

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ
БАЗАМИ ДАННЫХ «ЈАТОВА»

Руководство по настройке. Часть 8.
Синхронизация учетных записей служб каталогов и СУБД.
Компонент «ja_Sync_LDAP»

643.72410666.00067-07 98 01-08

Листов 120

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

АННОТАЦИЯ

Администратор СУБД «Jatoba» должен иметь навыки по работе с системами управления базами данных (СУБД) PostgreSQL или защищенной СУБД «Jatoba» (ООО «Газинформсервис»).



Примеры в данном документе приведены для СУБД «Jatoba» версии ядра 4.x и 5.x, для других версий все шаги выполняются аналогично, разница состоит в именах директорий.

Например, СУБД «Jatoba» версии 5.x по умолчанию устанавливается в директорию ОС Linux – «/usr/jatoba-5/bin».

Используемая версия компонента — 1.3



Важная информация

Для сертифицированной версии СУБД «Jatoba» поддерживается работа только на ОС, указанных в формуляре на поставку!

Степени важности примечаний, применяемые в документе:



Важная информация – указания, требующие особого внимания



Дополнительная информация – указания, позволяющие упростить работу с изделием

СОДЕРЖАНИЕ

1. Назначение компонента.....	6
1.1. Функциональные возможности	6
1.2. Условия применения.....	7
2. Использование	8
2.1. Общая схема работы	8
2.2. Алгоритм синхронизации	11
2.3. Описание служебных таблиц.....	12
3. Установка и настройка компонента	14
3.1. Установка компонента «ja_Sync_LDAP» в ОС GNU/Linux.....	15
3.2. Настройка конфигурационного файла postgresql.conf.....	16
3.2.1. Преобразование имен пользователей.....	17
3.3. Установка расширения ja_sync_ldap	18
4. Функции ja_Sync_LDAP	19
4.1. Функции профиля синхронизации.....	19
4.1.1. Добавление/изменение профиля синхронизации	19
4.1.2. Включение SSL-соединения для профиля синхронизации	20
4.1.3. Отключение SSL-соединения для профиля синхронизации	21
4.1.4. Просмотр профиля синхронизации.....	21
4.1.5. Удаление профиля синхронизации	21
4.2. Соответствие групп.....	22
4.2.1. Добавление/изменение соответствия групп	22
4.2.2. Просмотр соответствия групп.....	24
4.2.3. Удаление соответствия групп	24
4.3. Функции синхронизации.....	25
4.4. Функции работы с журналами событий (логами)	25
4.4.1. Просмотр событий безопасности	26
4.4.2. Удаление событий безопасности	27
4.4.3. Описание работы журнала событий	28
5. Примеры синхронизации.....	33
5.1. Выполнение синхронизации одного соответствия по атрибуту 'sAMAccountName'	33
5.1.1. Добавление профиля синхронизации	34
5.1.2. Просмотр профиля	35
5.1.3. Добавление соответствия групп.....	36
5.1.4. Синхронизация	39
5.1.5. Авторизация после синхронизации по атрибуту 'sAMAccountName'	40
5.2. Выполнение синхронизации одного соответствия по атрибуту 'cn'	43
5.2.1. Добавление профиля синхронизации	44

5.2.2. Просмотр профилей синхронизации.....	44
5.2.3. Добавление соответствия групп.....	45
5.2.4. Просмотр соответствия групп.....	46
5.2.5. Синхронизация	47
5.2.6. Авторизация после синхронизации по атрибуту 'cn'	48
5.2.7. Конфигурационный файл pg_hba при двух профилях синхронизации	49
5.3. Выполнение синхронизации одного соответствия по атрибуту 'name' из группы в Organizational Unit (OU).....	50
5.3.1. Добавление профиля синхронизации	51
5.3.2. Просмотр профилей синхронизации.....	52
5.3.3. Добавление соответствия групп.....	52
5.3.4. Просмотр соответствия групп.....	54
5.3.5. Синхронизация	54
5.3.6. Авторизация после синхронизации по атрибуту 'name'	55
5.4. Изменения профиля синхронизации.....	57
5.5. Изменение соответствия групп.....	58
5.6. Удаление профиля.....	59
5.7. Просмотр соответствия групп	59
5.8. Удаление соответствия групп.....	59
5.9. Просмотр событий безопасности.....	60
5.10. Удаление строки из журнала событий.....	60
5.11. Удаление выбранных строк из журнала событий	61
5.12. Удаление всех строк из журнала событий.....	62
5.13. Синхронизация с сервером ALD Pro	62
5.13.1. Настройка сервера СУБД	62
5.13.2. Настройка сервера ALD Pro	64
5.13.3. Создание нового профиля синхронизации	68
5.13.4. Установка параметров SSL для профиля.....	70
5.13.5. Включение SSL-соединения для профиля синхронизации	72
5.13.6. Отключение SSL-соединения для профиля синхронизации	73
5.13.7. Добавление соответствия групп.....	73
5.13.8. Выполнение синхронизации УЗ с сервером ALD Pro	73
5.14. Синхронизация с сервером FreeIPA	73
5.14.1. Настройка сервера СУБД.....	74
5.14.2. Настройка сервера FreeIPA	75
5.14.3. Создание профиля синхронизации	79
5.14.4. Установка параметров SSL для профиля.....	81
5.14.5. Включение SSL-соединения для профиля синхронизации	84
5.14.6. Отключение SSL-соединения для профиля синхронизации	84

5.14.7. Добавление соответствия групп.....	85
5.14.8. Выполнение синхронизации УЗ с сервером FreeIPA	85
5.15. Синхронизация с сервером Samba	86
5.15.1. Настройка сервера СУБД	86
5.15.2. Создание группы и пользователей группы в активном каталоге Samba	87
5.15.3. Создание профиля синхронизации	90
5.15.4. Добавление соответствия групп по атрибуту 'sAMAccountName'	92
5.15.5. Установка параметров SSL для профиля.....	94
5.15.6. Включение SSL-соединения для профиля синхронизации	97
5.15.7. Выполнение синхронизации УЗ с сервером Samba по атрибуту 'sAMAccountName'	98
5.15.8. Авторизация после синхронизации по атрибуту 'sAMAccountName'	99
5.15.9. Выполнение синхронизации УЗ с сервером Samba по атрибуту 'cn'	99
5.15.10. Отключение SSL-соединения для профиля синхронизации	99
6. Обновление и удаление компонента	100
7. Действия после сбоев и ошибок эксплуатации.....	101
Приложение 1	102
Приложение 2	108
Приложение 3	110
Приложение 4	113
Термины и определения	117
Перечень сокращений.....	119

1. НАЗНАЧЕНИЕ КОМПОНЕНТА

СУБД «Jatoba» (далее – СУБД) поддерживает множество методов аутентификации пользователей, различающихся сложностью, уровнем безопасности и другими факторами. Аутентификация пользователей может выполняться внешними по отношению к СУБД средствами (например, служба доменов Microsoft® Windows®, служба каталогов на основе LDAP и ряд других). При этом идентификация пользователей всегда осуществляется только средствами СУБД – в системном каталоге СУБД поддерживается соответствующая таблица учетных записей пользователей и их внутренних идентификаторов. В результате при настройке внешней системы аутентификации администратору требуется поддерживать соответствие идентификаторов пользователей, используемых в этой системе, и идентификаторов пользователей СУБД. Такая поддержка заключается в том, что администратор должен содержать два списка пользователей: один – на стороне используемой внешней системы аутентификации (например, пользователи службы доменов Microsoft Windows), другой – на стороне СУБД. Администратору также может потребоваться явная настройка соответствия пользователей внешней системы аутентификации и пользователей СУБД.

Использование компонента ja_Sync_LDAP (далее – ja_Sync_LDAP) позволяет упростить поддержание списка пользователей в СУБД при настройке следующих внешних методов аутентификации:

- аутентификация через службу каталогов по протоколу LDAP (LDAPS) (в том числе через службу доменов Active Directory и ее открытых аналогов, таких как ALD PRO, FreeIPA, Samba);
- аутентификация через GSSAPI/Kerberos;
- аутентификация через SSPI.

1.1. Функциональные возможности

Компонент обеспечивает администратора инструментом на уровне СУБД, выполняющим синхронизацию списка пользователей между внешней службой аутентификации (службы каталогов) и СУБД.

1.2. Условия применения

Компонент ja_Sync_LDAP может использоваться совместно с:

- СУБД «Jatoba», а также открытой СУБД PostgreSQL;
- компонентом пользовательского веб-интерфейса для администраторов «Jatoba data safe».

Компонент целесообразно использовать при внедрении СУБД в существующую IT-инфраструктуру компании с централизованной системой управления учетными записями пользователей, централизованными службами идентификации и аутентификации пользователей.

Компонент не поддерживает синхронизацию имен пользователей на кириллице (русском языке).

2. ИСПОЛЬЗОВАНИЕ

2.1. Общая схема работы

Компонент `ja_Sync_LDAP` является расширением СУБД, предоставляющим пользователю набор SQL-функций для настройки и проведения синхронизации пользователей между службой каталогов и СУБД.

Для реализации своих функций компонент использует следующие понятия:

- **профиль синхронизации** – набор настроек, отвечающих за подключение к службе каталогов;
- **правило сопоставления** – набор настроек, определяющих список пользователей, подлежащих синхронизации.

Профиль синхронизации включает название профиля, адрес и порт подключения к службе каталогов, учетную запись служебного пользователя службы каталогов, имеющего доступ на чтение соответствующих разделов каталога со списком пользователей и тип службы каталогов (ActiveDirectory/FreeIPA/AldPro/Samba).

Правило сопоставления включает ссылку на профиль, в рамках которого действует данное правило, описание группы пользователей на стороне службы каталогов, для которых определена необходимость доступа в СУБД, описание групповой роли в СУБД, к которой будут привязаны пользователи из службы каталогов в результате синхронизации и атрибут синхронизации (`cn/sAMAccountName/name` и др.)

Схематично работа компонента показана на рисунке 2.1 и включает следующий порядок действий со стороны системного администратора:

1. Администратором в службе каталогов должны быть определены одна или несколько групп пользователей, которым делегируется доступ в СУБД. Необходимость создания такой группы – структурное выделение пользователей, связанных фактом наличия доступа в конкретную СУБД, для последующего централизованного управления.

2. Администратором в СУБД создается структурная групповая роль, членам которой будет доступен вход в СУБД. Необходимость создания такой группы – структурное выделение пользователей для централизованной настройки их аутентификации и авторизации.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

3. Администратором в СУБД устанавливается расширение `ja_Sync_LDAP` и с помощью предоставляемых расширением SQL-функций производится настройка профиля (или профилей, если предполагается доступ к СУБД пользователей, контролируемых разными службами каталогов) и правил сопоставления групп между службой каталогов и СУБД.

4. Администратором СУБД выполняется вызов соответствующей SQL-функции синхронизации профиля (или профилей), которая согласно заданным правилам профиля на стороне СУБД сформирует список пользователей, соответствующий списку пользователей в службе каталогов.

5. Администратор может добавлять и удалять пользователей в соответствующую группу в службе каталогов и повторять операцию синхронизации для распространения сделанных изменений на стороне СУБД. Возможна настройка выполнения этой операции по расписанию для распространения изменений на регулярной основе.

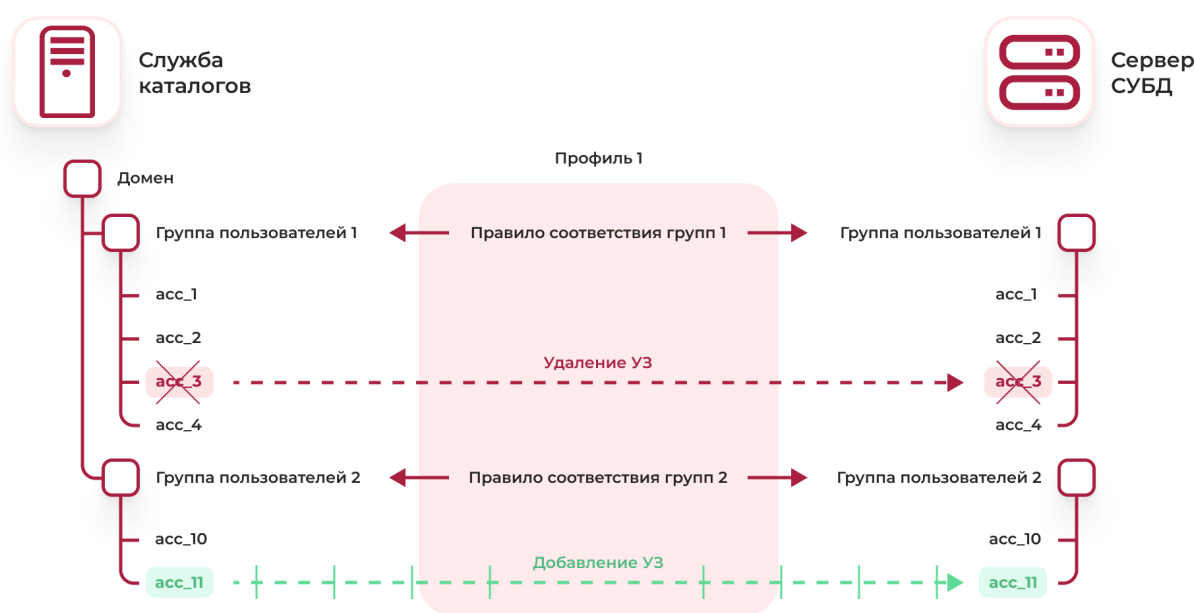


Рисунок 2.1 – Общая схема работы компонента

На рисунке 2.1 показано, что в службе каталогов в группах пользователей 1 и 2 имеются учетные записи `асс_1`, `асс_2`, `асс_3`, `асс_4` и `асс_10`, `асс_11` соответственно. В результате действий администратора по изменению состава групп 1 и 2 в службе каталогов был удален пользователь `асс_3` и добавлен пользователь `асс_11`. Тогда для синхронизации списков пользователей на стороне СУБД должны быть выполнены следующие команды:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

```
DROP ROLE acc_3;  
CREATE USER acc_11;
```

Компонент ja_Sync_LDAP обладает функциональной возможностью синхронизации вложенных групп. При наличии таких вложенных групп, компонент:

- проигнорирует их, т.е. не создаст никаких сущностей в СУБД;
- учетные записи, входящие в нее, синхронизируются в СУБД в одну групповую роль, вместе с учетными записями, входящими в вышестоящую группу.

Схема работы компонента с вложенными группами пользователей в службе каталогов представлена на рисунке 2.2.

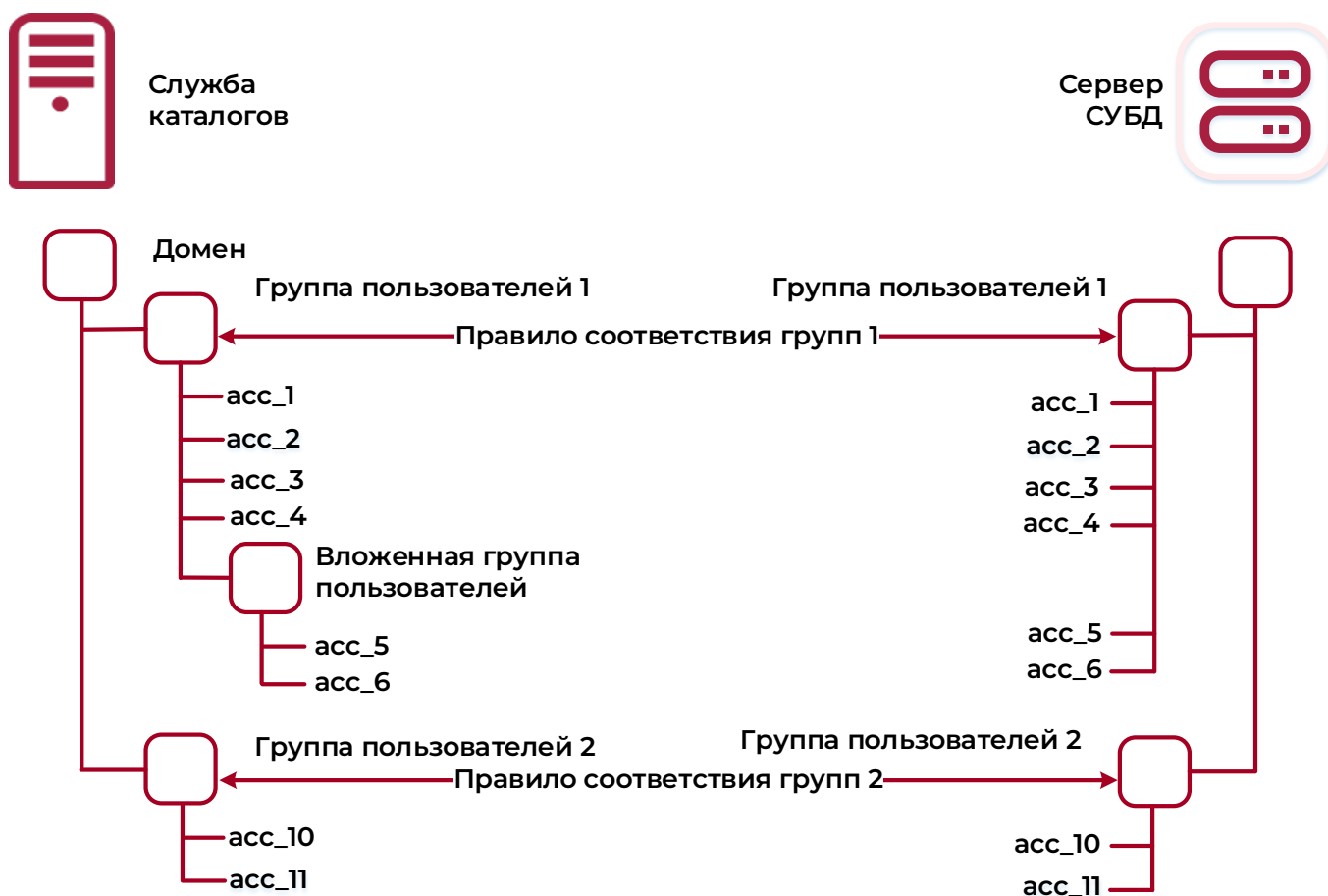


Рисунок 2.2 – Синхронизация вложенных групп

2.2. Алгоритм синхронизации

Изменения в составе группы в службе каталогов распространяются в СУБД по следующему алгоритму (справедливо для каждого правила сопоставления в рамках профиля):

- согласно настройкам профиля, выполняется запрос в службу каталогов для получения списка пользователей, подлежащих синхронизации. Список возвращается в отсортированном по имени пользователя виде. Поиск в каталоге ограничивается соответствующей структурной группой, заданной в правиле сопоставления;
- выполняется запрос в СУБД на получение списка пользователей, включенных в соответствующую групповую роль, заданную в правиле сопоставления. Этот список также возвращается в отсортированном виде;
- происходит сравнение двух отсортированных списков. На основании сравнения определяется, какие новые пользователи появились на стороне службы каталогов и какие пользователи были удалены. В соответствии с этими результатами сравнения формируется список изменений, которые надо выполнить на стороне СУБД для синхронизации списков;



Никаких изменений с пользователями и группами в службе каталогов не производится, все изменения всегда выполняются только на стороне СУБД.

- на основании списка изменений формируется SQL-скрипт из команд вида CREATE USER и/или DROP ROLE для добавления или удаления соответствующих ролей;
- данный список выполняется в рамках отдельного транзакционного блока. В результате все изменения либо принимаются полностью, и синхронизация правила признается завершенной, либо откатываются полностью, и синхронизация признается ошибочной;
- выходными данными алгоритма являются статус выполненной операции синхронизации и список сообщений о деталях выполнения соответствующих SQL-команд.

Описанный алгоритм в настоящее время обладает следующими ограничениями:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

1. Группы в правилах сопоставления профилей, относящиеся к одной службе каталогов, не должны содержать одинаковых пользователей. В противном случае будет ошибка синхронизации: невозможно создать двух пользователей с одинаковым именем.

2. Пользователи на стороне СУБД, созданные в результате синхронизации с использованием компонента ja_Sync_LDAP могут стать владельцами каких-либо объектов данных. При удалении такого пользователя из службы каталогов и повторной синхронизации –пользователь из СУБД удален не будет, т.к. в процессе синхронизации он будет исключен из групповой роли.



Операция DROP ROLE в компоненте ja_Sync_LDAP не применяется с флагом CASCADE, чтобы не допускать случайного удаления данных, связанных с пользователями, удаляемыми в результате синхронизации.

2.3. Описание служебных таблиц

Для хранения настроек профилей и правил сопоставления компонент ja_Sync_LDAP создает следующие объекты базы данных.

1) Схема для логического отделения объектов компонента от других данных пользователей. Имя схемы по умолчанию: ja_sync_ldap (все объекты далее будут созданы в этой схеме).

2) Таблица «profile» (профили синхронизации).

Поле	Тип данных	Описание
id	serial	идентификатор профиля (not null)
profile_name	text	имя профиля
host_ip	text	IP-адрес
port	text	порт (по умолчанию 389)
login	text	учетная запись администратора службы каталогов
pswd	text	пароль от учетной записи администратора службы каталогов
domain_type	text	тип службы каталогов
ssl	boolean	использование SSL (по умолчанию отключено)
ca_cert	text	путь до CA сертификата

3) Таблица «map» (правила сопоставления).

Поле	Тип данных	Описание
map_id	serial	идентификатор правила (not null)
profile_id	Int	идентификатор профиля (not null)
db_role_name	text	роль БД
domain_group_name	text	Группа в службе каталогов
attribute	text	атрибут синхронизации (атрибут записи в службе каталогов, который содержит имя пользователя)
objectclass	text	тип объекта синхронизации (по умолчанию для AD/Samba: user, для FreeIPA/ALD Pro: person)
basedn	text	база поиска (по умолчанию берется из поля domain_group_name)

4) Таблица «sync_log» (журнал сообщений).

Поле	Тип данных	Описание
id	serial	идентификатор строки (not null)
datetime	timestamp with time zone	дата регистрации события (not null)
profile_name	text	имя профиля
db_role_name	text	роль БД
domain_group_name	text	группа в службе каталогов
result	int	результат синхронизации профиля в числовом виде
message	text	пояснение результата синхронизации

5) Необходимый набор функций и пример их использования описан в разделе 4 и п. 4.4.3 данного руководства.

3. УСТАНОВКА И НАСТРОЙКА КОМПОНЕНТА

Установка модуля должна производиться от имени пользователя, обладающего административными привилегиями в системе. Данный модуль штатным образом может быть установлен только с СУБД «Jatoba» (см. документ «Защищенная система управления базами данных «Jatoba». Руководство по установке).

В результате установки служебные файлы, указанные в таблице 3.1, должны располагаться по соответствующим путям.

Таблица 3.1 – Расположение служебных файлов

Файл	Расположение
Семейство GNU/Linux	
ja_sync_ldap.so	корневая директория jatoba/lib
ja_sync_ldap.control	корневая директория jatoba/share/extension/
ja_sync_ldap--1.0.sql	корневая директория jatoba/share/extension/
ja_sync_ldap--1.0--1.1.sql	корневая директория jatoba/share/extension/
ja_sync_ldap--1.1--1.2.sql	корневая директория jatoba/share/extension/
ja_sync_ldap--1.2--1.3.sql	корневая директория jatoba/share/extension/
ja_sync_ldap--1.3.sql	корневая директория jatoba/hare/extension/
ja_sync_ldap--1.3--1.3.1.sql	корневая директория jatoba/share/extension/
ja_sync_ldap—1.3.*.sql	корневая директория jatoba/share/extension/

3.1. Установка компонента «ja_Sync_LDAP» в ОС GNU/Linux

Компонент устанавливается в составе СУБД «Jatoba». Его возможно установить при первичной установке СУБД, либо доустановить.

Установку компонента возможно провести двумя способами:

- 1) Установка из локального репозитория (CDROM) – производится из файлов, записанных на компакт-диск или скопированных с него.
- 2) Установка непосредственно из deb/rpm-файлов – производится опционально, по усмотрению пользователя.

Компонент выполнен в виде отдельного deb или rpm-пакета. Установка компонента осуществляется средствами пакетного менеджера ОС. Для разных типов пакетных менеджеров команда установки немного отличается. Ниже приведены основные типы:

– для систем на основе пакетного менеджера APT (к таким системам относятся все ОС семейства Debian, использующие deb-пакеты) команда установки следующая:

```
apt-get install jatoba<ver>-ja-sync-ldap
```

– для систем на основе пакетных менеджеров YUM/DNF (к таким системам относятся все ОС семейства RedHat и вышедшие из нее, использующие rpm-пакеты) команда установки следующая:

```
yum install jatoba<ver>-ja_sync_ldap
```

Отдельного уточнения требуют операционные системы ALT Linux и openSUSE.

– ALT Linux использует пакетный менеджер APT, но распространяется в виде rpm-пакетов и для нее команда установки выглядит аналогично Debian:

```
apt-get install jatoba<ver>-ja_sync_ldap
```

Установка компонента в составе других версий СУБД «Jatoba» осуществляется аналогично. Отличие будет только в номере версии СУБД, в составе которой он распространяется. Например, jatoba5-ja-sync-ldap и т.п.

– Удаление модуля также осуществляется средствами пакетного менеджера ОС. Вместо команды `install` нужно использовать соответствующую данному пакетному менеджеру команду удаления (`remove`, `purge`, `erase` и т.п.).

