Интеграция GLPI со службой каталога ALD Pro

11/07/2025

Содержание

1 Введение

GLPI (Gestionnaire Libre de Parc Informatique) —это бесплатная система управления IT-услугами (ITSM), предназначенная для работы с активами, инцидентами и заявками в организации. Система оптимизирует техническую поддержку и ресурсы благодаря инвентаризации аппаратного и программного обеспечения, управлению контрактами и лицензиями, предоставляя централизованный обзор всей IT-инфраструктуры.

Интеграция GLPI со службой каталога позволяет синхронизировать пользователей и группы через защищённое соединение LDAPS с ALD Pro. Это обеспечивает централизованное управление учётными записями и повышает уровень безопасности системы.

2 Настройка сервисной учетной записи

2.1 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
```

3 Настройка доверия сертификатов

Если GLPI развернут на сервере, который не введен в домен ALD Pro, необходимо настроить доверие к корневому сертификату сервера для безопасного подключения к LDAPS без ошибок о недоверенном сертификате.

3.1 Добавление CA-сертификата домена

1. Скопировать CA-сертификат с удалённого сервера:

```
scp <remote_user>@<remote_host>:/etc/ipa/ca.crt /tmp/ald_ca.crt
```

Разъяснения:

- ***<remote_user>*** *– пользователь на удалённом сервере,*
- ***<remote_host>*** *– адрес или имя контроллера домена,*
- ***/etc/ipa/ca.crt*** *– путь к CA-сертификату на контроллере домена,*
- ***/tmp/ald_ca.crt*** *– временный файл на локальной машине.*

2. Перенести сертификат в системное хранилище:

```
sudo cp /tmp/ald_ca.crt /usr/local/share/ca-certificates/ald_ca.crt
```

Разъяснения:

- ***/usr/local/share/ca-certificates/*** *– каталог для локальных доверенных сертификатов*

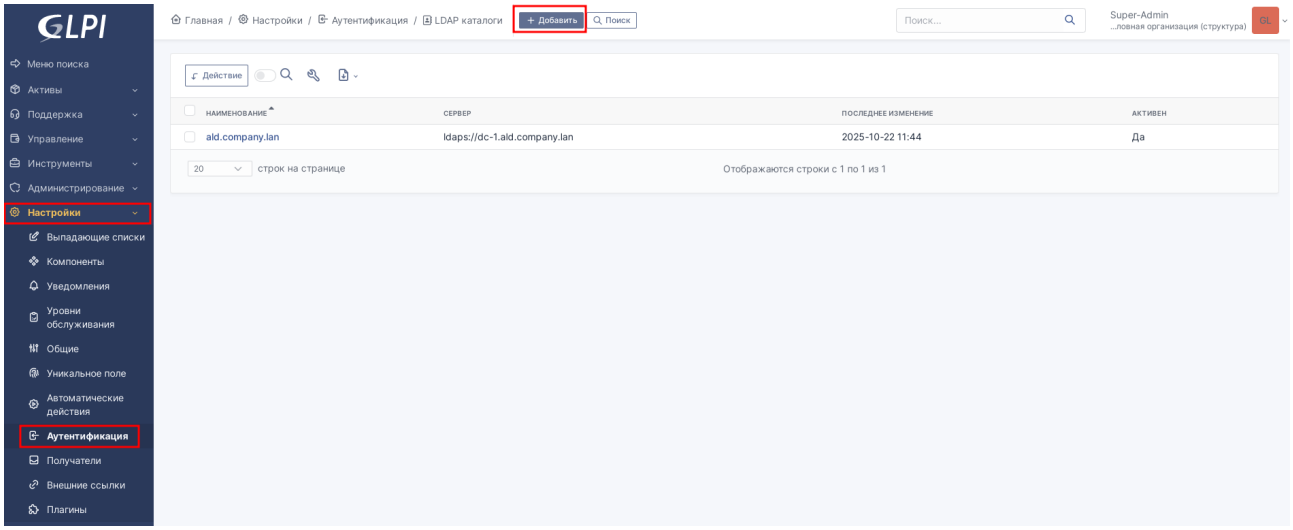
3. Обновить системное хранилище доверенных сертификатов:

```
sudo update-ca-certificates
```

4 Настройка интеграции в GLPI

4.1 Переход к настройкам аутентификации

1. В веб-интерфейсе GLPI перейдите в меню **Настройки → Аутентификация**.
2. Выберите раздел **LDAP-каталоги**.
