ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

СИСТЕМА РЕДАКТИРОВАНИЯ И СОВМЕСТНОЙ РАБОТЫ

СИСТЕМА ХРАНЕНИЯ ДАННЫХ

3.2

ИНТЕГРАЦИЯ С ВНЕШНИМИ КАТАЛОГАМИ

Версия 1

На 21 листах

Дата публикации: 17.12.2024

Москва
2024

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис», «MyOffice» и «Squadus» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

В настоящем документе используются следующие сокращения с соответствующими расшифровками (табл. 1).

Таблица 1 — Сокращения и обозначения

Сокращение, термин	Расшифровка и определение
AD	Microsoft Active Directory, служба каталогов, разработанная Microsoft для доменных сетей Windows
API	Application Programming Interface, интерфейс программирования приложений
CO	Система редактирования и совместной работы
PGS	Система хранения данных
Тенант	Логический объект, включающий в себя совокупность вычислительных ресурсов, репозиторий и пользователей
ПО	Программное обеспечение
Маппинг	Сопоставление двух каталогов пользователей
LDAP	Lightweight Directory Access Protocol, облегченный протокол доступа к каталогам, открытый стандартизированный протокол, применяемый для работы с различным реализациям служб каталогов, в том числе и Active Directory

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

В настоящем документе описан процесс настройки интеграции Системы редактирования и совместной работы и Системы хранения данных с внешними каталогами.

1.2 О компонентах

Система хранения данных — компонент, предназначенный для безопасного хранения корпоративных файлов и обеспечения возможностей авторизации, аутентификации и разграничения прав доступа пользователей.

Система редактирования и совместной работы — компонент, предназначенный для индивидуального и совместного редактирования текстовых и табличных документов, а также просмотра и демонстрации презентаций.

Представленные компоненты входят в состав следующих продуктов:

– «МойОфис Частное Облако 3»;

– «МойОфис Профессиональный 2»;

– «МойОфис Профессиональный 3»;

– «МойОфис Схема»;

– Squadus PRO.

Список возможностей приложения приведен в документе «Функциональные возможности»

2 ИНТЕГРАЦИЯ С AD

2.1 Настройка интеграции с AD

Для настройки интеграции в PGS необходимо произвести следующие действия:

1. Открыть доступ к компоненту Keycloak из внешней сети, выполнив следующую команду:

```
docker service update --publish-add published=8091,target=8080\
pgs-keycloak_keycloak
```

2. Перезапустить сервисы `pgs_aristoteles` и `pgs_euclid`.

3. Открыть веб-интерфейс Keycloak.

(адрес по умолчанию `http://<ENV>.<DEFAULT_DOMAIN>:8091`).

4. Перейти в Administration Console и ввести данные для входа (табл. 2).

Таблица 2 — Параметры подключения к Keycloak

Параметр	Значение
Имя пользователя	pgs
Пароль	значение переменной KEYCLOAK_PASSWORD

5. Выбрать тенант (или realm), для которого нужна интеграция.

6. Нажать `User Federation`.

7. Из выпадающего меню выбрать провайдера LDAP (Add provider) с именем `pgsldapnew`.

8. Заполнить параметры в соответствии с таблицей 3.

Таблица 3 — Значение параметров для интеграции PGS с AD

Параметр	Значение	Комментарий
usernameLDAPAttribute	sAMAccountName (или другое текущее значение атрибута в AD)	Атрибут, назначаемый как имя пользователя в Keycloak
uuidLDAPAttribute	sAMAccountName (или другое текущее значение атрибута в AD)	Атрибут уникального идентификатора объекта
editMode	UNSYNCED	Внутренний атрибут Keycloak, позволяющий обновлять пользовательские данные на LDAP-сервере в режиме «только чтение»
connectionUrl	Хост в формате ldap://111.1.1.1	Хост для подключения к каталогу AD
usersDn	Данные для подключения к AD соответственно настройкам сервера	Путь до OU (организационной единицы), в которой хранятся учетные записи пользователей

Параметр	Значение	Комментарий
bindDn	Логин пользователя AD	Полное имя (DN, distinguished name) учетной записи пользователя в каталоге, от имени которого будет выполняться работа с каталогом
bindCredential	Пароль пользователя AD	Пароль учетной записи пользователя в каталоге, от имени которого будет производиться работа с каталогом

9. Остальные параметры оставить по умолчанию.

10. Нажать `Save` и `Synchronize all users`.

На вкладке `Users` в левом меню можно просмотреть список всех импортированных пользователей.

В случае наличия ошибок возможно вернуться на вкладку `User Federation` к провайдеру `pgsldapnew` и нажать `Remove imported` для очистки списка пользователей.

При длине DN больше чем 255 символов, возникают проблемы, связанные с ограничением на количество символов в таблице postgres, в этом случае необходимо выполнить следующую команду:

```
docker exec $(docker ps -q -f name=pgs-postgres) psql -U\
 keycloak -c "ALTER TABLE user_attribute ALTER COLUMN\
 value TYPE TEXT;"
```


3 НАСТРОЙКА ИНТЕГРАЦИИ С FREEIPA

3.1 Описание

FreeIPA — это программное обеспечение, распространяемое с открытым исходным кодом, являющееся аналогом AD, работающее по протоколу LDAP.

3.2 Использование ldapsearch

ldapsearch — это инструмент командной строки, с помощью которого можно проверить информацию о схеме пользователей в каталоге LDAP перед конфигурированием и устранить неисправности во время настройки.

