Интеграция Atlassian Confluence со службой каталога ALD Pro

03/10/2026

Содержание

Confluence — система управления задачами и проектами, поддерживающая централизованную аутентификацию и синхронизацию пользователей из внешних каталогов.
В настоящей инструкции описана процедура интеграции Confluence со службой каталога ALD Pro. Данная интеграция обеспечит аутентификацию через единую точку входа по протоколу LDAP/LDAPS, автоматическую загрузку профиля (имя, фамилия, e-mail), а также даст возможность управлять доступом через группы (в Confluence локально или через LDAP — в зависимости от выбранного режима).

1 Настройка сервисной учетной записи в ALD Pro

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.

Порядок создания сервисной учетной записи

1. Перед выполнением команды задайте следующие параметры:

```
PASS='Pa$$w0rd'
LDAP_USER='system'
LDAP_BASE_DN='dc=ald,dc=company,dc=lan'
```

Разъяснения:

- `PASS` — пароль сервисной учётной записи,
- `LDAP_USER` — имя создаваемой сервисной LDAP-учётной записи,
- `LDAP_BASE_DN` — базовый DN вашего домена LDAP.

Примеры базового DN:

```
ald.company.lan → dc=ald,dc=company,dc=lan
```

2. Подключитесь по SSH к контроллеру домена и выполните следующую команду:

```
PASS='Pa$$w0rd'
LDAP_USER='system'
LDAP_BASE_DN='dc=ald,dc=company,dc=lan'

sudo bash -c '
PW_B64=$(printf "%s" "'"$PASS"'" | base64 -w0)
LDAP_USER="'"$LDAP_USER"'"
LDAP_BASE_DN="'"$LDAP_BASE_DN"'"
EXPIRATION=$(date -u -d "+5 years" +"%Y%m%d%H%M%SZ")

cat > /tmp/${LDAP_USER}.update <<EOF
dn: uid=${LDAP_USER},cn=sysaccounts,cn=etc,${LDAP_BASE_DN}
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: ${LDAP_USER}
add:userPassword:: ${PW_B64}
add:passwordExpirationTime: ${EXPIRATION}
add:nsIdleTimeout: 0
EOF

kinit admin && ipa-ldap-updater /tmp/${LDAP_USER}.update
'
```

Команда выполняет следующие действия:

- кодирует указанный пароль в Base64 и сохраняет его в переменную `PW_B64;`

- создаёт файл `/tmp/${LDAP_USER}.update`, содержащий LDIF-описание сервисной учётной записи;
- получает Kerberos-билет администратора (`kinit admin`);
- применяет изменения из созданного LDIF-файла к LDAP-каталогу с помощью `ipa-ldap-updater`.

2 Настройка LDAP/LDAPS в Confluence

Настройка выполняется в интерфейсе Confluence по следующему пути (рис. 1 и рис. 2): **Администрирование → Управление пользователями → Каталоги пользователей → Добавить каталог.**

