Интеграция Контур.Толк со службой каталога ALD Pro

11/07/2025

Содержание

1 Введение

Контур.Толк - российский сервис для проведения видеоконференций. Объединяет функции видеовстреч, чатов, вебинаров, онлайн-досок и приложения для переговорных комнат.

Интеграция позволяет упростить администрирование сервиса Контур.Толк при помощи организации SSO на базе решений ALD Pro и Keycloak, где каталог ALD Pro является источником учетных записей пользователей с централизованным управлением, а Keycloak выступает связующим звеном для предоставления аутентификации в веб-портале Контур.Толк.

Данная интеграция протестирована продуктовой командой ALD Pro.

Подробная инструкция по интеграции с Keycloak доступна по ссылке: https://t.me/ald_professionals/5342/9390

Проверка интеграции проводилась с использованием лабораторного стенда. Для успешной интеграции понадобится настроенный Keycloak с публичным IP-адресом, а также пространство КонтурТолк с подключенной функцией SSO.

Лабораторный стенд включает в себя:

- пространство КонтурТолк с подключенной функцией SSO,
- сервер Keycloak: keycloak.example.com <публичный ip-адрес>,
- сервер ALD Pro: dc-1.example.com 10.0.2.10.

2 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=konturtalk,cn=sysaccounts,cn=etc,dc=example,dc=com
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: konturtalk
add:userPassword: password
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 Подготовка пространства Контур.Толк

Для настройки SSO в Контур.Толк нужно, чтобы была приобретена функция SSO для данного продукта. Когда будут произведены все настройки из данного руководства, потребуется написать в тех. поддержку для активации SSO в вашем пространстве.
Также в настройке используется адрес пространства. Чтобы его узнать , нужно зайти в **Общие настройки** (Рисунок 1), где в первых строчках будет указан адрес пространства. Данный адрес потребуется в дальнейших настройках и при обращении в тех. поддержку.

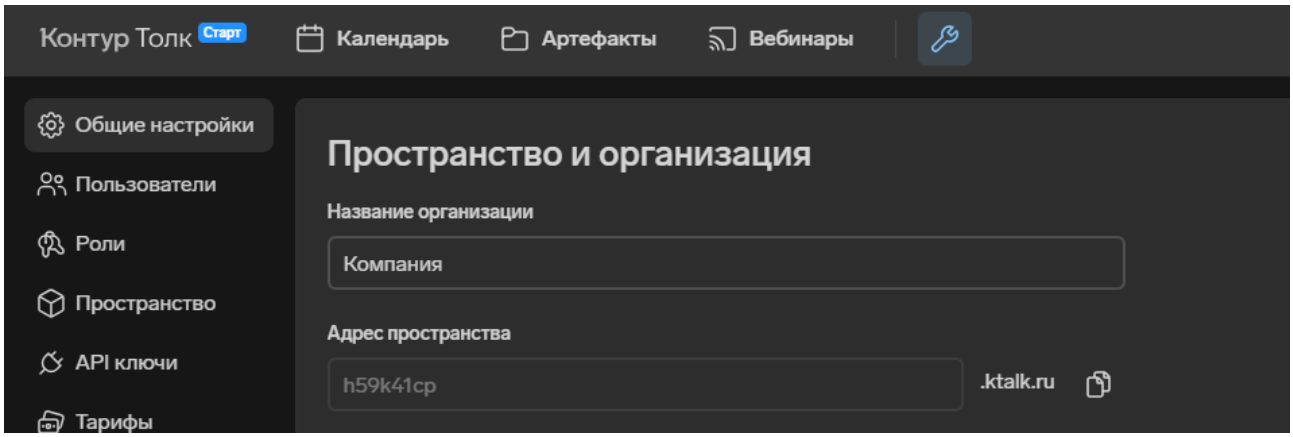

Рисунок 1 - Интерфейс настроек Контур.Толк

4 Создание Realm

Realm — это пространство Keycloak, в котором происходит управление набором пользователей, учетных данных, ролей и групп. Одно развертывание Keycloak позволяет создавать множество Realm.

Создайте новый Realm. Для этого:

1. Перейдите в панель администратора Keycloak и авторизуйтесь под учетной записью администратора. Для авторизации используйте данные из ранее заданных переменных.
2. В левом верхнем углу нажмите на выпадающий список и выберите Create Realm (Рисунок 2).