Для получения детальной информации по пакетному менеджеру рекомендуется обратиться к документации по ОС.

3.2. Настройка конфигурационного файла `postgresql.conf`

В конфигурационном файле «`postgresql.conf`» внести параметры:

- 1) максимальное время подключения к серверу AD:

```
ja_sync_ldap.max_time_connect = <1-60>
```

Значение по умолчанию - 10.

- 2) максимальное количество соответствий групп в одном профиле:

```
ja_sync_ldap.max_maps = <1-100>
```

Значение по умолчанию - 10.



Рисунок 3.1 – Конфигурационный файл `postgresql.conf`

3) Значение `ja_sync_ldap.max_page_size` определяет число значений, которые возвращаются для атрибута объекта вне зависимости от того, сколько атрибутов имеет объект или сколько объектов содержались в результатах поиска

```
ja_sync_ldap.max_page_size = 1000
```

Значение по умолчанию - 500.

Параметр является обязательным.

3.2.1. Преобразование имен пользователей

Механизм преобразования имен используется в компоненте ja_Sync_LDAP для преобразования имен пользователей «на лету», синхронизируемых из LDAP-каталога в СУБД.

Механизм преобразования имен чаще всего требуется тогда, когда аутентификация в СУБД происходит с использованием LDAP-каталога опосредованно, через другую службу, а не напрямую через СУБД.

Рассмотрим пример настроек аутентификации пользователей в СУБД. В операционной системе сервера СУБД настроена на системную LDAP-аутентификацию через службу SSSD или другие. Настройка такой аутентификации обычно включает определение формата, в котором будет представлено имя пользователя в операционной системе, например, только маленькие буквы, только большие, имя пользователя маленькими, а домен большими и прочее. Зачастую это представление не совпадает с тем представлением, которое хранится в LDAP каталоге. Тогда, если для входа локально в СУБД будет использоваться метод «реег», т.е. от имени пользователя операционной системы, а имена пользователей синхронизируются через ja_Sync_LDAP, то в результате синхронизации пользователи будут созданы с ошибочными именами (не совпадают синхронизированные имена с теми, которые использует операционная система). Таким образом, нетипичные способы аутентификации, которые потенциально может использовать администратор СУБД, могут приводить к невозможности использования ja_Sync_LDAP и в результате к ошибкам аутентификации.

Для использования механизма преобразования имен в конфигурационном файле «postgresql.conf» внести параметры:

```
ja_sync_ldap.transform_method = 'lower'
```



В конфигурационном файле «postgresql.conf» значение параметра «ja_sync_ldap.transform_method» может указываться без кавычек

По умолчанию параметр имеет значение «none».

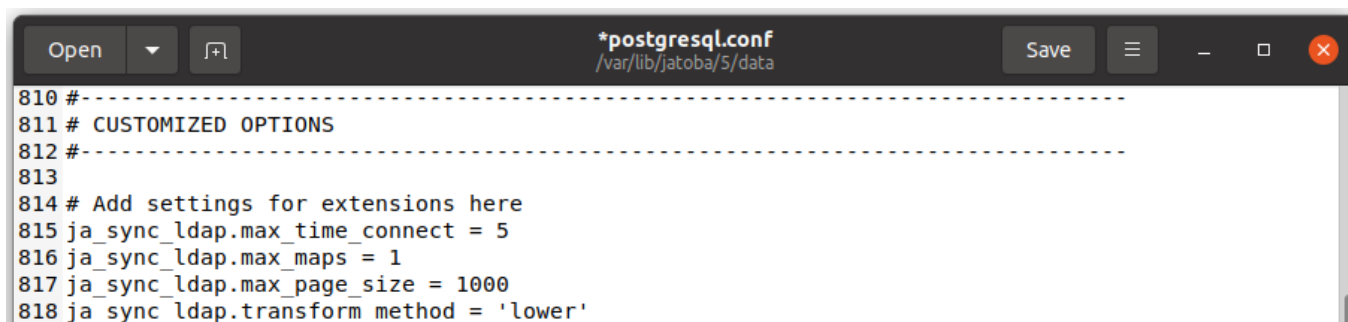


Рисунок 3.2 – Конфигурационный файл postgresql.conf с параметром ja_sync_ldap.transform_method

Примеры использования приведены в таблице 3.2.

Таблица 3.2 – Примеры преобразования имен

Значение параметра	Наименование УЗ в LDAP	Наименование УЗ в СУБД	Комментарий
none (по умолчанию)	j.USER01@cntr.gazPROM.Loc	j.USER01@cntr.gazPROM.Loc	никаких преобразований не производится. УЗ в LDAP и СУБД идентичны.
lower	j.USER01@cntr.gazPROM.Loc	j.user01@cntr.gazprom.loc	все символы переводятся в нижний регистр
	j.USER 01@cntr.gazPROM.Loc	j.user01@cntr.gazprom.loc	все символы переводятся в нижний регистр и пробелы в имени убраны

Для применения изменений параметров необходимо перезагрузить СУБД.

3.3. Установка расширения ja_sync_ldap

Расширение ja_Sync_LDAP устанавливается SQL-командой:

```
CREATE EXTENSION ja_sync_ldap;
```

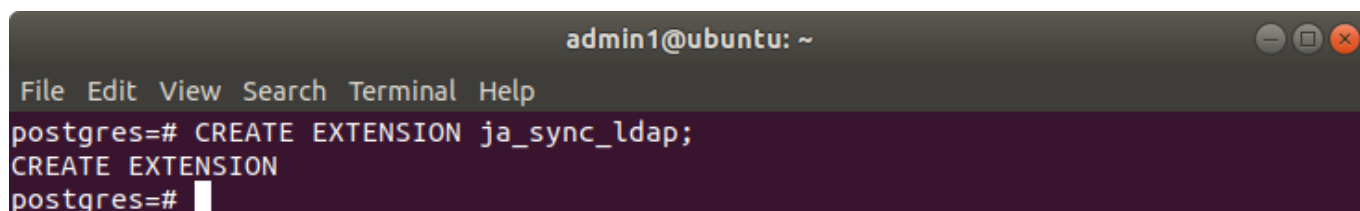


Рисунок 3.3 – Установка расширения

4. ФУНКЦИИ JA_SYNC_LDAP

Все последующие функции выполняются от пользователя, обладающего правами SUPERUSER или CREATEROLE.

4.1. Функции профиля синхронизации

Далее в подразделах описаны функции, отвечающие за управление профилями.

4.1.1. Добавление/изменение профиля синхронизации

Для создания профиля используется команда:

```
select ja_sync_ldap.set_sync_profile(in_profile_id int,  
in_profile_name text, in_host_ip text, in_port text, in_login  
text, in_pswd text, in_domain_type text);
```

В таблице 4.1 приведены параметры, используемые для создания профиля.

Таблица 4.1 – Параметры и обозначения для создания профиля

Параметр	Тип данных	Обозначение
in_profile_id	int	идентификатор профиля
in_profile_name	text	имя профиля
in_host_ip	text	IP-адрес
in_port	text	порт (по умолчанию 389)
in_login	text	учетная запись администратора службы каталогов
in_pswd	text	пароль от учетной записи администратора службы каталогов
in_domain_type	text	тип службы каталогов (activedirectory/freeipa/aldpro/samba)

Пароли профиля синхронизации будут храниться в кодировке BASE64 в поле pswd таблицы profile.

При написании запроса select ja_sync_ldap.set_sync_profile первым параметром указать null или какое-то значение, обозначающее идентификатор профиля, затем остальные параметры.

Значение null указывается при создании нового профиля, т.е. в таблице профилей появится новая строчка, в которой автоматически проставляется уникальное значение идентификатора.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Числовое значение идентификатора обозначает редактирование существующего профиля. При изменении каких-либо параметров в профиле нужно указать существующий числовой идентификатор и указать новые значения полей в изменяемом профиле.

Количество создаваемых профилей не ограничено.

В параметре «наименование профиля (in_profile_name)» нельзя использовать одноименные профили, т.к. этот параметр уникален.

При работе с функцией могут появляться следующие сообщения и результаты работы функции. Перечень сообщений приведен в таблице 4.2.

Таблица 4.2 – Перечень сообщений при добавлении/изменении профиля

Сообщения	Описание
Добавление профиля	
id	выполнено успешно. Отображается ID созданного профиля синхронизации.
-1	ошибка
Изменение профиля	
id	выполнено успешно. Отображается ID измененного профиля синхронизации.
0	профиля не существует
-1	ошибка

Для изменения существующего профиля требуется указать значение параметра идентификатора профиля (id). Просмотр существующих профилей, описан в п. 4.1.2.



Имя профиля (profile_name) можно изменять, но нельзя использовать одноименные наименования профилей.

4.1.2. Включение SSL-соединения для профиля синхронизации

Включение SSL-соединения для профиля синхронизации выполняется SQL-командой, имеющей синтаксис:

```
select ja_sync_ldap.set_ssl_profile(<Profile_ID>, true);
```

При просмотре профилей синхронизации, функция SSL-соединения станет включенной. В поле «SSL» установится значение «t», т.е. «true».

4.1.3. Отключение SSL-соединения для профиля синхронизации

Отключить SSL-соединение для профиля синхронизации возможно SQL-командой:

```
select ja_sync_ldap.set_ssl_profile(<Profile_ID>, false);
```

4.1.4. Просмотр профиля синхронизации

Просмотреть существующие профили можно следующей командой:

```
select ja_sync_ldap.get_sync_profiles();
```

В таблице 4.3 указаны выходные параметры команды просмотра профилей.

Таблица 4.3 – Выходные параметры просмотра профилей

Параметр	Тип данных	Обозначение
id	int	идентификатор профиля
profile_name	text	имя профиля
host_ip	text	IP-адрес
port	text	порт
login	text	учетная запись администратора службы каталогов
pswd	text	пароль от учетной записи администратора службы каталогов
domain_type	text	тип службы каталогов
ssl	boolean	использование SSL
ca_cert	text	путь до СА сертификата

4.1.5. Удаление профиля синхронизации

Удаление существующего профиля синхронизации осуществляется командой:

```
select ja_sync_ldap.drop_sync_profile(in_profile_id int);
```

В таблице 4.4 приведены параметры, используемые для удаления профиля.

Таблица 4.4 – Параметры и обозначения для удаления профиля

Параметр	Тип данных	Обозначение
in_profile_id	int	идентификатор профиля

СУБД удалит существующий профиль синхронизации со всеми зависимыми профилями соответствия групп.

При работе с функцией могут появляться следующие сообщения и результаты работы функции. Перечень сообщений приведен в таблице 4.5.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Таблица 4.5 – Перечень сообщений при удалении профиля

Сообщения	Описание
id	выполнено успешно. Отображается ID удаленного профиля синхронизации.
0	профиля не существует
-1	ошибка

4.2. Соответствие групп

Далее в подразделах описаны функции, отвечающие за соответствие групп.

4.2.1. Добавление/изменение соответствия групп

Соответствие групп создается для связки группы пользователей в службе каталогов, регистрации их в СУБД и присвоения им атрибутов ролей и (или) включение их в групповую роль, от которой они будут наследовать атрибуты и привилегии



Функциональные возможности компонента позволяют создавать и поддерживать множественные профили соответствия групп относительно профиля синхронизации

Для создания соответствия групп используется команда:

```
select ja_sync_ldap.set_sync_profile_map(in_map_id int,
in_profile_id int, in_role_bd text, in_domain_group text,
in_attribute text);
```

Для выполнения команды потребуются параметры, приведенные в таблице 4.6.

Таблица 4.6 – Входные значения для создания соответствия групп

Параметр	Тип данных	Обозначение
in_map_id	int	идентификатор соответствия групп
in_profile_id	int	идентификатор профиля
in_role_bd	text	роль БД
in_domain_group	text	группа в службе каталогов
in_attribute	text	атрибут синхронизации (атрибут записи в службе каталогов, который содержит имя пользователя)



Для корректного формирования строки «in_domain_group», рекомендуется найти написание «DistinguishedName» через программу PowerShell.

Для этого необходимо открыть командную строку PowerShell и написать команду:

```
Get-ADGroup -Identity db_admins
```

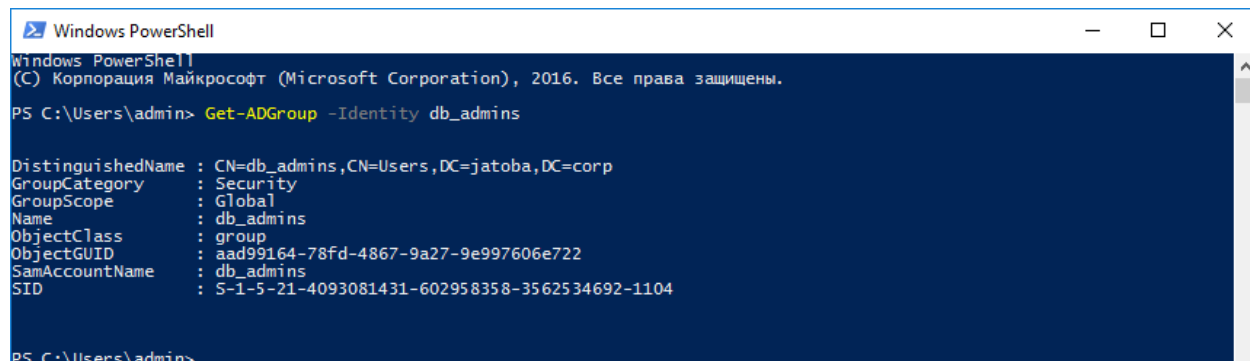


Рисунок 4.1 – Строка «in_domain_group»

Синтаксис команды следующий:

- Get-ADGroup – вывод информации о группе;
- Identity – оператор «идентичность»;
- [имя группы].

Для изменения существующего соответствия групп требуется указать значения параметров идентификаторов соответствия (map_id) и профиля (profile_id). Просмотр существующих профилей, описан в п. 4.2.2.



Роль БД (role_bd) и группу службы каталогов (in_domain_group) можно изменять, но нельзя использовать одноименные наименования.

При работе с функцией могут появляться следующие сообщения и результаты работы функции. Перечень сообщений приведен в таблице 4.7.

Таблица 4.7 – Перечень сообщений при добавлении/изменении соответствия групп

Сообщения	Описание
Добавление соответствия групп	
-1	ошибка
map_id	выполнено успешно. Отображается ID созданного мапинга.
Изменение соответствия групп	
map_id	выполнено успешно. Отображается ID измененного мапинга.
0	соответствия групп не найдено

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Сообщения	Описание
-1	ошибка

4.2.2. Просмотр соответствия групп

Просмотреть существующие соответствия групп к профилю синхронизации можно следующей командой:

```
select ja_sync_ldap.get_sync_profile_maps(in_profile_id int);
```

В таблице 4.8 указаны входные параметры команды для просмотра соответствия групп.

Таблица 4.8 – Параметры и обозначения для просмотра соответствия групп

Параметр	Тип данных	Обозначение
in_profile_id	int	идентификатор профиля

В таблице 4.9 указаны выходные параметры команды.

Таблица 4.9 – Выходные параметры соответствия групп

Параметр	Тип данных	Обозначение
map_id	int	идентификатор соответствия групп
profile_name	text	имя профиля
role_db	text	роль БД
domain_group_name	text	группа в службе каталогов
attribute	text	атрибут синхронизации (атрибут записи в службе каталогов, который содержит имя пользователя)
objectclass	text	тип объекта синхронизации (по умолчанию для AD/Samba: user, для FreeIPA/ALD Pro: person)
basedn	text	база поиска (по умолчанию берется из поля domain_group_name))

4.2.3. Удаление соответствия групп

Удаление соответствия групп происходит командой:

```
select ja_sync_ldap.drop_sync_profile_map(in_map_id int);
```

В таблице 4.10 приведены параметры, используемые для удаления соответствия групп.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Таблица 4.10 – Параметры и обозначения для удаления соответствия групп

Параметр	Тип данных	Обозначение
in_map_id	int	идентификатор соответствия групп

При работе с функцией могут появляться следующие сообщения и результаты работы функции. Перечень сообщений приведен в таблице 4.11.

Таблица 4.11 – Перечень сообщений при удалении соответствия групп

Сообщения	Описание
map_id	выполнен успешно. Отображается ID удаленного соответствия групп
0	соответствие групп не найдено
-1	ошибка

4.3. Функции синхронизации

Синхронизация выполняется функцией ja_sync_ldap.ldap_synchronize_jds.

Для этого используется команда:

```
select ja_sync_ldap.ldap_synchronize_jds(prof_id int);
```

В таблице 4.12 приведены параметры, используемые для синхронизации.

Таблица 4.12 – Входные параметры и обозначения для синхронизации

Параметр	Тип данных	Обозначение
prof_id	int	идентификатор профиля

При работе с функцией могут появляться следующие сообщения и результаты работы функции. Перечень сообщений приведен в таблице 4.13.

Таблица 4.13 – Перечень сообщений при синхронизации

Сообщения	Описание
-1	синхронизация не выполнена
0	синхронизация выполнена
> 0	количество неуспешных соответствий групп. (т.е. количество групп в которых возникли ошибки)

4.4. Функции работы с журналами событий (логами)

Компонент ja_Sync_LDAP обладает функциональной возможностью просмотра событий за требуемый интервал времени, а также удаления всех или определенных записей. Далее в подразделах описаны функции, отвечающие за работу с журналами событий.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

4.4.1. Просмотр событий безопасности

Для просмотра событий безопасности необходимо ввести команду:

```
select * from ja_sync_ldap.get_sync_log(from_date date, to_date  
date, row_count int);
```

В таблице 4.14 приведены входные параметры для просмотра событий безопасности.

Таблица 4.14 – Входные данные для просмотра журнала

Параметр	Тип данных	Обозначение
from_date	date	начало периода
to_date	date	конец периода
row_count	int	количество выводимых записей



Дата указывается в формате ГГГГ-ММ-ДД.

В таблице 4.15 указаны выходные значения команды.

Таблица 4.15 – Выходные значения просмотра журнала

Параметр	Тип данных	Обозначение
id	int	идентификатор строки
datetime	date	дата регистрируемого события
profile_name	text	имя профиля
db_role_name	text	роль БД
domain_group_name	text	группа в службе каталогов
result	text	результат
message	text	сообщение

Например

Вывод последних 10 сообщений выполняется SQL-командой:

```
SELECT * FROM ja_sync_ldap.get_sync_log('2019-01-  
01'::date, '2030-12-30'::date, 10);
```

```

root@admin1: /home
postgres=# SELECT * FROM ja_sync_ldap.get_sync_log('2019-01-01'::date,'2030-12-30'::date,10);
 id |      datetime      | profile_name | db_role_name | domain_group_name | result | message
-----+-----+-----+-----+-----+-----+-----
 37 | 2024-01-12 13:27:43.197786+03 | samba_usr   | SUCCESS      | SUCCESS           | 0      | Successful synchronization (All use
rs are synchronized)
 35 | 2024-01-12 12:24:39.147509+03 | samba_usr   | FAILED       | FAILED            | -1     | ldap_sasl_bind_s: Cannot contact th
e LDAP server.

```

Рисунок 4.2 – Вывод событий безопасности

4.4.2. Удаление событий безопасности

Из журнала событий можно удалить одну, несколько или все строки.

4.4.2.1 Удаление строки из журнала событий

Удаление одной определенной строки производится следующей командой:

```
select ja_sync_ldap.drop_sync_log_row(row_id int);
```

В таблице 4.16 указаны входные параметры команды.

Таблица 4.16 – Параметры и обозначения при удалении строки

Параметр	Тип данных	Обозначение
row_id	int	идентификатор выбранной строки

По результатам выполнения команды, СУБД вернет сообщение, указанное в таблице 4.17.

Таблица 4.17 – Перечень сообщений, возвращаемых при выполнении удаления события безопасности

Сообщение	Описание
id строки	успешно
0	строка не найдена
-1	остальные ошибки

4.4.2.2 Удаление выбранных строк из журнала событий

Удаление нескольких строк происходит следующей командой:

```
SELECT ja_sync_ldap.drop_sync_log_rows(row_id int[]);
```

В таблице 4.18 указаны входные параметры команды.

Таблица 4.18 – Параметры и обозначения при удалении строк

Параметр	Тип данных	Обозначение
row_id	int	идентификатор выбранной строки
№ изменения: _____		Подпись отв. лица: _____
		Дата внесения изм: _____

По результатам выполнения команды СУБД возвратит сообщение, указанное в таблице 4.19.

Таблица 4.19 – Перечень сообщений, возвращаемых при выполнении удаления событий безопасности

Сообщение	Описание
0	успешно
-1	длина массива 0 или ошибка
-2	ни одной строки не существует

Дополнительные примеры представлены в п.п. 5.11, настоящего документа.

4.4.2.3 Удаление всех строк из журнала событий

Удаление всех строк происходит следующей командой:

```
select ja_sync_ldap.drop_sync_log_all();
```

По результатам выполнения команды СУБД вернет сообщение, указанное в таблице 4.20.

Таблица 4.20 – Перечень сообщений, возвращаемых при выполнении удаления событий безопасности

Сообщение	Описание
0	успешно
-1	ошибка

4.4.3. Описание работы журнала событий

В журнале событий появляются сообщения о статусе операций после запуска функции синхронизации. При успешной синхронизации в журнал будет добавлена строка с нулевым количеством ошибок, в противном случае добавляется строка с ошибкой и причиной неуспешной синхронизации.

Сообщения в журналах:

1) со стороны СУБД:

Сообщение	Перевод
role "<наименование>" does not exist	Соответствия групп на стороне СУБД не существует
0	Все соответствия групп выполнены успешно

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Сообщение	Перевод
>0	Количество проблемных соответствий групп (т.е. количество групп в которых возникли ошибки)
-1	Все соответствия групп синхронизированы неудачно
There is no mapping with this id	В профиле нет ни одного соответствия групп
No profile with this id	Данный профиль не существует

2) ошибки со стороны LDAP:

Сообщение	Перевод
LDAP ERROR: Operations error occurred.	Произошла ошибка операции
LDAP ERROR: Protocol error occurred.	Произошла ошибка протокола
LDAP ERROR: Time limit, set by the server side time limit parameter, was exceeded.	Лимит времени, установленный параметром ограничения времени на стороне сервера, превышен
LDAP ERROR: Size limit was exceeded.	Превышен лимит размера
LDAP ERROR: This message is returned if the function succeeds, and the attribute and known values do not match.	Это сообщение возвращается, если функция завершается успешно, а атрибут и известные значения не совпадают
LDAP ERROR: This message is returned if the function succeeds, and the attribute and known values match.	Это сообщение возвращается, если функция завершается успешно, а атрибут и известные значения совпадают
LDAP ERROR: The authentication method is not supported.	Метод аутентификации не поддерживается
LDAP ERROR: Strong authentication is required.	Требуется надежная аутентификация
LDAP ERROR: A referral was returned from the server.	Реферал был возвращен с сервера
LDAP ERROR: Administration limit on the server was exceeded.	Превышен лимит администрирования на сервере

Сообщение	Перевод
LDAP ERROR: The control is critical and the server does not support the control.	Элемент управления является критическим, и сервер не поддерживает элемент управления
LDAP ERROR: Confidentiality is required.	Требуется конфиденциальность
LDAP ERROR: The client must send the server the same SASL Mechanism to continue the process.	Клиент должен отправить серверу тот же механизм SASL, чтобы продолжить процесс
LDAP ERROR: Requested attribute does not exist.	Запрошенный атрибут не существует
LDAP ERROR: Type is not defined.	Тип не определен
LDAP ERROR: There was an inappropriate matching.	Произошло неуместное сопоставление
LDAP ERROR: There was a constraint violation.	Произошло нарушение ограничений
LDAP ERROR: The attribute exists or the value has been assigned.	Атрибут существует или ему присвоено значение
LDAP ERROR: The syntax is invalid.	Неверный синтаксис
LDAP ERROR: Object does not exist.	Объект не существует
LDAP ERROR: The alias is invalid.	Псевдоним недействителен
LDAP ERROR: The distinguished name has an invalid syntax.	Отличительное имя имеет недопустимый синтаксис
LDAP ERROR: The object is a leaf.	Объект является листом
LDAP ERROR: Cannot dereference the alias.	Не удастся разыменовать/отменить ссылку на псевдоним
LDAP ERROR: Authentication is inappropriate.	Аутентификация не подходит
LDAP ERROR: The supplied credential is invalid.	Предоставленные учетные данные недействительны
LDAP ERROR: The user has insufficient access rights.	У пользователя недостаточно прав доступа

Сообщение	Перевод
LDAP ERROR: The server is busy.	Сервер занят
LDAP ERROR: The server is not willing to handle directory requests.	Сервер не желает обрабатывать запросы каталога
LDAP ERROR: The chain of referrals has looped back to a referring server.	Цепочка рефералов заиклилась на реферальном сервере
LDAP ERROR: There was a naming violation.	Произошло нарушение именования
LDAP ERROR: There was an object class violation.	Произошло нарушение класса объекта
LDAP ERROR: Operation is not allowed on a nonleaf object.	Операция не разрешена для нелистового объекта
LDAP ERROR: Operation is not allowed on RDN.	Операция не разрешена на RDN
LDAP ERROR: The object already exists.	Объект уже существует
LDAP ERROR: Cannot modify object class.	Невозможно изменить класс объекта
LDAP ERROR: Results returned are too large.	Возвращаемые результаты слишком велики
LDAP ERROR: Multiple directory service agents are affected.	Затрагиваются несколько агентов службы каталогов
LDAP ERROR: An error occurred when attempting to perform a requested Virtual List View operation.	Произошла ошибка при попытке выполнить запрошенную операцию просмотра виртуального списка
LDAP ERROR: Unknown error occurred.	Произошла неизвестная ошибка
LDAP ERROR: Local error occurred. If this error occurs during a binding operation, for more information, see ldap_bind_s.	Произошла локальная ошибка. Если эта ошибка возникает во время операции привязки, дополнительные сведения см. в разделе ldap_bind_s
LDAP ERROR: Encoding error occurred.	Произошла ошибка кодирования

Сообщение	Перевод
LDAP ERROR: Decoding error occurred.	Произошла ошибка декодирования
LDAP ERROR: The search was aborted due to exceeding the limit of the client side timeout parameter.	Поиск был прерван из-за превышения ограничения параметра времени ожидания на стороне клиента
LDAP ERROR: The feature is not supported.	Функция не поддерживается
LDAP ERROR: Results are not returned.	Результаты не возвращаются
LDAP ERROR: Cannot contact the LDAP server.	Не удастся связаться с сервером LDAP
LDAP ERROR: More results are to be returned.	Должны быть возвращены другие результаты
LDAP ERROR: Client loop was detected.	Обнаружена петля на стороне клиента
LDAP ERROR: The referral limit has been exceeded.	Реферальный лимит превышен
LDAP ERROR: Unknown error occurred.	Произошла неизвестная ошибка

5. ПРИМЕРЫ СИНХРОНИЗАЦИИ

Функциональные возможности компонента ja_Sync_LDAP позволяют выполнять:

- синхронизацию по атрибуту 'sAMAccountName';
- синхронизацию по атрибуту 'cn';
- синхронизацию по атрибуту 'name';
- синхронизацию по любому атрибуту, по которому можно идентифицировать

пользователя.

