Интеграция Atlassian Bitbucket со службой каталога ALD Pro

03/10/2026

Содержание

Bitbucket — система управления репозиториями исходного кода (Git), поддерживающая совместную разработку, контроль доступа и интеграцию с централизованной аутентификацией и внешними каталогами пользователей.
В настоящей инструкции описана процедура интеграции Bitbucket 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 Bitbucket 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 Bitbucket

Настройка выполняется в интерфейсе Bitbucket по следующему пути (рис. 1, рис. 2): **Administration** → **User Directories** → **Add Directory**.

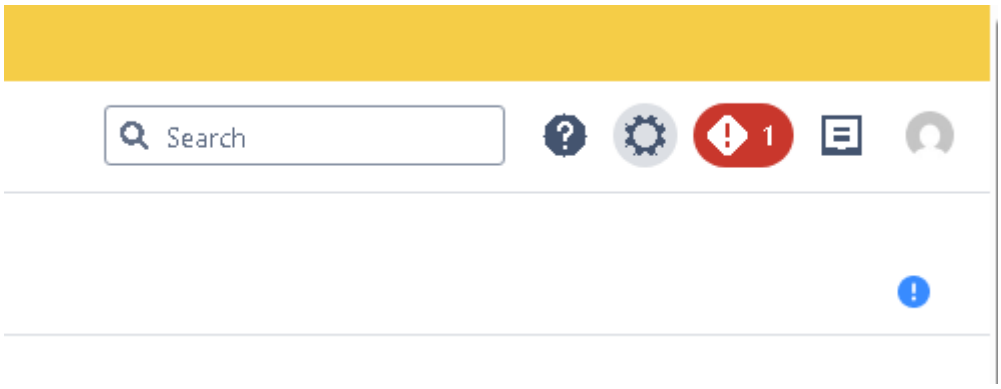

Рисунок 1 — Переход в настройки

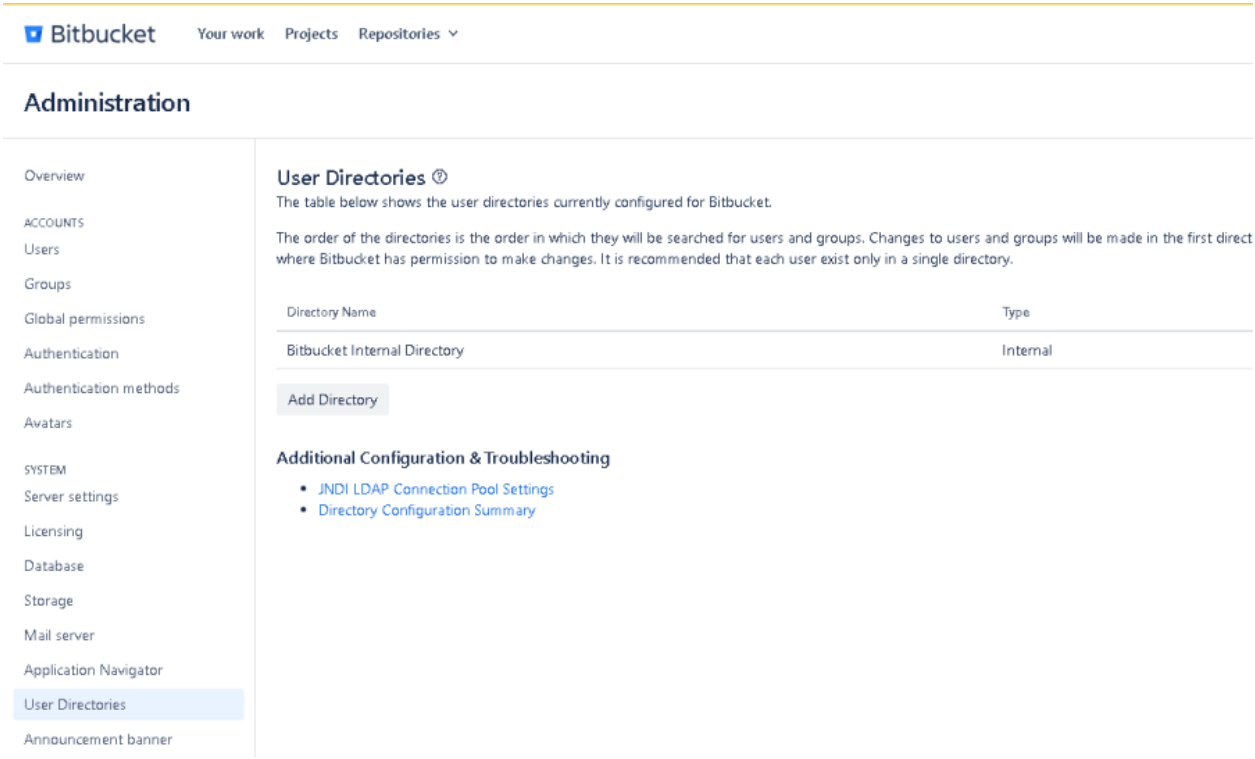

Рисунок 2 — Добавление LDAP-сервера

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

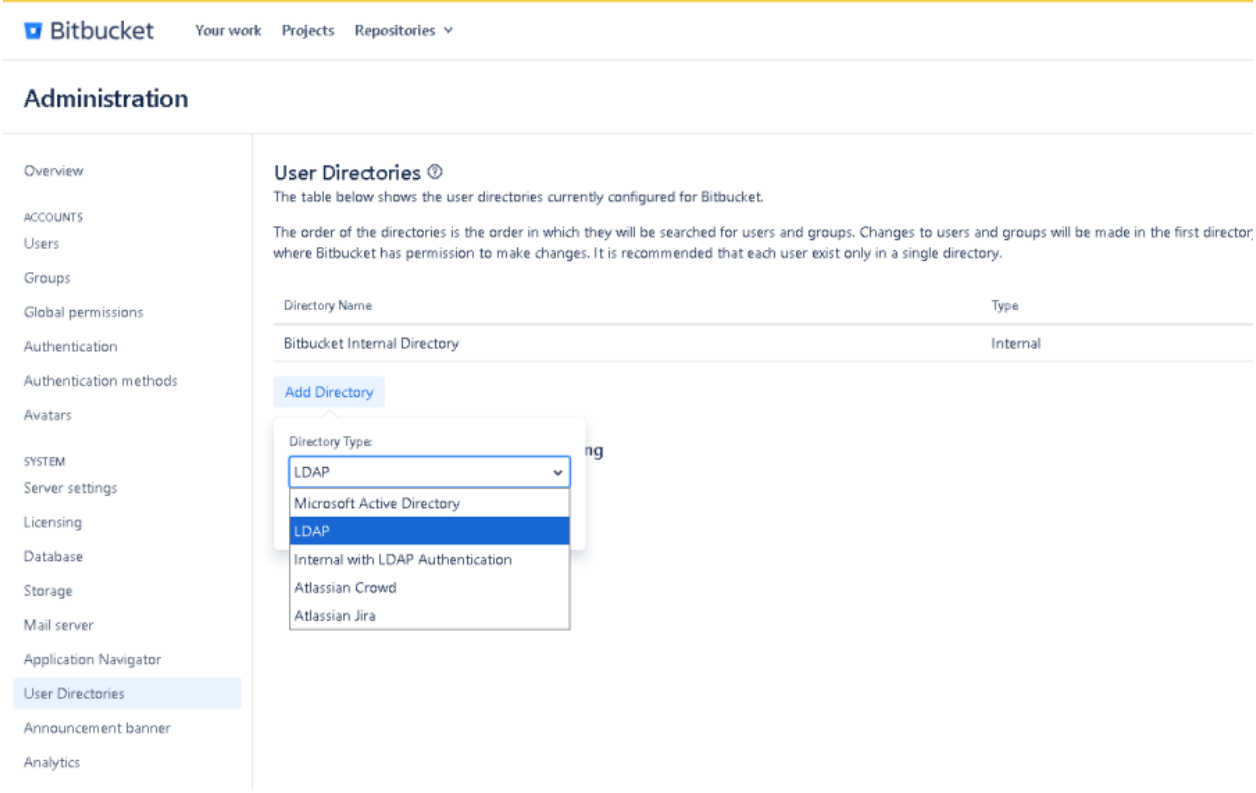

Рисунок 3 — Выбор типа сервера при добавлении

2.1 Настройки сервера (Server settings)

