

Интеграция Atlassian Bitbucket со службой каталога ALD Pro



03/10/2026

Содержание

1	Настройка сервисной учетной записи в ALD Pro	3
2	Настройка LDAP/LDAPS в Bitbucket	5
2.1	Настройки сервера (Server settings)	6
2.2	Дополнительные настройки (синхронизация и параметры подключения) ...	7
2.3	Параметры схемы пользователя	8
2.4	Настройки групповой схемы	9
2.5	Сохранение и проверка	10
3	Настройка доступа в Bitbucket.....	12
4	Примечание по LDAPS и «Безопасный SSL».....	13

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 учётной 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 учётной 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**.

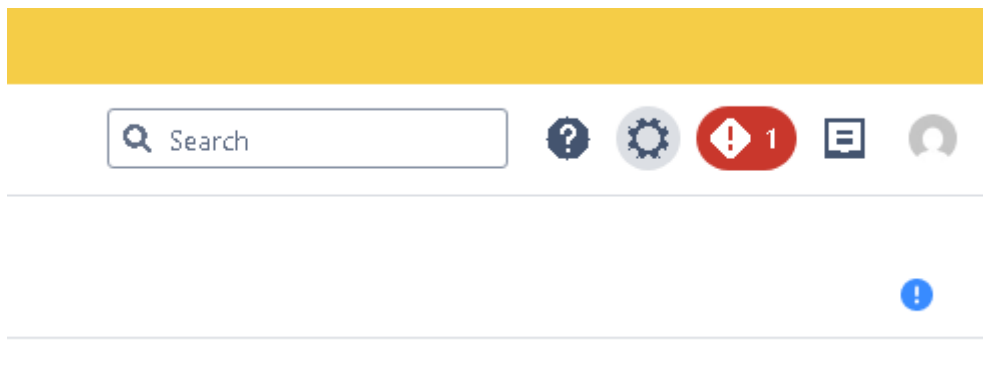


Рисунок 1 — Переход в настройки

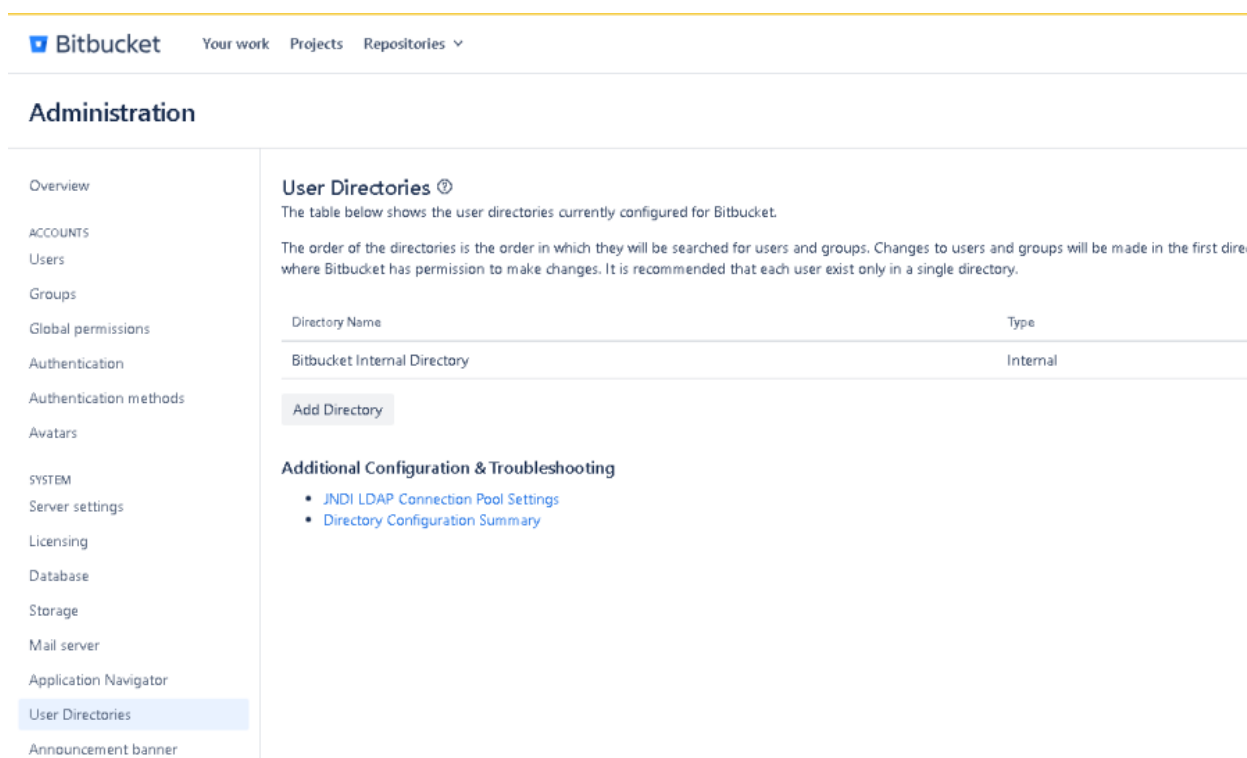


Рисунок 2 — Добавление LDAP-сервера

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

Administration

- Overview
- ACCOUNTS
- Users
- Groups
- Global permissions
- Authentication
- Authentication methods
- Avatars
- SYSTEM
- Server settings
- Licensing
- Database
- Storage
- Mail server
- Application Navigator
- User Directories**
- Announcement banner
- Analytics

User Directories ⓘ

The table below shows the user directories currently configured for Bitbucket.

The order of the directories is the order in which they will be searched for users and groups. Changes to users and groups will be made in the first directory where Bitbucket has permission to make changes. It is recommended that each user exist only in a single directory.

Directory Name	Type
Bitbucket Internal Directory	Internal

Add Directory

Directory Type:

- LDAP
- Microsoft Active Directory
- LDAP**
- Internal with LDAP Authentication
- Atlassian Crowd
- Atlassian Jira

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.

Server Settings

Name:

Directory Type:

Making a selection will automatically enter default values for several options below.

Hostname:

Hostname of the server running LDAP. Example: ldap.example.com

Port: Use SSL

Username:

User to log in to LDAP. Examples: user@domain.name or cn=user,dc=domain,dc=name.