В качестве примера используется сервер под управлением Windows Server с ролью контролера домена и сервер СУБД «Jatoba» под управление ОС Ubuntu 22.04. Сервера имеют IP-адреса, приведенные в таблице 5.1.

Таблица 5.1 – Сетевая адресация серверов стенда

№	Имя сервера	IP-адрес	Маска подсети	DNS	Роль
1	ad-2016	10.116.102.46	255.255.255.0	10.116.102.2	Контролер домена
2	ldap	10.116.102.47	255.255.255.0	10.116.102.2	СУБД

5.1. Выполнение синхронизации одного соответствия по атрибуту 'sAMAccountName'

В домене «jatoba.corp» создана глобальная группа безопасности пользователей «db_admins», в которую входят пользователи

- admin1;
- admin2;
- admin3;

которых необходимо синхронизировать с СУБД.



Не рекомендуется создавать групповую роль при помощи CREATE ROLE через двойные кавычки в верхнем регистре и/или с пробелами, так как компонент ja_Sync_LDAP преобразует все поля в профиле и правилах сопоставления (маппинга) в нижний регистр. При попытке синхронизации это приводит к возникновению ошибки из-за не найденной групповой роли.

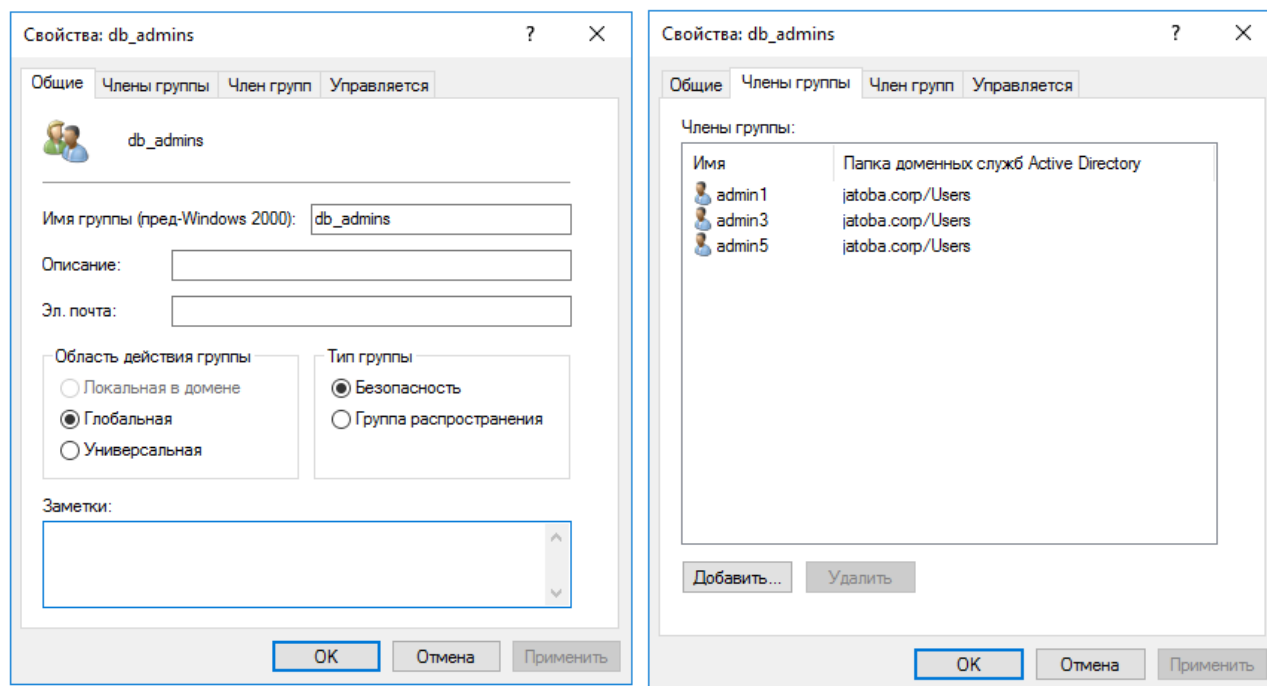


Рисунок 5.1 – Группа пользователей в AD

В СУБД существует групповая роль «admin» создаваемая SQL-командой:

```
CREATE ROLE "admin" SUPERUSER NOCREATEDB NOCREATEROLE INHERIT
NOLOGIN NOREPLICATION NOBYPASSRLS;
```

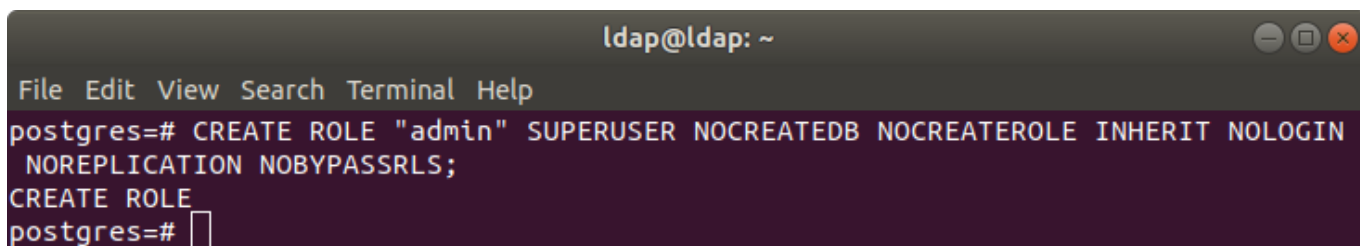


Рисунок 5.2 – Групповая роль в СУБД

Пользователи, внесенные с данной групповой ролью, унаследуют права суперпользователя.

5.1.1. Добавление профиля синхронизации

Для создания профиля синхронизации требуется аутентифицироваться в СУБД:

```
su -l postgres
cd /usr/jatoba-5/bin/
psql -h localhost -d postgres -U postgres
```

Для создания профиля используется SQL-команда, синтаксис которой приведен в п. 4.1.1:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

```
select ja_sync_ldap.set_sync_profile(in_profile_id int,  
in_profile_name text, in_host_ip text, in_port text, in_login  
text, in_pswd text, in_domain_type text);
```

Для создания профиля используется SQL-команда:

```
select  
ja_sync_ldap.set_sync_profile(null,'user','10.116.102.46','389'  
, 'admin_ad', 'P@ssword', 'activedirectory');
```

The screenshot shows a terminal window with the prompt 'root@admin1: /home'. The user enters the command: `postgres=# select ja_sync_ldap.set_sync_profile(null,'user','10.116.102.46','389', 'admin_ad', 'P@ssword', 'activedirectory');`. The output shows the command being executed and then the prompt returns to `postgres=#`. Below the command, the text 'set_sync_profile' is displayed, followed by a horizontal line and the number '1'. At the bottom, it says '(1 row)'.

Рисунок 5.3 – Создание профиля синхронизации

Параметры и значения, используемые в SQL-команде приведены в таблице 5.2.

Таблица 5.2 – Параметры и значения для создания профиля

Параметр	Тип данных	Значение	Обозначение
in_profile_id	int	null	идентификатор профиля
in_profile_name	text	user	имя профиля
in_host_ip	text	10.116.102.46	IP-адрес AD
in_port	text	389	порт (по умолчанию 389) AD
in_login	text	admin_ad	учетная запись администратора AD
in_pswd	text		пароль от учетной записи администратора AD
in_domain_type	text	activedirectory	тип службы каталогов

5.1.2. Просмотр профиля

Для просмотра существующих профилей используется команда:

```
select ja_sync_ldap.get_sync_profiles();
```

В результате сформируется таблица, представленная на рисунке 5.4.

```

root@admin1: /home
postgres=# select ja_sync_ldap.get_sync_profiles();
               get_sync_profiles
-----
(1,user,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)
(1 row)
postgres=#

```

Рисунок 5.4 – Просмотр существующих профилей

5.1.3. Добавление соответствия групп

Для создания соответствия групп используется команда:

```

select ja_sync_ldap.set_sync_profile_map(in_map_id int,
in_profile_id int, in_role_bd text, in_domain_group text,
in_attribute text);

```

Синтаксис SQL-команды описан в п. 4.2.1.

В представляемом примере, к имеющемуся профилю синхронизации с идентификатором «1» создается профиль соответствия групп, в котором создаваемые пользователи будут входить в групповую роль «admin» и наследовать от нее атрибуты.

```

ldap@ldap: ~
File Edit View Search Terminal Help
postgres=# \du
                                List of roles
Role name |                               Attributes                               | Member
-----+-----+-----
admin     | Superuser, Cannot login                                             | {}
postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS         | {}
postgres=#

```

Рисунок 5.5 – Список пользователей и групп пользователей в СУБД

При этом пользователи будут синхронизироваться из каталога «db_admins» группы «Users», домена «jatoba.corp», с атрибутом «sAMAccountName». Атрибут «sAMAccountName» выбирается по усмотрению администратора СУБД и зависит от структуры каталога AD.

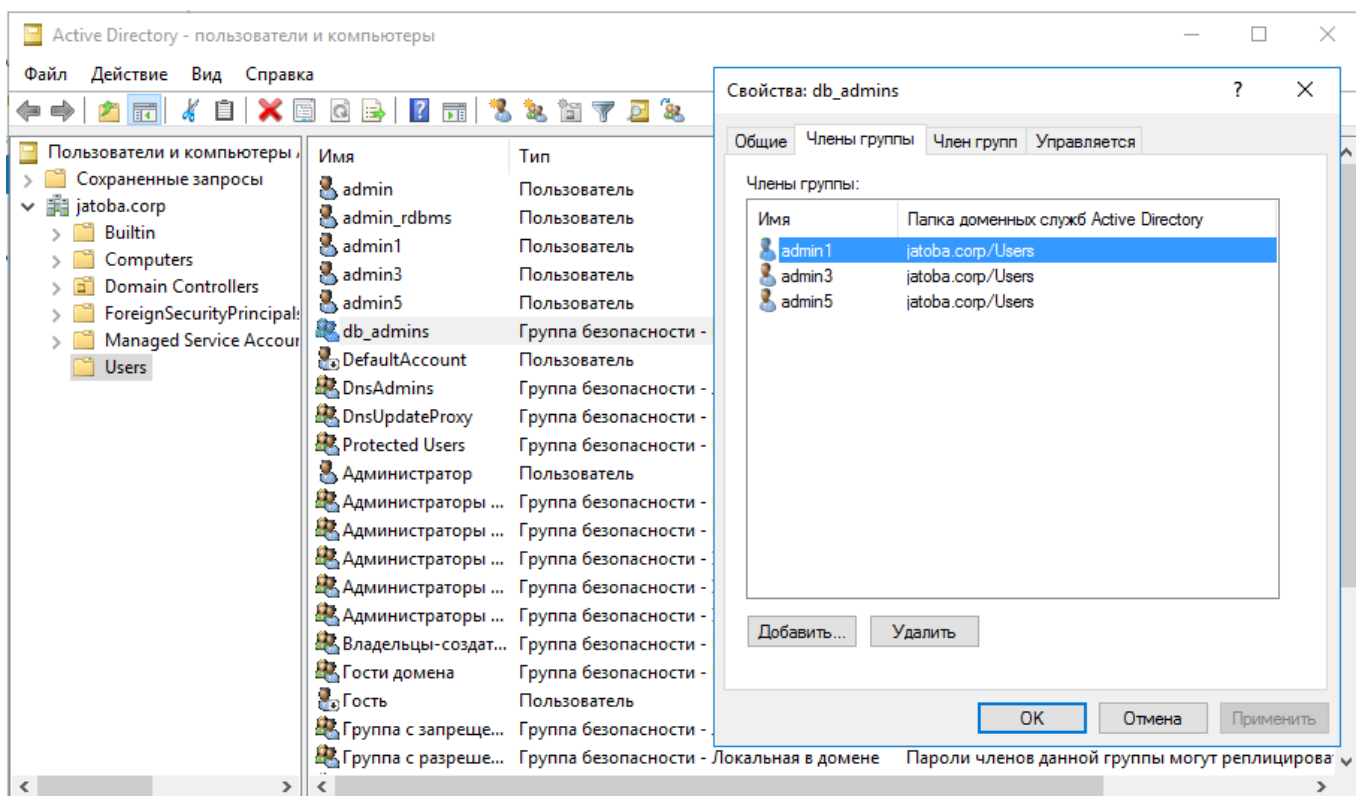


Рисунок 5.6 - Каталог «db_admins» группы «Users», домена «jatoba.corp»

Учитывая вышеизложенное, SQL-команда будет следующей:

```
select
ja_sync_ldap.set_sync_profile_map(null,1,'admin','CN=db_admins,CN=Users,DC=jatoba,DC=corp','sAMAccountName');
```

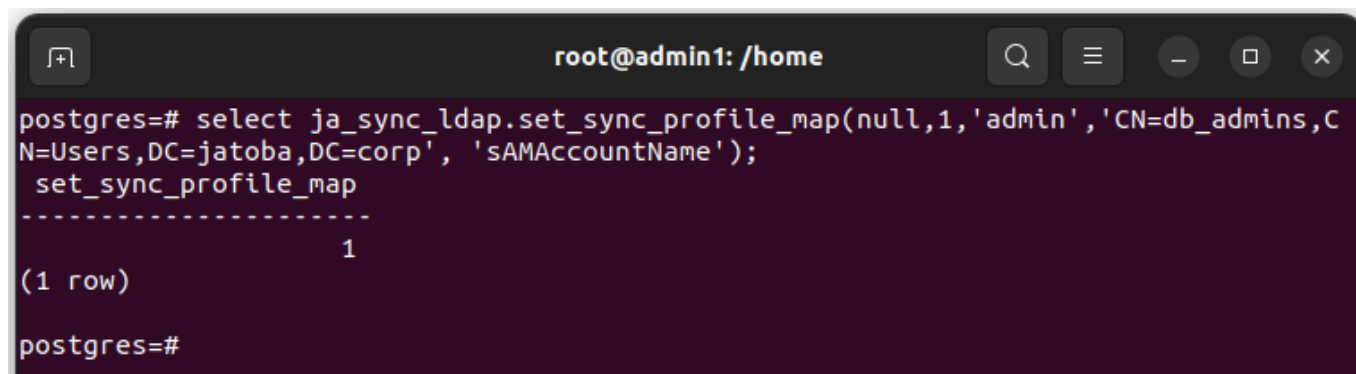


Рисунок 5.7 – SQL-команда добавления соответствия групп

Для выполнения команды потребуются параметры, приведенные в таблице 4.6.

Таблица 5.3 – Параметры и значения для создания соответствия групп

Параметр	Значение	Обозначение
in_map_id	null	идентификатор соответствия групп
in_profile_id	1	идентификатор профиля синхронизации
in_role_bd	admin	Групповая роль СУБД
in_domain_group	CN=db_admins,CN=Users,DC=jatoba,DC=corp	группа AD
in_attribute	sAMAccountName	имя атрибута записи в AD, который содержит имя пользователя

В идентификаторе соответствия групп указывается значение «null», т.к. ID назначается автоматически.

В параметре «in_profile_id», указывается значение «1», соответствующее ID профиля синхронизации.

В параметре «role_bd» указывается имя групповой роли в СУБД, в данном случае «admin», в которую будут включены учетные записи пользователей.

В параметре «in_domain_group» указывается строка значений «DistinguishedName», полученная из глобальной группы безопасности пользователей «db_admins». Группу можно получить путем запроса в PowerShell.

```

Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation), 2016. Все права защищены.

PS C:\Users\admin> Get-ADGroup -Identity db_admins

DistinguishedName : CN=db_admins,CN=Users,DC=jatoba,DC=corp
GroupCategory     : Security
GroupScope        : Global
Name              : db_admins
ObjectClass       : group
ObjectGUID        : aad99164-78fd-4867-9a27-9e997606e722
SamAccountName    : db_admins
SID               : S-1-5-21-4093081431-602958358-3562534692-1104

PS C:\Users\admin>
  
```

Рисунок 5.8 – Информация о глобальной группе безопасности «db_admins»

В параметре «in_attribute» указывается параметр «sAMAccountName» – это уникальное имя входа и в данном случае указание имени глобальной группы безопасности пользователей (см. рис. 5.9).

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

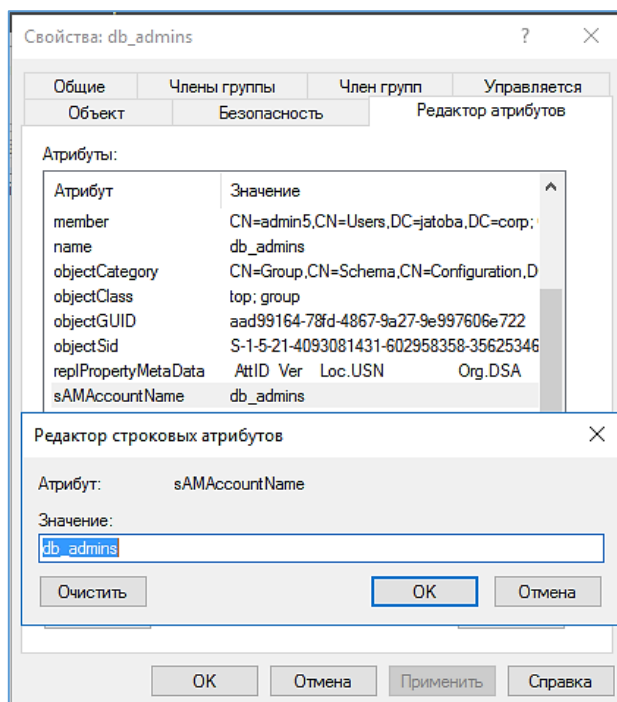


Рисунок 5.9 – Атрибут «sAMAccountName» группы пользователей «db_admins»

5.1.4. Синхронизация

Синхронизация осуществляется командой:

```
select ja_sync_ldap.ldap_synchronize_jds(1);
```

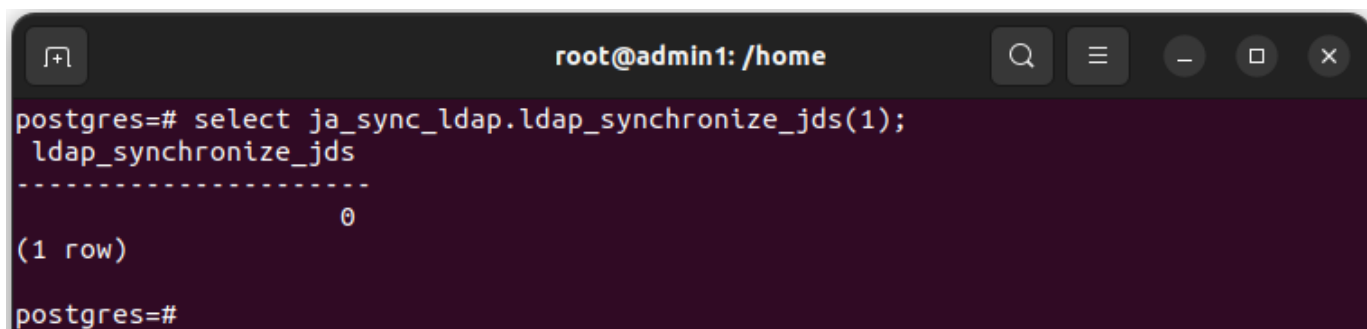


Рисунок 5.10 – Синхронизация AD и СУБД

При просмотре списка пользователей видно, что все пользователи из AD были синхронизированы в СУБД.

А именно из глобальной группы безопасности AD «db_admins» созданы пользователи СУБД:

- admin1;
- admin2;

- admin3;

в групповой роли «admin», как представлено на рисунке 5.11.

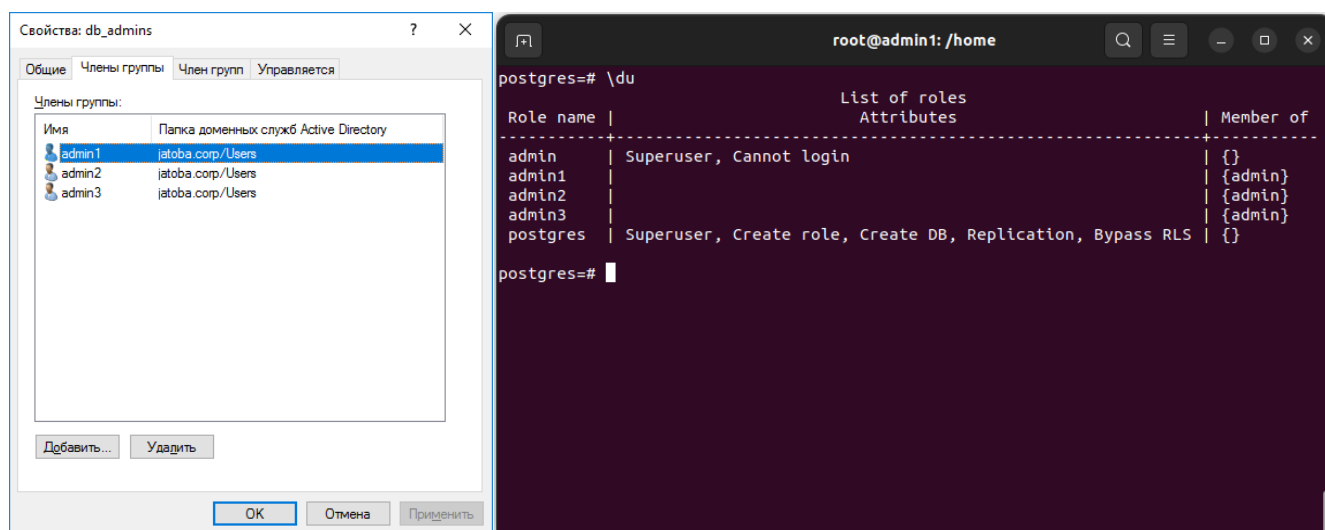


Рисунок 5.11 – Результат синхронизации пользователей группы «db_admins»



Для вывода информации о членстве в ролях, с указанием всех параметров и прав доступа, в СУБД «Jatoba» с версией ядра 6 используется команда \drg

5.1.5. Авторизация после синхронизации по атрибуту 'sAMAccountName'

Для авторизации через синхронизированных пользователей по механизму LDAP требуется отредактировать конфигурационный файл pg_hba.conf:

```
host all all 10.116.102.0/24 ldap ldapserver=10.116.102.46
ldapbasedn="CN=Users,DC=jatoba,DC=corp"
ldapbinddn="CN=admin_ad,CN=Users,DC=jatoba,DC=corp"
ldapbindpasswd="P@ssword" ldapsearchattribute="sAMAccountName"
```

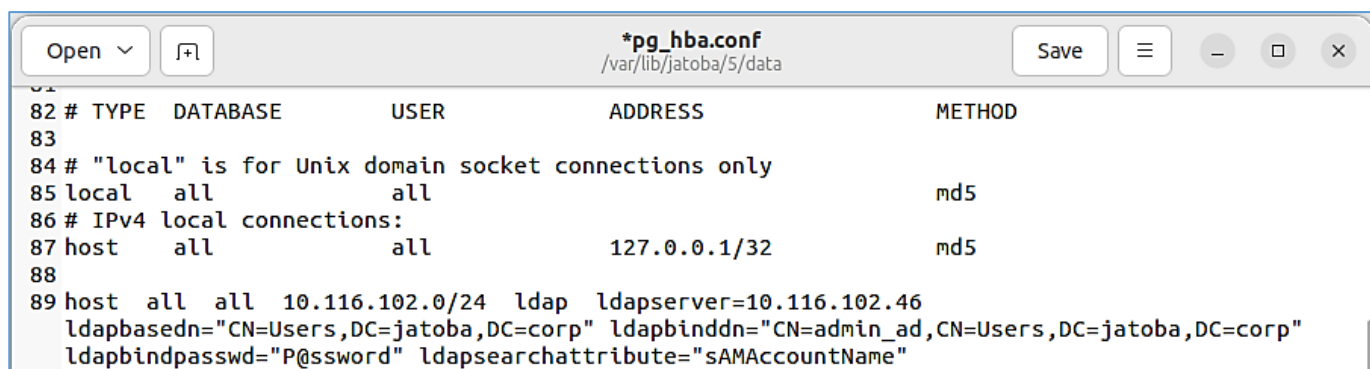


Рисунок 5.12 – Параметры конфигурационного файла «pg_hba.conf»

В конфигурационном файле, в столбце «ADDRESS» указываем подсеть, от которой СУБД будет принимать соединения с методом аутентификации LDAP. В приводимом примере это подсеть 10.116.102.0, с маской подсети 255.255.255.0, т.е. с длиной префикса /24.

