых драйверов кластера	Позволяет пользователю создавать новые драйверы кластера и становиться их владельцем
Настроить драйверы ноды	Позволяет пользователю включать, настраивать и удалять параметры драйвера ноды
Настройка каталогов	Позволяет пользователю добавлять, редактировать и удалять ресурсы каталогов
Настроить фича-флаги	Позволяет пользователю включать и отключать пользовательские функции через фича-флаги
Просмотр метрик	Позволяет пользователю просматривать метрики через API
Создать новые кластеры	Позволяет пользователю создавать новые кластеры и становиться их владельцем

После установки необходимых ролей и прав нажмите кнопку "`Save`" для сохранения изменений.

4.2 Назначение пользователей к проектам

Для назначения пользователя из группы контроллера домена к конкретному проекту необходимо:

1. Перейдите в левом меню в раздел "`Home`" (рус. "Главная")
2. Выберите интересующий кластер
3. Перейдите в раздел "`Cluster`" → "`Projects/Namespaces`" (рус. "Кластер" → "Проекты/Пространства имен")
4. Выберите интересующий проект (например, "Default")
5. На странице проекта откройте вкладку "`Configuration`" (рус. "Конфигурация")
6. Нажмите на кнопку "Edit Config (More Options)" в контекстном меню (три точки ⋮)

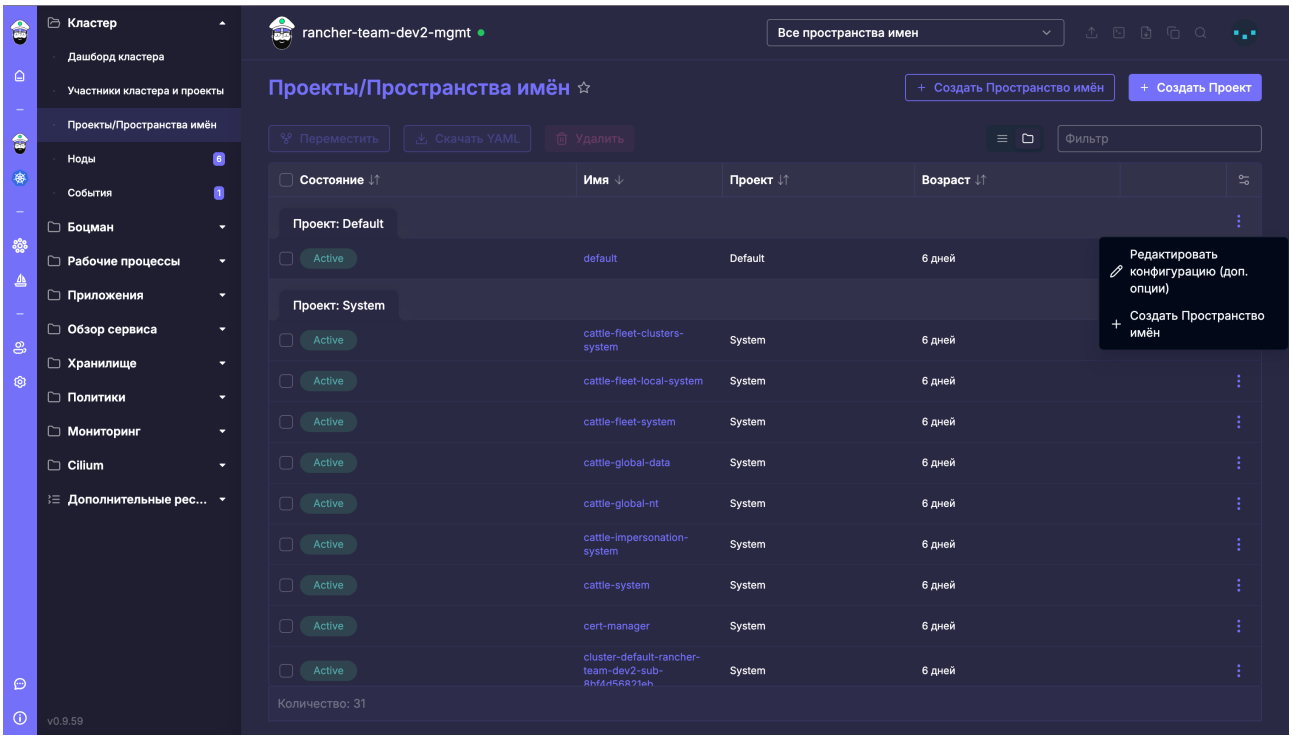

Рис. 7 Переход к настройке проекта через контекстное меню.