3. Нажмите кнопку "Добавить" для создания нового подключения.

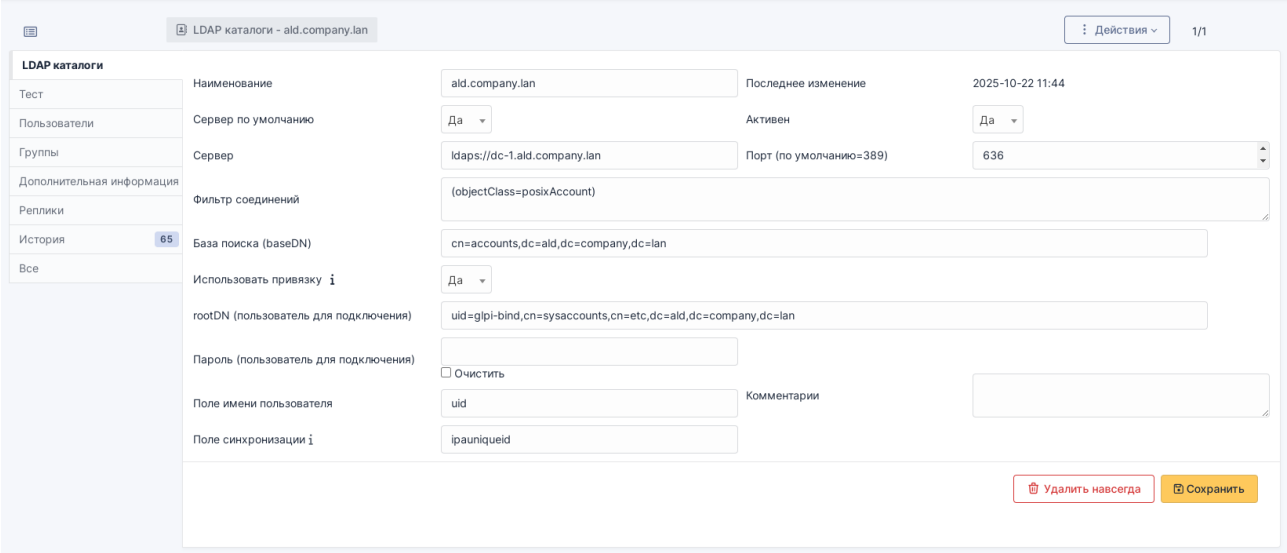


4.2 Заполнение основных параметров подключения

В форме создания LDAP-каталога заполните следующие поля:

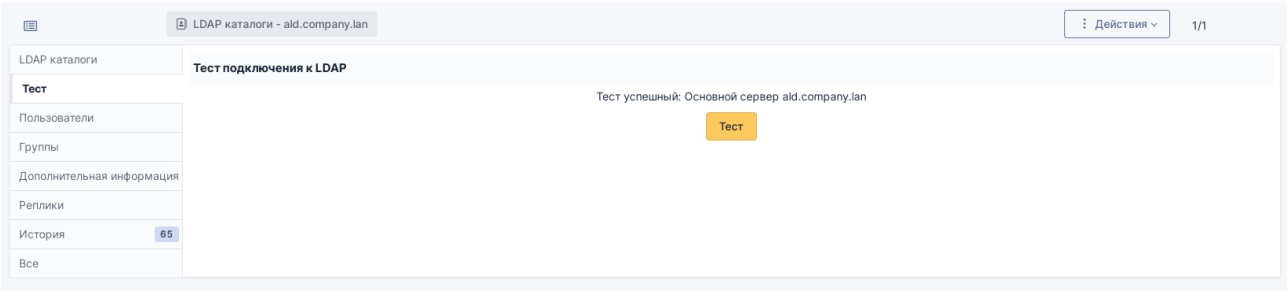
Основные настройки:

- Наименование: **ALD Pro LDAP (или любое описательное название)**
- Сервер по умолчанию: **Да (если это единственный LDAP-сервер)**
- Активен: **Да**
- Сервер: **FQDN контроллера домена с префиксом ldaps://**
- Порт: **636 (стандартный порт для LDAPS)**
- Фильтр соединений: **(objectClass=posixAccount)**
- База поиска (baseDN): **cn=accounts,dc=ald,dc=company,dc=lan**
- Использовать привязку: **Да**
- rootDN (пользователь для подключения): **uid=glpi-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan**
- Пароль (пользователь для подключения): **securePassword (пароль, указанный при создании сервисной учетной записи)**
- Поле имени пользователя: **uid**
- Поле синхронизации: **ipauniqueid**



4.3 Тестирование подключения