Password:

LDAP Schema

Base DN:

Root node in LDAP from which to search for users and groups. Example: cn=users,dc=example,dc=com.

Additional User DN:

Prepended to the base DN to limit the scope when searching for users.

Additional Group DN:

Prepended to the base DN to limit the scope when searching for groups.

LDAP Permissions

Read Only
Users, groups and memberships are retrieved from your LDAP server and cannot be modified in Bitbucket.

Read Only, with Local Groups
Users, groups and memberships are retrieved from your LDAP server and cannot be modified in Bitbucket. Users from LDAP can be added to groups maintained in Bitbucket's internal directory.

Default Group Memberships:

A comma-separated list of groups that users will be added to when they first log in. This will only be done once per user. These groups will be created if they don't already exist.

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

Advanced Settings

Secure SSL
Verify that the SSL certificate is valid for this connection.

Enable Nested Groups
If true, groups can contain other groups. Enabling this option may degrade performance.

Use Paged Results 1000 results per page

Follow Referrals
Allow the LDAP server to redirect requests to other servers.

Naive DN Matching
If your directory will always return a consistent string representation of a DN, you can enable naive DN matching. Using naive DN matching provides significant performance benefits, so we recommend enabling it where possible.

Update group memberships when logging in

Whether to update the user's group memberships on each log in. This ensures the group list is up to date, but can slow down authentication.

Synchronisation* Interval (minutes):
Time to wait between directory updates.

Read Timeout (seconds):
Time to wait for a response to be received. If there is no response within the specified time period, the read attempt will be aborted. Value of 0 means there is no limit.

Search Timeout (seconds):
Time to wait for a response from a search operation. Value of 0 means there is no limit.