Пример ldapsearch:

```
ldapsearch -D
"uid=private_cloud_acc,cn=techaccounts,cn=etc,dc=co,dc=dev,dc=myoffice,dc=group"
-w '7DZbhi:$mhp8EtG' -LLL -H ldap://example.net -b
"dc=co,DC=dev,DC=myoffice,DC=group" "(uid=user.user)"
```

3.3 Настройка с помощью Keycloak

Интеграция в Keycloak аналогична интеграции с AD и отличается параметрами конфигурации. Порядок настройки FreeIPA:

1. Для начала работы следует открыть вкладку **User federation** и нажать кнопку **Add Pgsldapnew providers** (рис. 1):

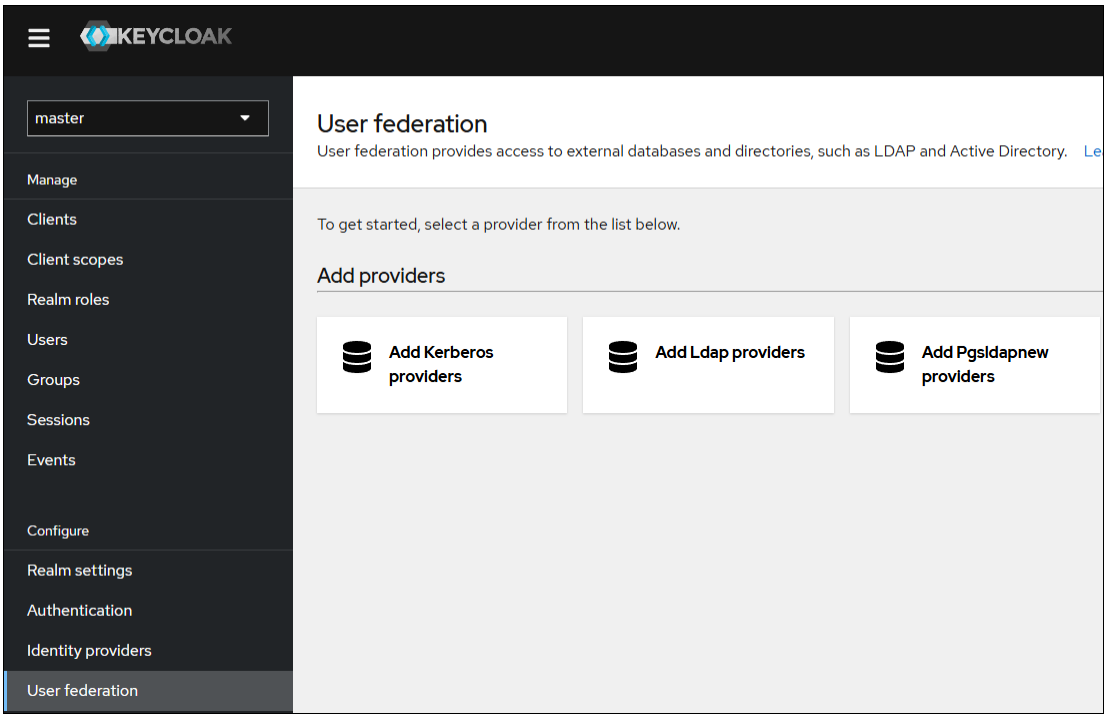

Рисунок 1 — Окно создания плагина

2. В окне **Add Pgsldapnew providers** ввести параметры подключения (рис. 2):