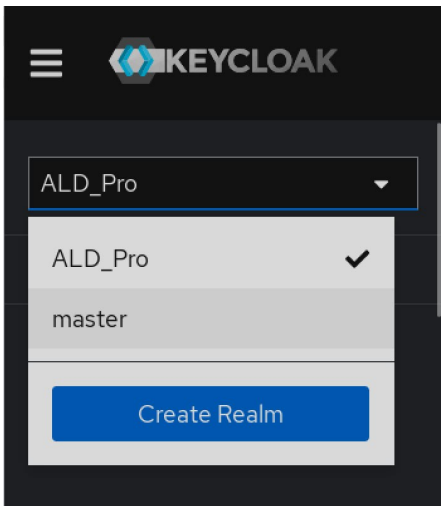

Рисунок 2 – Создание Realm

3. В появившемся поле Real name укажите имя для Realm.
4. Нажмите Create.

5 Создание client

Client - это приложение, которое будет обрабатывать аутентификацию пользователей.

1. Перейдите в созданный Realm и на панели слева выберите раздел Clients.
2. Нажмите Create client.
3. В появившемся поле укажите Client ID (идентификатор, который будет передаваться в Контур.Толк в ID-токене). Сохраните этот идентификатор, он понадобится для завершения настроек на стороне Контур.Толк
4. Нажмите Next.
5. Включите следующие параметры:
    a. Client authentication;
    b. Authorization;
    c. Implicit Flow;
    d. Standard flow.
6. Нажмите Next.
7. Если Keycloak настраивается для облачной версии Контур.Толк:
    - в поле Valid redirect URLs введите адреса:
        - https://auth-gateway.kontur.ru/login/callback;
        - https://auth-gateway.testkontur.ru/login/callback;
    - в поле Home URL введите адрес вашего пространства в Контур.Толк в формате https://%SPACE%.ktalk.ru/.
8. Если Keycloak настраивается для серверной версии Контур.Толк (On-premise):
    a. в поле Root URL введите опубликованный адрес, по которому доступен Keycloak, в формате https://keycloak.mycompany.ru/;
    b. в поле Valid redirect URLs введите символ * (звездочку);
    c. в поле Valid post logout redirect URIs введите следующие адреса (без кавычек):
        - «https://auth-gateway.kontur.ru/logout/callback*»;
        - «https://auth-gateway.kontur.ru/logout/callback?logoutId=*».
9. Нажмите Save.
10. В блоке Login settings → Login theme выберите keycloak или кастомную тему.
11. Нажмите Save.

6 Настройка LDAP-провайдера (Подключение к каталогу ALD Pro)

Чтобы настроить синхронизацию, выполните следующее:

1. На панели слева выберите User federation.
2. Нажмите Add Ldap providers.
3. В поле UI display name укажите любое имя поставщика, например ALD Pro.
4. В поле Vendor укажите имя поставщика Red Hat Directory Server.
5. В блоке Connection and authentication settings заполните поля, как на рисунках 3 и 4:

   - Connection URL: укажите адрес сервера LDAP: ldap://,
   - Bind type: выберите simple.

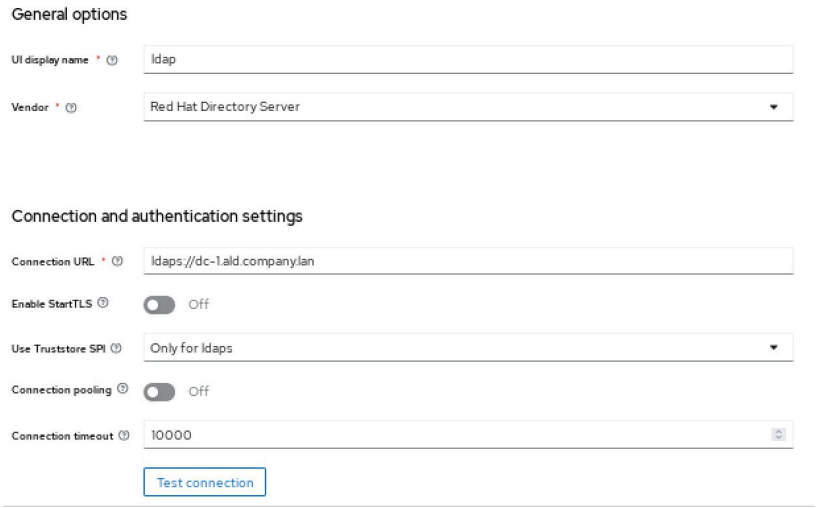

Рисунок 3 – Пример LDAP-адреса сервера

   - Bind DN: укажите путь до ранее созданной сервисной учетной записи LDAP (например, uid=kontur, cn =sysaccounts, cn=etc, dc=ald,dc=company, dc=lan),
   - Bind credentials: введите пароль от сервисной учетной записи,
   - при необходимости можете задать Connection timeout.