После чего последовательно указываются параметры:

- ldapserver – IP - адрес сервера AD:

```
ldapserver=10.116.102.46
```

При создании профиля синхронизации параметр указывался как «in_host_ip» (см. таб. 4.1).

- ldapbasedn – адрес каталога пользователей:

```
ldapbasedn="CN=Users,DC=jatoba,DC=corp"
```

- ldapbinddn – адрес каталога администратора AD, который указывался в профиле синхронизации. Указывается не имя администратора AD в параметре «in_login», а именно путь к его каталогу.

```
ldapbinddn="CN=admin,CN=Users,DC=jatoba,DC=corp"
```

В MS AD это атрибут учетной записи пользователя AD «distinguishedName», который возможно получить в вкладке «Редактор атрибутов» карточки пользователя.

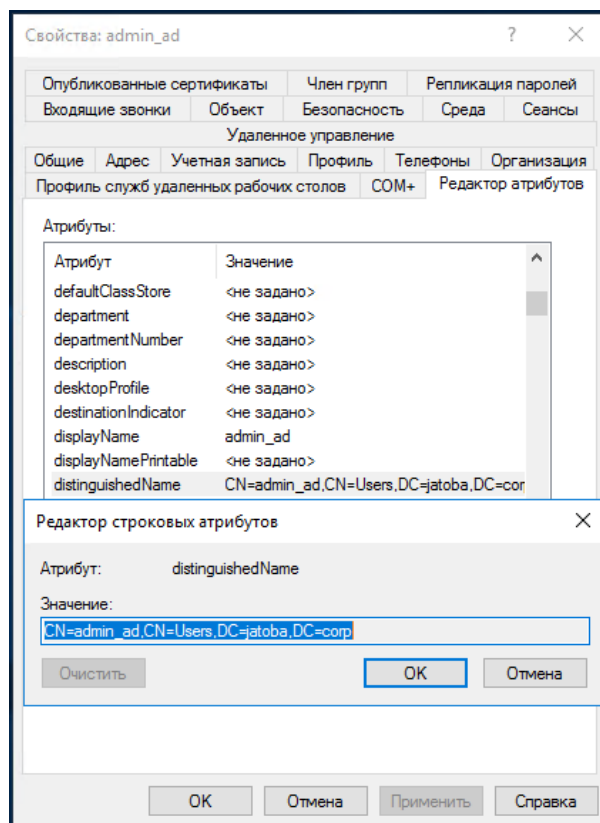


Рисунок 5.13 – Атрибут «distinguishedName»

- ldapbindpasswd – пароль администратора AD. В профиле синхронизации это параметр «in_pswd» (см. таб. 4.1);
- ldapsearchattribute – атрибут для соотнесения с именем пользователя в ходе аутентификации:

```
ldapsearchattribute="sAMAccountName"
```

Значение «sAMAccountName» использовалось в параметре «in_attribute», как имя атрибута записи в AD, который содержит имя пользователя при добавлении соответствия групп (см. табл. 4.6).

После проделанного шага необходимо авторизоваться в СУБД через LDAP:

```
psql -h 10.116.102.47 -p 5432 -d postgres -U admin1
```

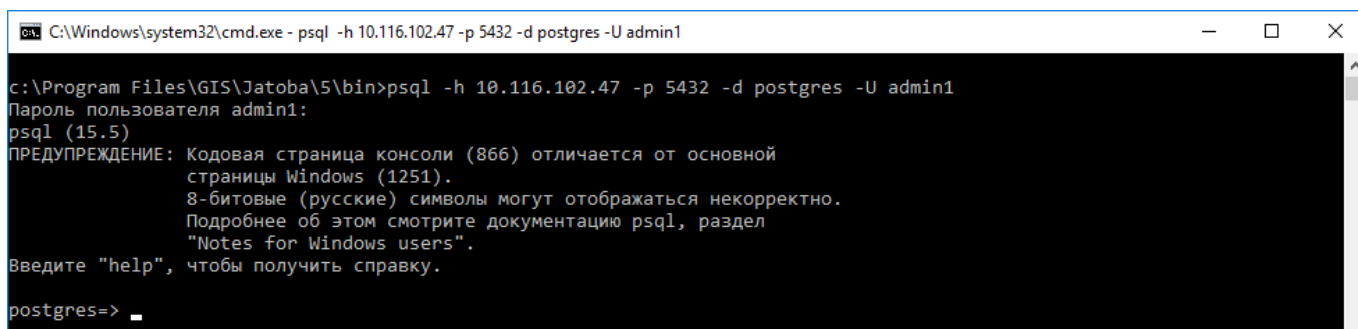


Рисунок 5.14 – Аутентификация в СУБД по методу LDAP пользователя «admin1»

5.2. Выполнение синхронизации одного соответствия по атрибуту 'cn'

Для примера используются те же сервера с параметрами, указанными в таблице 5.1.

Созданы пользователи MS AD:

- user_1;
- user_2;
- user_3.

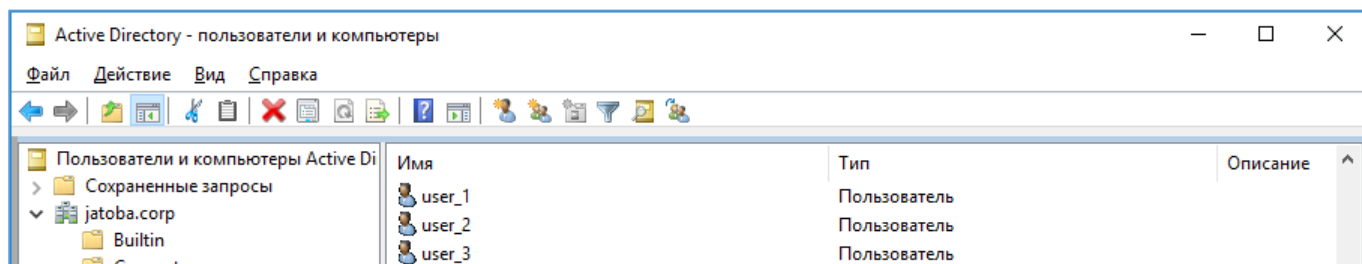


Рисунок 5.15 – Учетные записи пользователей MS AD

Пользователи входят в глобальную группу безопасности «db_users».

В СУБД создана групповая роль «ad_user» SQL-командой:

```

CREATE ROLE ad_users NOSUPERUSER NOCREATEDB NOCREATEROLE
INHERIT NOLOGIN NOREPLICATION NOBYPASSRLS;

```

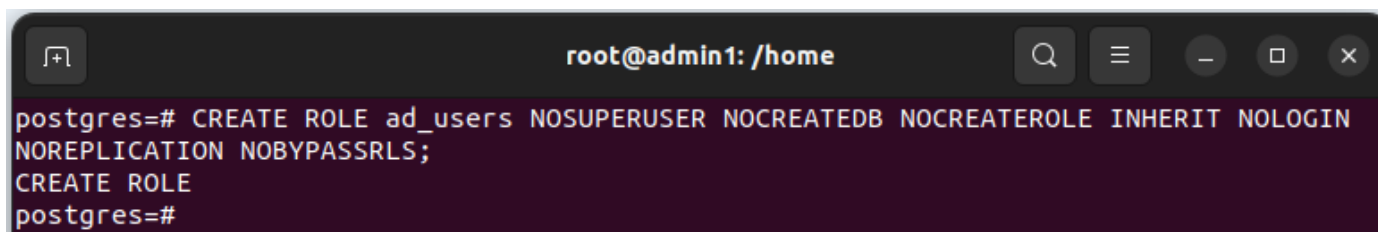


Рисунок 5.16 – SQL-команда создания групповой роли «ad_users»

Созданная групповая роль не имеет никаких привилегий в СУБД.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

5.2.1. Добавление профиля синхронизации

Для удобства восприятия зададим имя профиля синхронизации по имени групповой роли в СУБД «ad_users».

Относительно разбираемого примера используется SQL-команда:

```
SELECT  
ja_sync_ldap.set_sync_profile(null,'ad_users','10.116.102.46','  
389','admin_ad','P@ssword', 'activedirectory');
```

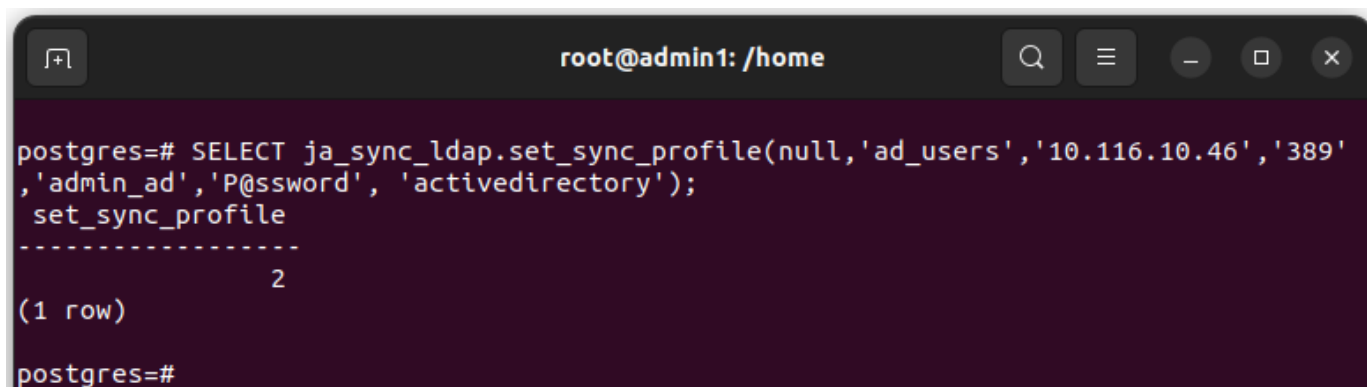


Рисунок 5.17 - Создание профиля синхронизации с именем «ad_users»
Создан профиль синхронизации с ID=2.

5.2.2. Просмотр профилей синхронизации

Убеждаемся, что созданный профиль синхронизации действительно получил свой ID и присутствует в общем списке профилей синхронизации, выполнив SQL- команду:

```
select ja_sync_ldap.get_sync_profiles();
```

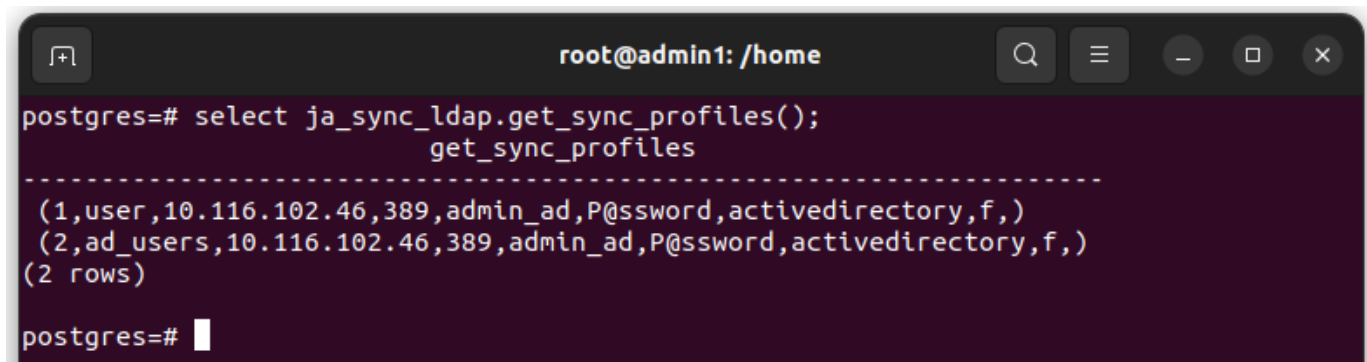


Рисунок 5.18 – Список созданных профилей синхронизации
СУБД выведет общий список профилей синхронизации.

5.2.3. Добавление соответствия групп

Следующим шагом на сервере AD получаем атрибут «DistinguishedName» группы «db_users» командой:

```
Get-ADGroup -Identity db_users
```

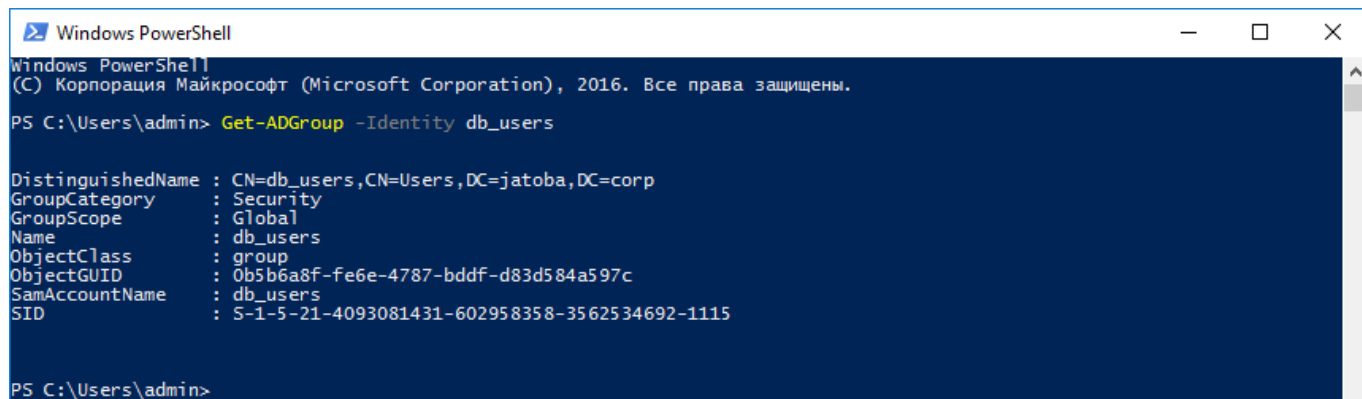


Рисунок 5.19 – Атрибут «DistinguishedName» группы «db_users»

Полученные параметры используются для формирования SQL-команды, которая будет следующей:

```
select
ja_sync_ldap.set_sync_profile_map(null,2,'ad_users','CN=db_users,CN=Users,DC=jatoba,DC=corp','cn');
```

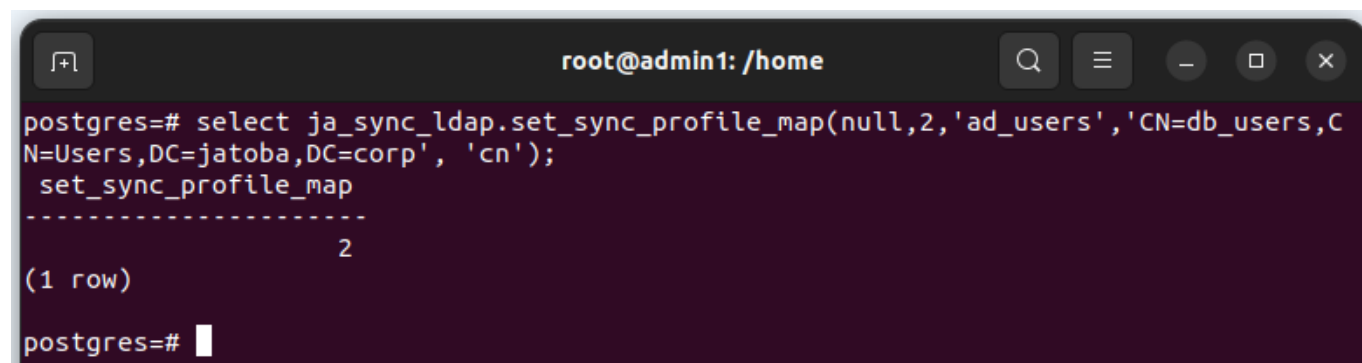


Рисунок 5.20 – Создание соответствия групп

СУБД выведет ID созданного маппинга (map_id) (см. табл. 4.7).

В данной SQL-команде указано:

- null (in_map_id) – идентификатор соответствия групп, т.е. присвоение нового значения;

- 2 (in_profile_id) – идентификатор профиля синхронизации, который был получен при создании профиля синхронизации (см. п. 5.2.1) и проверен при выводе списка профилей синхронизации (см. п. 5.2.2);
- ad_users (role_bd) – созданная в СУБД групповая роль;
- 'CN=db_users,CN=Users,DC=jatoba,DC=corp' (in_domain_group) – путь к каталогу глобальной группы безопасности «db_users» в MS AD;
- cn (in_attribute) — имя атрибута записи в AD, который содержит имя пользователя (см. рис. 5.21).

Иными словами, создается указание СУБД: «СУБД, создай новый профиль соответствия групп, для профиля синхронизации «2» в котором в групповую роль СУБД «ad_users», будут синхронизироваться учетные записи пользователей MS AD, состоящих в глобальной группе безопасности «db_users» и имеющих атрибут «cn».

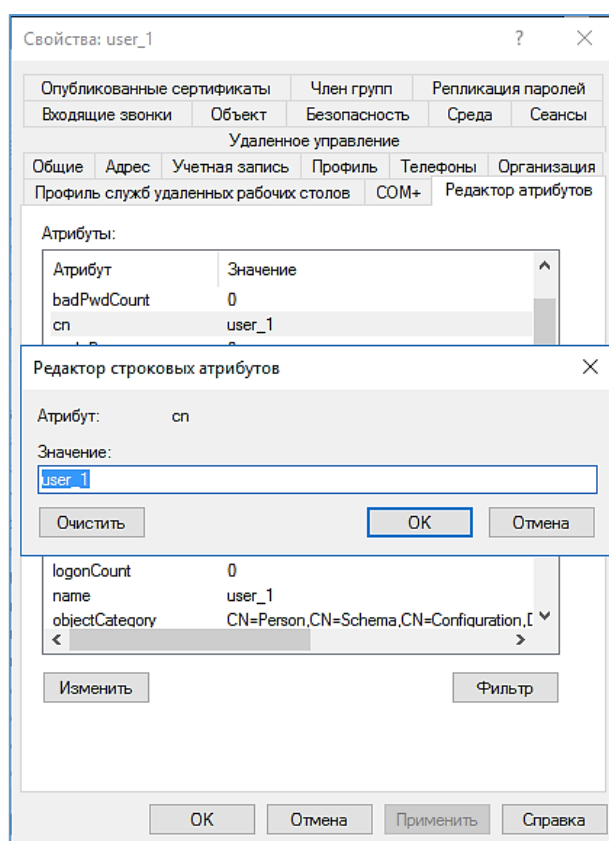


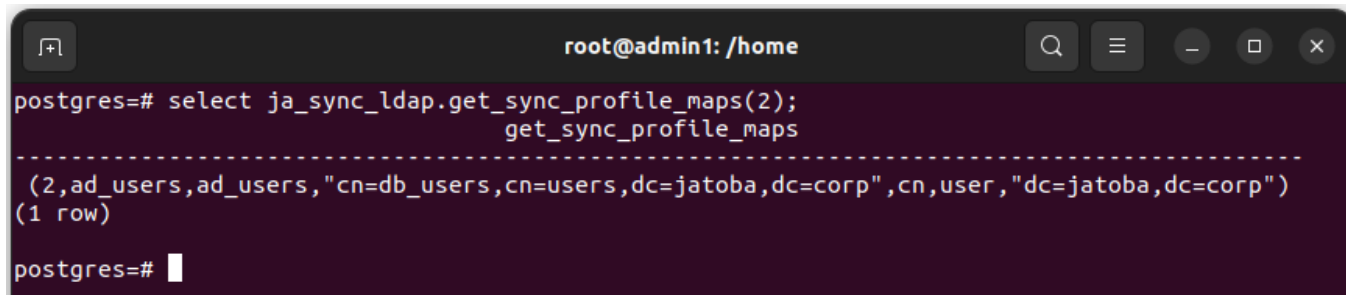
Рисунок 5.21 – Атрибут «cn» в карточке пользователя

5.2.4. Просмотр соответствия групп

Просмотреть соотнесенные к профилю синхронизации профили соответствия групп можно командой:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

```
select ja_sync_ldap.get_sync_profile_maps(2);
```



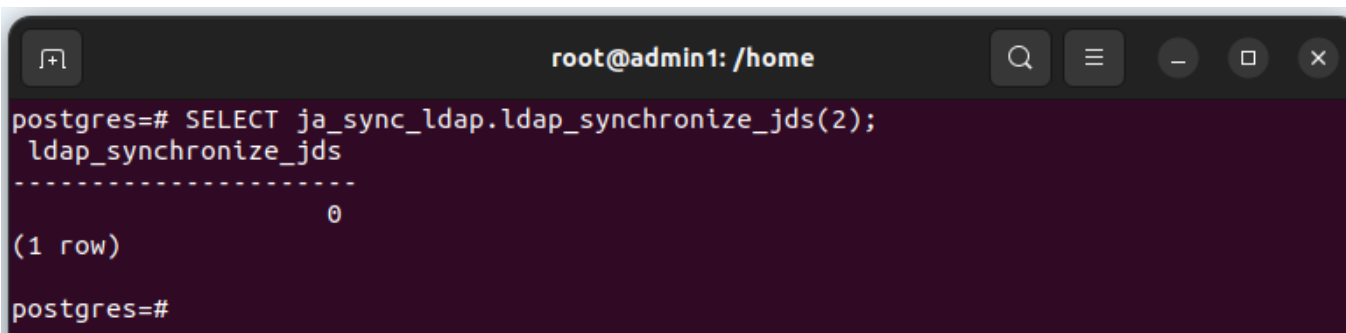
```
root@admin1: /home
postgres=# select ja_sync_ldap.get_sync_profile_maps(2);
               get_sync_profile_maps
-----
(2,ad_users,ad_users,"cn=db_users,cn=users,dc=jatoba,dc=corp",cn,user,"dc=jatoba,dc=corp")
(1 row)
postgres=#
```

Рисунок 5.22– Синхронизация УЗ AD с СУБД

5.2.5. Синхронизация

Синхронизация осуществляется командой:

```
SELECT ja_sync_ldap.ldap_synchronize_jds(2);
```



```
root@admin1: /home
postgres=# SELECT ja_sync_ldap.ldap_synchronize_jds(2);
 ldap_synchronize_jds
-----
0
(1 row)
postgres=#
```

Рисунок 5.23 – Синхронизация УЗ AD с СУБД

В которой указывается ID профиля синхронизации.

При просмотре списка пользователей видно, что учетные записи пользователей из глобальной группы безопасности «db_users» были синхронизированы в СУБД в групповую роль «ad_users».

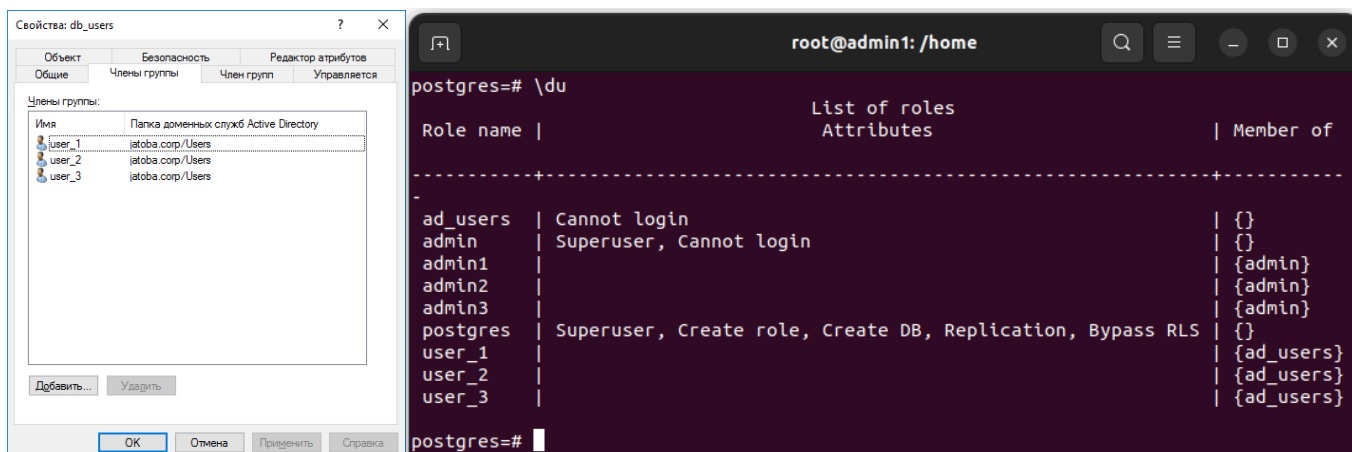


Рисунок 5.24 – Результат синхронизации пользователей группы «db_users»



Для вывода информации о членстве в ролях, с указанием всех параметров и прав доступа, в СУБД «Jatoba» с версией ядра 6 используется команда `\drg`

5.2.6. Авторизация после синхронизации по атрибуту 'cn'

Для авторизации через синхронизированных пользователей по механизму LDAP требуется отредактировать конфигурационный файл `pg_hba.conf`:

```
host all all 10.116.102.0/24 ldap ldapserver=10.116.102.46
ldapprefix="CN=" ldapsuffix=",CN=Users,DC=jatoba,DC=corp"
```

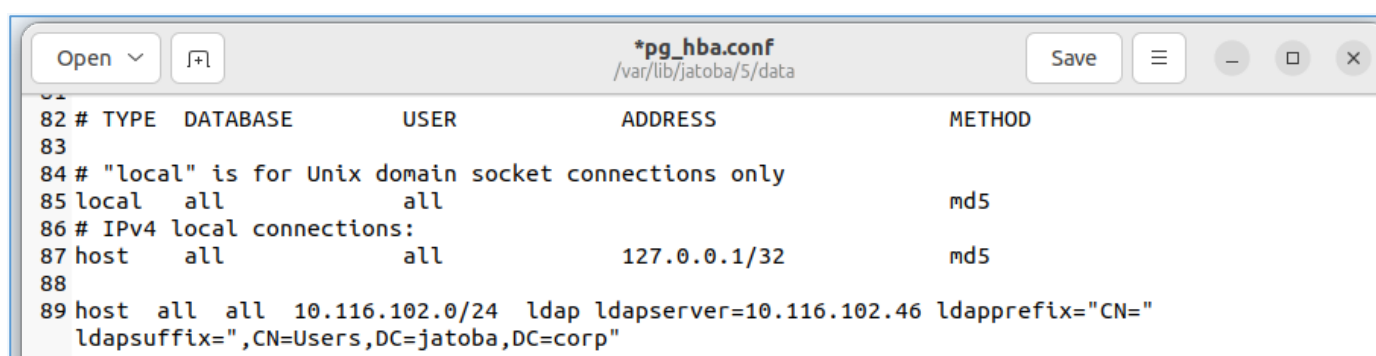


Рисунок 5.25 – Конфигурационный файл `pg_hba.conf` для аутентификации по атрибуту 'cn'

В конфигурационном файле, в столбце «ADDRESS» указывается подсеть, от которой СУБД будет принимать соединения с методом аутентификации LDAP. В приводимом примере это подсеть 10.96.1.0, с маской подсети 255.255.255.0, т.е. с длиной префикса /24.