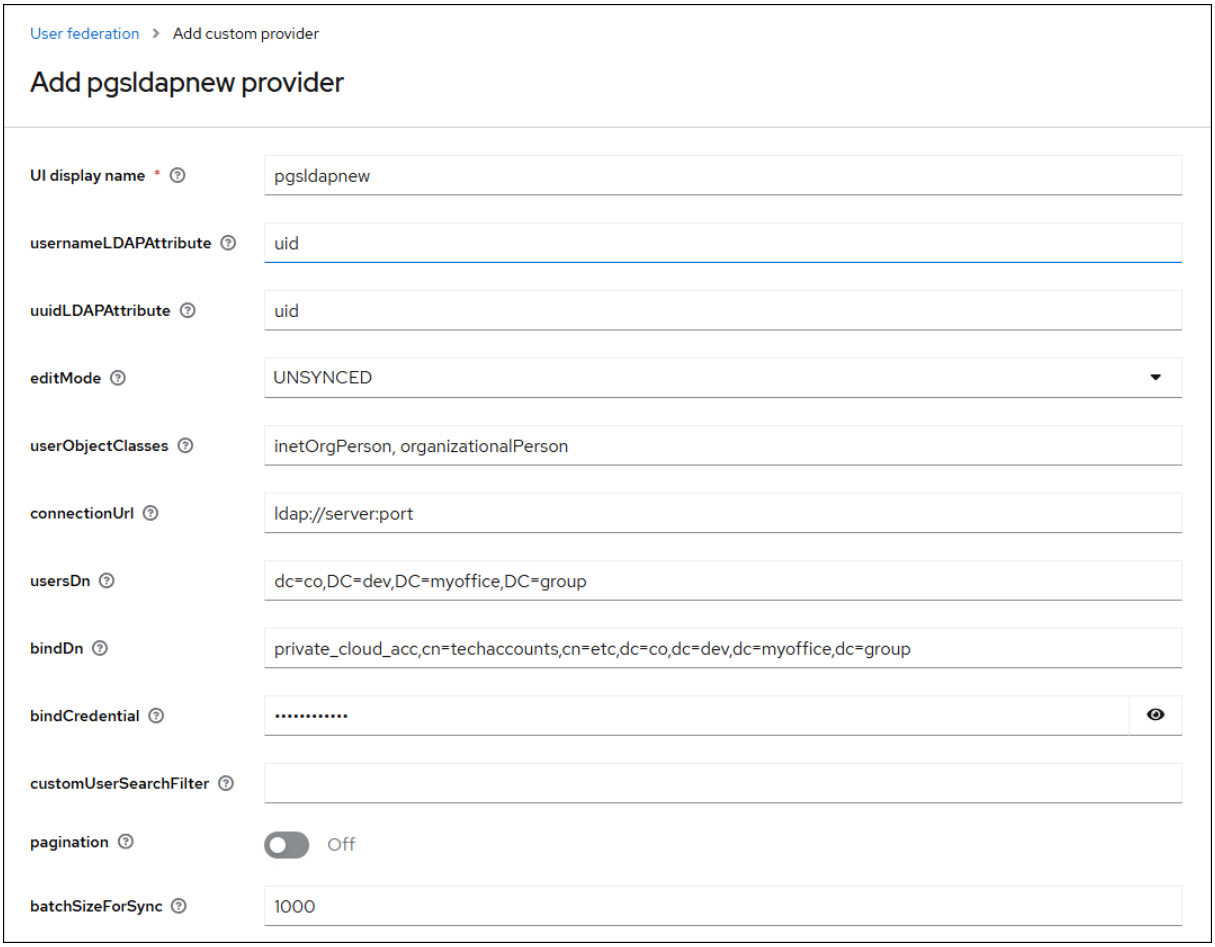

Рисунок 2 — Основные параметры настройки

3. В поле **Vendor** выбираем **Red Hat Directory Server** (рис. 3):

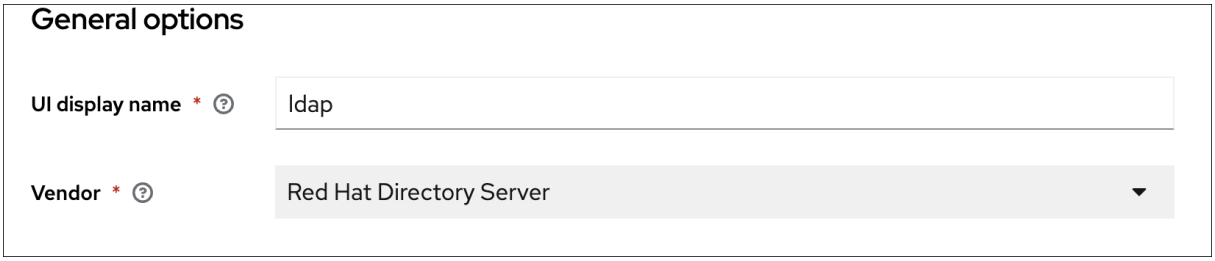

Рисунок 3 — Параметры настройки вендора

4. Маппинг `firstName` настраивается по атрибуту каталога `givenName` (рис. 4):

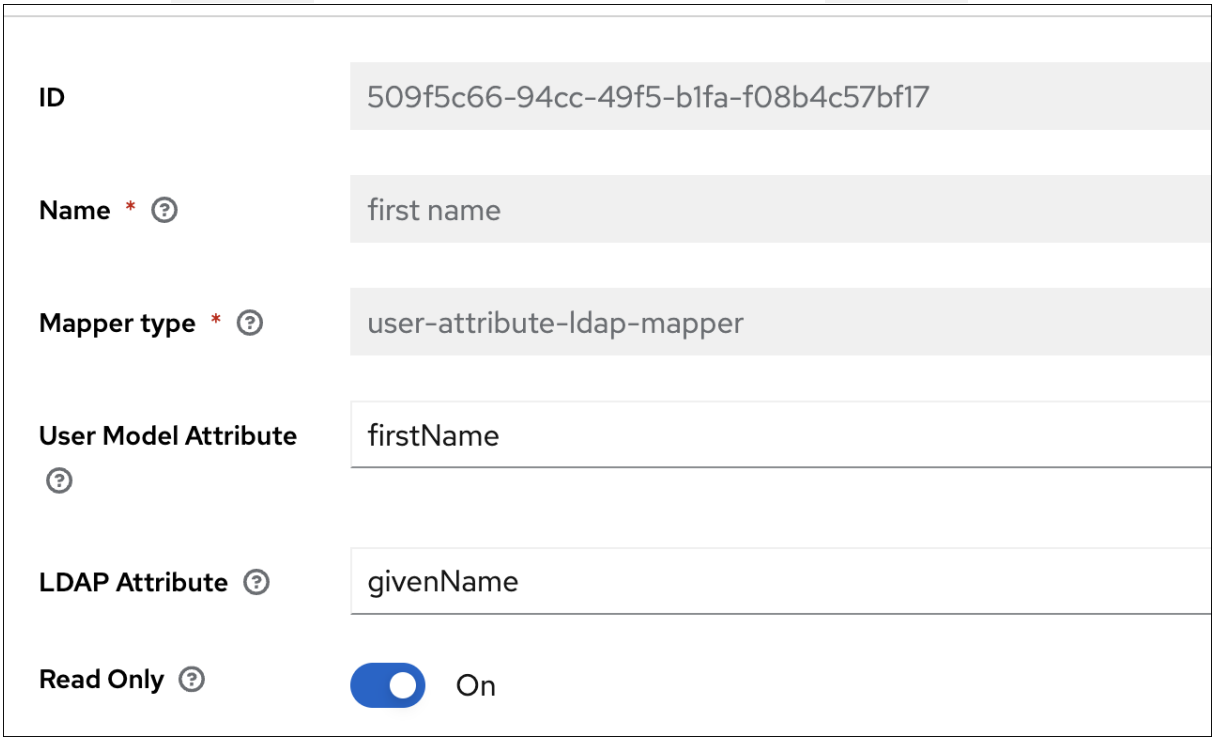

Рисунок 4 — Настройка маппинга

После интеграции для проверки следует использовать учетную запись из каталога в текущем продукте (с соответствующим доменным именем).

