Интеграция Apache OpenMeetings со службой каталога ALD Pro

11/07/2025

Содержание

1 Введение

Apache OpenMeetings - это открытая платформа для веб-конференций, обеспечивающая видеосвязь, обмен сообщениями, совместную работу с документами и другие инструменты для групповой работы. OpenMeetings поддерживает различные способы аутентификации пользователей и может работать как автономная система или интегрироваться с корпоративными каталогами.

Интеграция с ALD Pro позволяет использовать единую систему учетных записей для всей инфраструктуры организации. Пользователи могут входить в OpenMeetings под своими доменными учетными данными без необходимости создания отдельных аккаунтов. Это упрощает администрирование, повышает безопасность за счет централизованного управления паролями и политиками доступа, а также обеспечивает автоматическое создание профилей пользователей при первом входе (provisioning). Кроме того, интеграция с ALD Pro дает возможность синхронизировать группы пользователей и использовать корпоративные политики аутентификации.

2 Создание сервисной учетной записи в ALD Pro

Для подключения OpenMeetings к ALD Pro необходима служебная учетная запись с правами на чтение каталога пользователей. Эта учетная запись будет использоваться OpenMeetings для поиска и проверки пользователей.

2.1 Создание сервисной учетной записи

Для создания сервисной учетной записи 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=openmeetings-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: openmeetings-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 для LDAPS

Для защищенного соединения с контроллером ALD Pro (LDAPS на порту 636) необходимо импортировать сертификат LDAP-сервера в доверенное хранилище Java, используемое OpenMeetings.

3.1 Скопируйте CA-сертификат с удаленного сервера

Скопируйте сертификат с контроллера ALD Pro:

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

3.2 Найдите путь к Java и хранилищу cacerts

Определите версию Java, используемую OpenMeetings:

```
which java
# или
readlink -f $(which java)
```

Путь к хранилищу сертификатов обычно:

- /usr/lib/jvm/java-11-openjdk-amd64/lib/security/cacerts
- /usr/lib/jvm/java-17-openjdk-amd64/lib/security/cacerts
- /etc/ssl/certs/java/cacerts (в некоторых дистрибутивах)

Точный путь можно найти:

```
find /usr/lib/jvm -name cacerts 2>/dev/null
```

3.3 Импортируйте сертификат в cacerts

Замените путь к Java согласно вашей версии (**-keystore**):

```
sudo keytool -import -trustcacerts -alias ald-ca-cert \
  -file /tmp/ald_ca.crt \
  -keystore /usr/lib/jvm/java-17-openjdk-amd64/lib/security/cacerts \
  -storepass changeit
```

Успешный результат: **Certificate was added to keystore**

4 Создание конфигурационного файла LDAP

OpenMeetings использует конфигурационный файл для настройки параметров подключения к LDAPS/ALD Pro.

Расположение файла:

/opt/openmeetings/webapps/openmeetings/data/conf/aldpro-ldap.properties

Содержимое конфигурационного файла:

```
# =========================
# Подключение
# =========================
# Адрес контроллера домена ALD Pro
ldap_conn_host=dc-1.ald.company.lan
# Порт LDAPS (защищенный)
ldap_conn_port=636
# Использовать защищенное соединение LDAPS
ldap_conn_secure=true

# =========================
# Служебная учетная запись (только для чтения)
# =========================
# DN служебной учетной записи для поиска пользователей
ldap_admin_dn=uid=openmeetings-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
# Пароль служебной учетной записи (в продакшене хранить в защищенном виде)
ldap_passwd=securePassword

# =========================
# База поиска и запросы
# =========================
# Базовый DN, где расположены пользователи в ALD/FreeIPA
ldap_search_base=cn=users,cn=accounts,dc=ald,dc=company,dc=lan
# Поиск пользователя по uid (вводимому при логине)
ldap_search_query=(uid=%s)
# Область поиска: OBJECT | ONELEVEL | SUBTREE (SUBTREE безопаснее для вложенных OU)
ldap_search_scope=SUBTREE

# =========================
# Метод аутентификации
# =========================
# SIMPLEBIND: привязка от имени найденного пользователя
# SEARCHANDBIND: поиск через admin, затем привязка от пользователя
ldap_auth_type=SIMPLEBIND
# Формат DN пользователя для SIMPLEBIND (проверьте соответствие реальным DN)
ldap_userdn_format=uid=%s,cn=users,cn=accounts,dc=ald,dc=company,dc=lan

# =========================
# Provisioning и dereference
# =========================
# Автоматически создавать пользователя в OM при первом входе
ldap_provisioning=AUTOCREATE
# Режим разыменования алиасов: never | searching | finding | always
ldap_deref_mode=always
```