После чего последовательно указываются параметры:

- `ldapserver` – IP - адрес сервера AD:


```
ldapserver=10.116.102.46
```

- `ldapprefix` - строка для префиксации к имени пользователя при формировании DN для привязки:

```
ldapprefix="CN="
```

- `ldapsuffix` - строка для добавления к имени пользователя при формировании DN для привязки:

```
ldapsuffix=",CN=Users,DC=jatoba,DC=corp"
```

После проделанного шага необходимо авторизоваться в СУБД через LDAP:

```
psql -h 10.116.102.47 -p 5432 -d postgres -U user_1
```

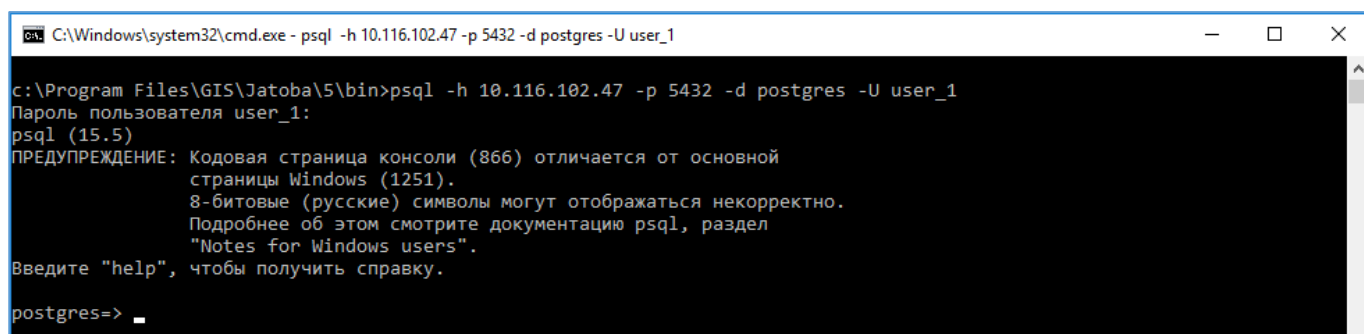


Рисунок 5.26 – Аутентификация пользователя user_1 в СУБД

5.2.7. Конфигурационный файл `pg_hba` при двух профилях синхронизации

В рассмотренных выше примерах синхронизации по атрибуту 'sAMAccountName' и по атрибуту 'cn', конфигурационный файл «`pg_hba`» содержит две строки для каждого из профилей синхронизации.

При этом СУБД поддерживает одновременную авторизацию пользователей каждой из групп безопасности AD.

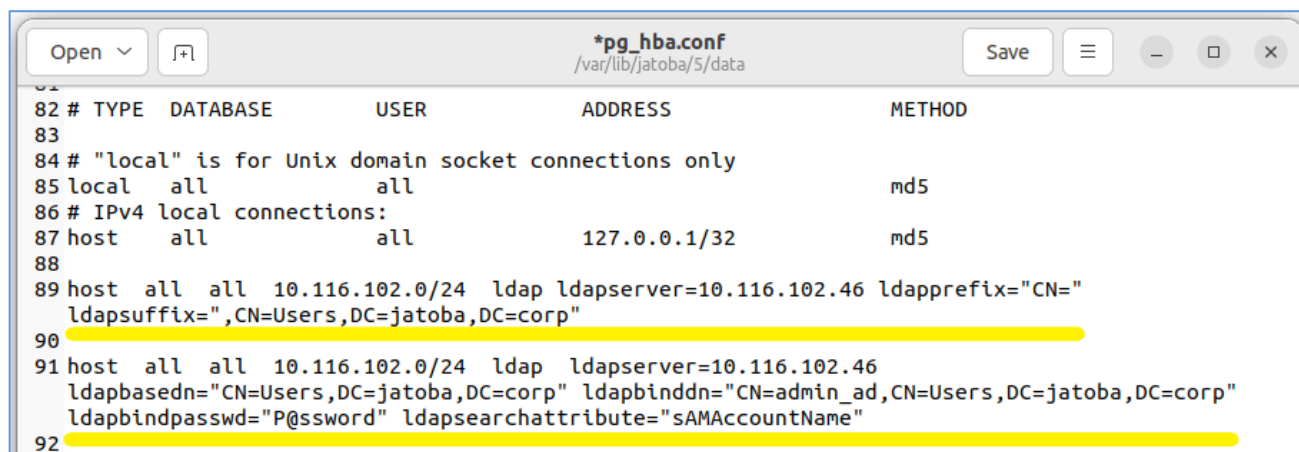


Рисунок 5.27 – Пример конфигурационного файла «pg_hba»

5.3. Выполнение синхронизации одного соответствия по атрибуту 'name' из группы в Organizational Unit (OU)

Для примера используются те же сервера с параметрами указанными в таблице 5.1.

Созданы пользователи MS AD:

- ivanov_ii;
- petrov_pp;

а также «Подразделение» Organizational Unit.

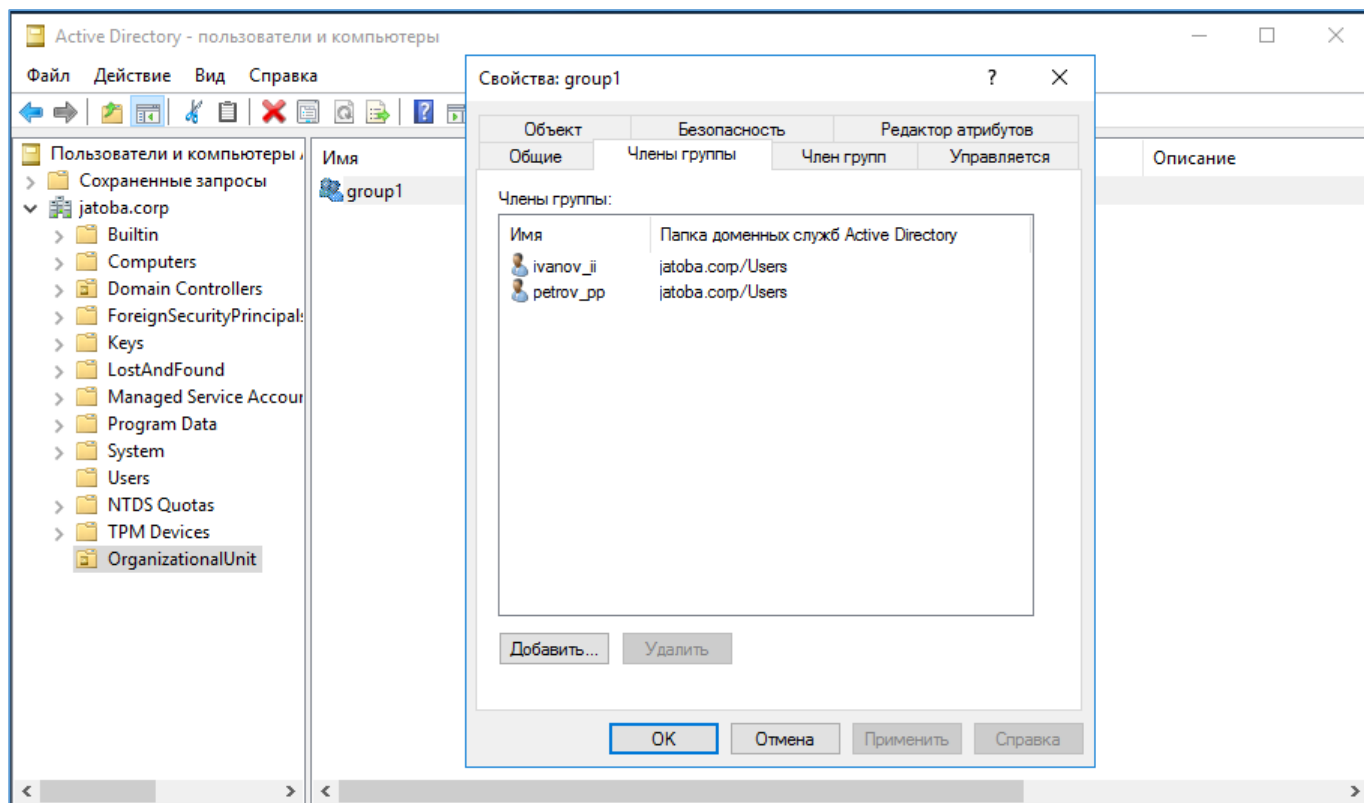


Рисунок 5.28 – Пользователи подразделения «Organizational Unit»



Пример создания «Organizational Unit» приведен в Приложении 2 настоящего документа

Пользователи входят в глобальную группу безопасности «group1» подразделения «Organizational Unit».

В СУБД создана групповая роль «ou_users» SQL-командой:

```
CREATE ROLE ou_users NOSUPERUSER NOCREATEDB NOCREATEROLE  
INHERIT NOLOGIN NOREPLICATION NOBYPASSRLS;
```

```
root@admin1: /home  
postgres=# CREATE ROLE ou_users NOSUPERUSER NOCREATEDB NOCREATEROLE INHERIT NOLOGIN  
NOREPLICATION NOBYPASSRLS;  
CREATE ROLE  
postgres=#
```

Рисунок 5.29 – Создание групповой роли СУБД «ou_users»

Созданная групповая роль не имеет никаких привилегий в СУБД.

5.3.1. Добавление профиля синхронизации

Для удобства восприятия, зададим имя профиля синхронизации по имени групповой роли в СУБД «ad_users».

Создадим профиль синхронизации с именем «ou_users», SQL-командой

```
SELECT  
ja_sync_ldap.set_sync_profile(null,'ou_users','10.116.102.46','  
389','admin','P@ssword', 'activedirectory');
```

```
root@admin1: /home  
postgres=# SELECT ja_sync_ldap.set_sync_profile(null,'ou_users','10.116.102.46','389  
, 'admin', 'P@ssword', 'activedirectory');  
set_sync_profile  
-----  
4  
(1 row)  
postgres=#
```

Рисунок 5.30 – Создание профиля синхронизации с именем «ou_users»

Создан профиль синхронизации с ID=4.

5.3.2. Просмотр профилей синхронизации

Убеждаемся, что созданный профиль синхронизации действительно получил свой ID и присутствует в общем списке профилей синхронизации, выполнив SQL- команду:

```
select ja_sync_ldap.get_sync_profiles();
```

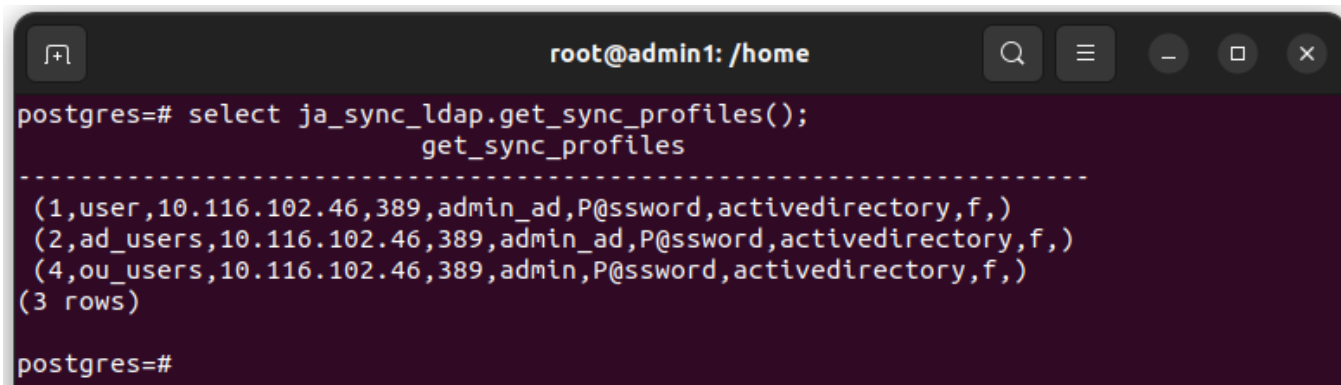


Рисунок 5.31 – Список созданных профилей синхронизации

СУБД выведет общий список профилей синхронизации.

5.3.3. Добавление соответствия группы

Следующим шагом на сервере AD получаем атрибут «DistinguishedName» группы «group1» командой:

```
Get-ADGroup -Identity group1
```

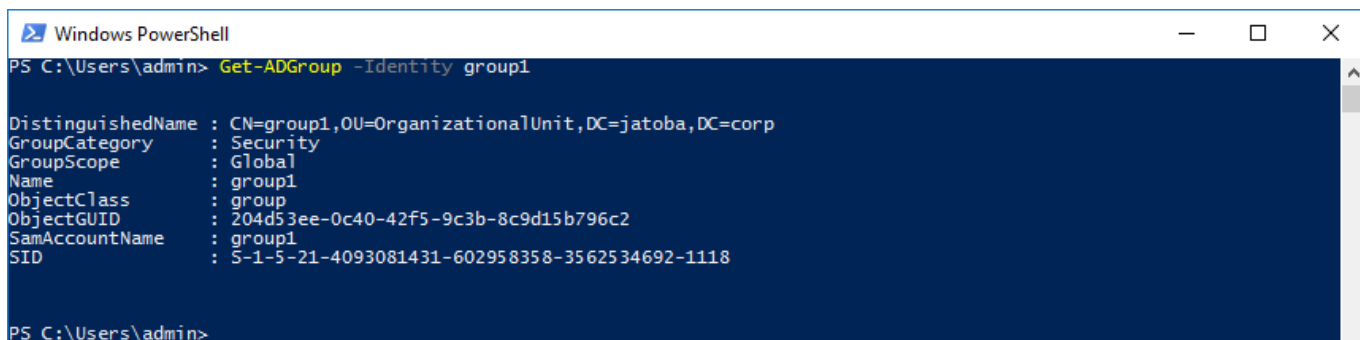
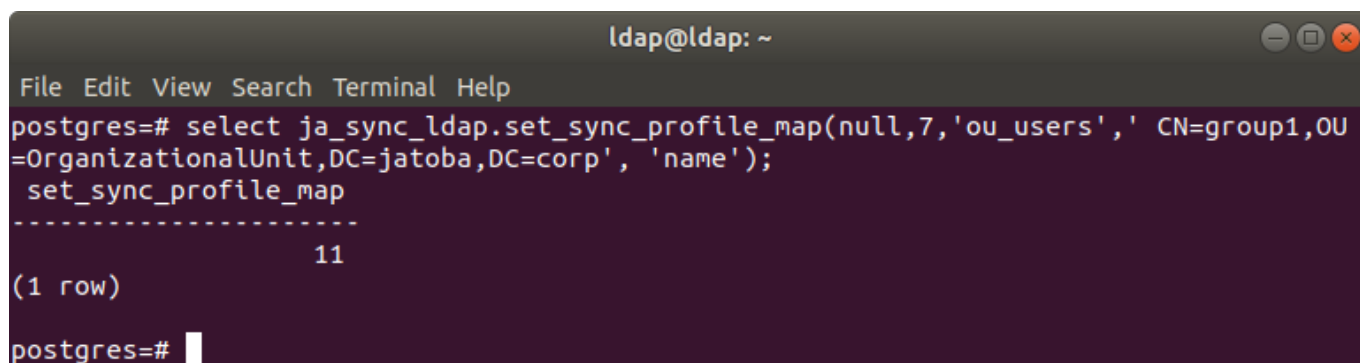


Рисунок 5.32 – Атрибут «DistinguishedName» группы «group1»

Полученные параметры используются для формирования SQL-команды, которая будет следующей:

```
SELECT ja_sync_ldap.set_sync_profile_map(null,7,'ou_users','  
CN=group1,OU=OrganizationalUnit,DC=jatoba,DC=corp','name');
```



The screenshot shows a terminal window titled 'ldap@ldap: ~'. The terminal has a menu bar with 'File Edit View Search Terminal Help'. The command entered is: `postgres=# select ja_sync_ldap.set_sync_profile_map(null,7,'ou_users',' CN=group1,OU=OrganizationalUnit,DC=jatoba,DC=corp','name');`. The output shows the function name `set_sync_profile_map` followed by a dashed line and the value `11`. Below this, it says `(1 row)`. The prompt `postgres=#` is visible at the bottom.

Рисунок 5.33 – Создание соответствия групп для OU

СУБД выведет ID созданного маппинга (`map_id`) (см. табл. 4.7).

В данной SQL-команде указано:

- `null` (`in_map_id`) – идентификатор соответствия групп, т.е. присвоение нового значения;
- `4` (`in_profile_id`) – идентификатор профиля синхронизации, который был получен при создании профиля синхронизации (см. п. 5.2.1) и проверен при выводе списка профилей синхронизации (см. п. 5.2.2);
- `ou_users` (`role_bd`) – созданная в СУБД групповая роль;
- `'CN=group1,OU=OrganizationalUnit,DC=jatoba,DC=corp'` (`in_domain_group`) – путь к каталогу подразделения «OrganizationalUnit», в которую входит глобальная группа безопасности «group1» в MS AD;
- `name` (`in_attribute`) – имя атрибута записи в AD, который содержит имя пользователя (см. рис. 5.34).

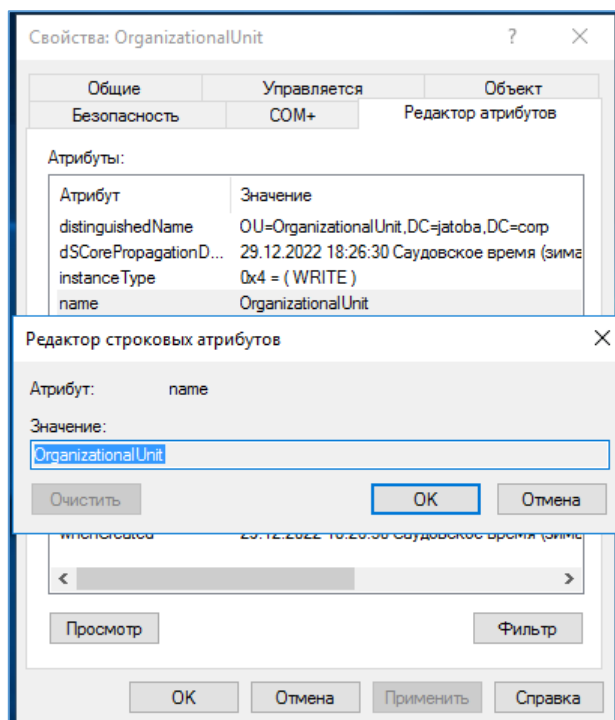


Рисунок 5.34 – Атрибут «name» подразделения в MS AD

5.3.4. Просмотр соответствия групп

Просмотреть соотнесенные к профилю синхронизации профили соответствия групп можно командой:

```
select ja_sync_ldap.get_sync_profiles();
```

5.3.5. Синхронизация

Синхронизация осуществляется командой:

```
select ja_sync_ldap.ldap_synchronize_jds(7);
```

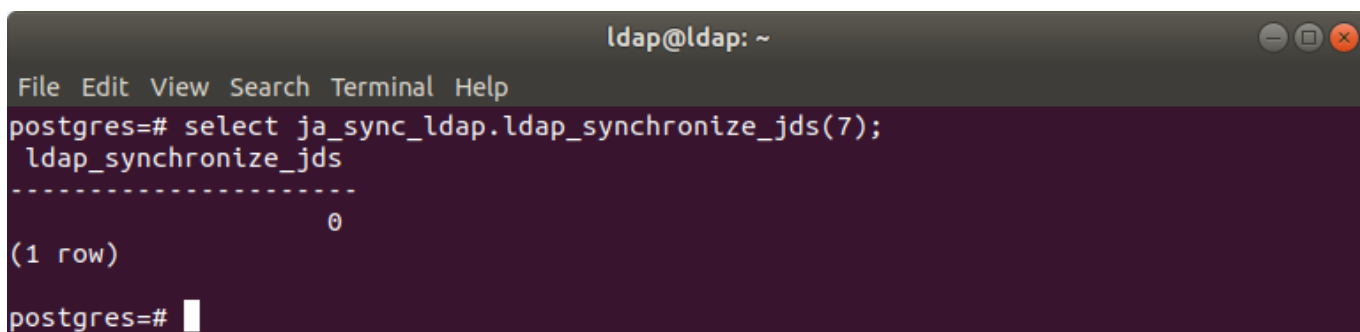


Рисунок 5.35 – Синхронизация УЗ AD с СУБД

В которой указывается ID-профиля синхронизации.

При просмотре списка пользователей видно, что учетные записи пользователей из глобальной группы безопасности «group1» были синхронизированы в СУБД в групповую роль «ad_users».

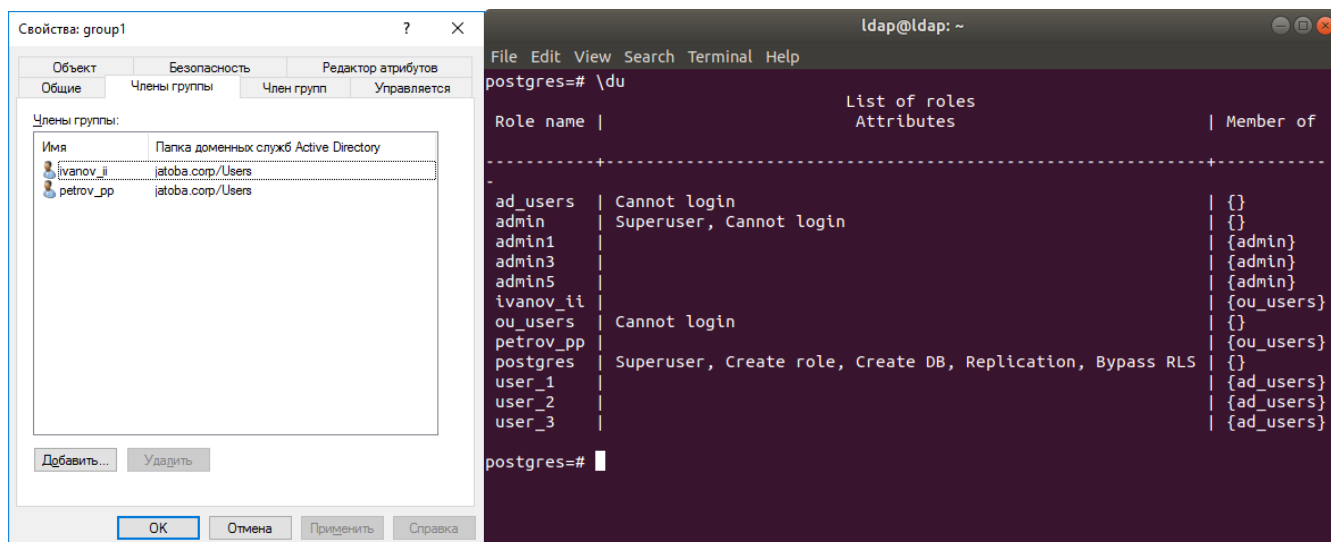


Рисунок 5.36 – Результат синхронизации пользователей подразделения «OrganizationalUnit»



Для вывода информации о членстве в ролях, с указанием всех параметров и прав доступа, в СУБД «Jatoba» с версией ядра 6 используется команда \drg

5.3.6. Авторизация после синхронизации по атрибуту 'name'

Для авторизации через синхронизированных пользователей по механизму LDAP требуется отредактировать конфигурационный файл pg_hba.conf:

```
host all all 10.96.1.0/24 ldap ldapserver=10.96.1.200
ldapbasedn="CN=group1,OU=OrganizationalUnit,DC=jatoba,DC=corp"
ldapbinddn="CN=admin,CN=Users,DC=jatoba,DC=corp"
ldapbindpasswd="P@ssword" ldapsearchattribute="name"
```



Рисунок 5.37 – Конфигурационный файл pg_hba.conf для аутентификации по атрибуту 'name'

В конфигурационном файле, в столбце «ADDRESS» указываем подсеть, от которой СУБД будет принимать соединения с методом аутентификации LDAP. В приводимом примере это подсеть 10.96.1.0, с маской подсети 255.255.255.0, т.е. с длиной префикса /24.