3.4 Настройка с помощью консоли

Для настройки параметров с помощью консоли следует использовать следующий пример, заменив необходимые параметры:

```
usernameLDAPAttribute uid
uuidLDAPAttribute uid
userObjectClasses inetOrgPerson, organizationalPerson
connectionUrl ldap://server
usersDn cn=users,cn=accounts,dc=co,DC=dev,DC=myoffice,DC=group
bindDn
uid=private_cloud_acc,cn=techaccounts,cn=etc,dc=co,dc=dev,dc=myoffice,dc=group
bindCredential 7DZbhi:$mhp8EtG
```

3.5 Дополнительные настройки FreeIPA

3.5.1 Смена имени администратора

Для исключения ошибки при перезаписи учетной записи администратора FreeIPA необходимо при создании тенанта для проверки интеграции использовать другое имя учетной записи администратора (параметр `admin_username`).

```
curl -X POST http://localhost:8852/tenants -H "Authorization: $euclid_token" -d
"name=freeipa21" -d "default_domain=freeipa21.ru" -d 'admin_password=Qwerty!123'
-d "admin_recovery_email=adminadmin@gmail.com" -d max_users=12000 -d
admin_username=adminmain@freeipa21.ru
```

3.5.2 Отображение статуса пользователя

Для корректного отображения статуса пользователя Keycloak необходимо использовать в каталоге атрибуты, указанные в таблице 4.

Таблица 4 — Параметры статуса пользователя

Параметр	Комментарий
`userAccountControl`	Определяет статус пользователя
`pwdLastSet`	Необходимо использовать ненулевое значение

4 НАСТРОЙКА ИНТЕГРАЦИИ С OPENLDAP

4.1 Описание

OpenLDAP — это программное обеспечение, распространяемое с открытым исходным кодом, являющееся аналогом AD, работающее по протоколу LDAP.

4.2 Настройка с помощью Keycloak

Создание плагина интеграции с федерацией доступно в веб-интерфейсе сервиса `keycloak`. Начиная с версии 3.2 доступен для использования нативный плагин (Add ldap providers). Пример настройки параметров интеграции с с нативным плагином (Add ldap providers):

Порядок действий:

1. Для начала работы открыть вкладку **User federation** и нажать кнопку **Add Ldap providers** (рис. 5):

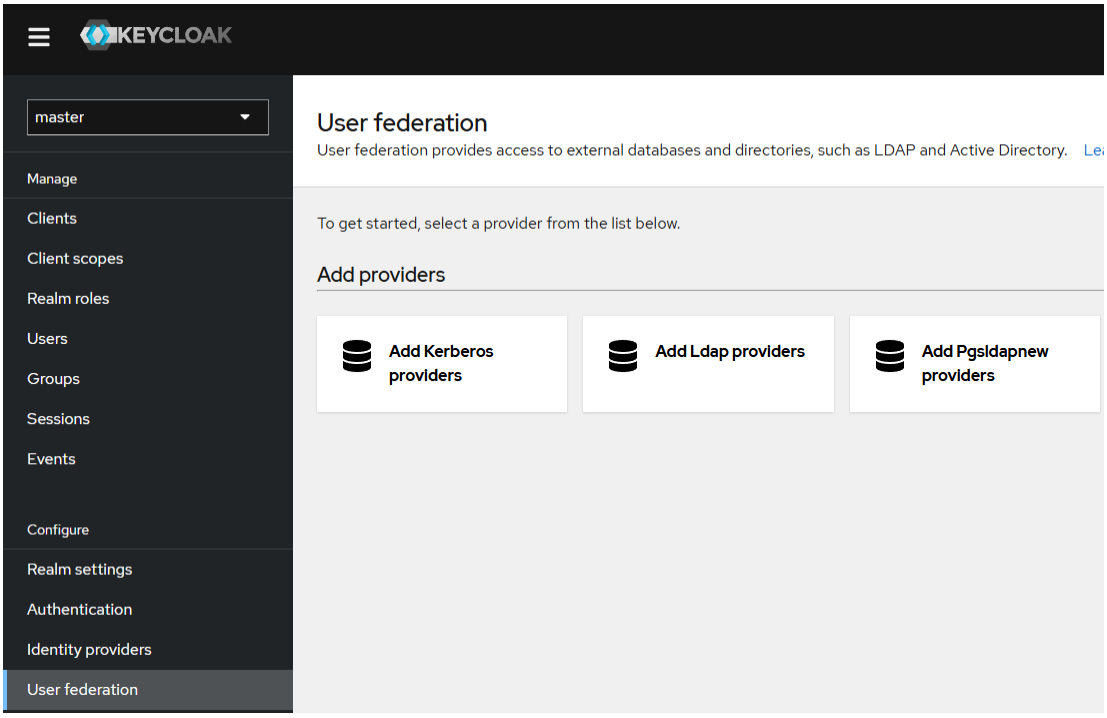

Рисунок 5 — Окно создания плагина

2. В поле **Vendor** следует выбрать пункт **Active directory** или **Other** (рис. 6).