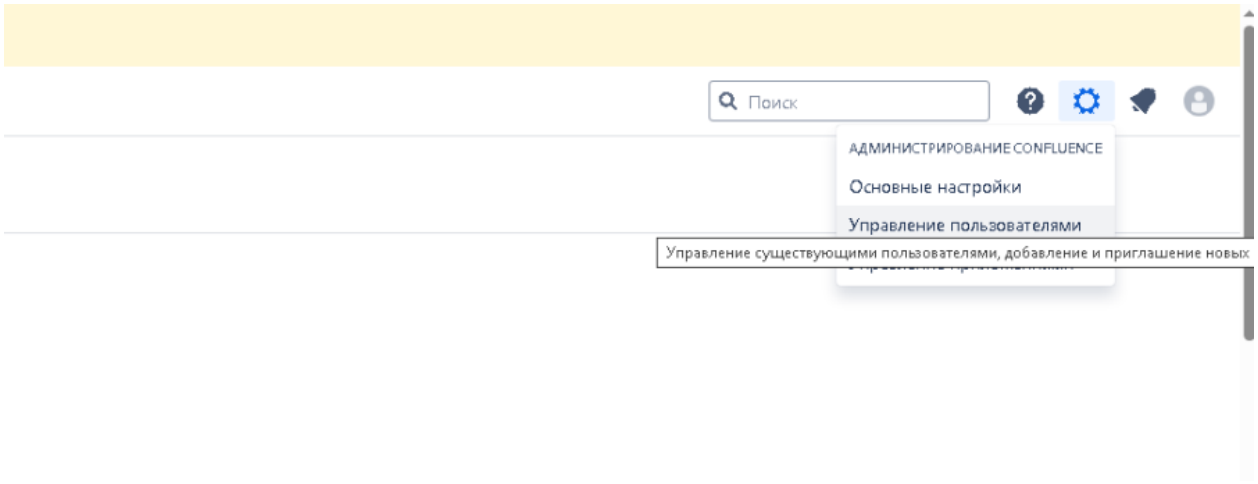

Рисунок 1 — переход в управление пользователями

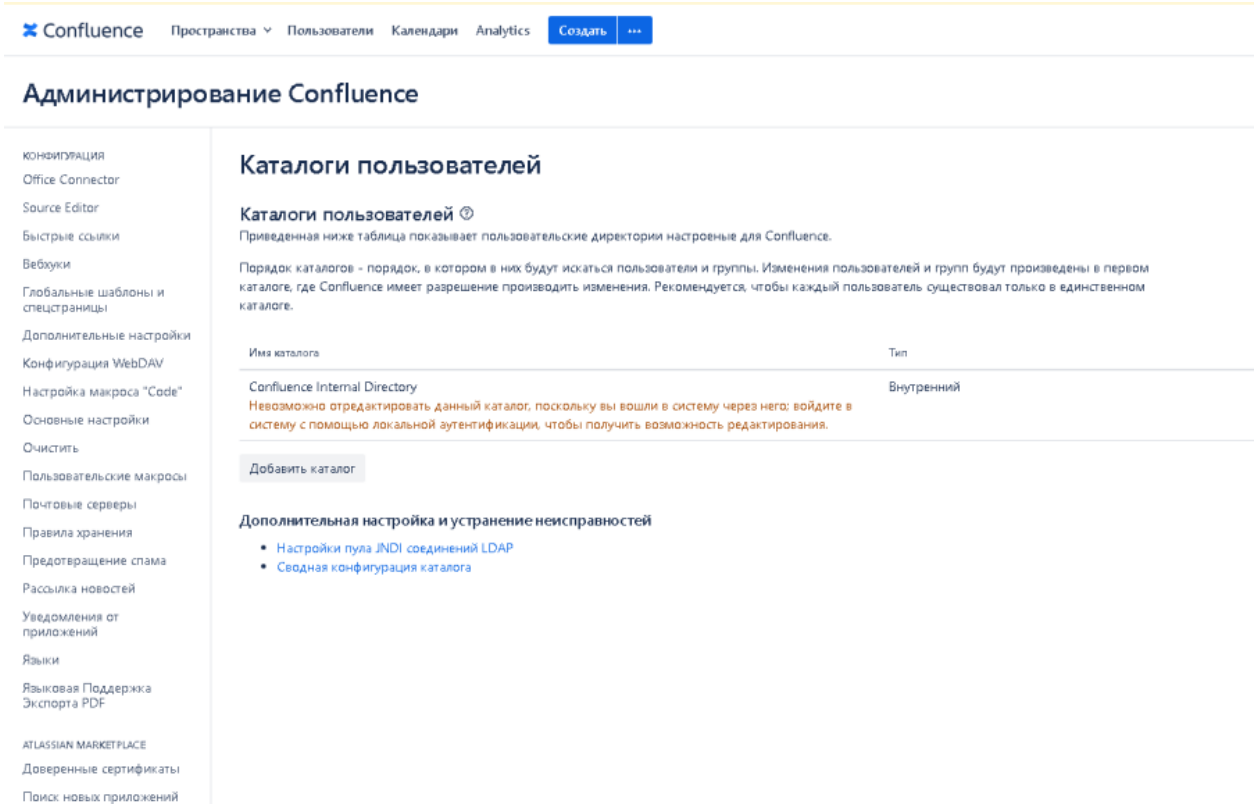

Рисунок 2 — Добавление LDAP-сервера

При добавлении выберите **«Настройки LDAP»** (рис. 3).