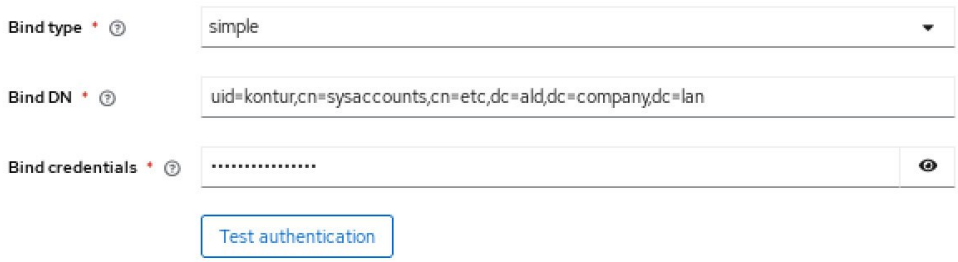

Рисунок 4 – Пример учетных данных

6. В блоке LDAP searching and updating заполните поля (Рисунок 5):

   - Edit mode: укажите значение «READ_ONLY»,

- Users DN: укажите путь до каталога с пользователями cn=users, cn=accounts, dc=ald, dc=company, dc=lan,
- Username LDAP attribute: uid,
- RDN LDAP attribute: uid,
- UUID LDAP attribute: entryUUID,
- User object classes: inetOrgPerson, organizationPerson,
- Search: One Level.

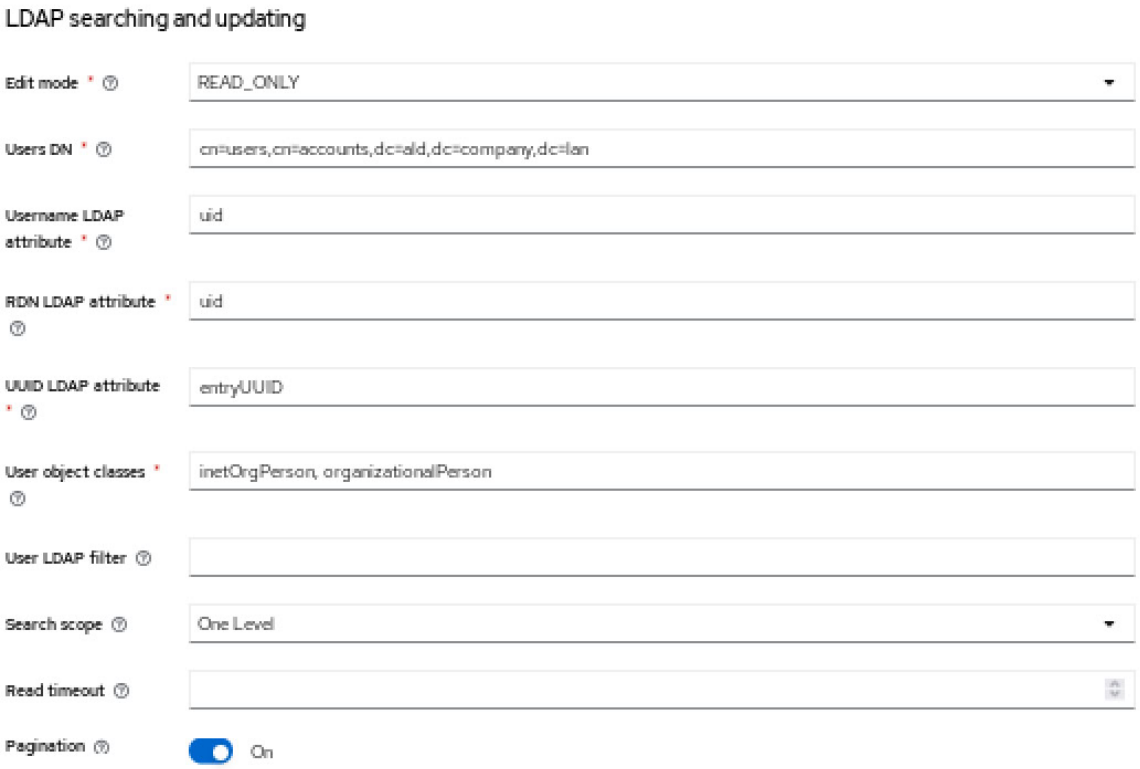

Рисунок 5 – Пример настройки атрибутов

7. В блоке Synchronization settings включите все параметры и укажите периодичность синхронизации (Рисунок 6).