7. На открывшейся странице перейдите в раздел "`Members`" (рус. "Участники")
8. Нажмите кнопку "`+ Add`" (рус. "Добавить")

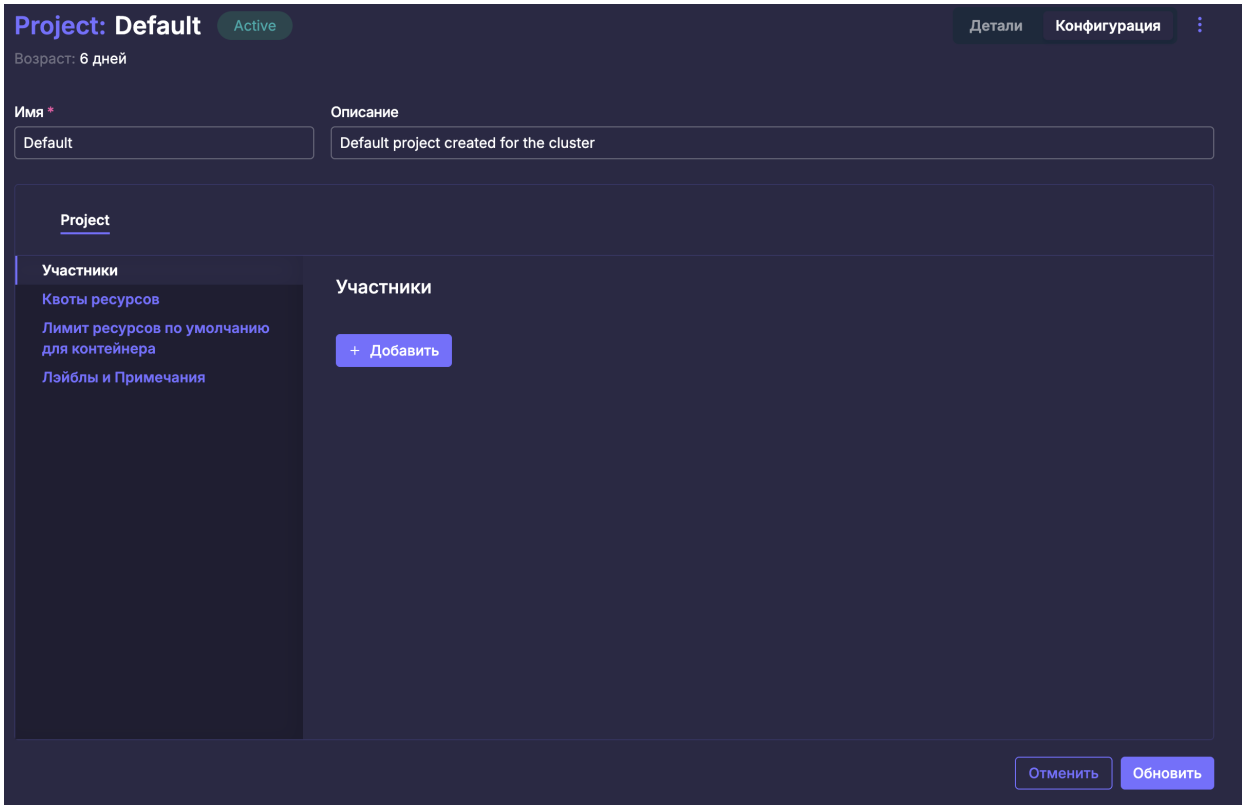

Рис. 8 Окно настроек проекта.

4.3 Добавление пользователя в проект

В открывшемся диалоговом окне выполните следующие шаги:

1. В поле поиска "Выберите участника" найдите нужного пользователя из ALD Pro
2. В раскрывающемся списке ролей выберите соответствующую роль

Роль проекта	Описание
Bootsman Project Member	Полный доступ к управлению проектом и его ресурсами
Default Project Member	Стандартный доступ к ресурсам проекта
Bootsman Project Viewer	Доступ только для чтения (read-only) к ресурсам проекта
Настраиваемый	Выбор индивидуальных ролей и разрешений для данного пользователя