Connection Timeout (seconds):
Time limit within which the connection to new server must be made. Value of 0 means the TCP network timeout will be used, which may be several minutes. When using JNDI connection pooling, this parameter also specifies the time to wait for a connection after the pool has been exhausted. Set to 0 for no limit. [Learn More](#)

Max authentication retries:
Maximum number of retries when an operational error occurs during user authentication (default 0).

Minimum retry delay (milliseconds):
Minimum delay between authentication retries in an exponential backoff when an operational error occurs (default 0).

Maximum retry delay (milliseconds):
Maximum delay between authentication retries in an exponential backoff when an operational error occurs (default 0).

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

▼ User Schema Settings

User Object Class*	<input type="text" value="inetorgperson"/>
	The LDAP user object class type to use when loading users.
User Object Filter*	<input type="text" value="(objectclass=inetorgperson)"/>
	The filter to use when searching user objects.
User Name*	<input type="text" value="uid"/>
Attribute:	The attribute field to use on the user object. Examples: cn, sAMAccountName.
User Name RDN	<input type="text" value="cn"/>
Attribute:	The RDN to use when loading the user username.Example: cn.
User First Name*	<input type="text" value="givenName"/>
Attribute:	The attribute field to use when loading the user first name.
User Last Name*	<input type="text" value="sn"/>
Attribute:	The attribute field to use when loading the user last name.
User Display Name*	<input type="text" value="cn"/>
Attribute:	The attribute field to use when loading the user full name.
User Email Attribute*	<input type="text" value="mail"/>
	The attribute field to use when loading the user email.
User Password*	<input type="text" value="userPassword"/>
Attribute:	The attribute field to use when manipulating a user password.
User Password Encryption:	<input type="text" value="SHA"/>
	Choose the encryption algorithm used for passwords on your directory.
User Unique ID	<input type="text" value="entryUUID"/>
Attribute:	The attribute field to use for tracking user identity across user renames.

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

▼ **Group Schema Settings**

Group Object Class:*
LDAP attribute objectClass value to search for when loading groups.

Group Object Filter:*
The filter to use when searching group objects.

Group Name Attribute:*
The attribute field to use when loading the group name.

Group Description Attribute:*
The attribute field to use when loading the group description.

▼ **Membership Schema Settings**

Group Members Attribute:*
The attribute field to use when loading the group members from the group.

User Membership Attribute:*
The attribute field to use when loading a user's groups.

Use the User Membership Attribute: When finding the user's group membership

Рисунок 7 – Настройка групповой схемы

2.5 Сохранение и проверка

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

Configure LDAP User Directory ⓘ

The settings below configure an LDAP directory which will be regularly synchronised with Bitbucket. Contact your server administrator to find out the required settings for your LDAP server.

✔ **Connection test successful.**
This only tests that the server is reachable and the credentials supplied are valid. You can perform more extensive testing after saving the configuration, from the 'test' link on the browse directories page.

