

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

СИСТЕМА РЕДАКТИРОВАНИЯ И СОВМЕСТНОЙ РАБОТЫ

СИСТЕМА ХРАНЕНИЯ ДАННЫХ

3.3

**РУКОВОДСТВО ПО НАСТРОЙКЕ ИНТЕГРАЦИИ
С ВНЕШНИМИ КАТАЛОГАМИ**

Версия 1

На 25 листах

Дата публикации: 18.03.2025

**Москва
2025**

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

1 Общие сведения	5
1.1 Назначение	5
1.2 О компонентах	5
2 Синхронизация статуса пользователя	6
2.1 Описание сервиса	6
2.2 Порядок установки	6
3 Настройка интеграции с AD	7
3.1 Настройка интеграции с AD	7
3.2 Настройка синхронизации	9
4 Настройка интеграции с FreeIPA	10
4.1 Описание	10
4.2 Использование ldapsearch	10
4.3 Настройка с помощью Keycloak	10
4.4 Настройка с помощью консоли	12
4.5 Дополнительные настройки FreeIPA	13
4.5.1 Смена имени администратора	13
4.5.2 Отображение статуса пользователя	13
4.5.3 Настройка синхронизации	13
5 Настройка интеграции с OpenLDAP	14
5.1 Описание	14
5.2 Настройка с помощью Keycloak	14
5.3 Настройка синхронизации	19
6 Дополнительные параметры интеграции	21
6.1 Решение ошибки синхронизации	21
6.2 Перенос файлов удаленного пользователя другому пользователю	21
6.3 Переключение кастомного плагина на нативный	22

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 атрибутов пользователей
LDAP	Lightweight Directory Access Protocol, облегченный протокол доступа к каталогам, открытый стандартизированный протокол, применяемый для работы с различными 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 Документы Онлайн»;
- «МойОфис Профессиональный 2»;
- «МойОфис Профессиональный 3»;
- «МойОфис Схема»;
- Squadus PRO.

Список возможностей приложения приведен в документе «Функциональные возможности»

2 СИНХРОНИЗАЦИЯ СТАТУСА ПОЛЬЗОВАТЕЛЯ

2.1 Описание сервиса

User Listener — сервис для обработки событий, связанных с изменением указанных в домене атрибутов пользователя. Смена статуса пользователя зависит от изменения атрибутов пользователя, связанных с его состоянием (userAccountControl, pwdEndTime и др.). Полная/периодическая синхронизация пользователей проводится повторными запросами к каталогу и перезаписью существующих в БД записей (user_entity, user_attribute).

2.2 Порядок установки

Для установки сервиса user_listener следует предварительно настроить маппер в Keycloak. Для настройки сервиса используются переменные, указанные в таблице 2.

Таблица 2 — Переменные для установки user_listener

Наименование переменной	Значение по умолчанию	Тип переменной	Описание
ldap_required	True	Boolean	По умолчанию добавляет сервис user_listener в систему. Значение false используется для системы без каталога
mapper_set	False	Boolean	Следует установить true после настройки атрибута в Keycloak. Если маппер не настроен, число реплик при установке равно 0

Во время первичной установки сервиса user_listener переменных следует указать следующие значения:

```
ldap_required=True  
mapper_set=False
```

При повторной установке значения переменных должны принимать следующий вид:

```
ldap_required=True  
mapper_set=True
```

3 НАСТОЙКА ИНТЕГРАЦИИ С AD

3.1 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. 3).

Таблица 3 — 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 4.

Таблица 4 — 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;"
```

3.2 Настройка синхронизации

Для настройки синхронизации статусов пользователей Active Directory используется атрибут `userAccountControl`, который необходимо указать в поле LDAP Attribute. Окно интерфейса для ввода атрибута представлено на рисунке 1.

ldapStatus

ID	1bff3ece-f011-4b5b-a4c8-9eb54fe678ca
Name * ⓘ	ldapStatus
Mapper type * ⓘ	user-attribute-ldap-mapper
User Model Attribute ⓘ	ldapStatus
LDAP Attribute ⓘ	userAccountControl
Read Only ⓘ	☒ On
Always Read Value From LDAP ⓘ	☐ Off
Is Mandatory In LDAP ⓘ	☐ Off
Attribute default value ⓘ	
Force a Default Value ⓘ	☐ Off
Is Binary Attribute ⓘ	☐ Off

Рисунок 1 — Настройка синхронизации статусов пользователей в AD

Для проверки настройки необходимо с помощью интерфейса AD заблокировать пользователя и проверить его статус.

4 НАСТРОЙКА ИНТЕГРАЦИИ С FREEIPA

4.1 Описание

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

4.2 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)"
```