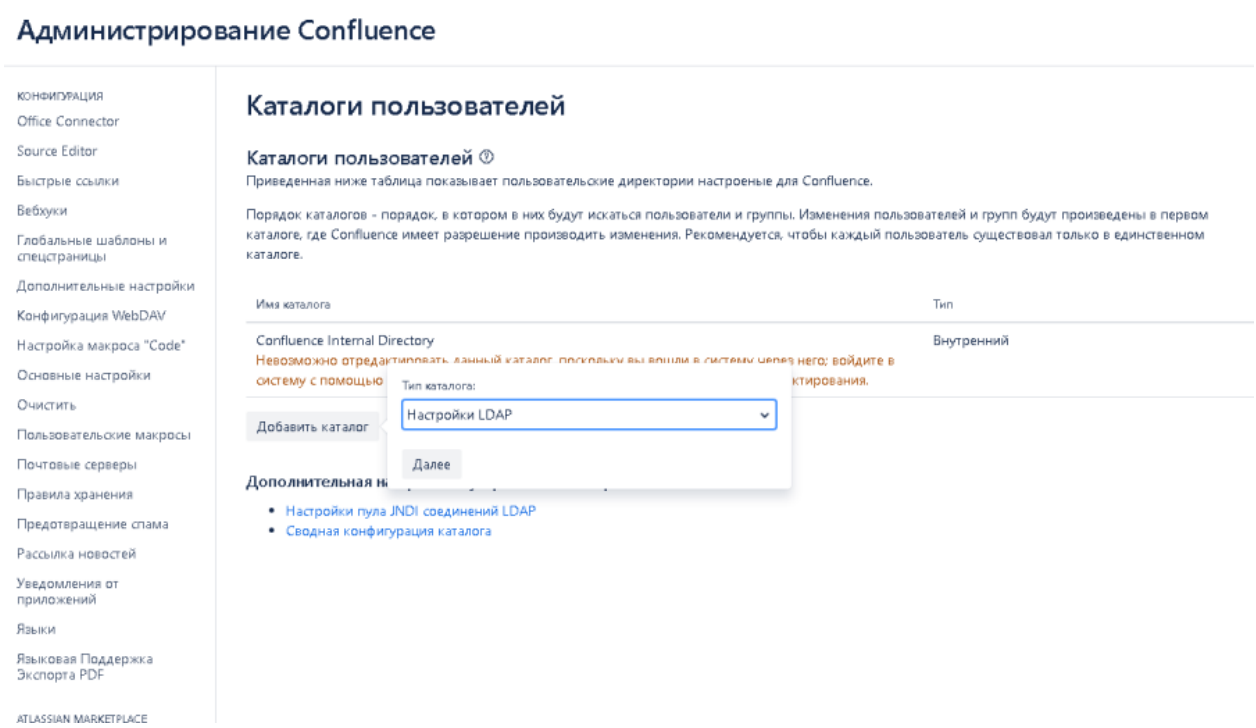

Рисунок 3 — Выбор типа сервера при добавлении

2.1 Настройки сервера (Server settings)

В открывшемся окне настроек заполните следующие поля (рис. 4):

- **Имя:** ALD
- **Тип каталога:** Generic Directory Server
- **Имя хоста:** dc01.ald.domain.lan
- **Порт:** 636
- **Использовать SSL:** да
- **Имя пользователя (Bind DN):** uid=bind_confluence,cn=users,cn=accounts,dc=ald,dc=domain,dc=lan
- **Пароль:** пароль сервисной учетной записи bind_confluence

В блоке **Схема LDAP** укажите следующее:

- **Base DN:** dc=ald,dc=domain,dc=lan

Дополнительные DN (ограничение области поиска):

- **Дополнительное DN пользователя:** cn=users,cn=accounts
- **Дополнительные DN группы:** cn=groups,cn=accounts

Это уменьшает объем поиска и ускоряет синхронизацию.
«Разрешения LDAP: Только для чтения, с локальными группами»
Данное разрешение означает следующее:

- пользователи загружаются из LDAP;
- группы для прав в Confluence ведутся локально (в Confluence);
- пользователей из LDAP можно добавлять к группам, ведение которых осуществляется во внутреннем каталоге Confluence;
- пользователи при входе в Confluence добавляются в локальную группу confluence-users.

Членство группы по умолчанию: confluence-users
При выборе «**Разрешения LDAP**: Только для чтения» пользователей требуется либо добавить к локальным группам доступа вручную, либо добавить разрешения на группы ALD в настройках доступа.