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

- **Name** (имя)**:** ALD
- **Directory Type** (тип каталога)**:** Generic Directory Server
- **Hostname** (имя хоста)**:** dc01.ald.domain.lan
- **Port** (порт)**:** 636
- **Use SSL** (использовать SSL)**:** да
- **Username** (имя пользователя (Bind DN): uid=bind_bitbucket,cn=users,cn=accounts,dc=ald,dc=domain,dc=lan
- **Password** (пароль): пароль сервисной учетной записи bind_bitbucket

В блоке **LDAP Schema** (схема LDAP) укажите следующее:

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

Дополнительные DN (ограничение области поиска):

- **Additional User DN** (дополнительное DN пользователя): cn=users,cn=accounts
- **Additional Group DN** (дополнительные DN группы): cn=groups,cn=accounts

Это уменьшает объем поиска и ускоряет синхронизацию.

LDAP Permissions: Read Only, with Local Groups (Разрешения LDAP: Только для чтения, с локальными группами)

Данное разрешение означает следующее:

- пользователи загружаются из LDAP;
- группы для прав в Bitbucket ведутся локально (в Bitbucket);

- пользователей из LDAP можно добавлять к группам, ведение которых осуществляется во внутреннем каталоге Bitbucket;
- пользователи при входе в Bitbucket добавляются в локальную группу stash-users.

Default Group Memberships (членство группы по умолчанию): stash-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 **Advanced settings** (дополнительные настройки) укажите следующее (рис. 5):

- **Secure SSL**
- **Update group memberships when logging in** (обновлять участие в группах при входе): Every time the user logs in (При каждом входе пользователя)
- **Synchronisation Interval (minutes)** (интервал синхронизации в минутах): 60
- **Read Timeout (seconds)** (время ожидания чтения в секундах): 120
- **Search Timeout (seconds)** (тайм-аут поиска в секундах): 60

Рисунок 5 — Дополнительные настройки

2.3 Параметры схемы пользователя

В разделе **User Schema Settings** (параметры настройки схемы пользователя) заполните поля следующим образом (рис. 6):

- **User Object Class** (класс объекта пользователя): inetorgperson.
- **User Object Filter** (фильтр пользовательских объектов): (objectClass= inetorgperson)
- **User Name Attribute** (атрибут "Полное имя пользователя"): uid
- **User Name RDN Attribute** (атрибут "RDN имени пользователя")**:** cn
- **User First Name Attribute** (атрибут "Имя пользователя"): givenName
- **User Last Name Attribute** (атрибут "Фамилия"): sn
- **User Display Name Attribute** (атрибут "Просмотр имени"): cn
- **User Email Attribute** (атрибут "Электронная почта"): mail
- **User Password Attribute** (атрибут "Пароль пользователя"): userPassword
- **User Password Encryption** (шифрование пароля пользователя): SHA
- **User Unique ID Attribute** (атрибут "Уникальный ID пользователя")**:** entryUUID

Рисунок 6 — Схема пользователя

2.4 Настройки групповой схемы

В разделе **Group Schema Settings** (настройки групповой схемы) заполните поля следующим образом (рис. 7):

- **Group Object Class** (класс группы объектов): ipausergroup
- **Group Object Filter** (фильтр объектов группы): (objectclass=ipausergroup)
- **Group Name Attribute** (атрибут "Имя группы"): cn
- **Group Description Attribute** (атрибут "Описание группы"): description

В разделе **Membership Schema Settings** (параметры настройки схемы участия) заполните следующее:

- **Group Members Attribute** (атрибут "Члены Группы"): member

- **User Membership Attribute** (атрибут «Участие пользователя»): memberof

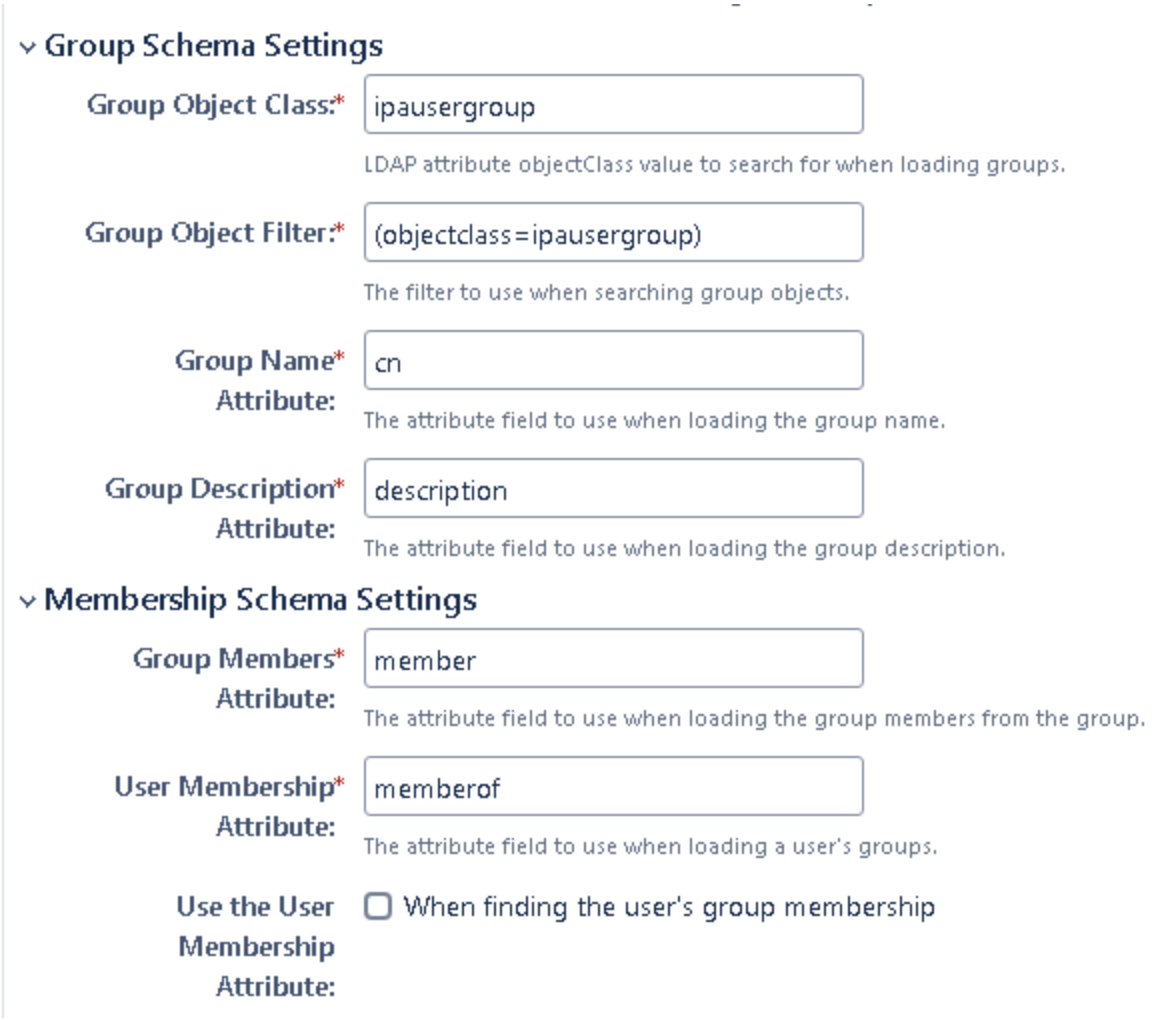

Рисунок 7 – Настройка групповой схемы

2.5 Сохранение и проверка

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

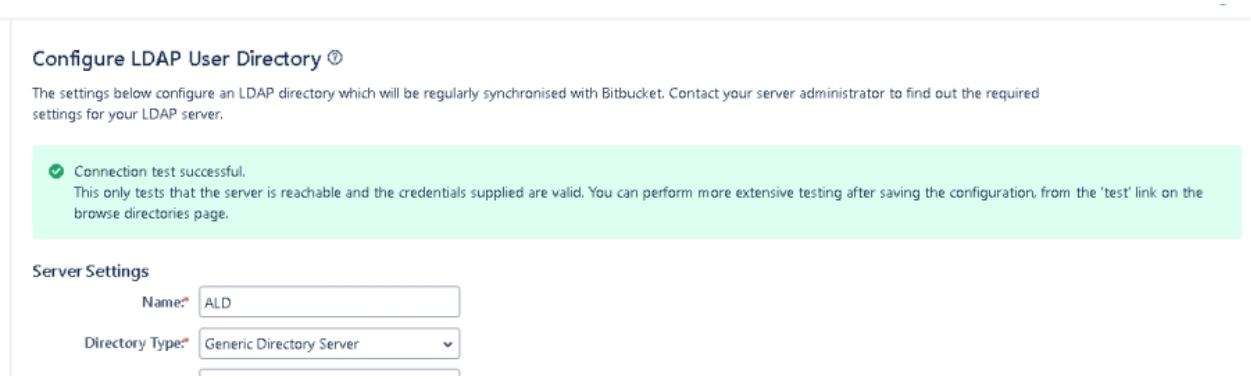

Рисунок 8 – Быстрый тест

- 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.