4.3 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 Pgsqlapnew providers** (рис. 2):

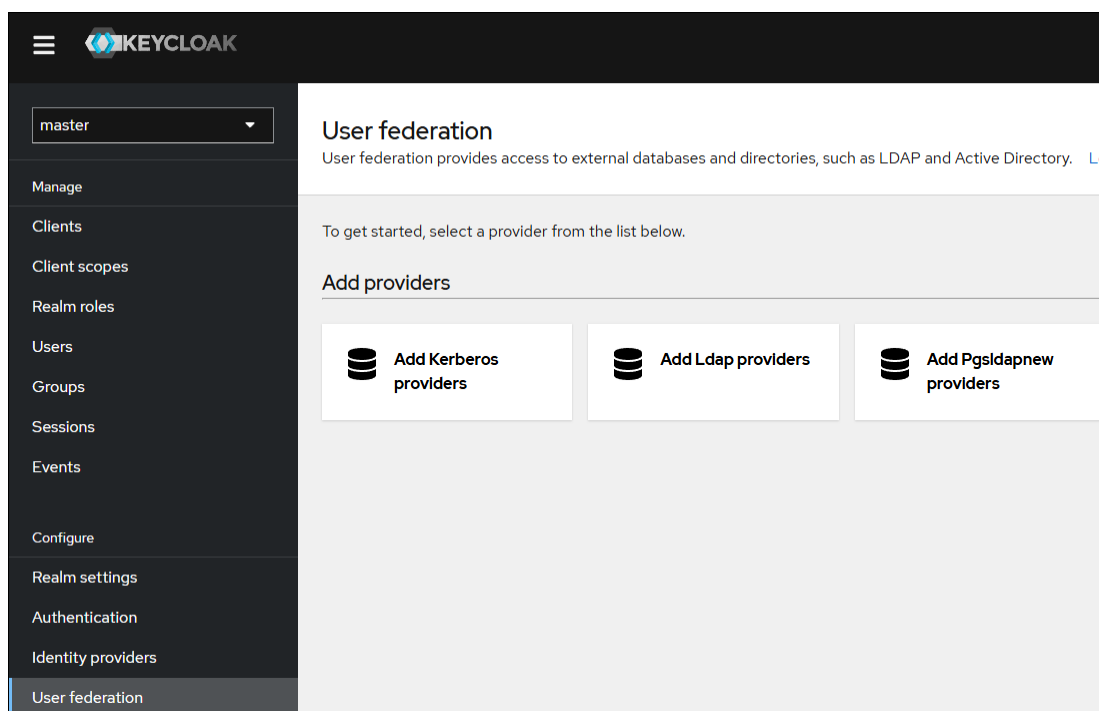
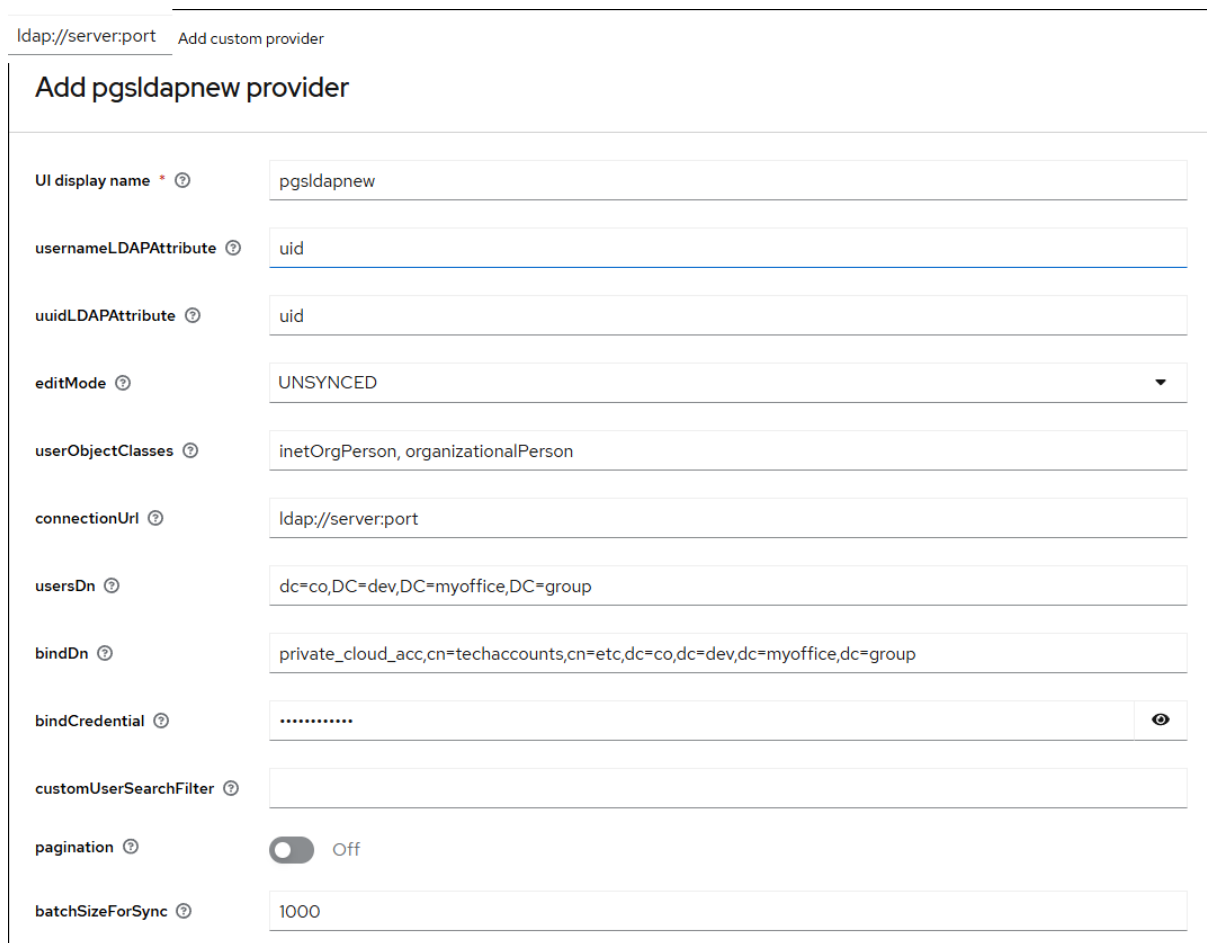