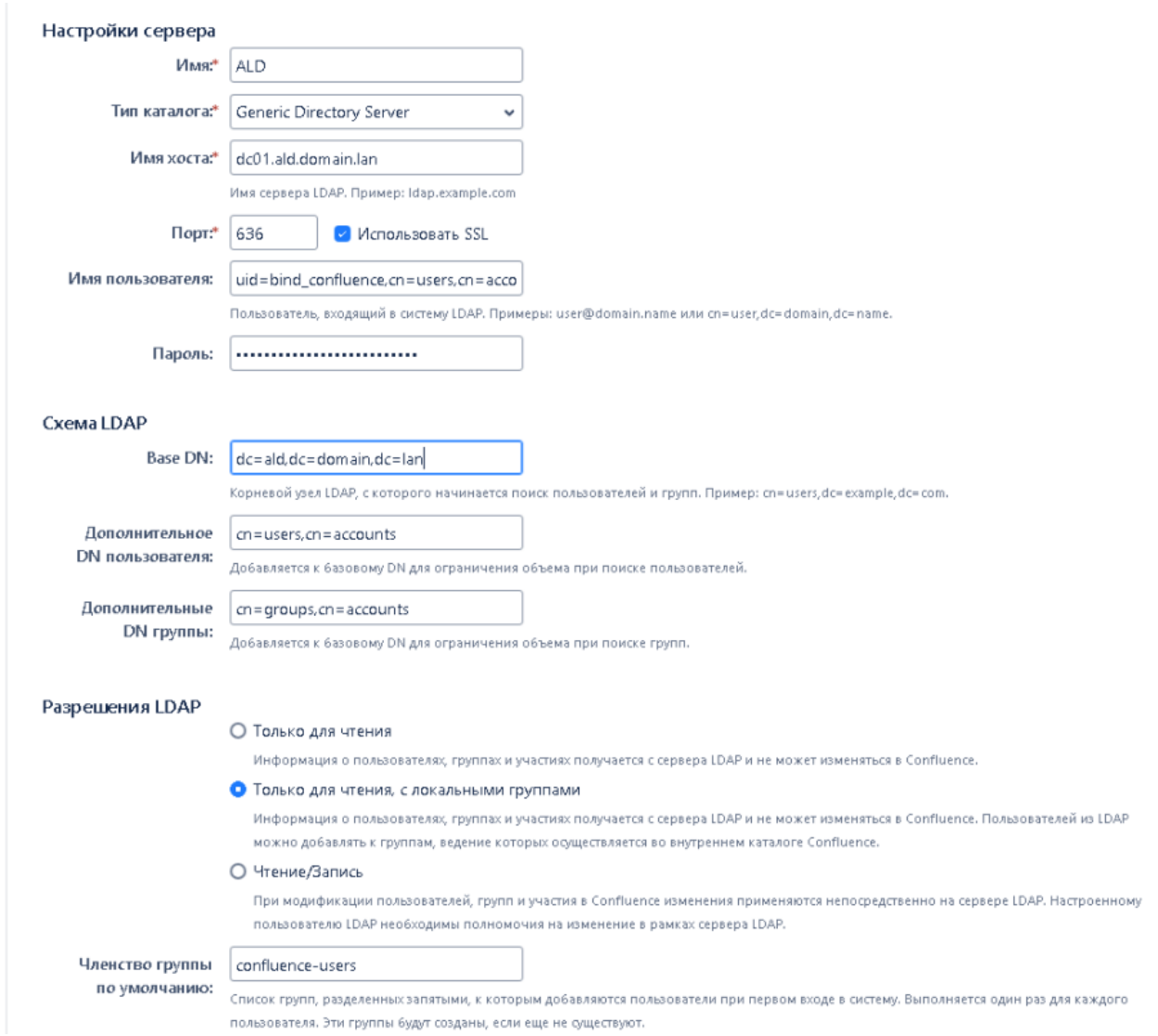

Рисунок 4 — Основные настройки сервера LDAP

2.2 Дополнительные настройки (синхронизация и параметры подключения)

В разделе **Дополнительные настройки** укажите следующее (рис. 5):

- **SSL и опции каталога :** Безопасный SSL
- **Обновлять участие в группах при входе:** При каждом входе пользователя
- **Интервал синхронизации (в минутах):** 60
- **Время ожидания чтения (в секундах):** 120
- **Тайм-аут поиска (в секундах):** 60

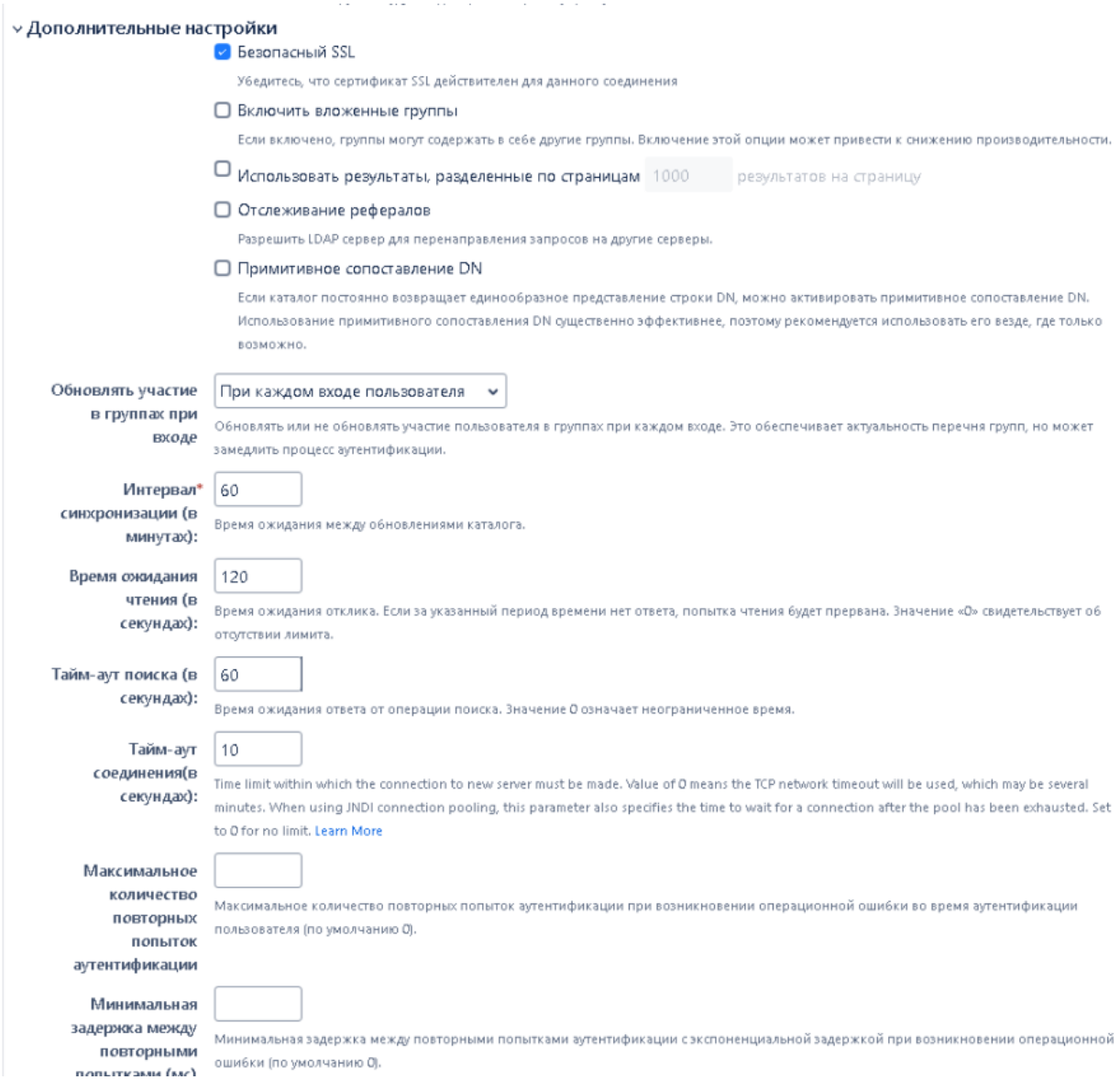

Рисунок 5. Дополнительные настройки

2.3 Параметры схемы пользователя

В разделе **Параметры настройки схемы пользователя** заполните поля следующим образом (рис. 6):