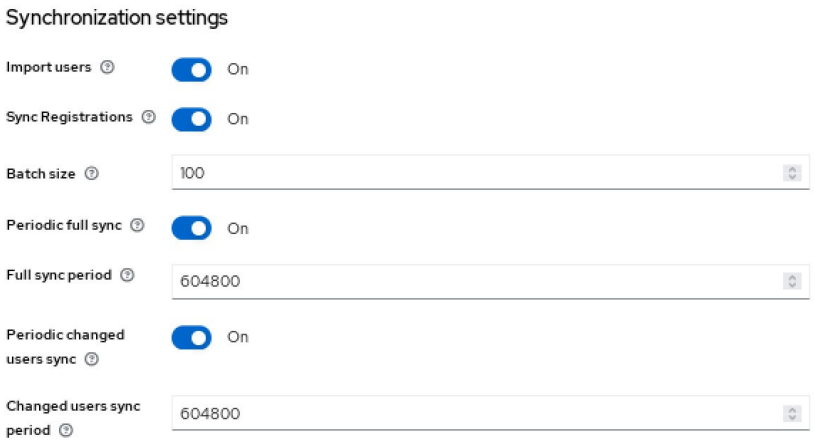

Рисунок 6 – Пример настроек синхронизации

8. В блоке Advanced settings включите параметр Trust email (Рисунок 7).

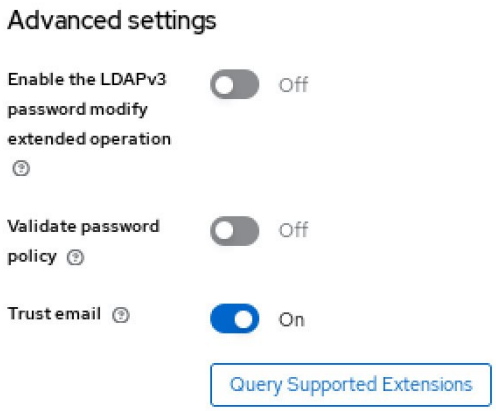

Рисунок 7 – Пример расширенных настроек

9. Нажмите Save.

10. Перейдите на вкладку Mappers и укажите наименования атрибутов:

- выберите mail. В поле User Model Attribute укажите значение «email», в поле LDAP Attribute укажите значение «mail»,
- нажмите Save,
- выберите first name. В поле User Model Attribute укажите значение «firstName», в поле LDAP Attribute укажите значение «givenName»,
- нажмите Save,
- нажмите last name. В поле User Model Attribute укажите значение «lastName», в поле LDAP Attribute укажите значение «sn»,
- нажмите Save.

11. Проверьте синхронизацию пользователей, для этого нажмите Sync all users в выпадающем меню, которое находится в правом верхнем углу настроек LDAP-подключения (Рисунок 8)

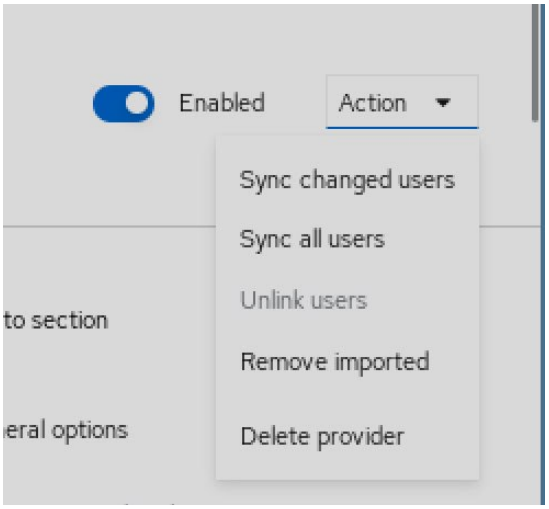

Рисунок 8 – Синхронизация пользователей

12. Проверьте доступность LDAP в Keycloak. Для этого перейдите в раздел Users, в поле поиска введите символ * (звездочку) и нажмите Enter.

Если пользователи появились, значит импорт выполнен успешно.

7 Настройка claims

Установите соответствия для claims (атрибутов).

Наименования атрибутов (claims) указаны ниже в качестве примера. В вашей базе данных наименования могут отличаться от предложенных.

Обязательные claims:

- email: email;
- surname: family_name;
- firstname: given_name.

Дополнительные claims:

- post: title;
- phone: phone_number;
- picture: picture.

8 Завершение настройки

Если вы используете серверную версию Контур.Толк (On-premise), настройка завершена. Подробнее о работе серверной версии, см. в инструкции.

Если вы используете облачную версию, для завершения настройки сообщите своему специалисту по внедрению следующие данные:

- название организации;
- адрес вашего пространства в формате «name.ktalk.ru».
  О том, как его узнать, см. в статье «Частые вопросы»;
- адрес сервера OpenID Connect в формате:
  https://<ваш_домен.ru>:/realms/<ваш_real_name>/.well-known/openid-configuration
- можно предоставить дискавери-документ. Для этого в сервисе администрирования Keycloak перейдите в раздел Realm settings → General → Endpoints. Скопируйте ссылку на OpenID Endpoint Configuration и приложите в качестве адреса сервера;
- **Client_id**. Укажите id, который вы установили при создании client;
- **Client_secret**. Его можно найти в сервисе администрирования Keycloak → раздел Clients → выберите нужного client → Credentials → Secret.