Рисунок 2 — Окно создания плагина

2. В окне **Add Pgsldapnew providers** ввести параметры подключения (рис. 3):



ldap://server:port Add custom provider

Add pgsldapnew provider

UI display name * ? pgsldapnew

usernameLDAPAttribute ? uid

uuidLDAPAttribute ? uid

editMode ? UNSYNCED

userObjectClasses ? inetOrgPerson, organizationalPerson

connectionUrl ? ldap://server:port

usersDn ? dc=co,DC=dev,DC=myoffice,DC=group

bindDn ? private_cloud_acc,cn=techaccounts,cn=etc,dc=co,dc=dev,dc=myoffice,dc=group

bindCredential ?

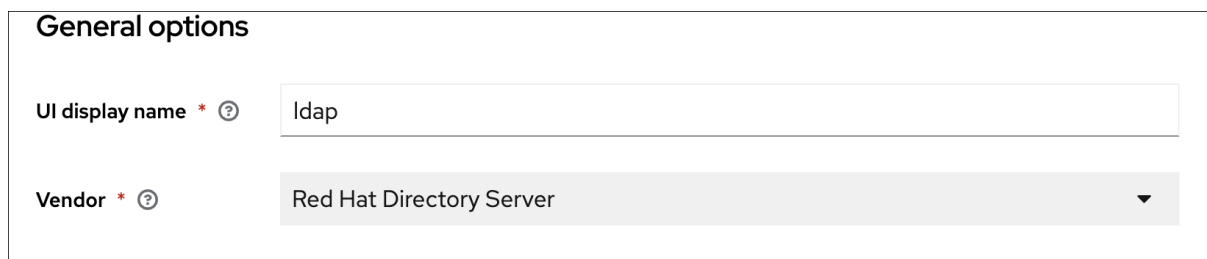
customUserSearchFilter ?

pagination ? ☐ Off

batchSizeForSync ? 1000

Рисунок 3 — Основные параметры настройки

3. В поле **Vendor** выбираем **Red Hat Directory Server** (рис. 4):



General options

UI display name * ? ldap

Vendor * ? Red Hat Directory Server

Рисунок 4 — Параметры настройки вендора

4. Маппинг `firstName` настраивается по атрибуту каталога `givenName` (рис. 5):

ID	509f5c66-94cc-49f5-b1fa-f08b4c57bf17
Name * ?	first name
Mapper type * ?	user-attribute-ldap-mapper
User Model Attribute ?	firstName
LDAP Attribute ?	givenName
Read Only ?	☒ On

Рисунок 5 — Настройка маппинга

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

4.4 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
```

4.5 Дополнительные настройки FreeIPA

4.5.1 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
```

4.5.2 Отображение статуса пользователя

Для корректного отображения статуса пользователя Keycloak необходимо использовать в каталоге атрибуты, указанные в таблице 5.