- **Класс объекта пользователя:** inetorgperson
- **Фильтр пользовательских объектов:** (objectClass= inetorgperson)
- **Атрибут "Полное имя пользователя":** uid
- **Атрибут "RDN имени пользователя":** cn
- **Атрибут "Имя пользователя":** givenName
- **Атрибут "Фамилия":** sn
- **Атрибут "Просмотр имени":** cn
- **Атрибут "Электронная почта":** mail
- **Атрибут "Пароль пользователя":** userPassword
- **Шифрование пароля пользователя:** SHA
- **Атрибут "Уникальный ID пользователя":** entryUUID

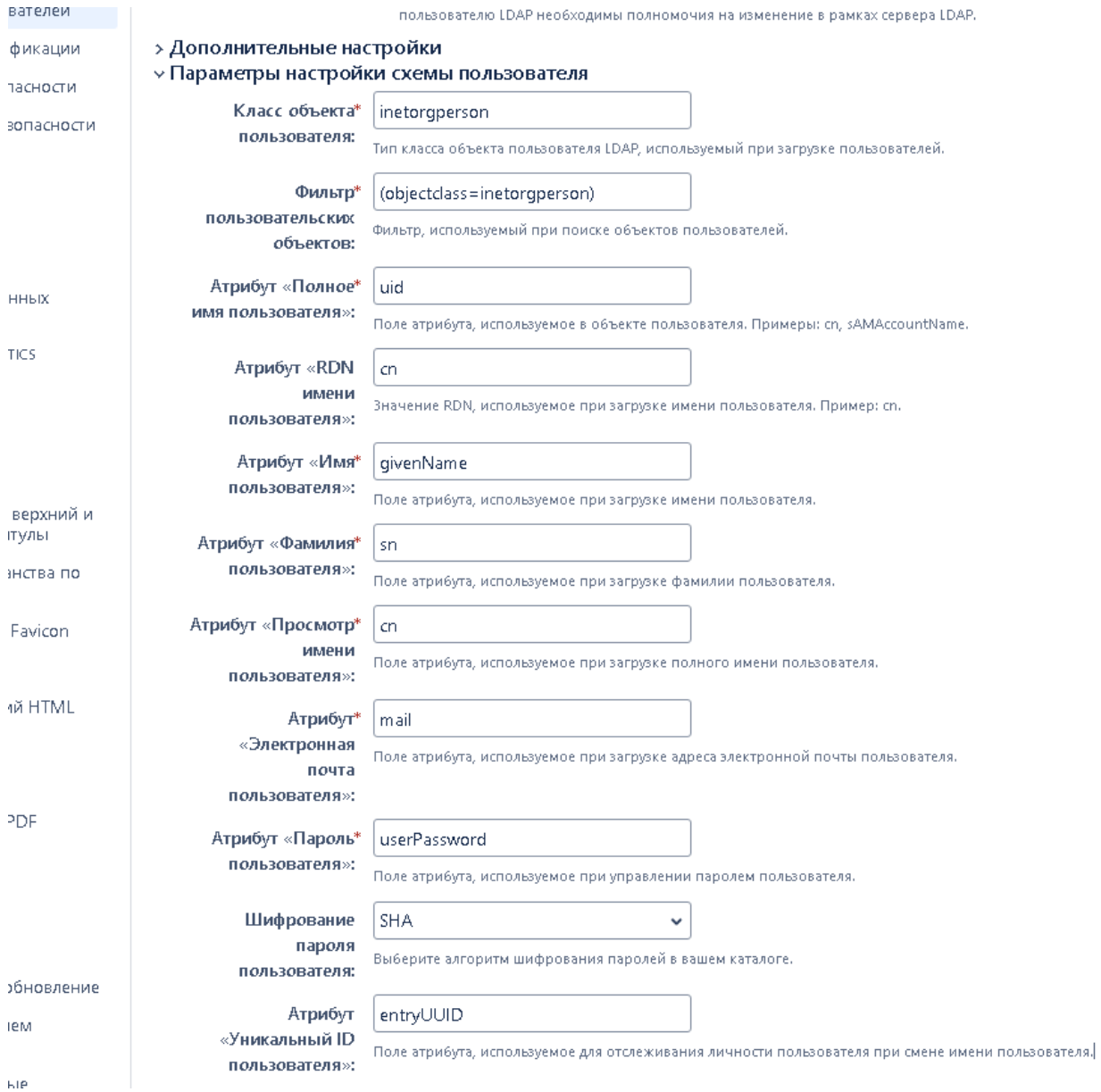

Рисунок 6 — Схема пользователя

2.4 Настройки групповой схемы

В разделе **Настройки групповой схемы** заполните поля следующим образом (рис. 7):