3. Указать IP-адрес и порт для сервера LDAP в поле **Connection_URL** (рис. 6):

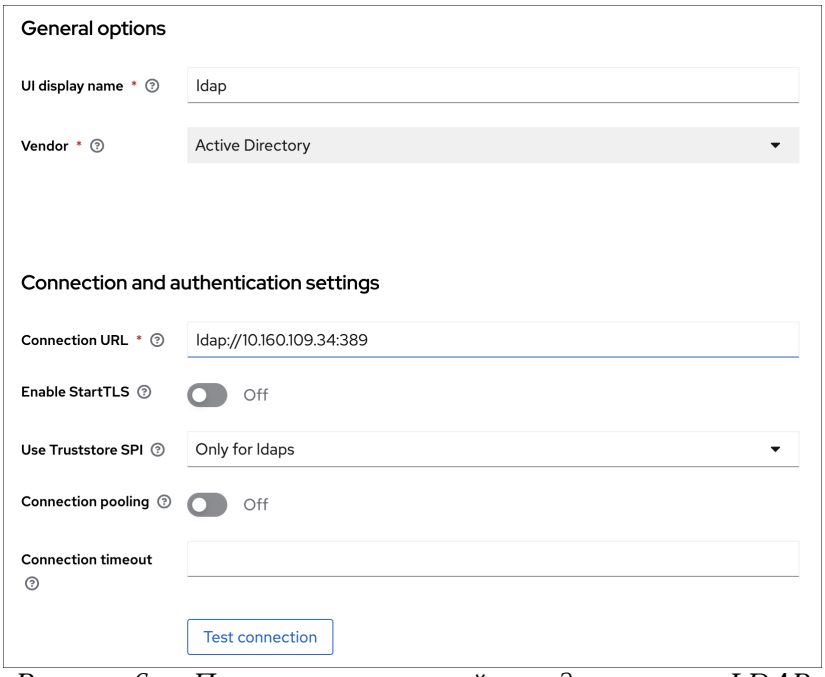

Рисунок 6 — Параметры настройки подключения к LDAP

3. Указать в поле **bind DN** — имя пользователя, а в поле **bind credentials** — пароль пользователя, полученные от администратора сервера LDAP (рис. 7). Проверить параметр **Username LDAP attribute**, отвечающий за имя пользователя в каталоге.

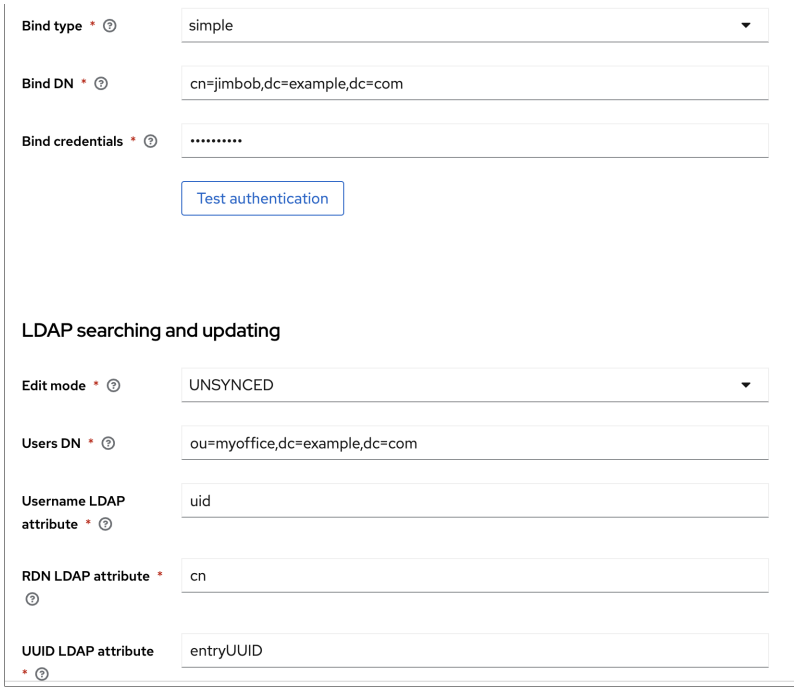

Рисунок 7 — Параметры настройки подключения к LDAP

4. Указать в поле **User object classes** — схему, используемую в каталоге openLdap, в поле **User LDAP filter** — фильтр поиска пользователей и в поле **search scope** — поиск по древовидной структуре, если имеются вложенные OU (рис. 8):

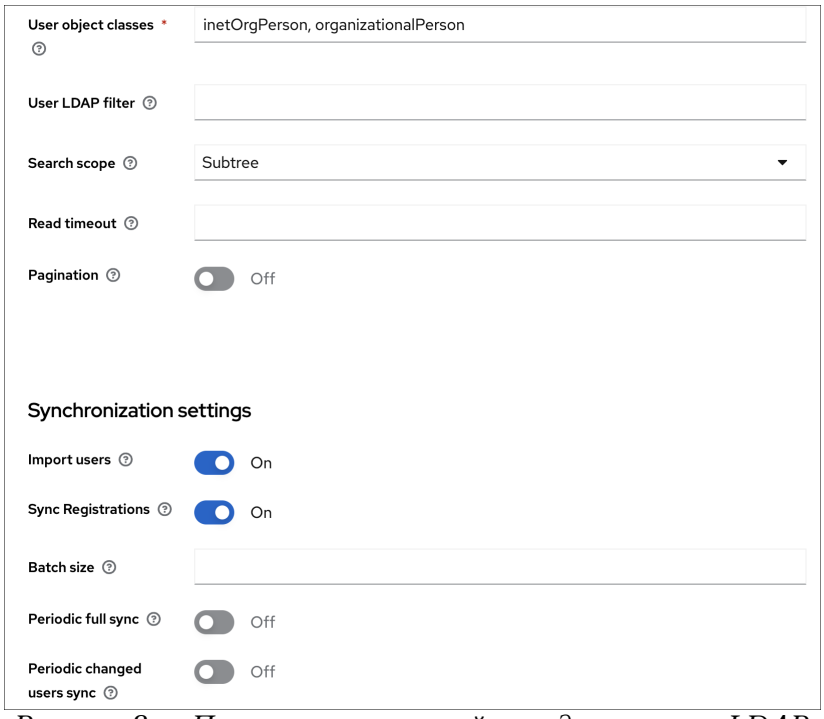

Рисунок 8 — Параметры настройки подключения к LDAP

5. Маппинг пользовательских данных настраивается во вкладке **Mappers** (рис. 9):