Server Settings

Name:*

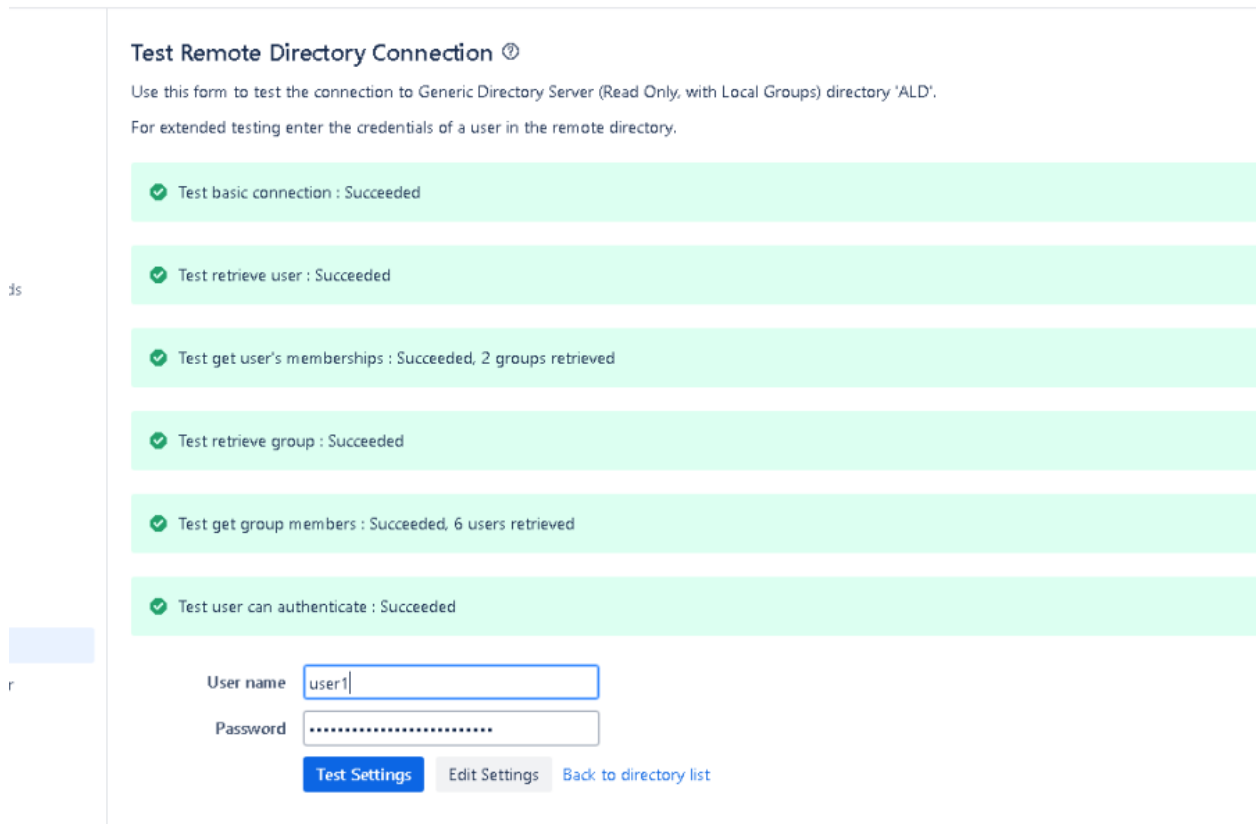
Directory Type:*

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.

»



Test Remote Directory Connection ⓘ

Use this form to test the connection to Generic Directory Server (Read Only, with Local Groups) directory 'ALD'.
For extended testing enter the credentials of a user in the remote directory.

- ✓ Test basic connection : Succeeded
- ✓ Test retrieve user : Succeeded
- ✓ Test get user's memberships : Succeeded, 2 groups retrieved
- ✓ Test retrieve group : Succeeded
- ✓ Test get group members : Succeeded, 6 users retrieved
- ✓ Test user can authenticate : Succeeded

User name

Password

[Test Settings](#) [Edit Settings](#) [Back to directory list](#)

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).