- **Класс группы объектов:** ipausergroup
- **Фильтр объектов группы:** (objectclass=ipausergroup)
- **Атрибут "Имя группы":** cn
- **Атрибут "Описание группы":** description

В разделе «**Параметры настройки схемы участия**» заполните следующее:

- **Атрибут Членов Группы:** member
- **Атрибут «Участие пользователя»:** memberof

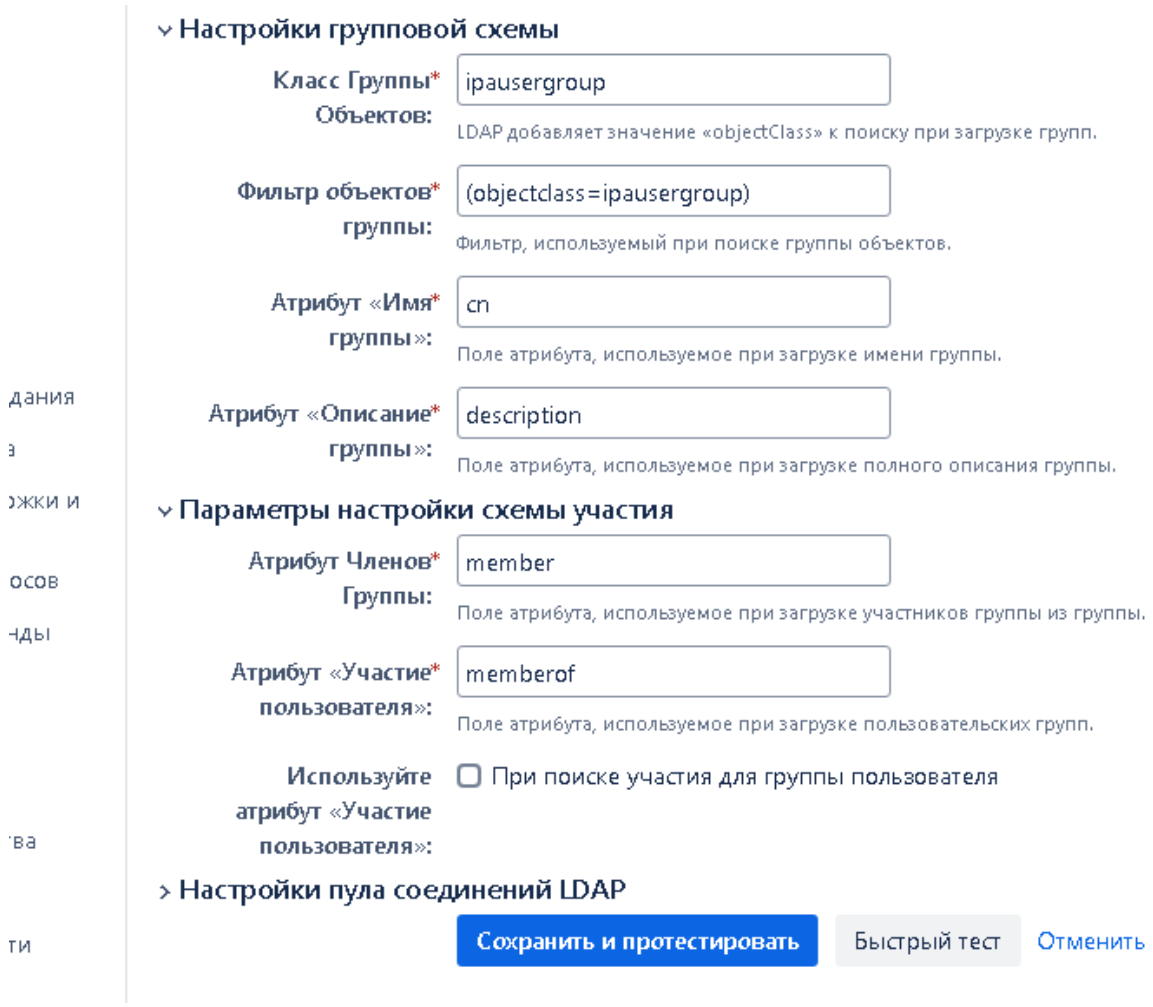

Рисунок 7 — Настройка групповой схемы

2.5 Сохранение и проверка

- Нажмите «**Быстрый тест**», если подключение пройдёт успешно, то вы увидите сообщение, приведенное на рисунке 8.