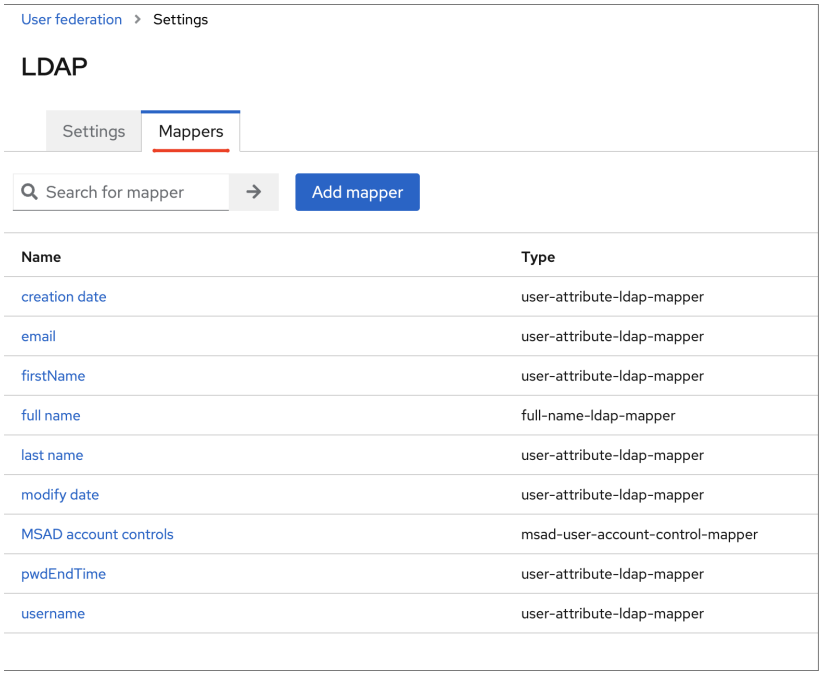

Рисунок 9 — Вкладка Mappers

6. Каждому полю из модели пользователя в `keycloak` должно соответствовать логически верное поле из каталога OpenLDAP. Например, маппинг имени пользователя по полю **givenName** из каталога (рис. 10):

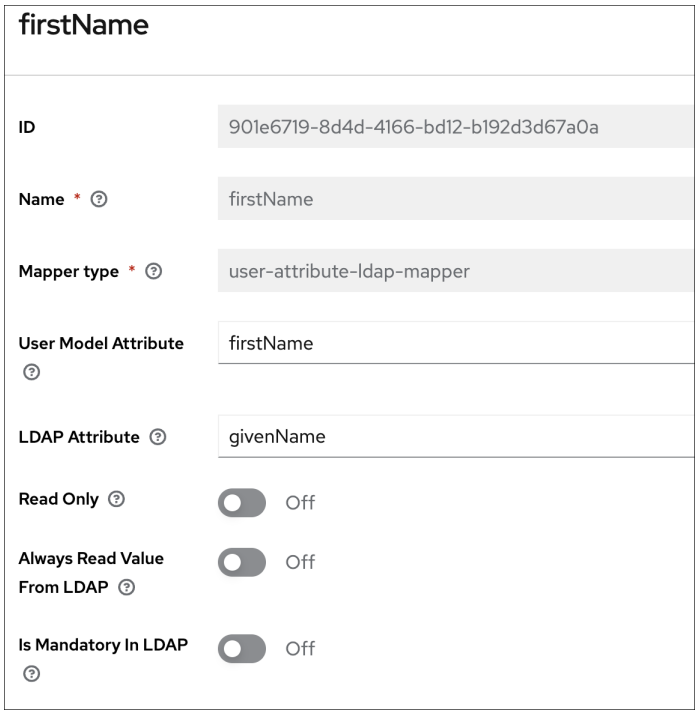

Рисунок 10 — Окно параметров пользователя

7. Запуск синхронизации пользователей осуществляется с помощью пункта **Sync all users** в выпадающем меню **Action** (рис. 11):

Рисунок 11 — Запуск синхронизации пользователей

После выполнения синхронизации список пользователей появиться во вкладке **Users** (рис. 12):