На вкладке **Тест** нажмите кнопку "Тест" для проверки работы подключения. При успешном подключении вы увидите сообщение о успешном соединении:



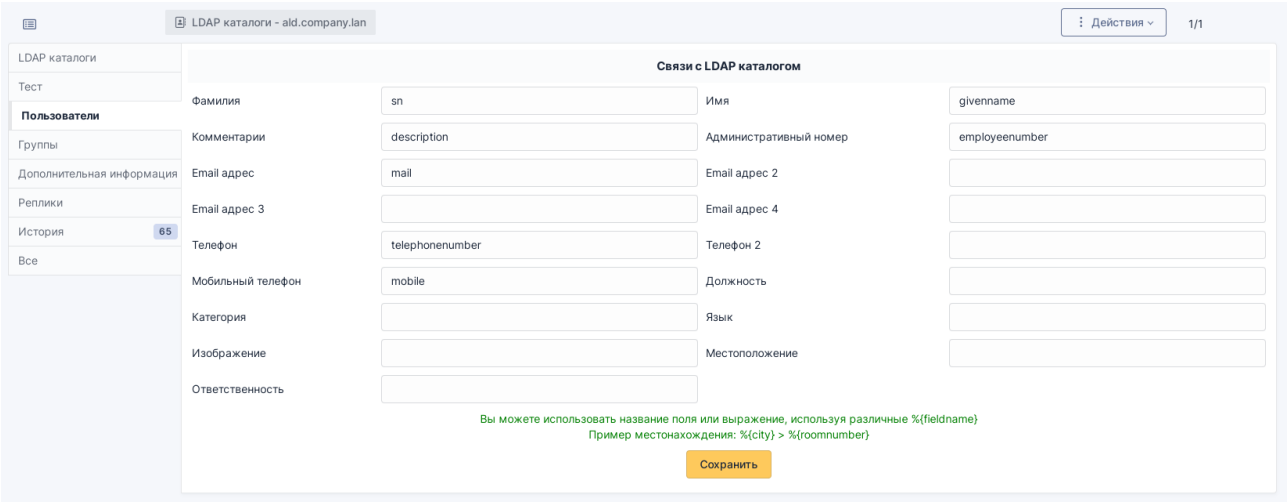
4.4 Настройка связи с пользователями

На вкладке **Пользователи** заполните таблицу "Связи с LDAP-каталогом" согласно следующим соответствиям:

Для корректной работы внешних сервисов с ALD Pro рекомендуется задать следующие параметры LDAP. Они обеспечивают правильную фильтрацию и отображение групп, а также расширяют профиль пользователя за счёт дополнительных атрибутов.

LDAP-параметр	Значение	Описание
Filter Disabled	(!(nsAccountLock=TRUE))	Исключение заблокированных учётных записей
Filter Login	(objectClass=inetOrgPerson)	Фильтр для определения учётных записей пользователя
Filter Group	(objectClass=groupofnames)	Фильтр для определения LDAP-групп

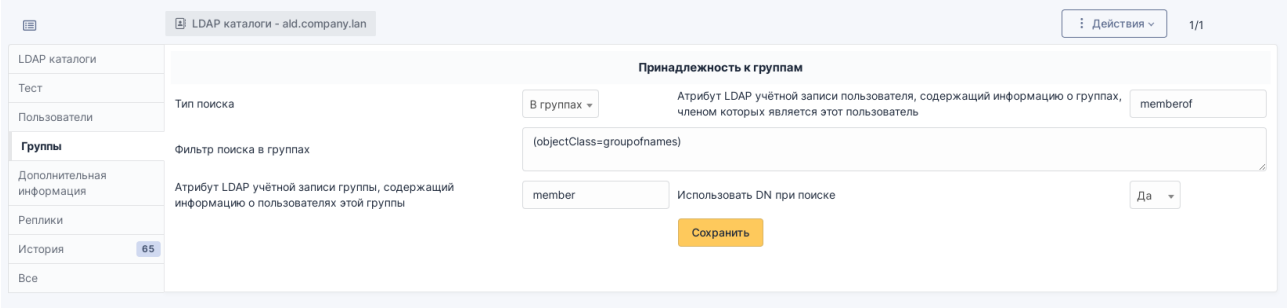
Group Member	member	Атрибут, определяющий состав группы
Member Of	memberOf	Атрибут групп, в которых состоит пользователь
Login	uid	Логин пользователя
Display Name	displayName	Отображаемое полное имя пользователя