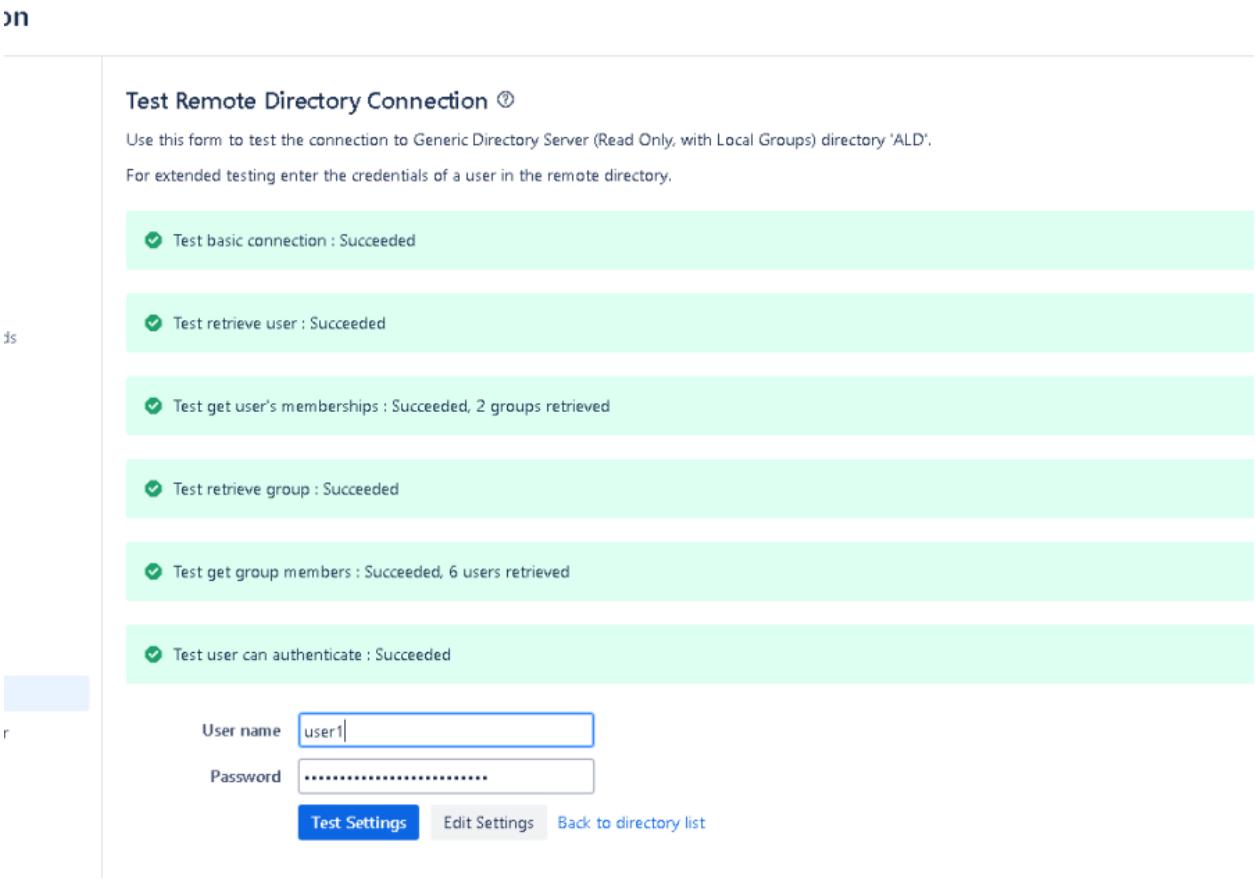

Рисунок 9 — Проверка настроек

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

3 Настройка доступа в Bitbucket

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

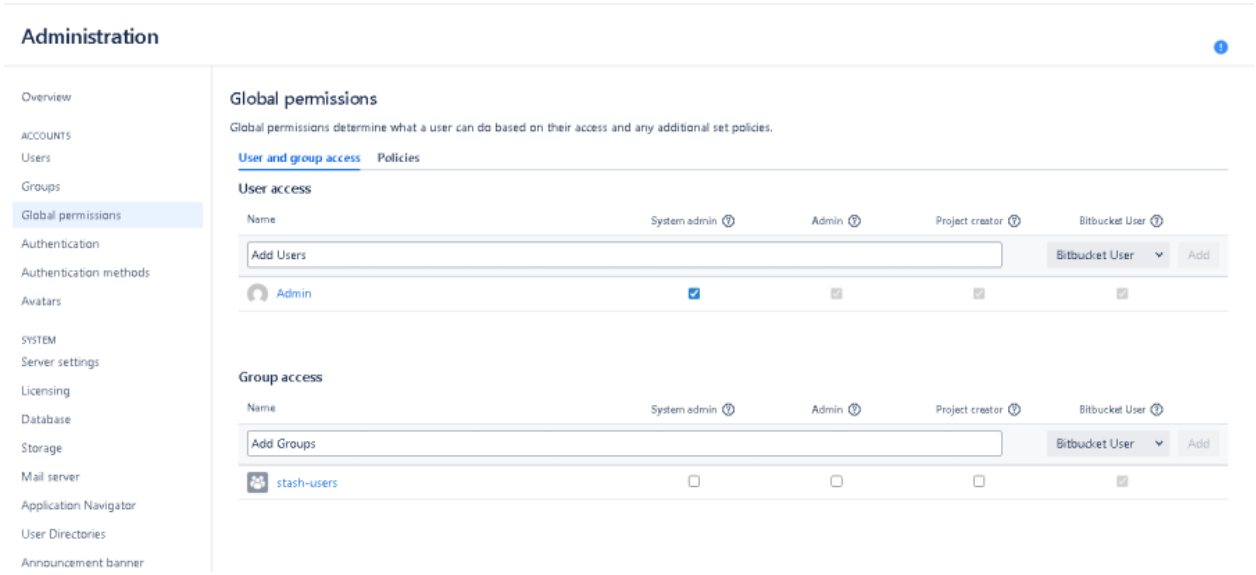

Рис 10 — Переход на страницу "Глобальные разрешения"

Если в разделе **LDAP Permissions** переключатель установлен в положение **«Read Only, with Local Groups»** и в поле **Default Group Memberships** указано «stash-users» (см. рис. 4), то пользователь получит доступ с правами, которые по умолчанию настроены в Bitbucket для группы «stash-users». Вы можете добавлять свои группы доступа и вносить в них пользователей по умолчанию в настройках пункта 2.1.