После чего последовательно указываются параметры:

- ldapserver – IP - адрес сервера AD:

```
ldapserver=10.96.1.200
```

При создании профиля синхронизации параметр указывался как «in_host_ip» (см. таб. 4.1).

- ldapbasedn – адрес каталога пользователей:

```
ldapbasedn="CN=group1,OU=OrganizationalUnit,DC=jatoba,DC=corp"
```

• ldapbinddn – адрес каталога администратора AD, который указывался в профиле синхронизации. Указывается не имя администратора AD в параметре «in_login», а именно путь к его каталогу.

```
ldapbinddn="CN=admin,CN=Users,DC=jatoba,DC=corp"
```

В MS AD это атрибут учетной записи пользователя AD «distinguishedName», который возможно получить в вкладке «Редактор атрибутов» карточки пользователя.

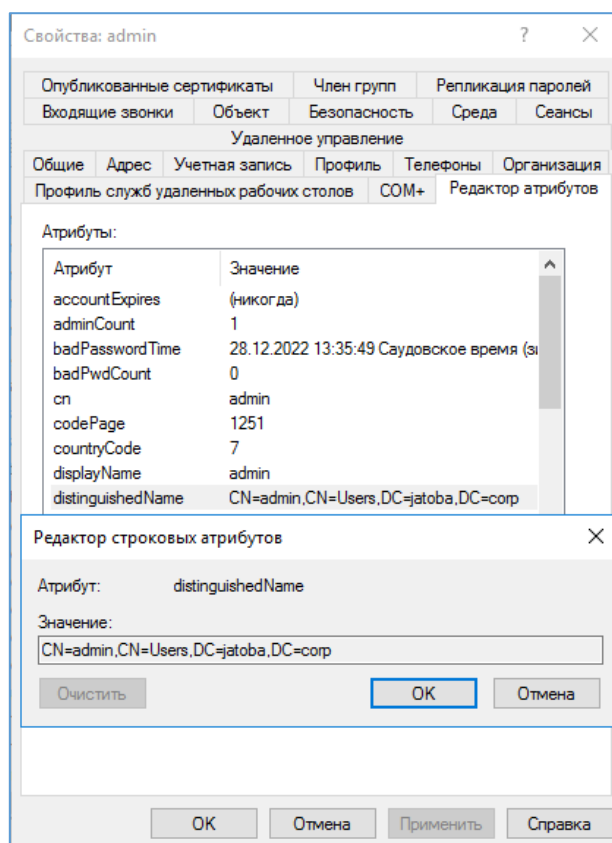


Рисунок 5.38 – Атрибут «distinguishedName»

- ldapbindpasswd – пароль администратора AD. В профиле синхронизации это параметр «in_pswd» (см. таб. 4.1);
- ldapsearchattribute – атрибут для соотнесения с именем пользователя в ходе аутентификации:

```
ldapsearchattribute="name"
```

После проделанного шага необходимо авторизоваться в СУБД через LDAP:

```
psql -h 10.96.1.100 -p 5432 -d postgres -U ivanov_ii
```

5.4. Изменения профиля синхронизации

При изменении существующего профиля требуется указать уникальное значение идентификатора профиля (profile_id), далее прописать параметры, как при создании профиля, при этом указывая изменяемые значения.

Имя профиля (profile_name) возможно изменить, но нельзя использовать одноименные профили, т.к. этот параметр уникален.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Например

Выведем список существующих профилей.

```
select ja_sync_ldap.get_sync_profiles();
```

Из вывода очевидно, что IP-адрес сервера указан некорректно. Указана 10-я подсеть, а должна быть 102-я

Изменяем IP-адрес сервера, формируя SQL-команду, в которой выберем профиль с profile_id равным 2.

```
SELECT  
ja_sync_ldap.set_sync_profile(2,'ad_users','10.116.102.46','389',  
'admin_ad','P@ssword','activedirectory');
```

```
root@admin1: /home  
postgres=# select ja_sync_ldap.get_sync_profiles();  
               get_sync_profiles  
-----  
(1,user,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)  
(2,ad_users,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)  
(2 rows)  
  
postgres=# SELECT ja_sync_ldap.set_sync_profile(2,'ad_users','10.116.102.46','389',  
admin_ad','P@ssword','activedirectory');  
      set_sync_profile  
-----  
                2  
(1 row)  
  
postgres=# select ja_sync_ldap.get_sync_profiles();  
               get_sync_profiles  
-----  
(1,user,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)  
(2,ad_users,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)  
(2 rows)  
  
postgres=#
```

Рисунок 5.39 – Изменение параметров профиля синхронизации

5.5. Изменение соответствия групп

При изменении существующего соответствия групп требуется указать уникальные значения идентификаторов соответствия (map_id) и профиля (profile_id), далее прописать параметры, как при создании соответствия групп, при этом указывая изменяемые значения.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

5.6. Удаление профиля

Для удаления существующего профиля используется SQL-команда:

```
select ja_sync_ldap.drop_sync_profile(in_profile_id int);
```

Например, при [in_profile_id=2](#), SQL-команда будет следующей:

```
select ja_sync_ldap.drop_sync_profile(2);
```

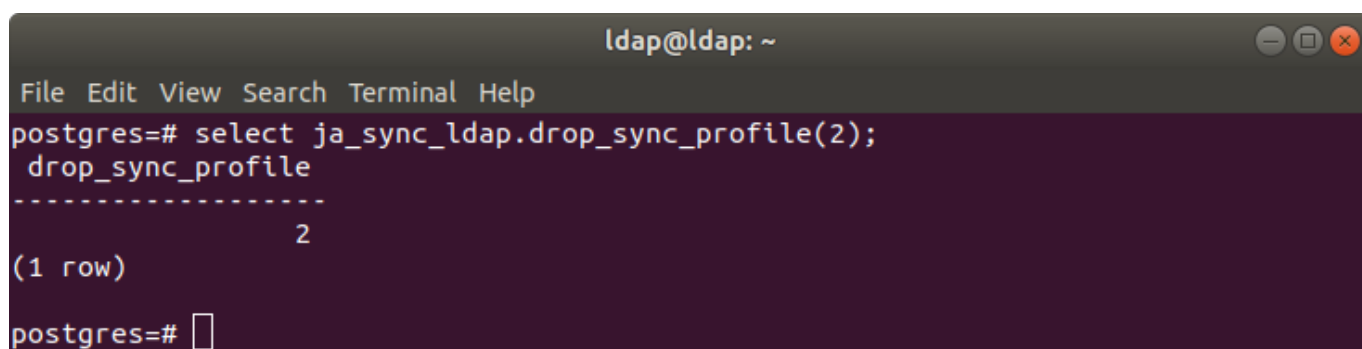


Рисунок 5.40 – Удаление профиля

Просмотрев существующие профили синхронизации, можно убедиться, что профиль синхронизации с `in_profile_id = 2` отсутствует.

5.7. Просмотр соответствия групп

Просмотреть связанные с профилем синхронизации профили соответствия групп можно командой:

```
select ja_sync_ldap.get_sync_profile_maps(3);
```

В результате сформируется таблица соответствия групп с тем идентификатором профиля, который был указан в команде.

Просмотреть все существующие соответствия групп можно командой:

```
select * from ja_sync_ldap.map;
```

5.8. Удаление соответствия групп

Подробно синтаксис SQL-команды описан в п. 4.2.3.

Профилю синхронизации с `profile_id` равным 4, соответствует группа с `map_id` равным 4. В качестве примера удалим соответствие групп `map_id` равным 4.

Удаление соответствия групп происходит командой:

```
select ja_sync_ldap.drop_sync_profile_map(4);
```

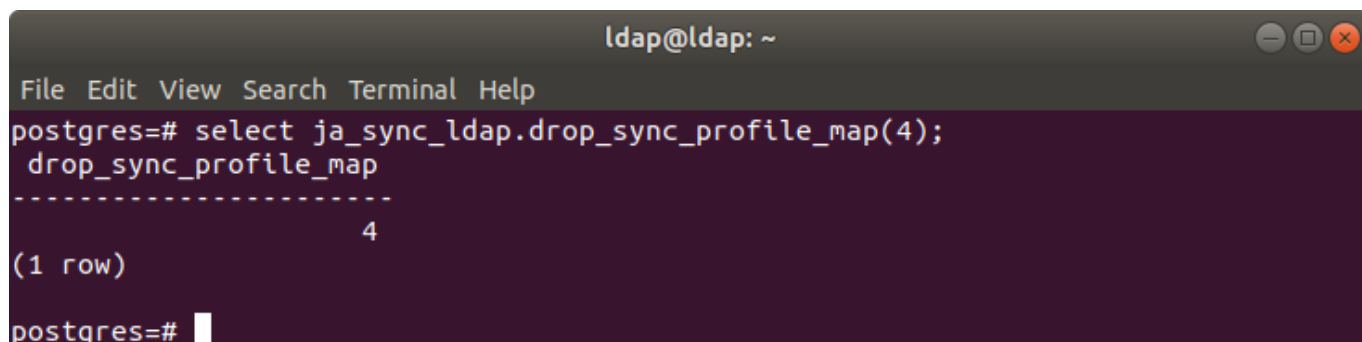


Рисунок 5.41 – Удаление соответствия групп

Можно убедиться, что профиль с `map_id=4` удален, через команду выведения списка соответствия групп

5.9. Просмотр событий безопасности

Для просмотра событий безопасности необходимо ввести команду:

```
select * from ja_sync_ldap.get_sync_log(from_date ::date,  
to_date ::date, row_count int);
```

Подробно синтаксис SQL-команды описан в п. 4.4.1.

В рассматриваемом примере указывается:

- 2019-01-01 (`from_date`) – дата начала периода;
- 2030-12-30 (`to_date`) – конец периода;
- 100 - `row_count` – количество выводимых записей.

```
select * from ja_sync_ldap.get_sync_log('2019-01-  
01'::date, '2030-12-30'::date, 100);
```

5.10. Удаление строки из журнала событий

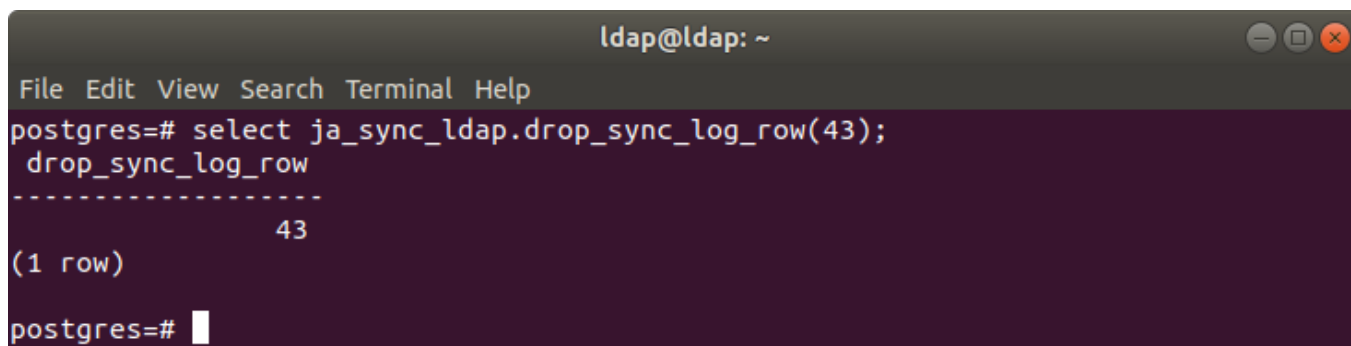
Удаление одной определенной строки происходит следующей командой:

```
select ja_sync_ldap.drop_sync_log_row(row_id int);
```

Подробно синтаксис SQL-команды описан в п. 4.4.2.1.

В качестве примера удалим строку №43:

```
select ja_sync_ldap.drop_sync_log_row(43);
```



The screenshot shows a terminal window titled 'ldap@ldap: ~'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command prompt is 'postgres=#'. The user enters the command 'select ja_sync_ldap.drop_sync_log_row(43);'. The output shows a single row with the value '43'. The prompt then returns to 'postgres=#'.

Рисунок 5.42 – Удаление одной строки

Для проверки выведем список событий безопасности и убедимся, что строка №43 отсутствует:

```
select * from ja_sync_ldap.get_sync_log('2019-01-01'::date, '2030-12-30'::date, 100);
```

5.11. Удаление выбранных строк из журнала событий

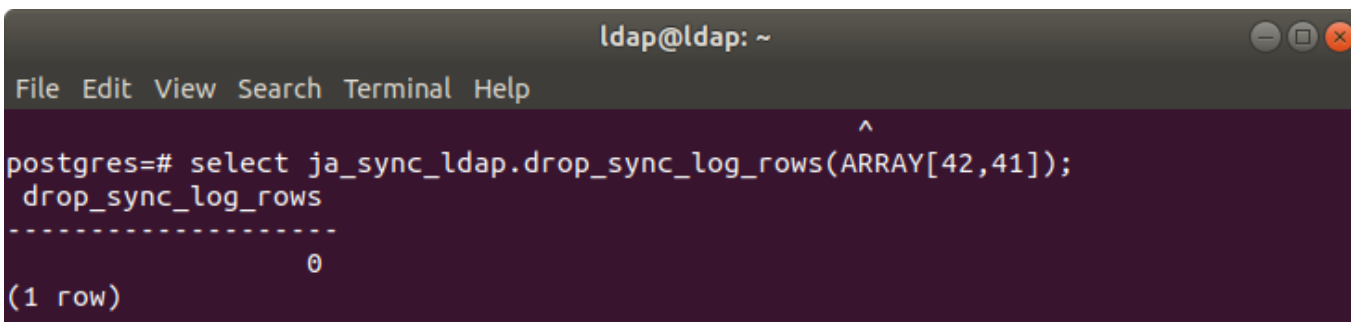
Удаление нескольких строк происходит следующей командой:

```
SELECT ja_sync_ldap.drop_sync_log_rows(row_id int[]);
```

Подробно синтаксис SQL-команды описан в п.4.4.2.2.

В качестве примера удалим строки №42 и №41:

```
SELECT ja_sync_ldap.drop_sync_log_rows(ARRAY[42,41]);
```



The screenshot shows a terminal window titled 'ldap@ldap: ~'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command prompt is 'postgres=#'. The user enters the command 'select ja_sync_ldap.drop_sync_log_rows(ARRAY[42,41]);'. The output shows a single row with the value '0'. The prompt then returns to 'postgres=#'.

Рисунок 5.43 – Удаление нескольких строк

Для проверки выведем список событий безопасности и убедимся, что строки № 42, 41 отсутствуют:

```
SELECT * from ja_sync_ldap.get_sync_log('2019-01-01'::date, '2030-12-30'::date, 100);
```

5.12. Удаление всех строк из журнала событий

Удаление всех строк происходит следующей командой:

```
SELECT ja_sync_ldap.drop_sync_log_all;
```

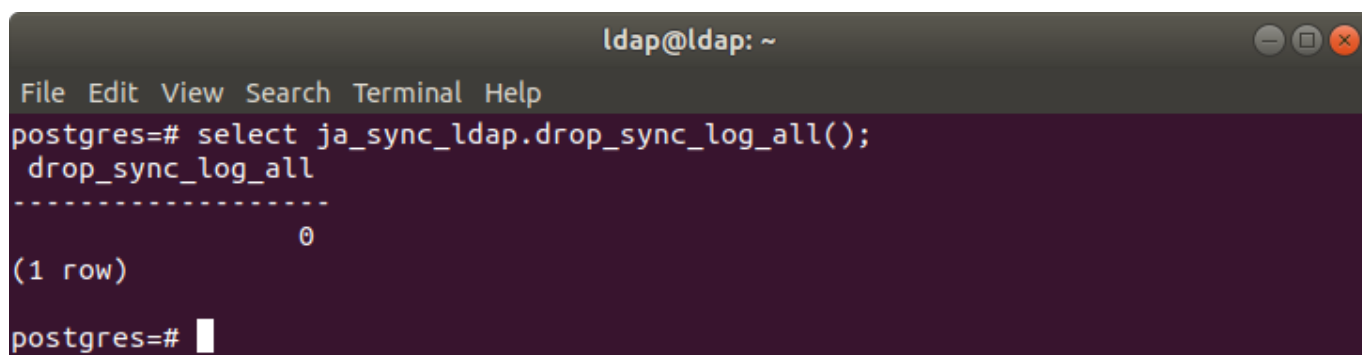


Рисунок 5.44 – Удаление всех строк

5.13. Синхронизация с сервером ALD Pro

В рассматриваемом примере синхронизации учетных записей пользователей сервера ALD Pro с СУБД «Jatoba» используются параметры сети, приведенные в таблице 5.4.

Таблица 5.4 – Конфигурация сети примера

№	Имя сервера	ОС	IP-адрес	Маска подсети	Роль
1	alt9caFreeIPA.FreeIPA.local	Альт Linux 9	10.116.102.48	255.255.255.0	Сервер службы каталогов
2	ja_Sync_Ldap	Ubuntu	10.116.101.105	255.255.255.0	Сервер СУБД

5.13.1. Настройка сервера СУБД

Настройка синхронизации учетных записей пользователей состоит из следующих шагов:

- Выполнить установку компонента (п. 3.1).
- Настроить конфигурационный файла «postgresql.conf» (п. 3.2).

- Создать расширение ja_Sync_LDAP:

```
CREATE EXTENSION ja_sync_ldap;
```

- Получить параметр «host» на сервере ALD Pro.

На сервере ALD Pro взять параметр «host» из конфигурационного файла:

```
/etc/ipa/default.conf
```



Рисунок 5.45 – Параметр «host» конфигурационного файла default.conf

- На сервере СУБД открыть файл «hosts» и внести строку с IP-адресом и параметром «host» сервера ALD Pro.

Например

```
10.116.101.105      dc.ald.local
```

Для GNU/Linux выполнить команду редактирования конфигурационного файла:

```
nano /etc/hosts
```

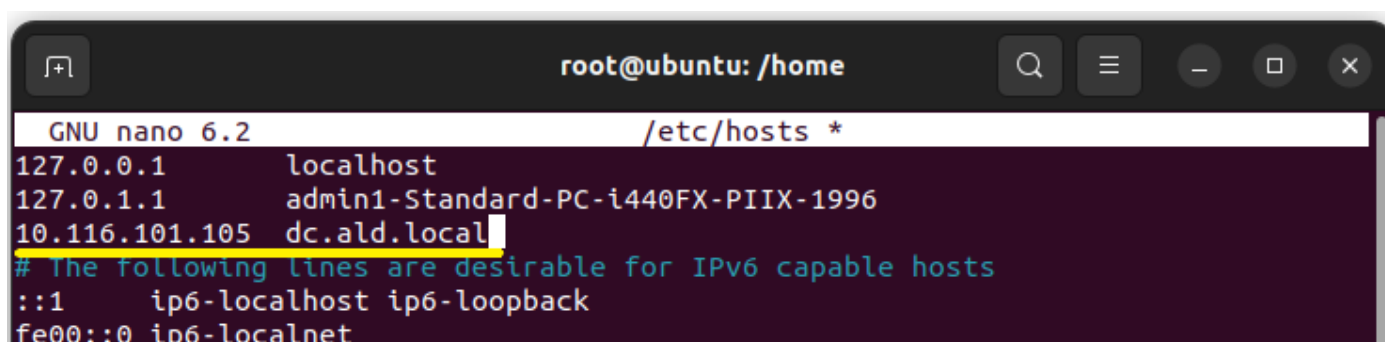


Рисунок 5.46 – Конфигурационный файл «hosts» в GNU/Linux

Внести указанные значения выше.

5.13.2. Настройка сервера ALD Pro

Первоначальная настройка сервера ALD Pro состоит из следующих шагов:

- открыть в браузере страницу сервера каталогов ALD Pro;

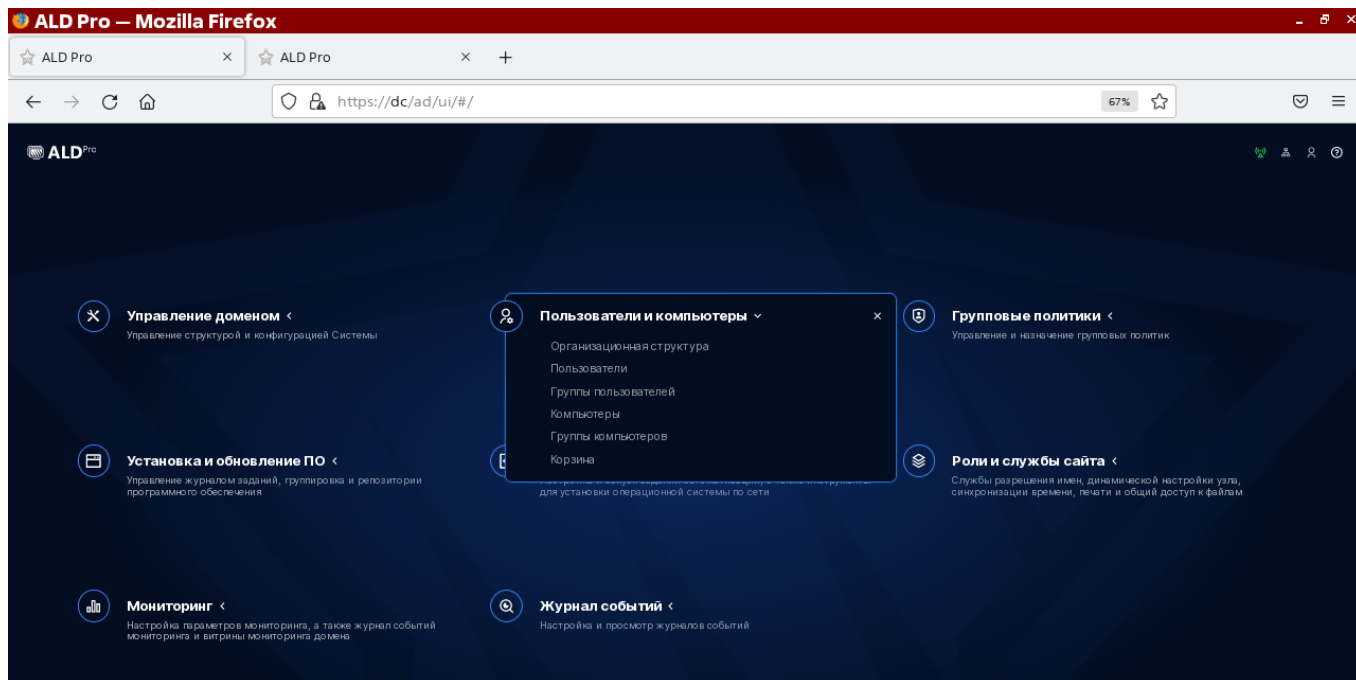


Рисунок 5.47 – Страница сервера каталогов ALD Pro

- перейти на вкладку «Группы Пользователей»;

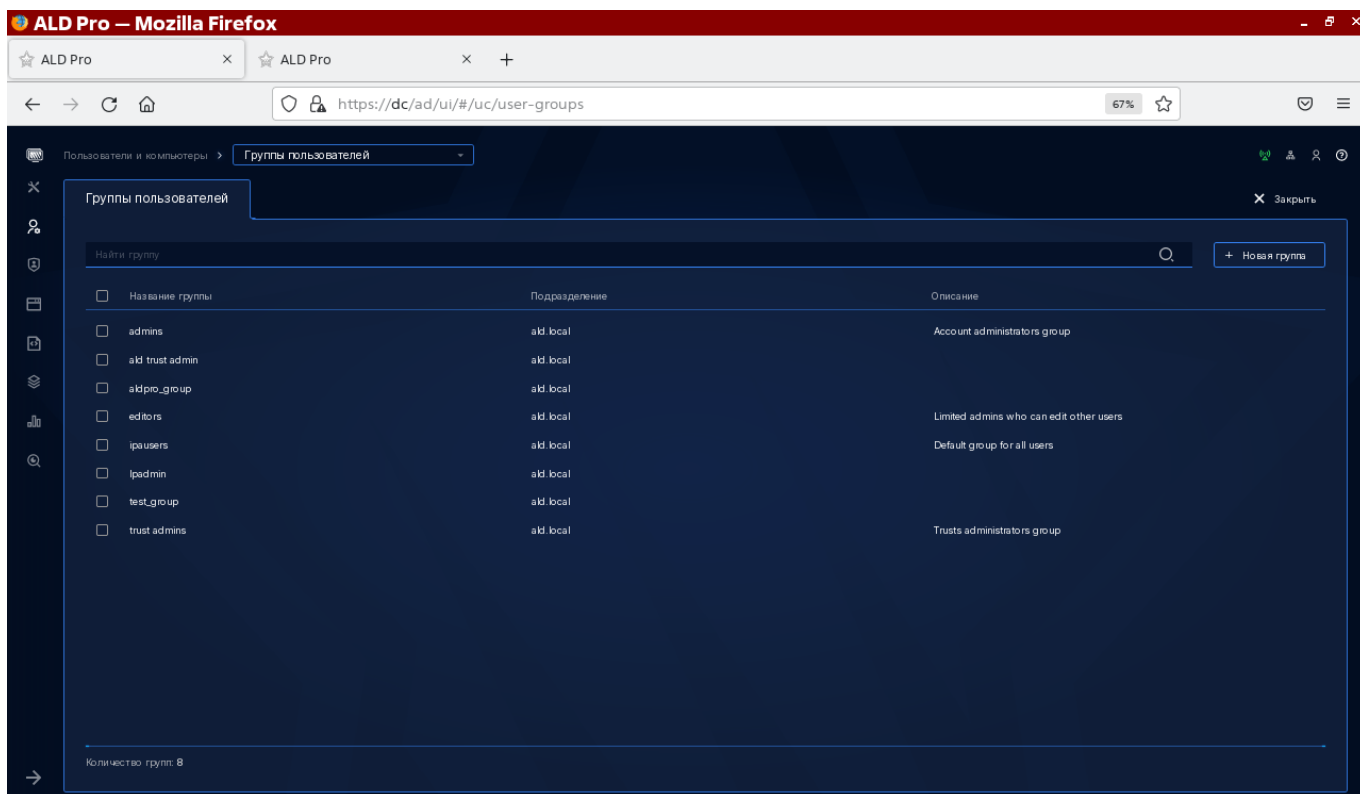


Рисунок 5.48 – Вкладка «Группы пользователей»

- создать группу пользователей, нажав кнопку «Новая группа».