First Name	givenName	Имя пользователя
Last Name	sn	Фамилия пользователя
Middle Name	rbtamiddlename	Отчество (специфично для ALD Pro)
Email	mail	Электронная почта пользователя
Mobile Phone	mobile	Мобильный телефон
Work Phone	telephoneNumber	Рабочий телефон
Home Phone	employeeNumber	Внутренний/добавочный номер



5 Настройка групп

В разделе **Группы** можно задать следующие параметры:

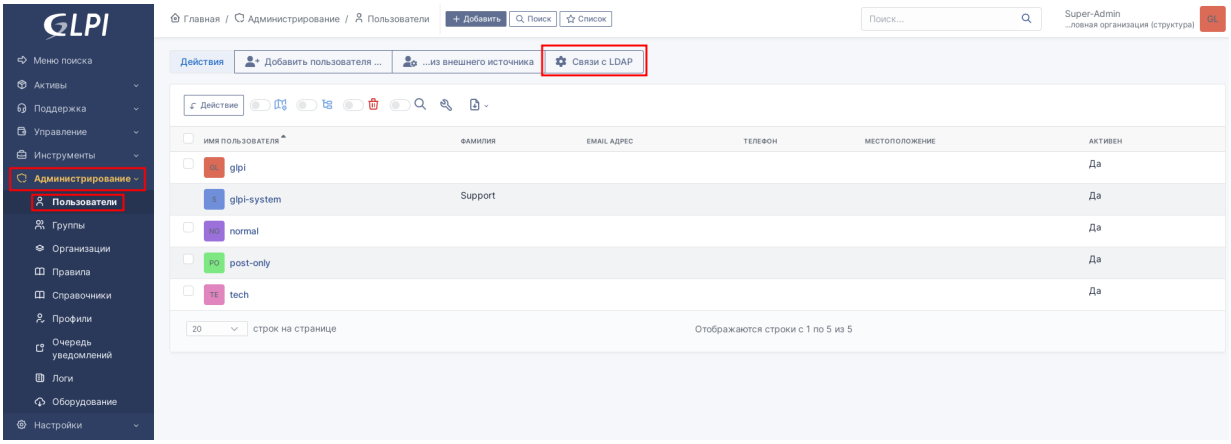
- Тип поиска: **В группах**
- Атрибут LDAP учётной записи пользователя, содержащий информацию о группах, членом которых является этот пользователь: **memberOf**
- Фильтр поиска в группах: **(objectClass=groupofnames)**
- Атрибут LDAP учетной записи пользователя, содержащий информацию о группах, членом которых является этот пользователь: **member**
- Использовать DN при поиске: **Да**



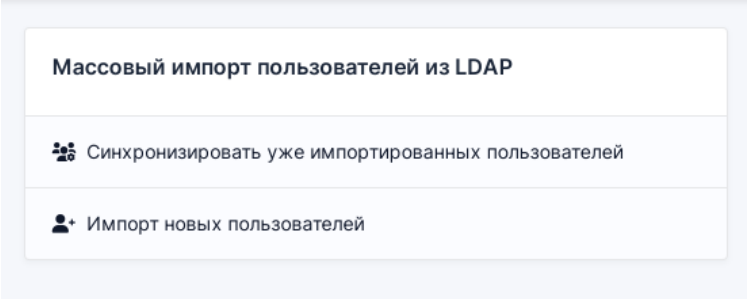
6 Импорт пользователей и групп

6.1 Импорт пользователей

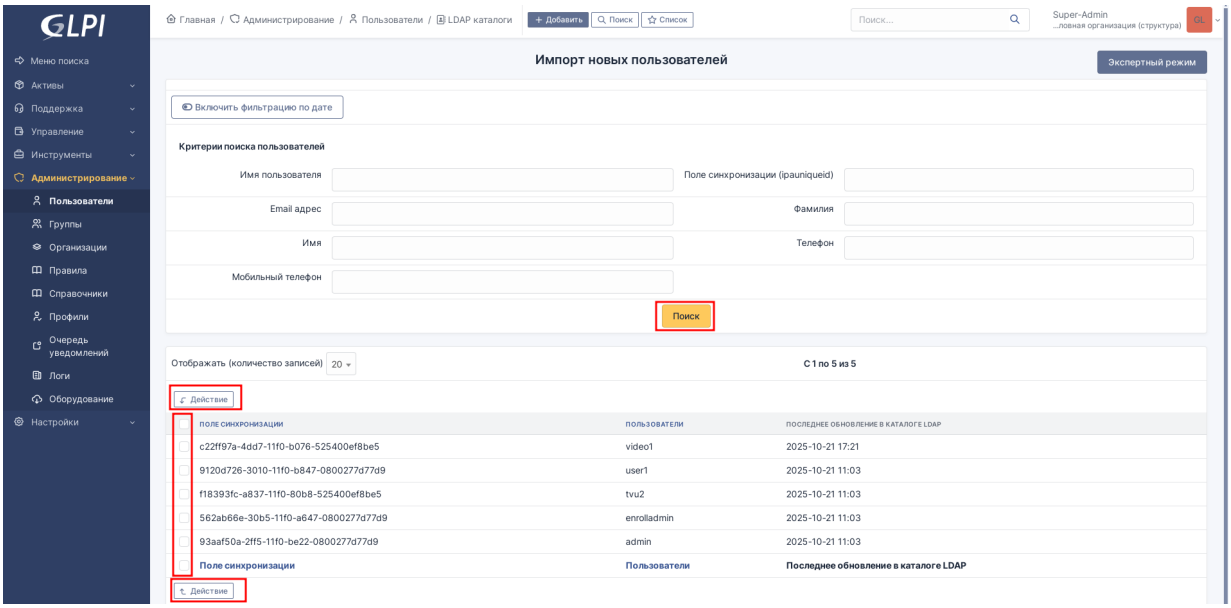
1. Перейдите в раздел **Администрирование → Пользователи**