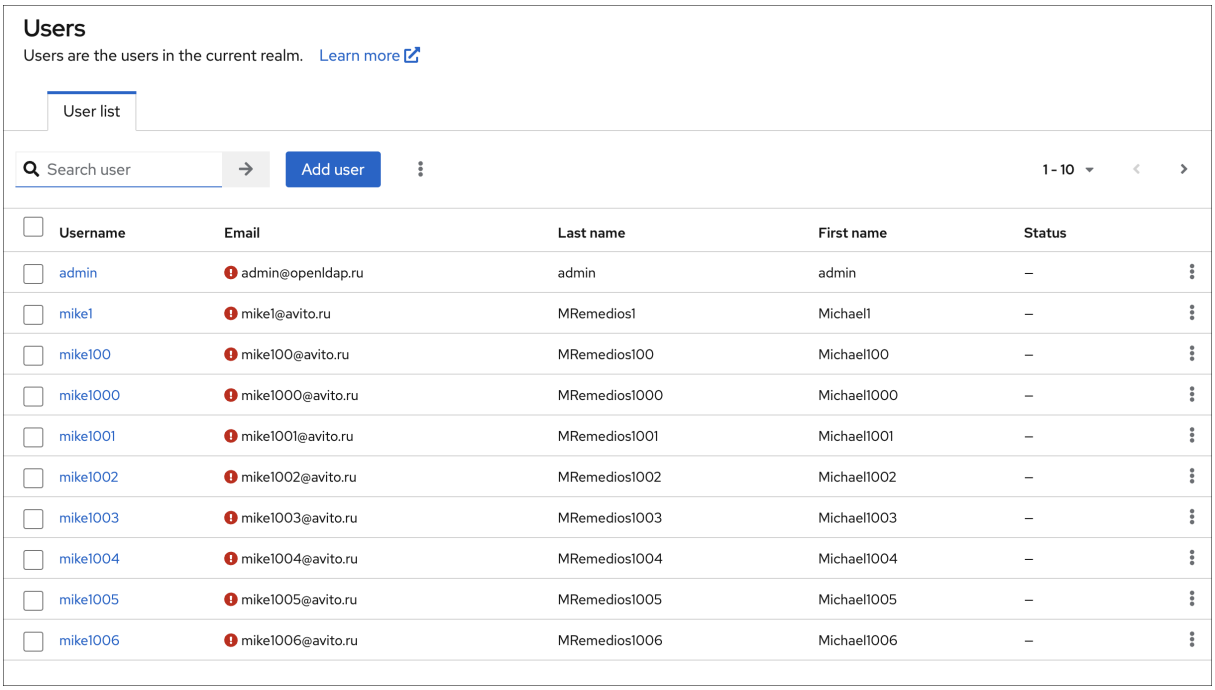

Рисунок 12 — Список пользователей после синхронизации

После успешного выполнения синхронизации интеграция с LDAP выполнена.

5 ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ ИНТЕГРАЦИИ

5.1 Решение ошибки синхронизации

При попытке синхронизации пользователей с AD/OpenLDAP в журнале событий keycloak появляется следующая ошибка:

```
[LDAPStorageProviderFactory] (executor-thread-17) Sync all users from LDAP to
local store: realm: 9aacad43-4aa0-43e5    -a3c6-dd4a85b6ad0f, federation
provider: pgsldapnew pgs-keycloak_keycloak.1.sb0qpf5mwsde@invsr-pgs-be1    |
2024-07-11 13:24:52,522 ERROR [org.keycloak.services.error.KeycloakErrorHandler]
(executor-thread-17) Uncaught server error: java.lang.NumberFormatException:
Cannot parse null string
```

Решение:

В веб-интерфейсе сервиса Keycloak включить и выключить федерацию `pgsldapnew`

5.2 Перенос файлов удаленного пользователя другому пользователю

В контейнере Aristoteles подготовлен скрипт для переноса одного/всех файлов пользователя другому пользователю с заменой нужных линий взаимосвязи между узлами в БД (для случаев, когда первоначальный пользователь удален).

Расположение файла: `.dev_utils/arango_manual_folder_reassign.py`

Примеры использования:

1. Для передачи одного файла другому пользователю следует выполнить команду:

```
docker exec $(docker ps -qof name=pgs_aristoteles) \
python3 .dev_utils/arango_manual_folder_reassign.py \
--target_user_login "<user_login>" --object_id "<folder_id>"
```

Параметры:

– `target_user_login` — пользователь, которому будет передан файл;

– `object_id` — ID объекта, пример: `74a0e524-f356-4fc5-92ad-0e55f448b30f`.

2. Для передачи всех файлов другому пользователю (в том числе административные права на корпоративные папки) следует выполнить команду:

```
docker exec $(docker ps -qof name=pgs_aristoteles) \
python3 .dev_utils/arango_manual_folder_reassign.py \
--source_user_login "<user_login>" --target_user_login "<user_login>"
```

Параметры:

– `source_user_login` — пользователь, файлы которого будут переданы;

– `target_user_login` — пользователь, которому будут переданы все файлы.

5.3 Переключение кастомного плагина на нативный

В продукте версии 3.2 был реализован отказ от кастомного плагина в пользу нативной реализации интеграции с каталогами на уровне keycloak. При первичной настройке интеграции на тенанте миграция выполняется автоматически.

В версии 3.2 реализован переход на измененную схему работы с внешними каталогами.Для исключения ошибки задвоения `user_domain` атрибутов у пользователей перед обновлением сервер на версию 3.2 необходимо:

– выполнить резервное копирование Postgres;

– отключить синхронизацию пользователей и запустить ее после выполнения всех пунктов настоящего раздела.

Если интеграция с AD была настроена ранее, необходимо выполнить следующие действия:

1. Проверить выполнение резервного копирования базы PostgreSQL.
2. Проверить выполнение миграции с помощью скрипта `remove_domain_from_username.py`. Характерный признак — в карточке пользователя `username` будет без доменной части (рис. 13), а в атрибутах будет новое поле `user_domain` (рис. 14).