Также можно добавить доменные группы ALD Pro по вводу имени группы в поле **Group access** и нажатию кнопки «Добавить». Например, добавим группу «ipausers» (рис. 11). В этом случае можно в настройках пункта 2.1 в разделе **LDAP Permissions** установить переключатель в положение «Read Only» и не добавлять пользователей при входе в локальные группы Bitbucket.

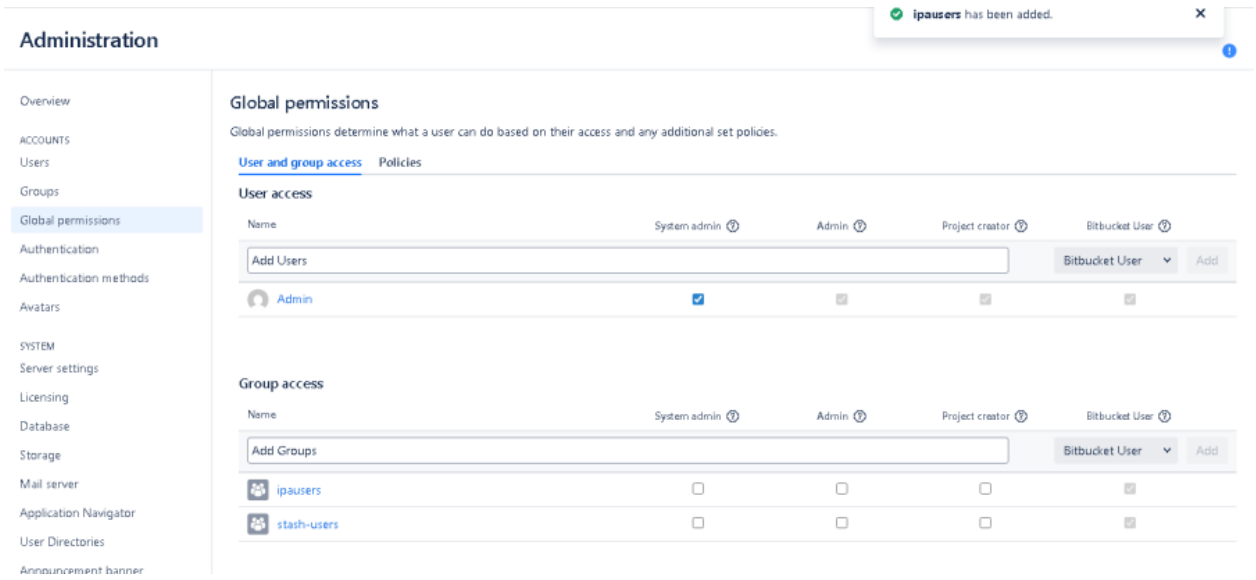

Рис 11 — Глобальные разрешения

4 Примечание по LDAPS и «Безопасный SSL»

Если включены **SSL (636)** и **«Безопасный SSL»**, система Bitbucket должна доверять сертификату LDAP-сервера (CA).Если у вас установлена java вместе с Bitbucket, то, возможно, java находится в каталоге /opt/atlassian/bitbucket/9.4.17/jre.

Импортировать сертификат aldpro в локальное хранилище можно командой /opt/atlassian/bitbucket/9.4.17/jre/bin/keytool -importcert -noprompt -alias aldpro-ca -file /etc/ipa/ca.crt -keystore /opt/atlassian/bitbucket/9.4.17/jre/lib/security/cacerts.

После этого обязательно требуется перезапустить сервис Bitbucket – *systemctl restart atlbitbucket*.