2. Нажмите "**Связи с LDAP**"



3. Выберите "**Импорт новых пользователей**"

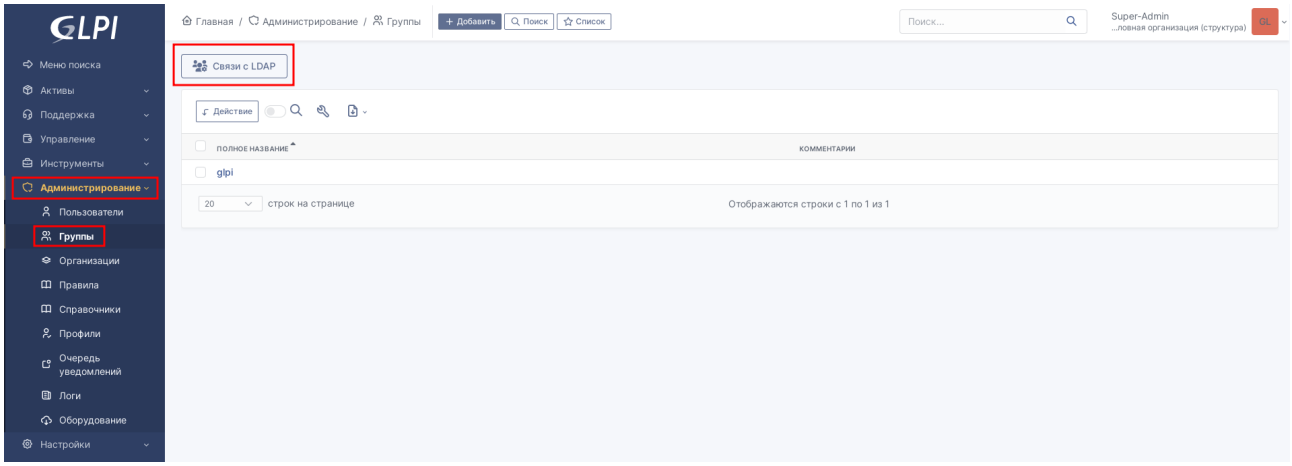


4. Нажмите "**Поиск**"
5. Выберите пользователей для импорта из списка найденных пользователей домена

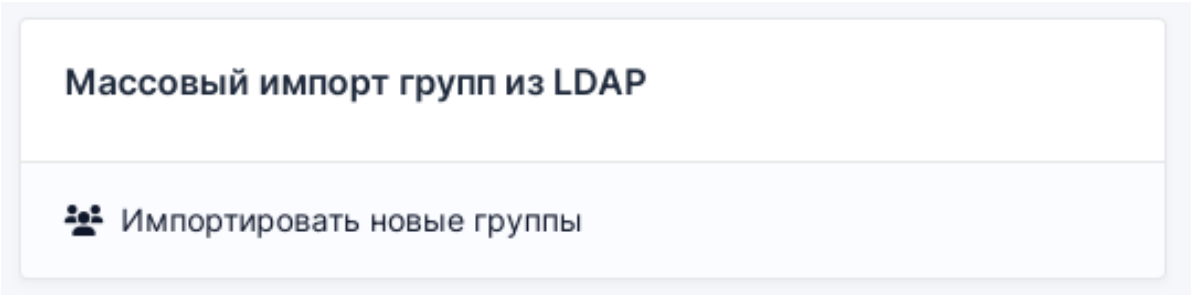


6.2 Импорт групп

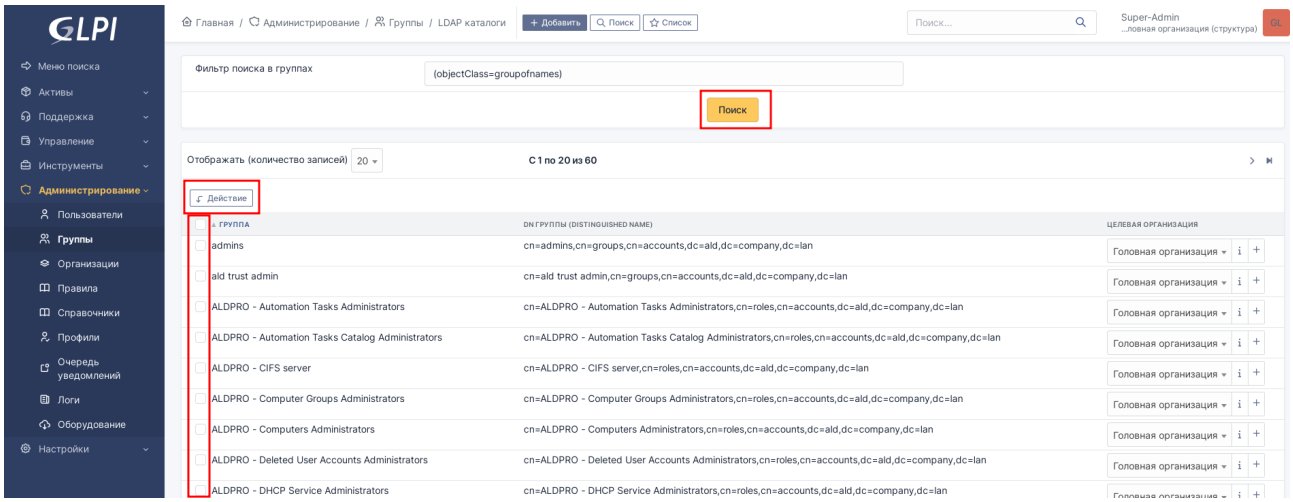
1. Перейдите в раздел **Администрирование → Группы**
2. Нажмите "**Связи с LDAP**"



3. Выберите "**Импортировать новые группы**"



4. Нажмите "**Поиск**"
5. Выберите группы для импорта из списка найденных групп домена


GLPI
Меню поиска
Активы
Поддержка
Управление
Инструменты
Администрирование
Пользователи
Группы
Организации
Правила
Справочники
Профили
Очередь уведомлений
Логи
Оборудование
Настройки
Главная / Администрирование / Группы / LDAP каталоги
Добавить
Поиск
Список
Super-Admin
Фильтр поиска в группах
(objectClass=groupofnames)
Поиск
Отображать (количество записей) 20
С 1 по 20 из 60
Действие
ГРУППА
DN ГРУППЫ (DISTINGUISHED NAME)
ЦЕЛЕВАЯ ОРГАНИЗАЦИЯ
admins
cn=admins,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
ald trust admin
cn=ald trust admin,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
ALDPRO - Automation Tasks Administrators
cn=ALDPRO - Automation Tasks Administrators,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
ALDPRO - Automation Tasks Catalog Administrators
cn=ALDPRO - Automation Tasks Catalog Administrators,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
ALDPRO - CIFS server
cn=ALDPRO - CIFS server,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
ALDPRO - Computer Groups Administrators
cn=ALDPRO - Computer Groups Administrators,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
ALDPRO - Computers Administrators
cn=ALDPRO - Computers Administrators,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
ALDPRO - Deleted User Accounts Administrators
cn=ALDPRO - Deleted User Accounts Administrators,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
ALDPRO - DHCP Service Administrators
cn=ALDPRO - DHCP Service Administrators,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
Головная организация