Таблица 5 — Параметры статуса пользователя

Параметр	Комментарий
<code>userAccountControl</code>	Определяет статус пользователя
<code>pwdLastSet</code>	Необходимо использовать ненулевое значение

4.5.3 Настройка синхронизации

Настройка синхронизации статусов пользователей FreeIPA идентична AD. FreeIPA использует атрибут `userAccountControl`.

5 НАСТРОЙКА ИНТЕГРАЦИИ С OPENLDAP

5.1 Описание

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

5.2 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 нативным плагином (Add ldap providers):

Порядок действий:

1. Для начала работы открыть вкладку **User federation** и нажать кнопку **Add Ldap providers** (рис. 6):

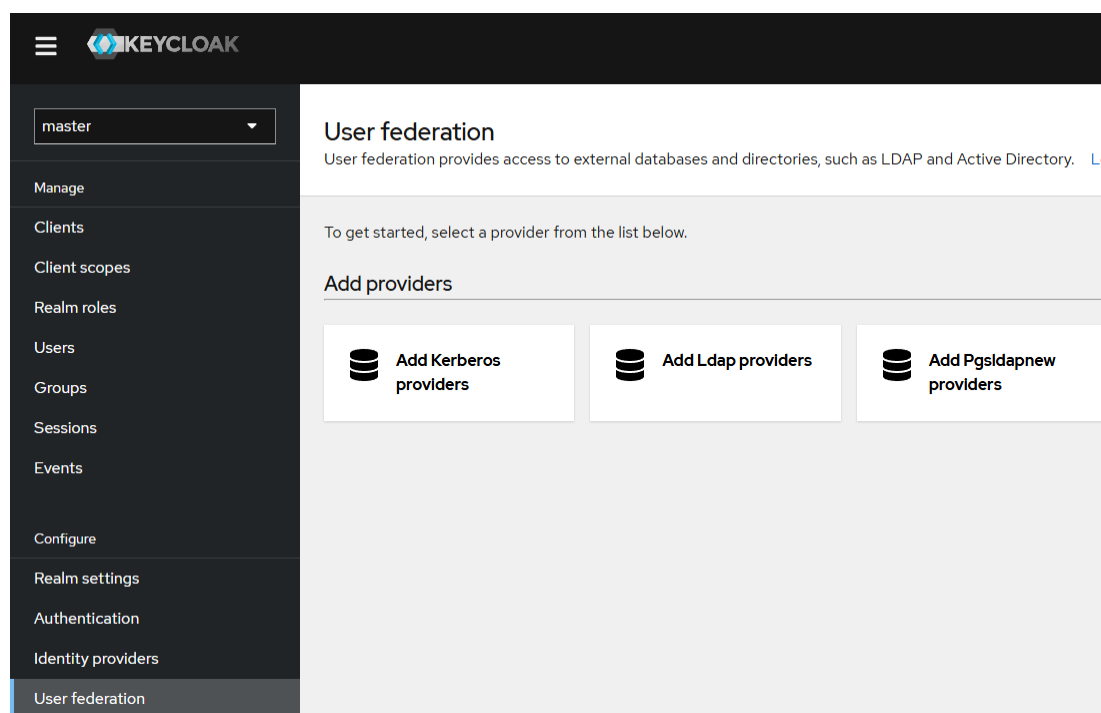


Рисунок 6 — Окно создания плагина

2. В поле **Vendor** следует выбрать пункт **Active directory** или **Other** (рис. 7).
3. Указать IP-адрес и порт для сервера LDAP в поле **Connection_URL** (рис. 7):

The screenshot shows the 'General options' section of a configuration interface. It includes a text field for 'UI display name' with the value 'ldap', a dropdown menu for 'Vendor' set to 'Active Directory', and a 'Connection and authentication settings' section. This section contains a 'Connection URL' field with 'ldap://server:port', a toggle for 'Enable StartTLS' set to 'Off', a dropdown for 'Use Truststore SPI' set to 'Only for ldaps', another toggle for 'Connection pooling' set to 'Off', and a 'Connection timeout' field. A 'Test connection' button is located at the bottom of the settings section.