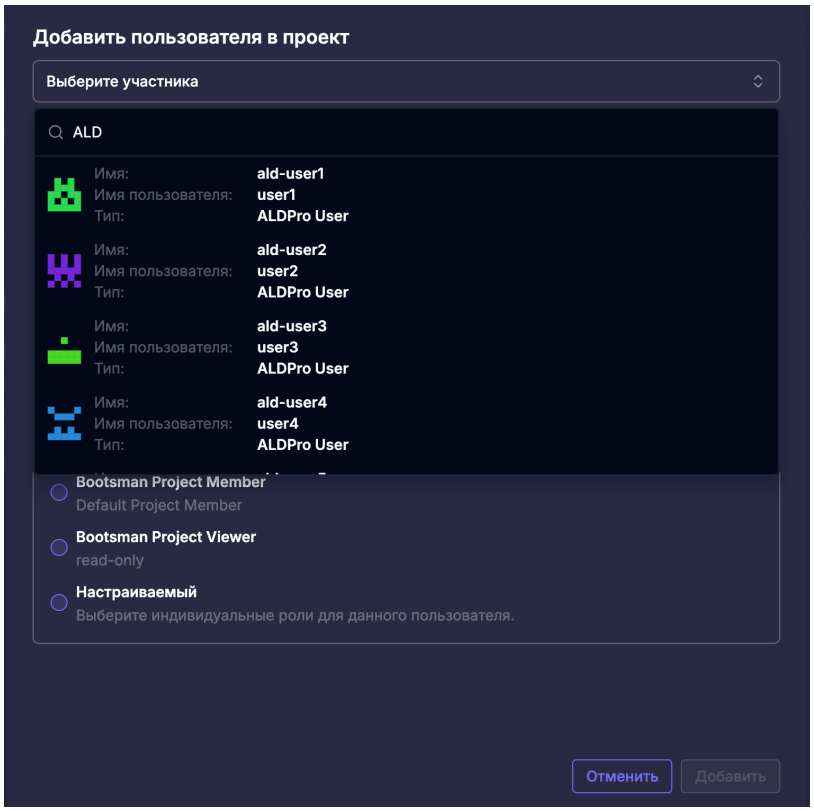

Рис.9 Поиск и выбор пользователя/группы. Назначение прав.

3. После выбора пользователя и роли нажмите кнопку "`Add`" (рус. "Добавить") в нижней части диалогового окна

Добавленный пользователь будет отображаться в списке участников на экране "Members" (рус. "Участники") в окне настроек проекта:

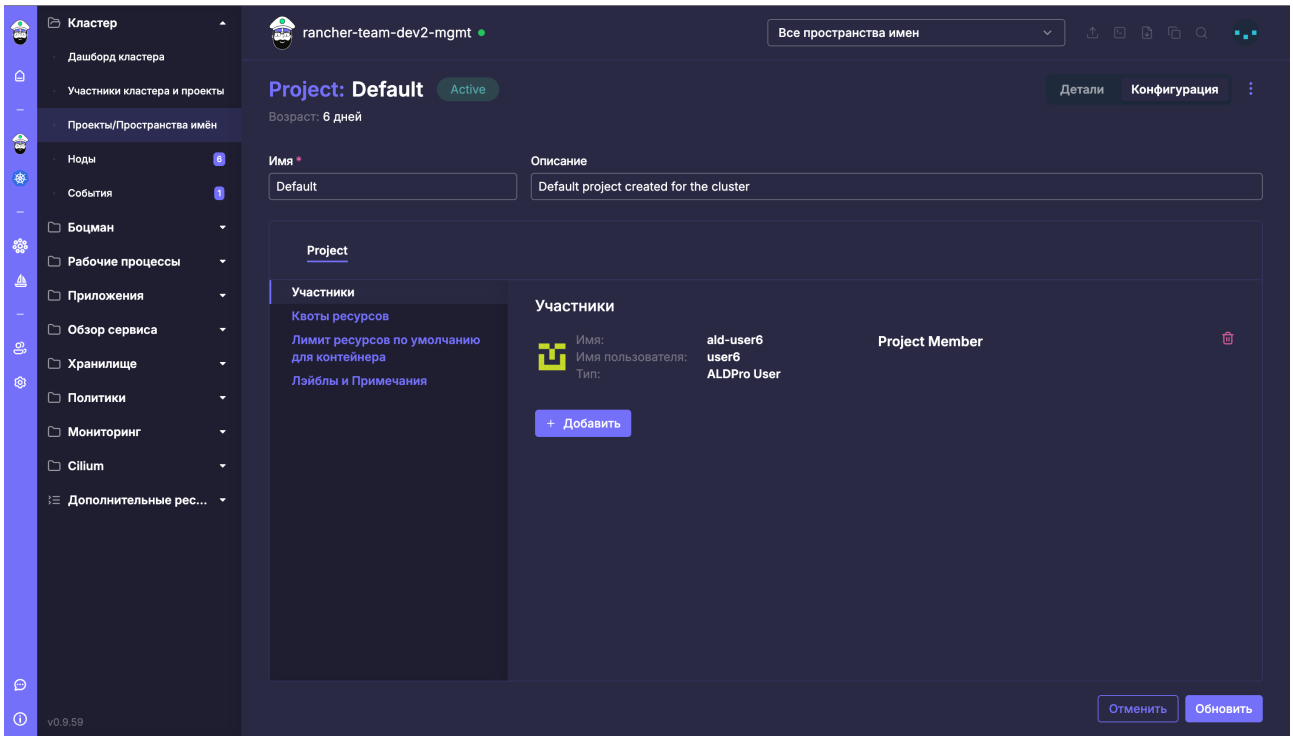

Рис.10 Отображение добавленного пользователя к проекту.

5 ПРОВЕРКА И ТЕСТИРОВАНИЕ

5.1 Проверка подключения LDAP

Перед полноценным использованием интеграции рекомендуется проверить подключение LDAP. Выполните следующие команды на сервере с Платформой Боцман или на контроллере домена:

```
ldapsearch -x -H ldap://dc-1.ald.company.lan \
  -D "uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan" \
  -W -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan" uid=*
```

Команда должна вернуть список всех пользователей в директории.

Проверьте поиск по группам:

```
ldapsearch -x -H ldap://dc-1.ald.company.lan \
  -D "uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan" \
  -W -b "cn=groups,cn=accounts,dc=ald,dc=company,dc=lan" cn=*
```

Команда должна вернуть список всех групп в директории.

5.2 Тестирование авторизации в Платформе Боцман

Откройте веб-браузер и перейдите на страницу входа в Платформу Боцман:

```
https://bootsman.ald.company.lan
```

На странице входа должны быть доступны следующие опции аутентификации:

- Локальная учетная запись администратора (Admin)
- Аутентификация через ALD Pro (если провайдер успешно подключен)

Выполните вход с учетной записью пользователя из ALD Pro:

1. В форме входа выберите провайдер "ALD Pro Bootsman" или "ALD Pro"
2. Введите username пользователя (значение атрибута uid из ALD Pro)
3. Введите пароль пользователя
4. Нажмите кнопку "Вход"

Если авторизация пройдена успешно, пользователь будет перенаправлен на главную страницу Платформы Боцман, где будут доступны все ресурсы и проекты в соответствии с назначенными ролями.

5.3 Проверка членства в группах

После успешной авторизации пользователя проверьте корректность синхронизации группы и прав. Перейдите в раздел "`Users & Authentication`" → "`Groups`" и убедитесь, что:

- Группа "bootsman" отображается в списке доступных групп
- Пользователи, включенные в группу на контроллере домена, отображаются как члены группы в Платформе
- Назначенные роли и разрешения применяются корректно

6 РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

1. **Использование TLS для LDAP:** Рекомендуется использовать защищенное подключение LDAPS (порт 636) вместо незащищенного LDAP (порт 389). Установите `"insecureNoSSL": false` и укажите порт 636 в параметре `host`
2. **Безопасность пароля сервисной учетной записи:** Используйте сложный пароль для учетной записи `ldap-bind` и храните его в защищенном хранилище (vault, secrets management system)
3. **Ограничение прав LDAP-bind:** Сервисная учетная запись должна иметь минимальные необходимые права только для чтения LDAP
4. **Аудит доступа:** Включите логирование всех попыток входа в Платформе Боцман и отслеживайте логи контроллера домена
5. **Регулярное обновление пароля:** Периодически обновляйте пароль сервисной учетной записи в соответствии с политиками безопасности
6. **Контроль доступа к сетевым портам:** Убедитесь, что порты LDAP (389, 636) доступны только авторизованным системам
7. **Резервная копия конфигурации:** Регулярно создавайте резервные копии конфигурации Платформы Боцман и контроллера домена