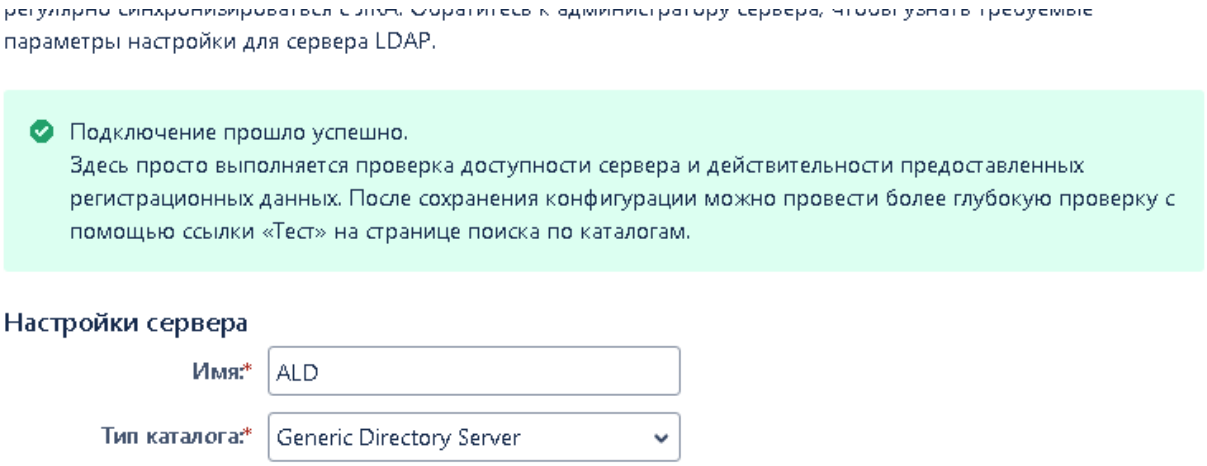

Рисунок 8 — Быстрый тест

- При успешном завершении теста нажмите **«Сохранить и протестировать»**.

- Убедитесь, что тест показывает успешное подключение и поиск объектов. При тестировании можно проверить аутентификацию пользователя ALD Pro. Пример приведён на рисунке 9.

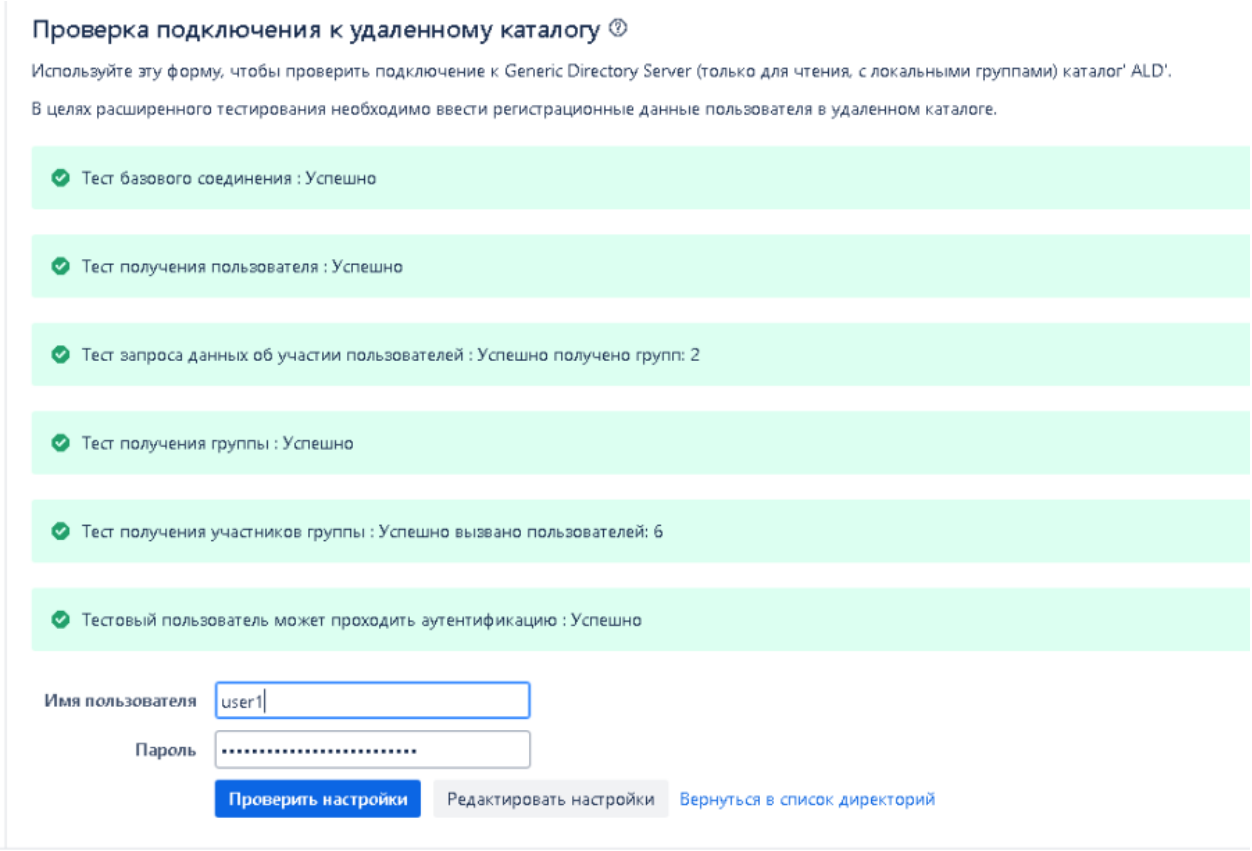

Рисунок 9 — Проверка настроек

- Проверьте вход в Confluence пользователем из ALD Pro и создание/обновление его профиля (имя, фамилия, mail).