Рисунок 7 — 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. 8). Проверить параметр **Username LDAP attribute**, отвечающий за имя пользователя в каталоге.

The screenshot shows the authentication and searching settings. The 'Bind type' dropdown is set to 'simple'. The 'Bind DN' field contains 'cn=jimbo,dc=example,dc=com'. The 'Bind credentials' field is masked with dots. A 'Test authentication' button is present. Below this is the 'LDAP searching and updating' section, which includes an 'Edit mode' dropdown set to 'UNSYNCD', a 'Users DN' field with 'ou=myoffice,dc=example,dc=com', a 'Username LDAP attribute' field with 'uid', an 'RDN LDAP attribute' field with 'cn', and a 'UUID LDAP attribute' field with 'entryUUID'.

Рисунок 8 — 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. 9):

User object classes *
inetOrgPerson, organizationalPerson

User LDAP filter

Search scope
Subtree

Read timeout

Pagination
Off

Synchronization settings

Import users
On

Sync Registrations
On

Batch size

Periodic full sync
Off

Periodic changed users sync
Off

Рисунок 9 — Параметры настройки подключения к LDAP

5. Маппинг пользовательских данных настраивается во вкладке **Mappers** (рис. 10):

User federation > Settings

LDAP

SettingsMappers

Search for mapper → Add mapper

Name	Type
creation date	user-attribute-ldap-mapper
email	user-attribute-ldap-mapper
firstName	user-attribute-ldap-mapper
full name	full-name-ldap-mapper
last name	user-attribute-ldap-mapper
modify date	user-attribute-ldap-mapper
MSAD account controls	msad-user-account-control-mapper
pwdEndTime	user-attribute-ldap-mapper
username	user-attribute-ldap-mapper

Рисунок 10 — 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. 11):

The screenshot shows the configuration for a user mapper named 'firstName'. The fields are as follows:

firstName	
ID	901e6719-8d4d-4166-bd12-b192d3d67a0a
Name *	firstName
Mapper type *	user-attribute-ldap-mapper
User Model Attribute	firstName
LDAP Attribute	givenName
Read Only	☐ Off
Always Read Value From LDAP	☐ Off
Is Mandatory In LDAP	☐ Off

Рисунок 11 — Окно параметров пользователя

7. Запуск синхронизации пользователей осуществляется с помощью пункта **Sync all users** в выпадающем меню **Action** (рис. 12):

The screenshot shows the 'LDAP' provider settings in Keycloak. The 'Settings' tab is active. The 'General options' section shows 'UI display name' as 'ldap' and 'Vendor' as 'Active Directory'. The 'Action' dropdown menu is open, showing options: 'Sync changed users', 'Sync all users', 'Unlink users', 'Remove imported', and 'Delete provider'. The 'Sync all users' option is highlighted.

Рисунок 12 — Запуск синхронизации пользователей

После выполнения синхронизации список пользователей появится во вкладке **Users** (рис. 13):

Users

Users are the users in the current realm. [Learn more](#)

User list

Q

Search user

→

Add user

1 - 10

☐	Username	Email	Last name	First name	Status
☐	admin	 admin@openldap.ru	admin	admin	—
☐	mike1	 mike1@openldap.ru	MRemedios1	Michael1	—
☐	mike100	 mike100@openldap.ru	MRemedios100	Michael100	—
☐	mike1000	 mike1000@openldap.ru	MRemedios1000	Michael1000	—
☐	mike1001	 mike1001@openldap.ru	MRemedios1001	Michael1001	—
☐	mike1002	 mike1002@openldap.ru	MRemedios1002	Michael1002	—
☐	mike1003	 mike1003@openldap.ru	MRemedios1003	Michael1003	—
☐	mike1004	 mike1004@openldap.ru	MRemedios1004	Michael1004	—
☐	mike1005	 mike1005@openldap.ru	MRemedios1005	Michael1005	—
☐	mike1006	 mike1006@openldap.ru	MRemedios1006	Michael1006	—

Рисунок 13 — Список пользователей после синхронизации

После успешного выполнения синхронизации интеграция с LDAP выполнена.