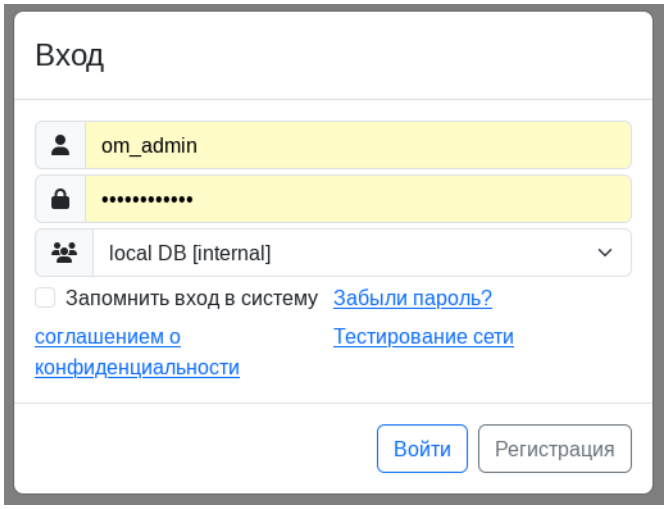
```
# Использовать admin DN для чтения атрибутов после аутентификации (рекомендуется с
 SIMPLEBIND)
ldap_use_admin_to_get_attrs=true

# Синхронизировать пароль LDAP во внутреннюю БД ОМ (рекомендуется отключить в
продакшене)
ldap_sync_password_to_om=false

# =========================
# Группы (опционально)
# =========================
# NONE: игнорировать группы; ATTRIBUTE: брать из атрибута; QUERY: искать по фильтру
ldap_group_mode=NONE
# Пример запроса для posix-групп (если понадобится позже)
ldap_group_query=(&(memberUid=%s)(objectClass=posixGroup))
# Атрибут, содержащий членство в группах (если используется режим ATTRIBUTE)
ldap_group_attr=memberOf

# =========================
# Сопоставление атрибутов
# =========================
# Отображение атрибутов LDAP на внутренние поля ОМ
ldap_user_attr_login=uid
ldap_user_attr_lastname=sn
ldap_user_attr_firstname=givenName
ldap_user_attr_mail=mail
ldap_user_attr_phone=telephoneNumber
# Опциональный атрибут LDAP для аватара пользователя
#ldap_user_attr_picture=
```