На вкладке в строку «Название группы» внести имя создаваемой группы. В рассматриваемом примере создается «ldap_group».

В поле «Подразделение» в выпадающем списке выбрать требуемое подразделение.

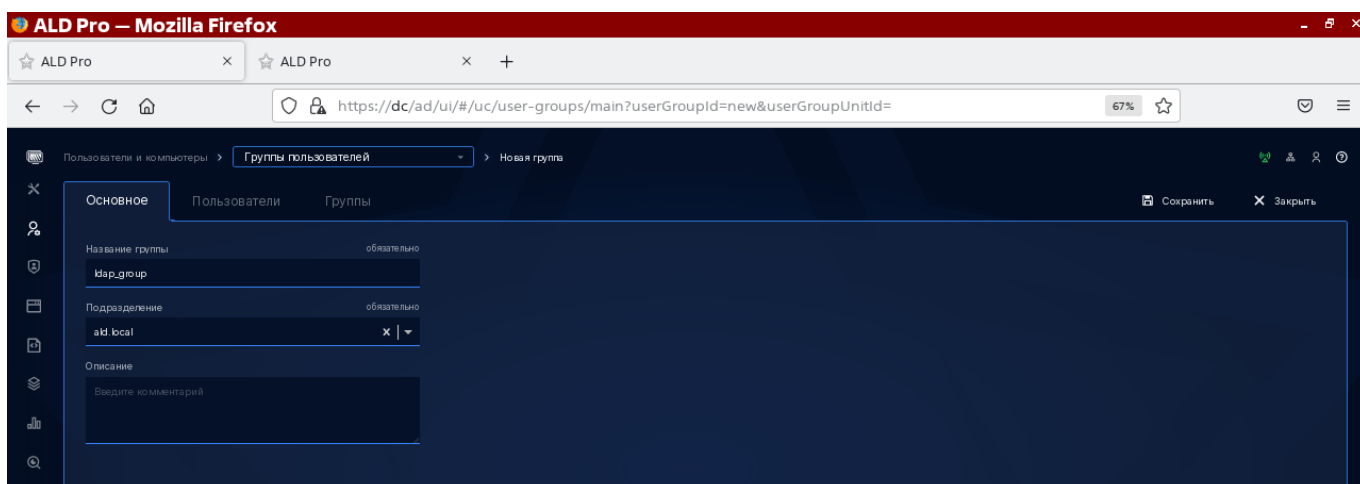


Рисунок 5.49 – Создание «Группы пользователей»

5.13.2.1 Создание пользователей и включение их в группу

Создание пользователей производится на вкладке «Пользователи». При нажатии кнопки «Новый пользователь» открывается окно «Новый пользователь».

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

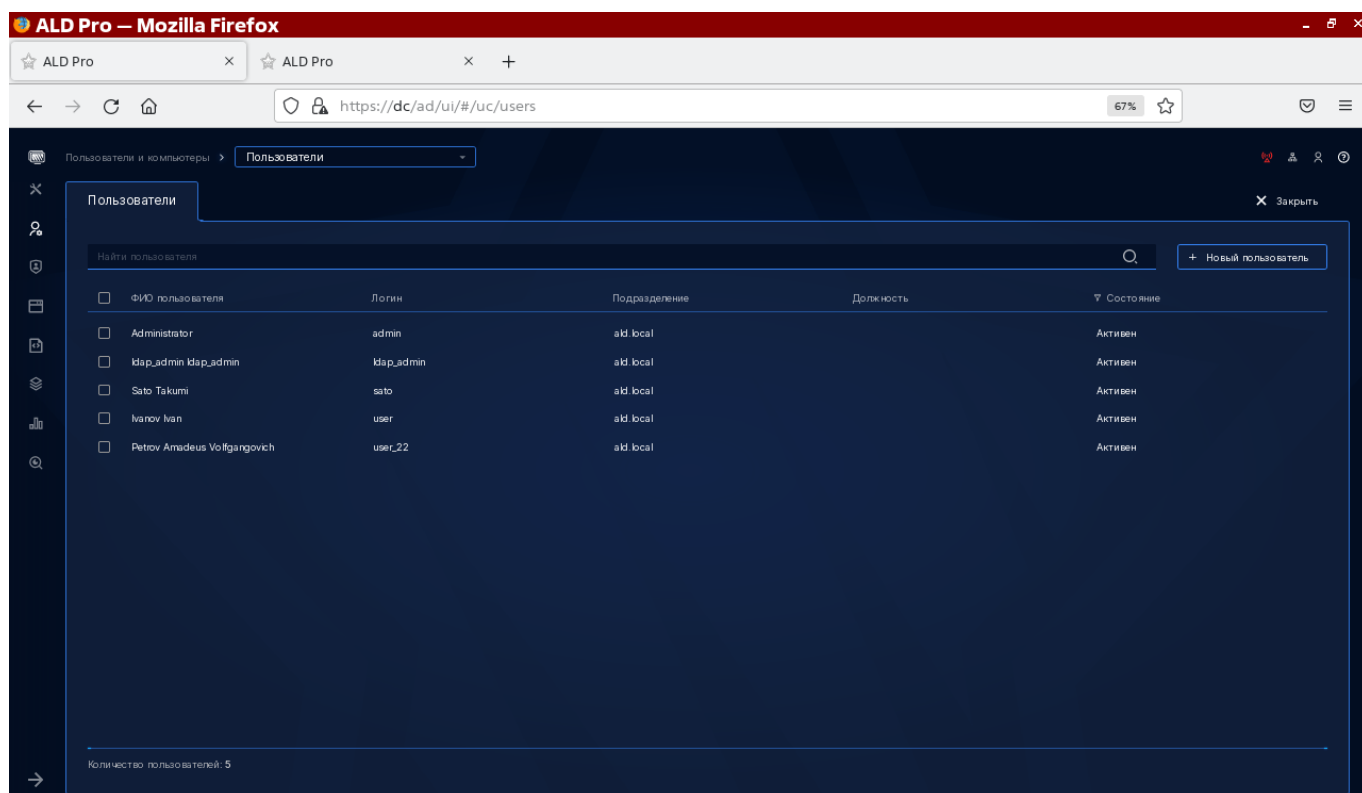


Рисунок 5.50 – Вкладка «Пользователи»

На вкладке «Новый пользователь» вносятся следующие данные:

- имя учетной записи;
- имя пользователя;
- фамилия;
- отчество (не обязательно);
- подразделение;
- пароль;
- подтверждение пароля.

Созданные или имеющиеся пользователи добавляются в созданную группу:

- путем выбора в окне «Все пользователи» пользователей, подлежащих синхронизации (рис. 5.51);

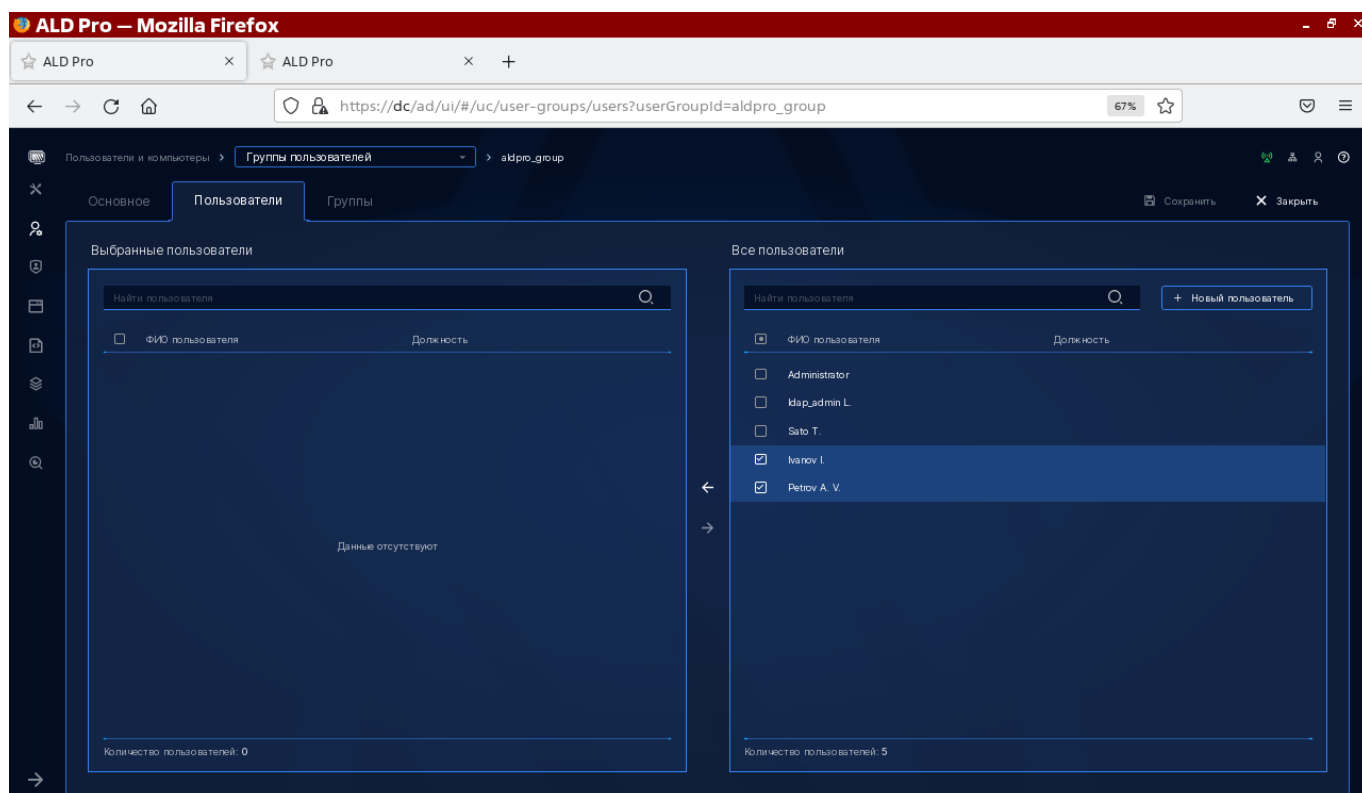


Рисунок 5.51 – Список пользователей

- добавлением их в окно «Пользователи» (рис. 5.52).

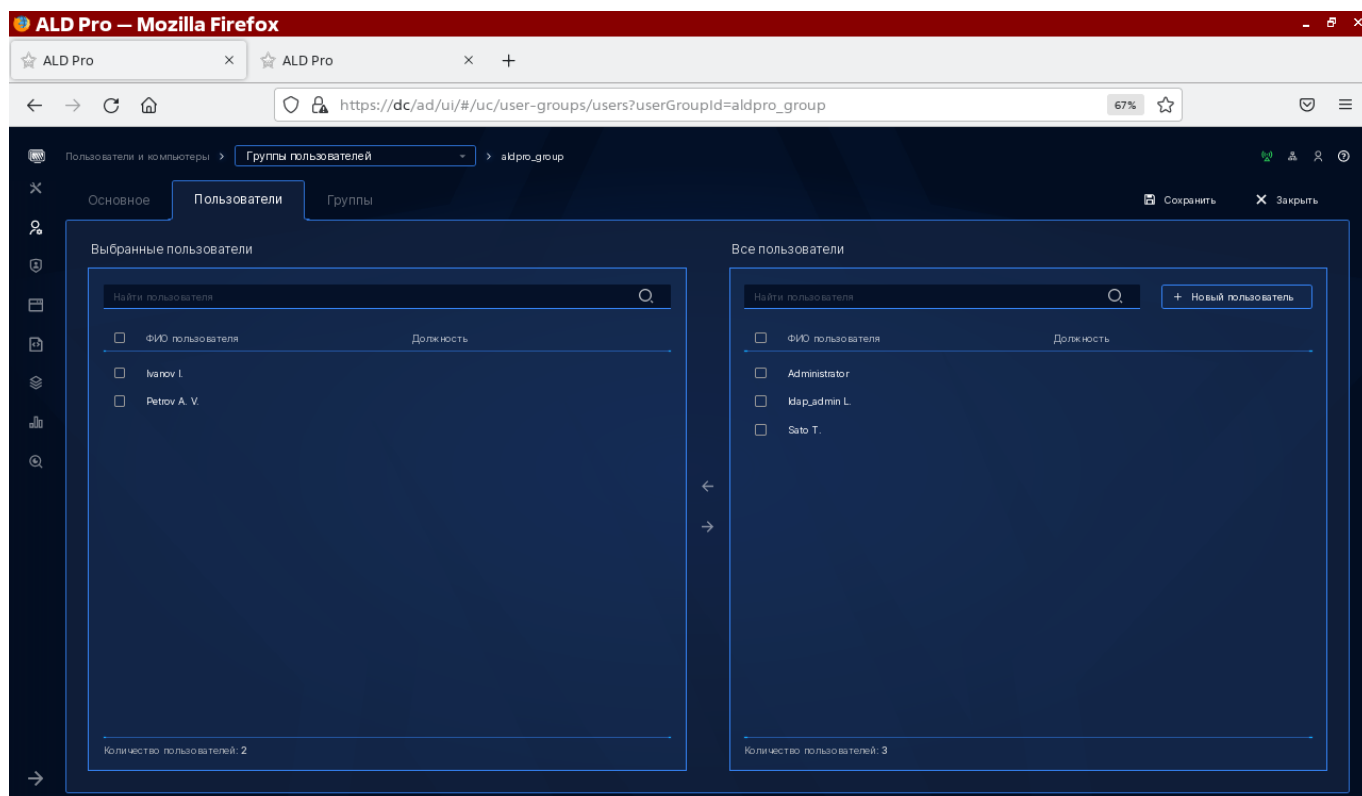


Рисунок 5.52 – Список группы пользователей

5.13.3. Создание нового профиля синхронизации

При создании профиля синхронизации потребуются два уникальных значения:

- Host;
- UID администратора сервера ALD Pro.

Значение «host» было получено из конфигурационного файла сервера ALD Pro

```
/etc/ipa/default.conf
```

Как было описано в п. 5.13.1 (см.рис. 5.45).

«UID» администратора сервера ALD Pro получается выполнением команды в терминале от имени и с правами «root»:

```
ldapsearch -x -LLL -b '<host ALD PRO>'  
' (&(objectClass=person) (uid=<имя_пользователя>)) '
```

В представляемом примере выполняется SQL-команда:

```
ldapsearch -x -LLL -b 'dc=ald,dc=local'  
' (&(objectClass=person) (uid=admin)) '
```



Рисунок 5.53 – Команда получения «UID» администратора сервера ALD Pro

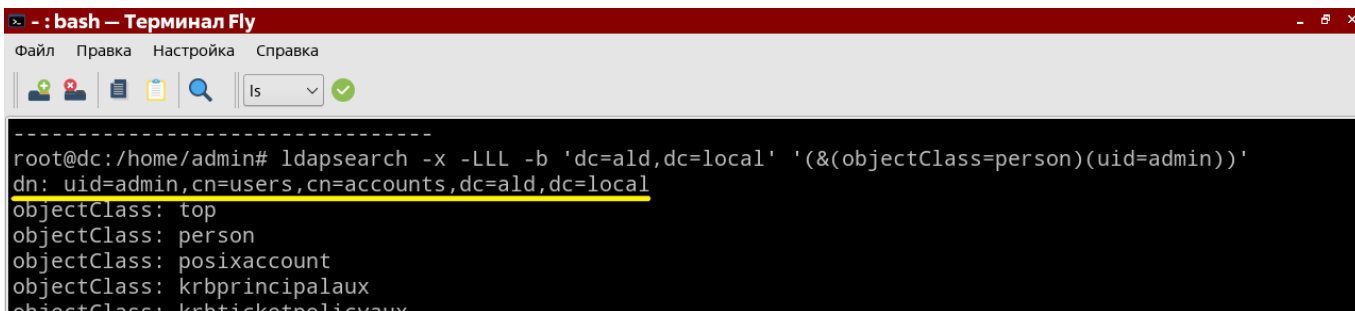


Рисунок 5.54 – «UID» администратора сервера ALD Pro

В результате получена строка «UID» администратора сервера ALD Pro, которая имеет следующий вид:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

```
uid=admin,cn=users,cn=accounts,dc=ald,dc=local
```

В зависимости от конкретной конфигурации сервера ALD Pro полученные значения будут отличаться.

Профиль синхронизации создается на сервере СУБД с установленным расширением «ja_sync_ldap» SQL-командой с синтаксисом:

```
select ja_sync_ldap.set_sync_profile(in_profile_id int,  
in_profile_name text, in_host_ip text, in_port text, in_login  
text, in_pswd text, in_domain_type text);
```

В таблице 5.5 приведены параметры, используемые для создания профиля для сервера ALD Pro.

Таблица 5.5 – Параметры и обозначения для создания профиля для сервера ALD Pro

Параметр	Тип данных	Обозначение
in_profile_id	int	идентификатор профиля
in_profile_name	text	имя профиля
in_host_ip	text	IP-адрес (или доменное имя) сервера ALD Pro
in_port	text	порт (по умолчанию 389)
in_login	text	UID администратора ALD Pro
in_pswd	text	Пароль от учетной записи администратора ALD Pro
in_domain_type	text	тип службы каталогов

Для параметра «in_domain_type» при создании профиля синхронизации сервера ALD Pro используется обязательное значение «aldpro».

В конкретном примере выполняется команда:

```
select  
ja_sync_ldap.set_sync_profile(null,'ald_users','10.116.101.105'  
, '389', '  
uid=admin,cn=users,cn=accounts,dc=ald,dc=local','Password',  
'aldpro');
```

```

root@ubuntu: /var/lib/jatoba/5/data
postgres=# select ja_sync_ldap.set_sync_profile(null,'ald_users','10.116.101.105',
', '389', ' uid=admin,cn=users,cn=accounts,dc=ald,dc=local', '12345678', 'aldpro');
set_sync_profile
-----
1
(1 row)
postgres=#
  
```

Рисунок 5.55 – Создание профиля синхронизации для сервера ALD Pro

5.13.4. Установка параметров SSL для профиля

Для установления SSL-соединения между сервером активного каталога ALD Pro и сервером СУБД, выполняются следующие действия:

- копирование сертификата с сервера ALD Pro;

На сервере ALD Pro сертификат «CA» находится в каталоге:

```
/etc/ipa/ca.crt
```

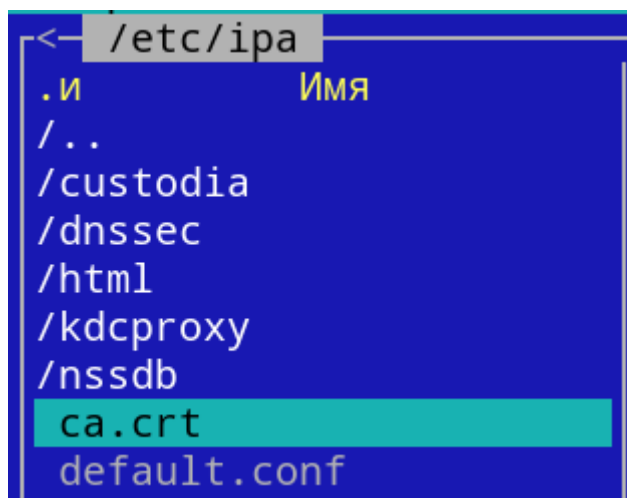


Рисунок 5.56 – Расположение файла сертификата на сервере ALD Pro

Для ОС GNU/Linux

Полученный сертификат копируется в любую директорию СУБД, на которую есть права у пользователя «postgres».

Например, в директорию:

```
/var/lib/jatoba/<версия>/
```

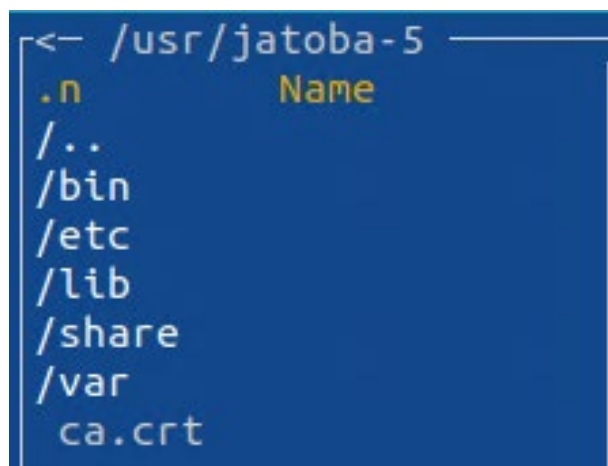


Рисунок 5.57 – Расположение файла сертификата на сервере СУБД

Назначить владельцем сертификата пользователя «postgres», выполнив команду в терминале:

```
chown postgres:postgres /путь/до/ca.crt
```

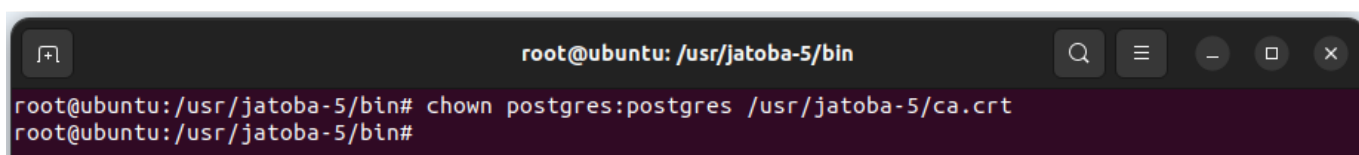


Рисунок 5.58 – Команда установки прав для пользователя «postgres»

Сертификат может быть добавлен к существующему профилю синхронизации, для чего в SQL-команде потребуется указать «Profile_ID», т.е. идентификатор профиля.

Указать список профилей SQL-командой:

```
select * from ja_sync_ldap.get_sync_profiles();
```

Получив «Profile_ID», добавить к профилю синхронизации путь до сертификата SQL-командой, имеющей синтаксис:

```
select ja_sync_ldap.set_ca_cert_profile(<Profile_ID>,  
'</путь/до/ca.crt>');
```

В рассматриваемом примере SQL-команда будет следующей:

```
select ja_sync_ldap.set_ca_cert_profile(1, '/usr/jatoba-  
5/ca.crt');
```

```

root@ubuntu: /var/lib/jatoba/5/data
postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl | ca_cert
-----+-----+-----+-----+-----+-----+-----+-----+-----
  1 | ald_users   | 10.116.101.105 | 389 | uid=admin,cn=users,cn=accounts,dc=ald,dc=local | 12345678 | aldpro | f |
(1 row)

postgres=# select ja_sync_ldap.set_ca_cert_profile(1, '/usr/jatoba-5/ca.crt');
 set_ca_cert_profile
-----
 1
(1 row)

postgres=#

```

Рисунок 5.59 – SQL-команда добавления сертификата к профилю синхронизации

При этом функция SSL-соединения останется выключенной. В поле «SSL» останется значение «f», т.е. «false».

```

root@ubuntu: /var/lib/jatoba/5/data
postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl | ca_cert
-----+-----+-----+-----+-----+-----+-----+-----+-----
  1 | ald_users   | 10.116.101.105 | 389 | uid=admin,cn=users,cn=accounts,dc=ald,dc=local | 12345678 | aldpro | f |
(1 row)

postgres=# select ja_sync_ldap.set_ca_cert_profile(1, '/usr/jatoba-5/ca.crt');
 set_ca_cert_profile
-----
 1
(1 row)

postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl | ca_cert
-----+-----+-----+-----+-----+-----+-----+-----+-----
  1 | ald_users   | 10.116.101.105 | 389 | uid=admin,cn=users,cn=accounts,dc=ald,dc=local | 12345678 | aldpro | f | /usr/ja
toba-5/ca.crt
(1 row)

postgres=#

```

Рисунок 5.60 – Вывод состояния SSL-соединения

5.13.5. Включение SSL-соединения для профиля синхронизации

Включение SSL-соединения для профиля синхронизации выполняется SQL-командой, имеющей синтаксис:

```
SELECT ja_sync_ldap.set_ssl_profile(<Profile_ID>, true);
```

В рассматриваемом примере выполняется SQL-команда:

```
SELECT ja_sync_ldap.set_ssl_profile(1, true);
```



```

root@ubuntu: /var/lib/jatoba/5/data
postgres=# select ja_sync_ldap.set_ssl_profile(1, true);
set_ssl_profile
-----
1
(1 row)

postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl |
-----+-----+-----+-----+-----+-----+-----+-----+
  1 | ald_users   | 10.116.101.105 | 389 | uid=admin,cn=users,cn=accounts,dc=ald,dc=local | 12345678 | aldpro | t | /usr/ja
toba-5/ca.crt>
(1 row)

postgres=#

```

Рисунок 5.61 – Включение SSL-соединения

При просмотре профилей синхронизации, функция SSL-соединения станет включенной. В поле «SSL» установится значение «t», т.е. «true».