5.3 Настройка синхронизации

Для настройки синхронизации статусов пользователей OpenLDAP использует атрибут `pwdEndTime`, представленный на рисунке 14. Для корректной работы синхронизации необходимо включить модуль `ppolicy`, на стороне `ldap`-сервера, отвечающий за `pwdEndTime`.

pwdEndTime

ID	05eb3bd8-c69c-49de-bef4-4c1d1b2127b3
Name * ?	pwdEndTime
Mapper type * ?	user-attribute-ldap-mapper
User Model Attribute ?	pwdEndTime
LDAP Attribute ?	pwdEndTime
Read Only ?	☒ On
Always Read Value From LDAP ?	☐ Off
Is Mandatory In LDAP ?	☐ Off
Attribute default value ?	
Force a Default Value ?	☐ Off
Is Binary Attribute ?	☐ Off

Рисунок 14 — Настройка синхронизации статусов пользователей в OpenLDAP

Проверка работы синхронизации выполняется с помощью утилиты `ldapmodify` и `ldif`-файлов.

Параметры пользователя, используемые в примерах:

```
uid=mikel
users_dn="ou=it,dc=example,dc=com"
```

1. Файл `block_mikel.ldif`

```
dn: uid=mikel,ou=it,dc=example,dc=com
changetype: modify
add: pwdEndTime
pwdEndTime: 100001010000Z
```

Для блокировки следует установить атрибут `pwdEndTime` для `mikel`, `pwdEndTime` — дата в прошлом, означающая, что время действия пароля истекло:

```
ldapmodify -H ldap://my_ldap_url -x -D "cn=admin,dc=example,dc=com" \  
-f block_mikel.ldif -w admin_password
```

2. Файл `delete_pwdendtime_mikel.ldif`

```
dn: uid=mikel,ou=it,dc=example,dc=com  
changetype: modify  
delete: pwdEndTime
```

Удалить атрибут `pwdEndTime`:

```
ldapmodify -H ldap://my_ldap_url -x -D "cn=admin,dc=example,dc=com" \  
-f delete_pwdendtime_mikel.ldif -w admin_password
```

3. Файл `unblock_mikel.ldif`

```
dn: uid=mikel,ou=it,dc=example,dc=com  
changetype: modify  
add: pwdEndTime  
pwdEndTime: 21000101000000Z
```

Для разблокировки следует установить атрибут `pwdEndTime`, где значение `pwdEndTime` - дата в будущем, означающая, что пароль еще не истек.

```
ldapmodify -H ldap://my_ldap_url -x -D "cn=admin,dc=example,dc=com" \  
-f unblock_mikel.ldif -w admin_password
```

6 ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ ИНТЕГРАЦИИ

6.1 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-bel | 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

6.2 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.

6.3 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 сервера 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. 15), а в атрибутах будет новое поле `user_domain` (рис. 16).

User Name	
ID *	abc8acff-bbe2-43d4-80b5-edbd5e1810e2
Created at *	7/1/2024, 3:50:58 PM
Required user actions ⓘ	Select action
Username *	User Name

Рисунок 15 — Карточка пользователя

User Name	
Details Attributes Credentials Role mapping Groups Consents Identity provider links Sessions	
Key	Value
LDAP_ENTRY_DN	CN=user name, OU=ou1, OU=pgs2, DC=volyn,DC=ru
user_domain	@ad.ru
quota	10000000000

Рисунок 16 — Вкладка 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 6.

Таблица 6 — 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. 17):

```
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=lyn,DC=ru
instanceType: 4
whenCreated: 20241205145058.0Z
whenChanged: 20241205145147.0Z
displayName: ad01 ad01
uSNCreated: 3984840
uSNChanged: 3984846
name: ad01 ad01
objectGUID:: i6ry24ewW0iS9Pz10yzmIw==
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 133782071707315123
lastLogoff: 0
lastLogon: 133782071854033855
pwdLastSet: 133778838585596312
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAQAQHBr3RFtIaXQltEu44IAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: ad01
sAMAccountType: 805306368
userPrincipalName: ad01@lyn.ru
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=lyn,DC=ru
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133778839075283833
```

Рисунок 17 — Пользователь в каталоге AD

Если имени пользователя соответствует поле `givenName`, то маппинг должен выглядеть в соответствии с рисунком 18.

User federation > Settings > Mapper details

first name

ID	8c7dba9d-2081-4023-9fd4-2b2bf4a6901e
Name *	first name
Mapper type *	user-attribute-ldap-mapper
User Model Attribute	firstName
LDAP Attribute	givenName

Рисунок 18 — 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`.