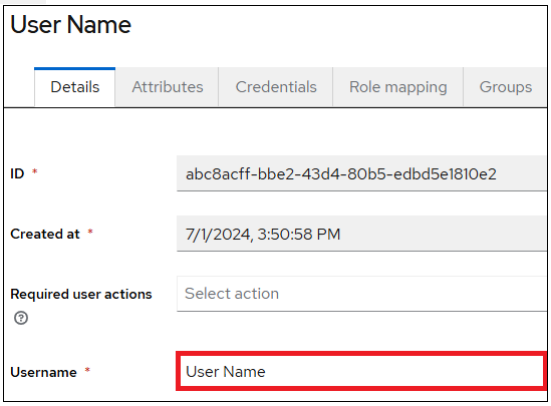

Рисунок 13 — Карточка пользователя

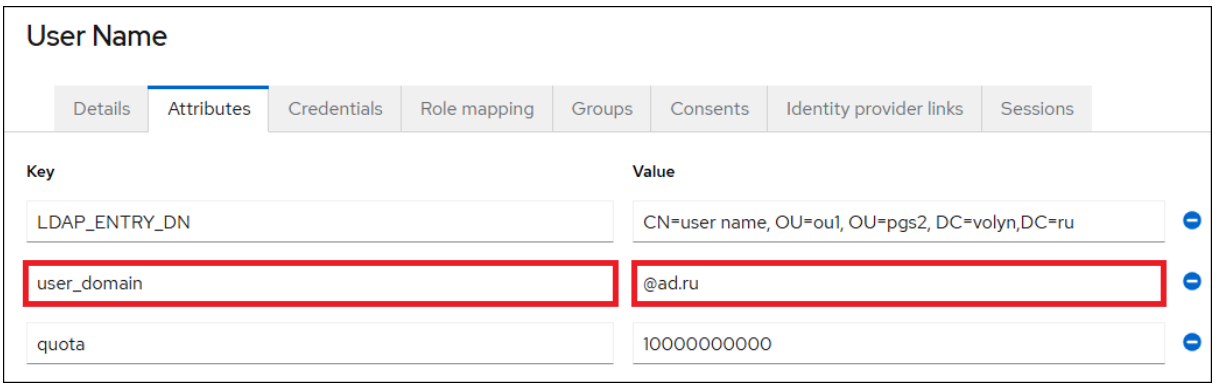

Рисунок 14 — Владка атрибутов пользователя

Если карточка пользователя содержит в поле `username` доменную часть и в атрибутах поле `user_domain`, необходимо выполнить миграцию повторно, с помощью скрипта `remove_domain_from_username.py`.

3. Выполнить настройку интеграции в соответствии с требованиями раздела «Настройка интеграции с LDAP».
4. Перенести уже созданные маппинги. Существующие маппинги на федерацию следует проверить по ссылке:

http://domain_or_ip:8091/admin/master/console/#/tenant_name/
user-federation/ldap/federation_id/mappers

Параметры, используемые в создании ссылок описаны в таблице 5.

Таблица 5 — *Параметры настройки LDAP в федерации*

Параметр	Значение
host/IP-адрес	Указать для сервера
tenant_name	Имя тенанта
federation_id	ID старой федерации
ldap	Не изменять

5. При использовании ссылки на федерацию допускается установить значения в следующий формат:

http://<host/IP-адрес>:<port>/admin/master/console/#/<tenant_name>/
user-federation/<federation_id>

6. Для переноса маппингов в федерацию можно использовать ссылку, в которой заменить ID федерации и добавить mappers в конце строки. Пример:

– Старая федерация:
http://example.net:8091/admin/master/console/#/ad/user-federation/ldap/
d00daf68-b4b9-4cff-856d-b788b614bf57/mappers
– Новая федерация:
http://example.net:8091/admin/master/console/#/ad/user-federation/ldap/
1c4c28bd-4bd7-4456-82ab-a179cc17c1d4/mappers

7. Настроить маппинг согласно схеме LDAP каталога. Например, пользователь в AD-каталоге (рис. 15):

```
dn: CN=ad01 ad01,OU=ou1,OU=pgs2,DC=volyn,DC=ru
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: ad01 ad01
sn: ad01
givenName: ad01
distinguishedName: CN=ad01 ad01,OU=ou1,OU=pgs2,DC=volyn,DC=ru
instanceType: 4
whenCreated: 20241205145058.0Z
whenChanged: 20241205145147.0Z
displayName: ad01 ad01
uSNCreated: 3984840
uSNChanged: 3984846
name: ad01 ad01
objectGUID:: i6ry24ewW0iS9Pzl0yzmIw==
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 133782071707315123
lastLogoff: 0
lastLogon: 133782071854033855
pwdLastSet: 133778838585596312
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAQHBr3RFtIaXQltEu44IAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: ad01
sAMAccountType: 805306368
userPrincipalName: ad01@volyn.ru
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=volyn,DC=ru
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133778839075283833
```

Рисунок 15 — Пользователь в каталоге AD

Если имени пользователя соответствует поле `givenName`, то маппинг должен выглядеть в соответствии с рисунком 16.

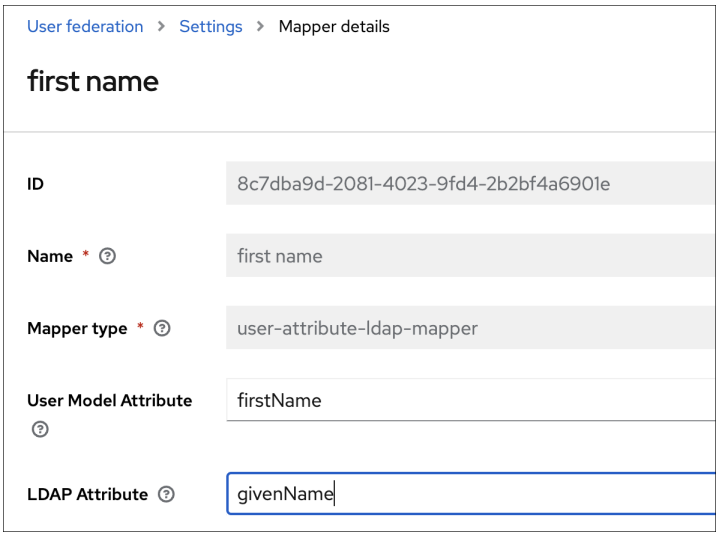

Рисунок 16 — Атрибуты пользователя в LDAP

9. После создания новой федерации необходимо подключиться к сервису Aristoteles на сервере PGS:

```
ssh centos@pgs-server-node-1.example.net

sudo su
docker ps | grep aris
docker exec -it tag bash
```

10. Запустить скрипт внутри приложения Aristoteles:

```
python3.11 ./dev_utils/update_fed_link_tenant.py --old_fed_link old_id \
--new_fed_link new_id
```

где

– `old_id` — ID старой федерации;

– `new_id` — ID новой созданной федерации.

11. Проверить выполнение авторизации пользователя и возможность работы с файлами пользователя в файловом менеджере.

12. После успешного завершения проверок удалить кастомный плагин pgsldapnew.