3 Настройка доступа в Confluence

Настройка производится на странице «Глобальные разрешения», переход на которую осуществляется через пункт бокового меню «Глобальные права» (рис. 10).

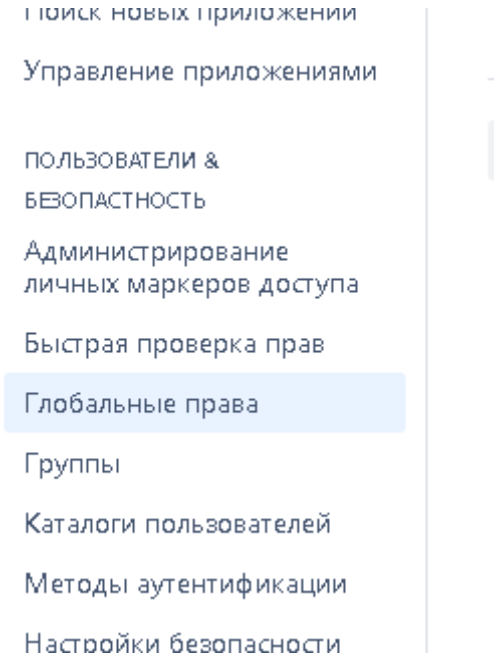

Рис 10. Переход на страницу "Глобальные разрешения"

Если в разделе **Разрешение LDAP** переключатель установлен в положение «Только для чтения» и в поле **Членство группы по умолчанию** указано «confluence-users» (см. рис. 4), то пользователь получит доступ с правами, которые по умолчанию настроены в Confluence для группы «confluence-users» в настройках глобальных разрешений. Вы можете создавать свои группы доступа и добавлять в них пользователей по умолчанию в настройках пункта 2.1.

Также в настройках глобальных разрешений можно добавить доменные группы ALD Pro по вводу имени группы в поле **Grant browse permission to** и нажатию кнопки «Добавить». Например, добавим группу ipausers (рис. 11). В этом случае можно в настройках пункта 2.1 в разделе **Разрешения LDAP** установить переключатель в положение «Только для чтения» и не добавлять пользователей при входе в локальные группы Confluence.

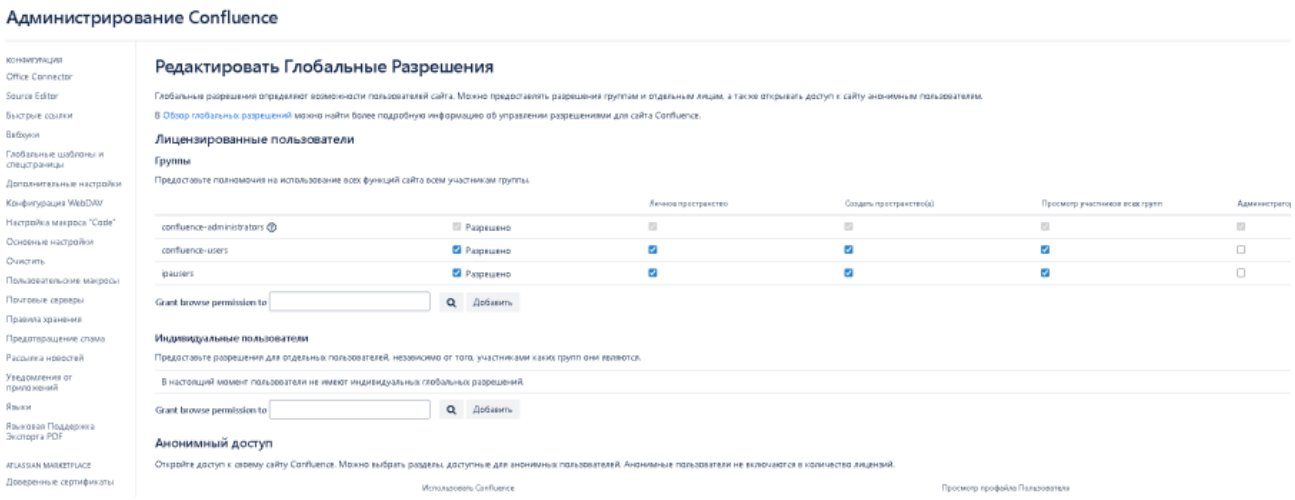

Рис 11. Глобальные Разрешения

4 Примечание по LDAPS и "Безопасный SSL"

Если включены **SSL (636)** и **«Безопасный SSL»**, система Confluence должна доверять сертификату LDAP-сервера (CA).Если у вас установлена java вместе с Confluence, то, возможно, java находится в каталоге /opt/atlassian/confluence/jre.

Импортировать сертификат aldpro в локальное хранилище можно командой /opt/atlassian/confluence/jre/bin/keytool -importcert -noprompt -alias aldpro-ca -file /etc/ipa/ca.crt -keystore /opt/atlassian/confluence/jre/lib/security/cacerts.

После этого обязательно требуется перезапустить сервис Confluence – *systemctl restart confluence*.