5 Настройка OpenMeetings через веб-интерфейс

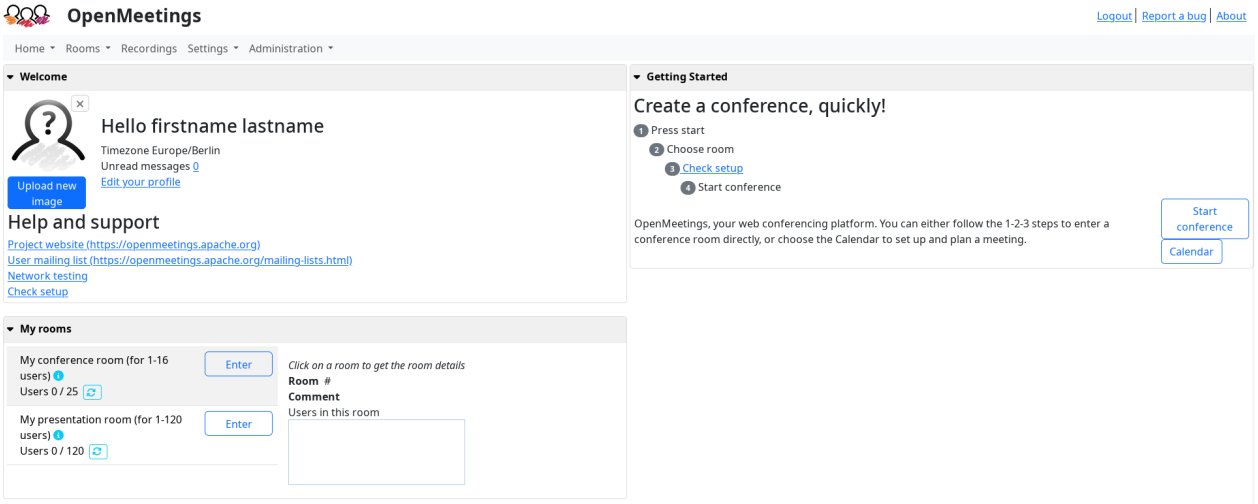
После завершения подготовки сертификата и конфигурационного файла необходимо настроить параметры LDAP в веб-интерфейсе OpenMeetings.

Настройки в веб-интерфейсе:

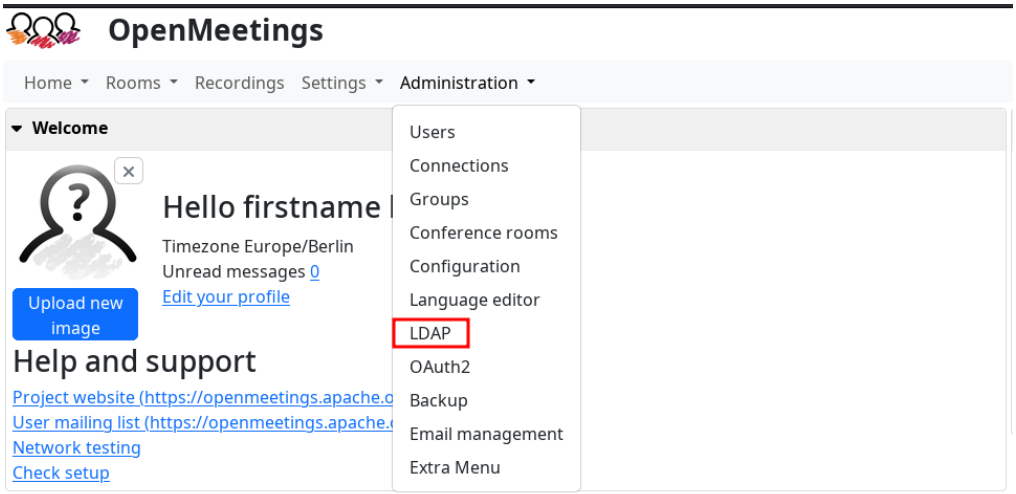
1. Откройте административную панель OpenMeetings:



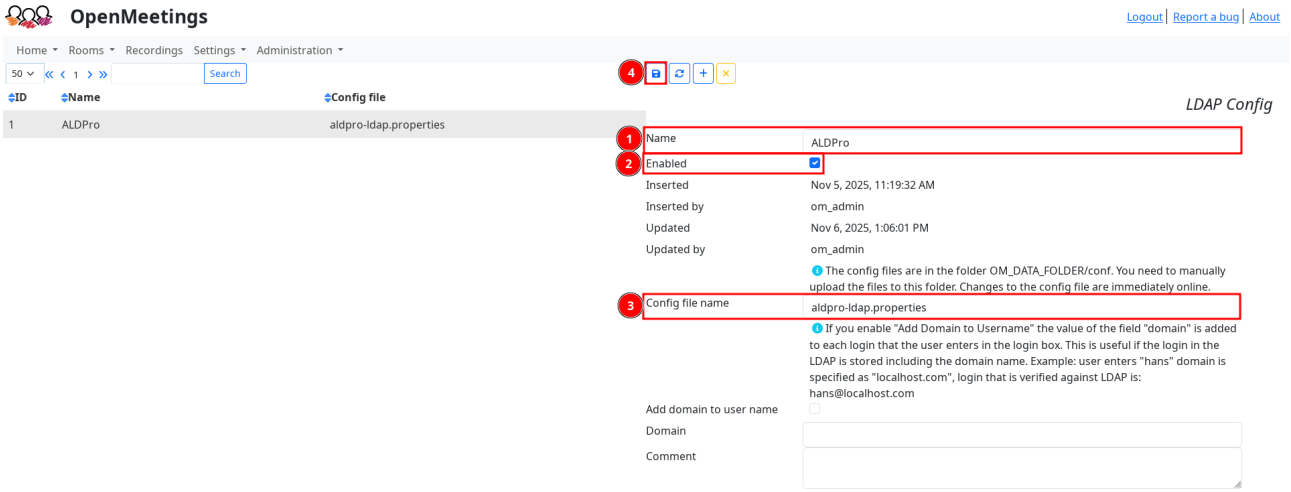
2. Авторизуйтесь под учетной записью администратора:



3. Перейдите в раздел **Administration (Администрирование)** и выберите **LDAP**:



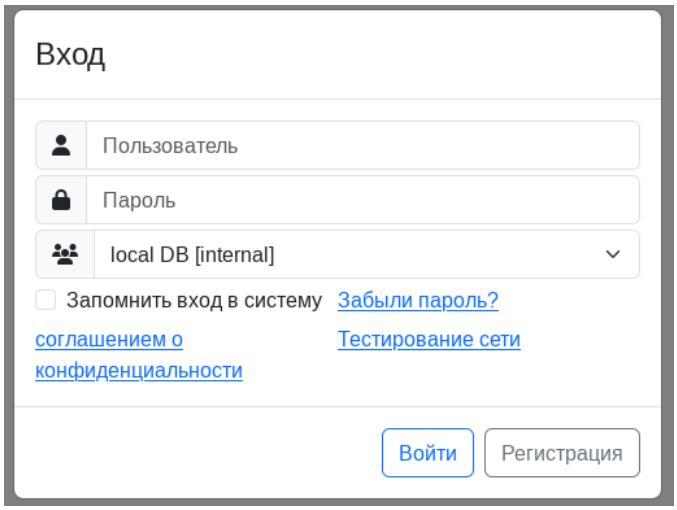
4. Заполните необходимые поля:
    1. Имя соединения.
    2. Отметьте чекбокс Enabled.
    3. Имя файла конфигурации LDAP, созданного в разделе 4 данной инструкции.
    4. После заполнения нажмите кнопку **Сохранить**.



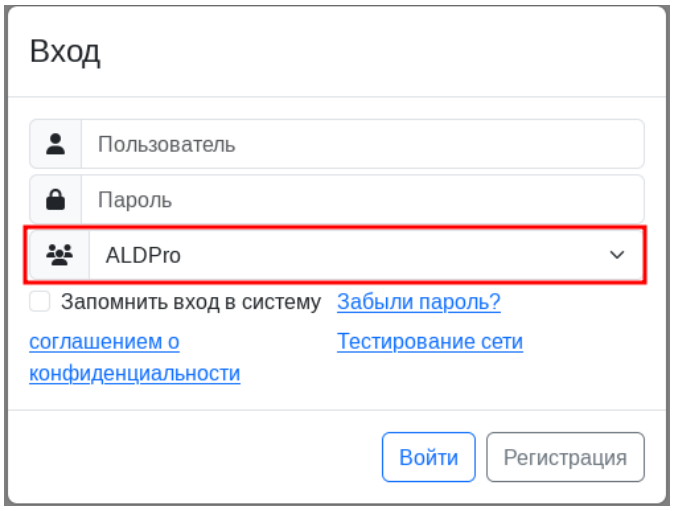
6 Проверка работоспособности интеграции

После завершения конфигурации проверьте работоспособность интеграции:

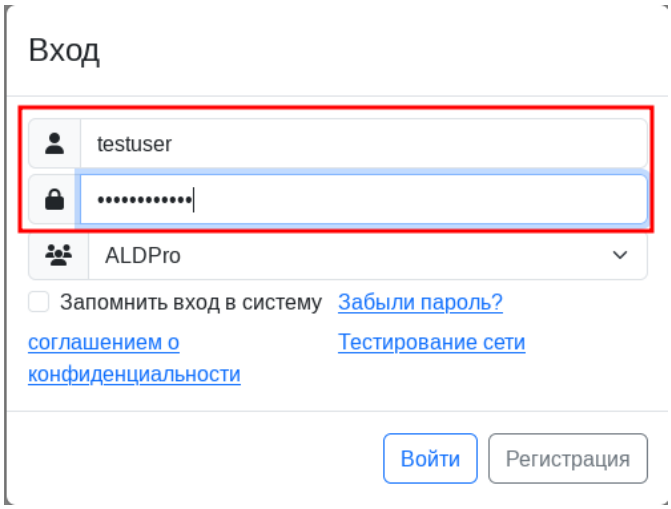
1. Откройте страницу входа OpenMeetings в браузере:



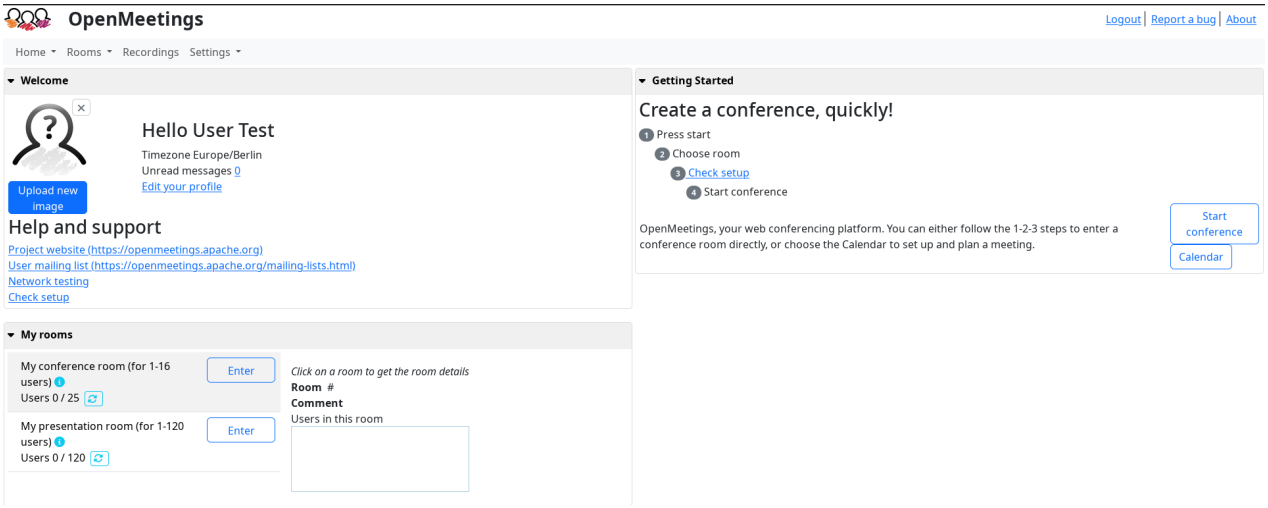
2. Выберите базу пользователей ALDPro:



3. Попытайтесь войти с использованием учетной записи из ALD Pro (например, testuser):



4. Если вход успешен, пользователь будет автоматически создан в базе данных OpenMeetings с правом обычного пользователя:



5. Проверьте логи OpenMeetings для выявления возможных ошибок:

```
tail -f /opt/openmeetings/logs/openmeetings.log | grep -i ldap
```