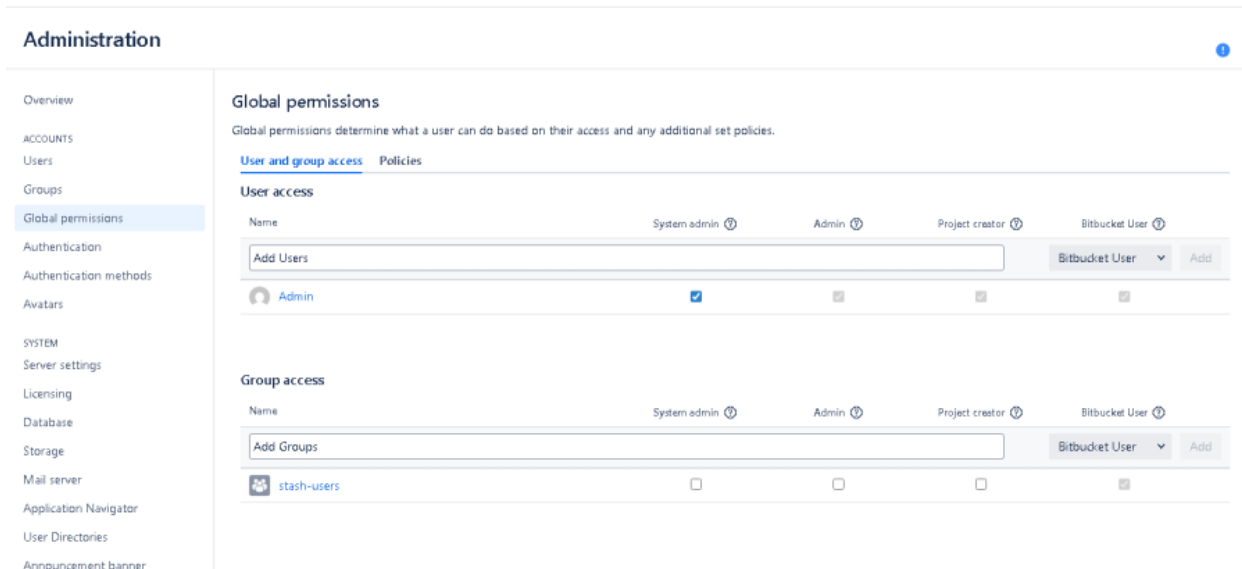


Рис 10 – Переход на страницу "Глобальные разрешения"

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 нажатую кнопки «Добавить». Например, добавим группу «ipusers» (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.

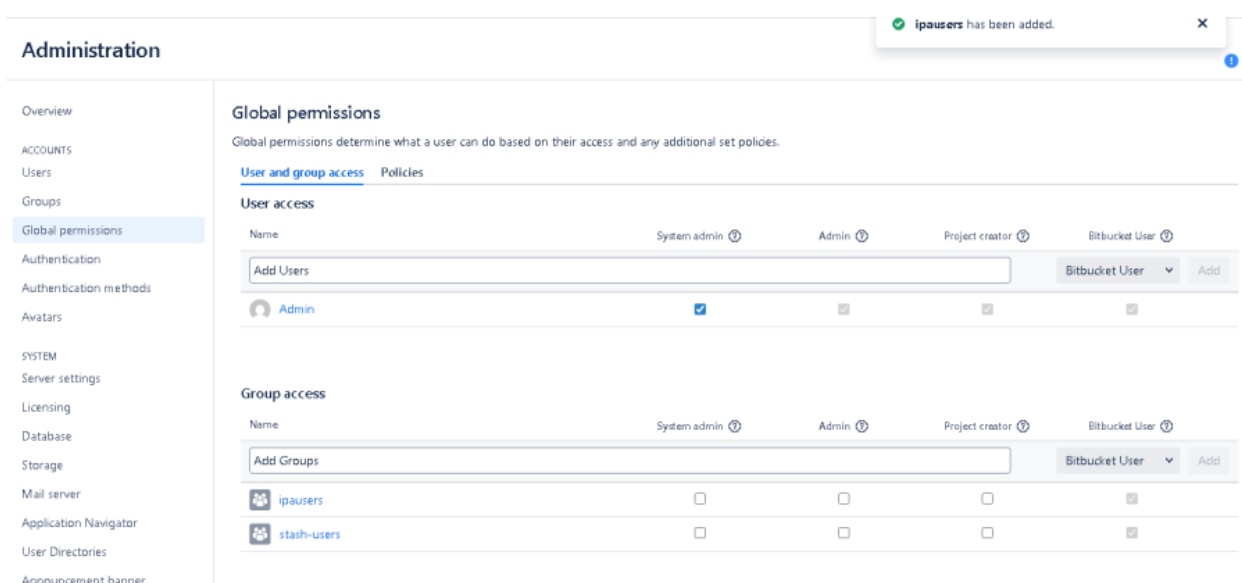


Рис 11 – Глобальные разрешения

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 atlassian-bitbucket`.