Для выполнения синхронизации по SSL необходимо изменить порт в профиле на 636.

5.13.6. Отключение SSL-соединения для профиля синхронизации

Отключить SSL-соединение для профиля синхронизации возможно SQL-командой:

```
SELECT ja_sync_ldap.set_ssl_profile(<Profile_ID>, false);
```

5.13.7. Добавление соответствия групп

Добавление соответствия групп описано в п. 4.2 настоящего документа.

5.13.8. Выполнение синхронизации УЗ с сервером ALD Pro

Синхронизация учетных записей активного каталога с СУБД описана в п. 4.3 настоящего документа.

5.14. Синхронизация с сервером FreeIPA

В рассматриваемом примере синхронизации учетных записей пользователей сервера FreeIPA с СУБД «Jatoba» используются параметры сети, приведенные в таблице 5.6.

Таблица 5.6 – Конфигурация сети примера

№	Имя сервера	ОС	IP-адрес	Маска подсети	Роль
1	alt9caFreeIPA.FreeIPA.local	Альт Linux 9	10.72.9.11/24	255.255.255.0	Сервер службы каталогов
2	ja_Sync_Ldap	Ubuntu	10.72.9.12/24	255.255.255.0	Сервер СУБД

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

5.14.1. Настройка сервера СУБД

Настройка синхронизации учетных записей пользователей состоит из следующих шагов:

- выполнить установку компонента (п. 3.1).
- настроить конфигурационный файл «postgresql.conf» (п. 3.2).
- создать расширение ja_Sync_LDAP:

```
CREATE EXTENSION ja_sync_ldap;
```

- открыть файл hosts:

Для Linux выполнив команду:

```
gedit /etc/hosts
```

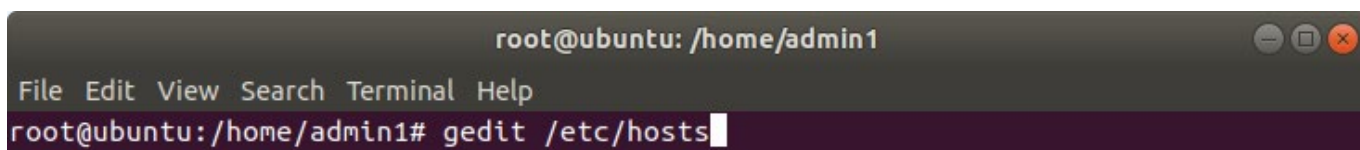


Рисунок 5.62 – Команда открытия конфигурационного файла /etc/hosts

Внести строку два значения и сохранить изменения.

```
10.72.9.11      alt9caFreeIPA.FreeIPA.local
```

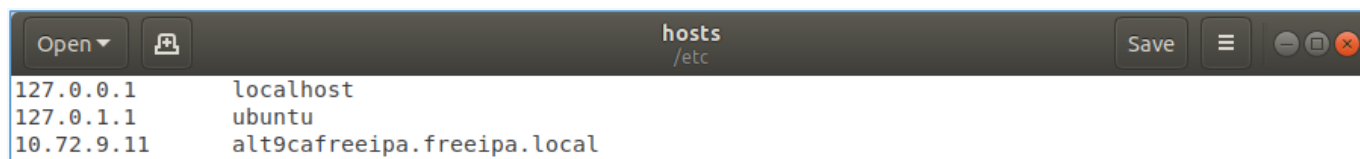


Рисунок 5.63 – Конфигурационный файл /etc/hosts

Первое значение – IP-адрес сервера FreeIPA.

Второе значение необходимо взять из параметра «host» конфигурационного файла «default.conf» сервера FreeIPA расположенного по пути:

```
/etc/ipa/default.conf
```

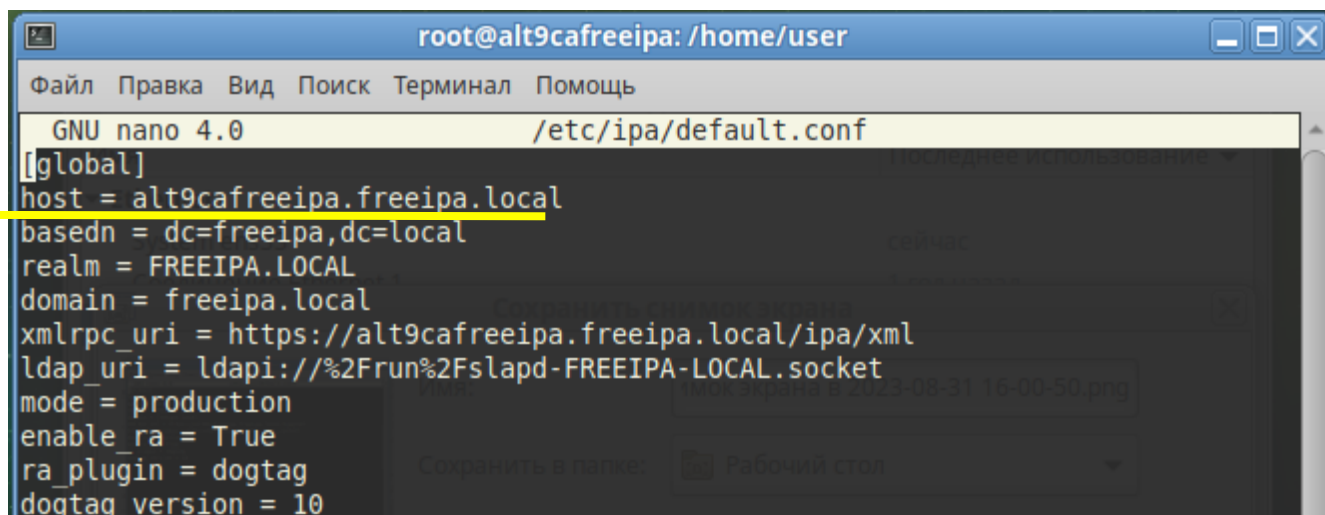



Рисунок 5.64 – Конфигурационный файл «default.conf» сервера FreeIPA

5.14.2. Настройка сервера FreeIPA

Первоначальная настройка сервера FreeIPA состоит из следующих шагов:

- открыть в браузере страницу сервера каталогов FreeIPA;

 Существует функциональная возможность автоматического обновления сертификатов ОС. Для чего от имени и с правами «root» в терминале выполняется команда:

```
ipa-cert-fix
```

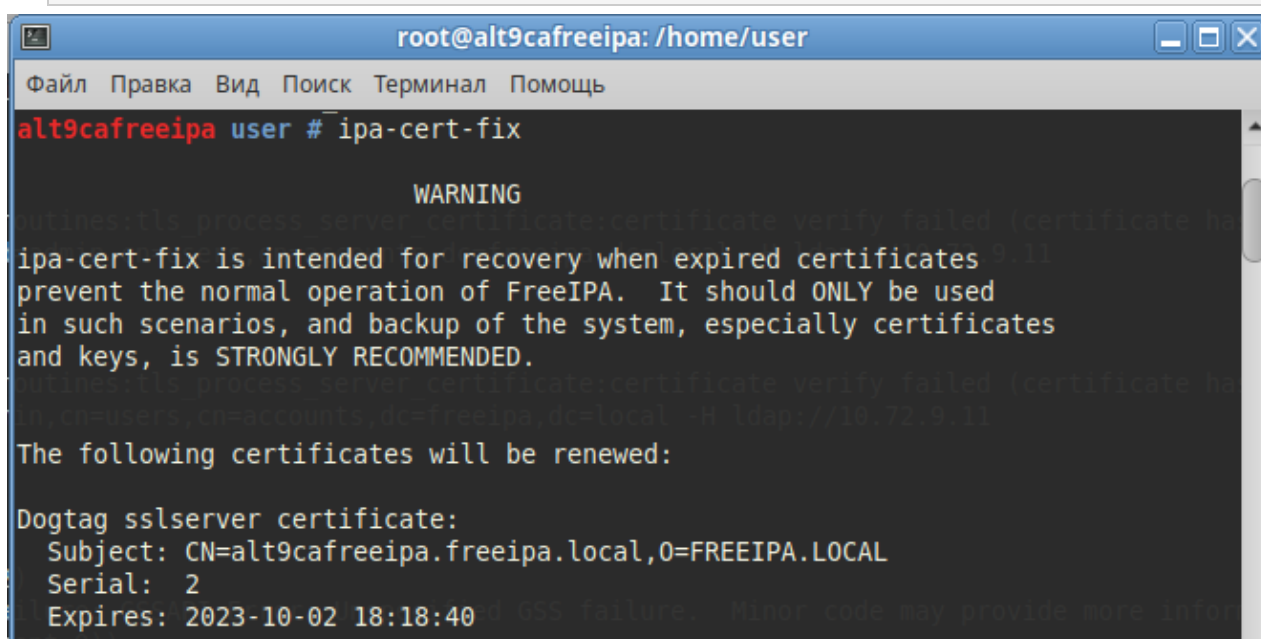


Рисунок 5.65 – Команда обновления сертификатов

ОС сама найдет просроченные сертификаты и при подтверждении, обновит их.

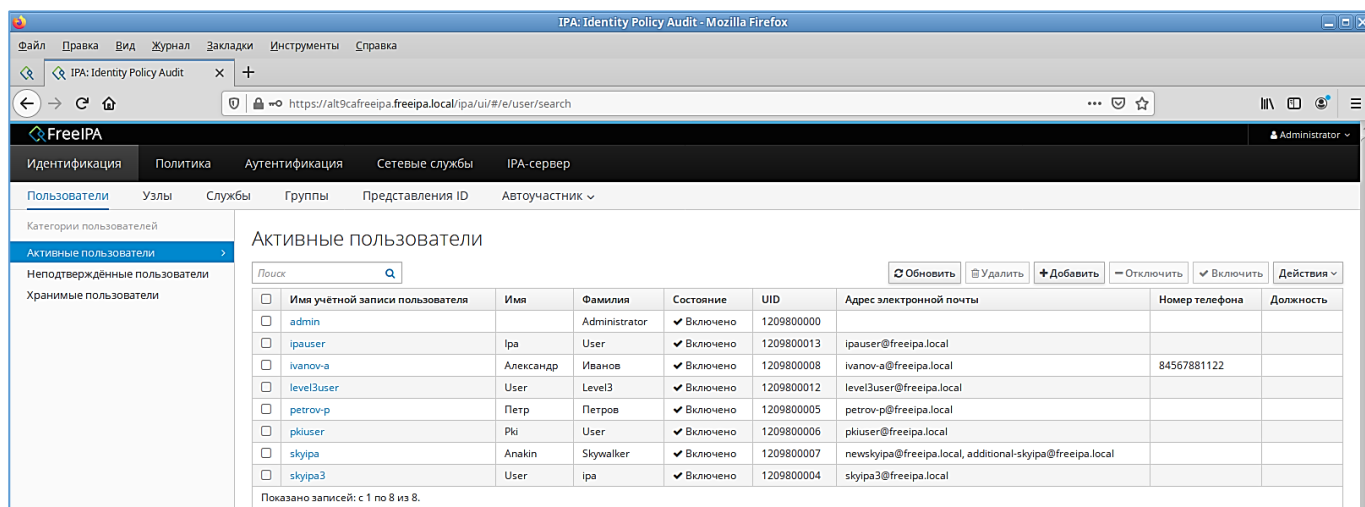


Рисунок 5.66 – Страница сервера каталогов FreeIPA

- перейти на вкладку «Группы»;

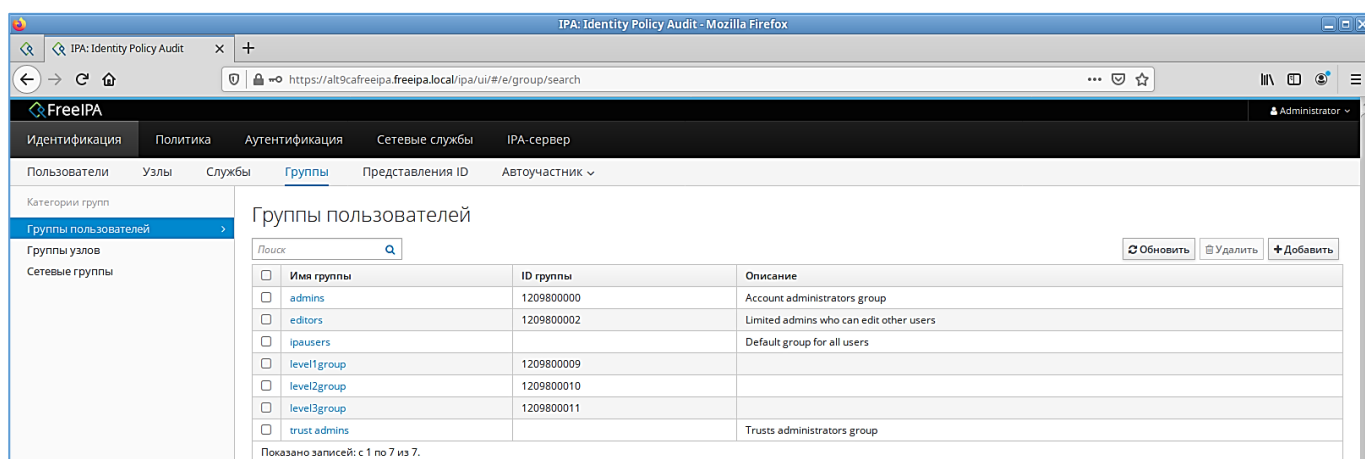


Рисунок 5.67 – Вкладка «Группы»

- создать группу пользователей, нажав кнопку «Добавить».

В окне «Добавить группу пользователей» в строку «Имя группы» внести имя группы, в которую будут входят учетные записи пользователей для синхронизации с СУБД. В рассматриваемом примере имя группы «user_db».

В поле «Тип группы» оставить значение по умолчанию «POSIX». ID будет установлено по умолчанию.

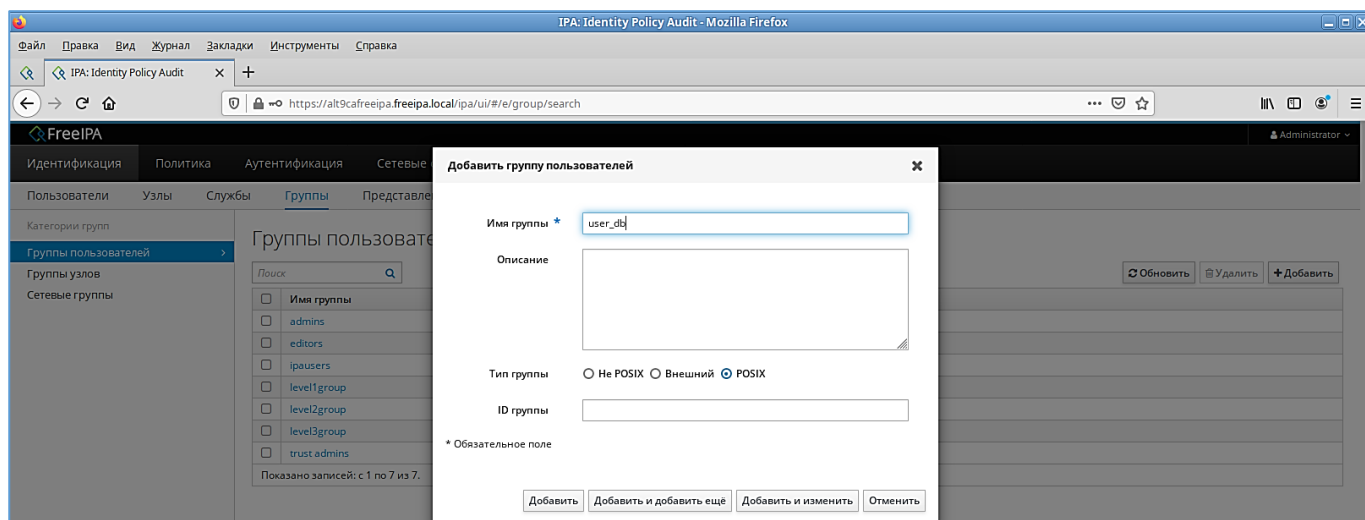


Рисунок 5.68 – Окно «Добавить группу пользователей»

5.14.2.1 Создание пользователей и включение их в группу

Пользователи создаются на вкладке «Пользователи». Для создания нового пользователя требуется нажать кнопку «Добавить», которая вызовет окно «Добавить пользователя».

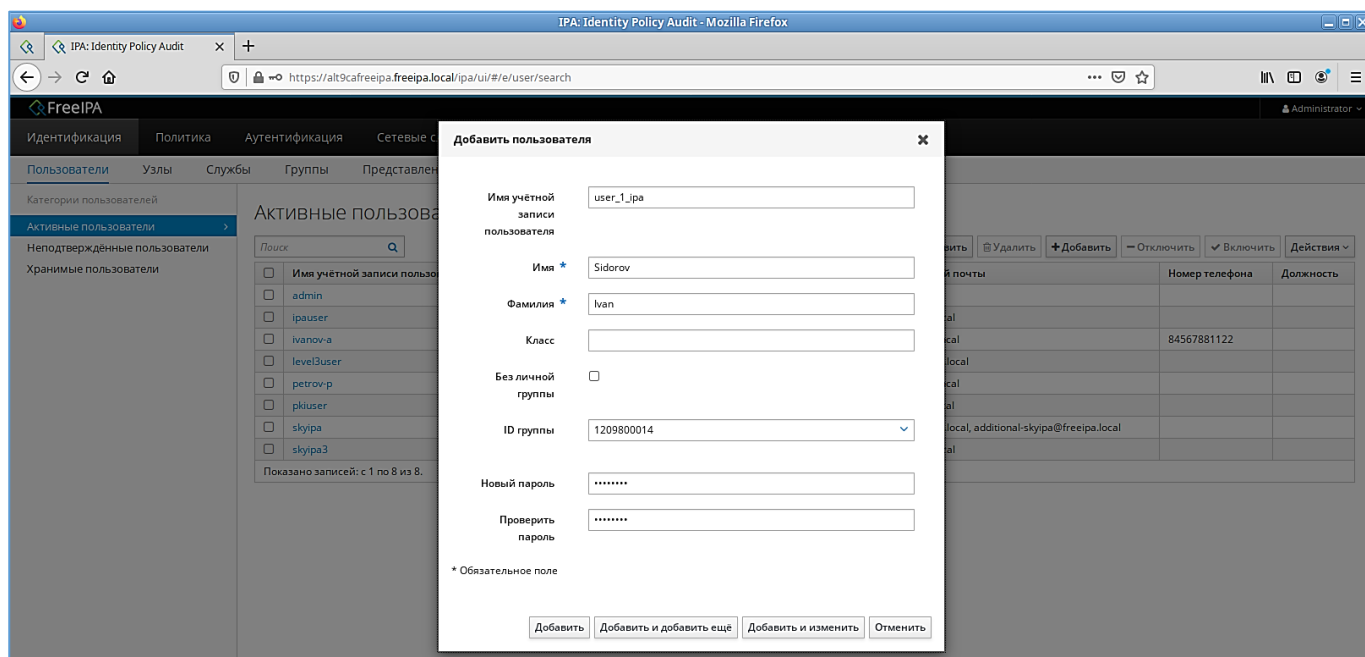


Рисунок 5.69 – Окно «Добавить пользователя»

В окне вносятся данные:

- имя учетной записи пользователя;
- имя;
- фамилия;

- ID группы;
- новый пароль;
- проверить пароль.

В выпадающем списке «ID группы» возможно сразу выбрать группу пользователей, в которую пользователь будет автоматически включен.

Если группа уже существует, то добавить в нее пользователя возможно:

- перейдя в вкладку «Группы»;

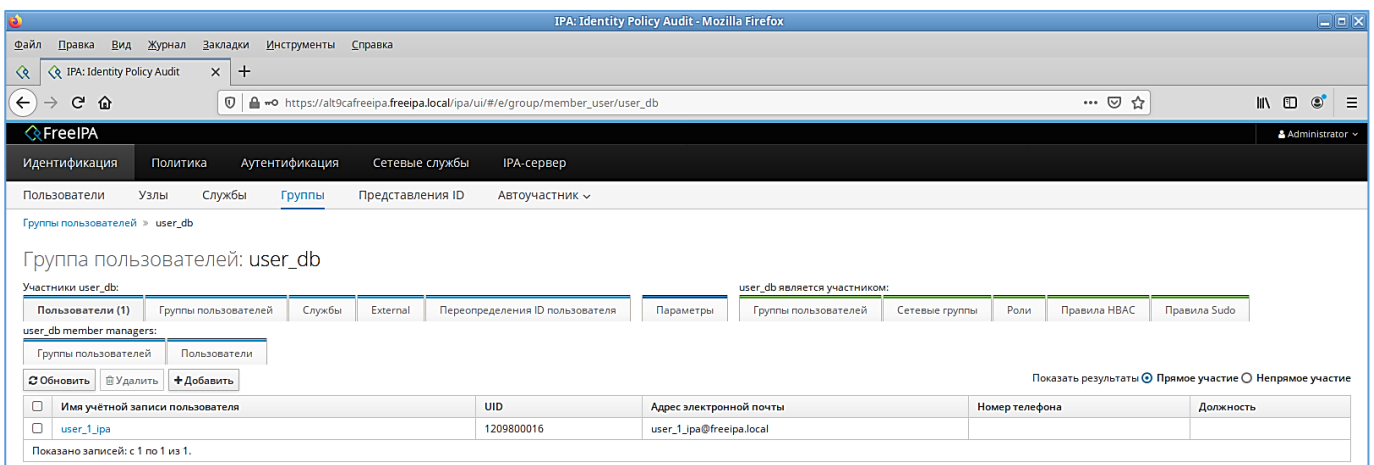


Рисунок 5.70 – Вкладка «Группы»

- нажать кнопку «Добавить»;
- в окне «Добавить пользователей в группу пользователей» установить флаги в строках требуемых учетных записей;

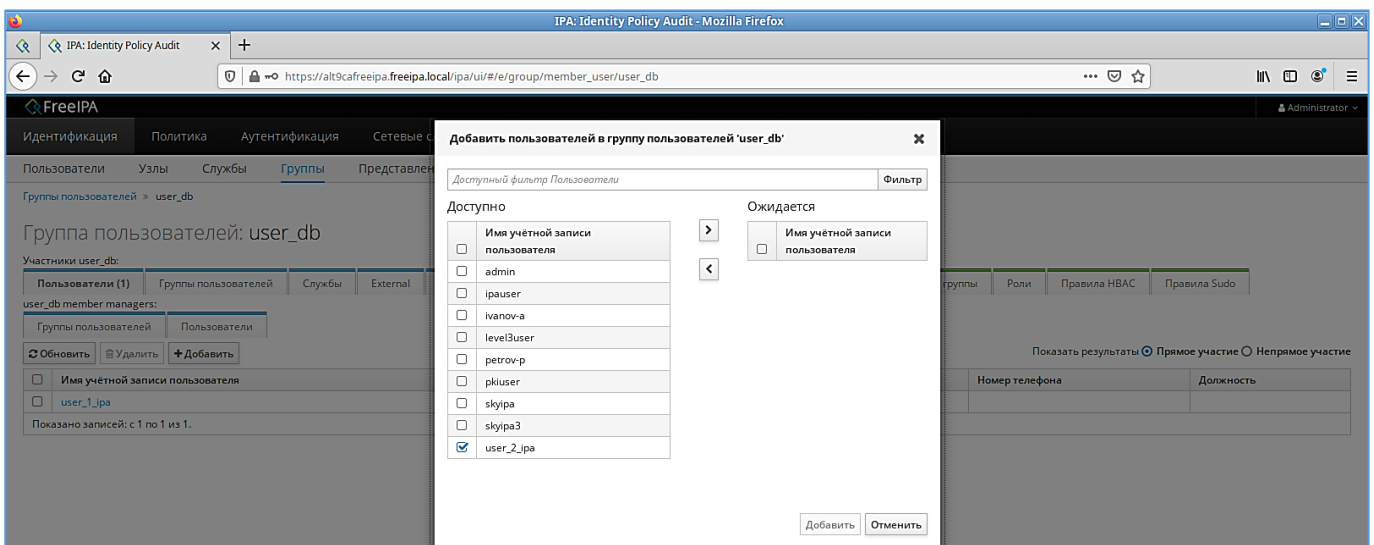


Рисунок 5.71 – Окно «Добавить пользователей в группу пользователей»

- из столбца «Доступно» перенести в столбец «Ожидается».

Рисунок 5.72 – Столбец «Ожидается» окна «Добавить пользователей в группу пользователей»

5.14.3. Создание профиля синхронизации

При создании профиля синхронизации потребуются два уникальных значения:

- Host;
- UID администратора сервера FreeIPA.

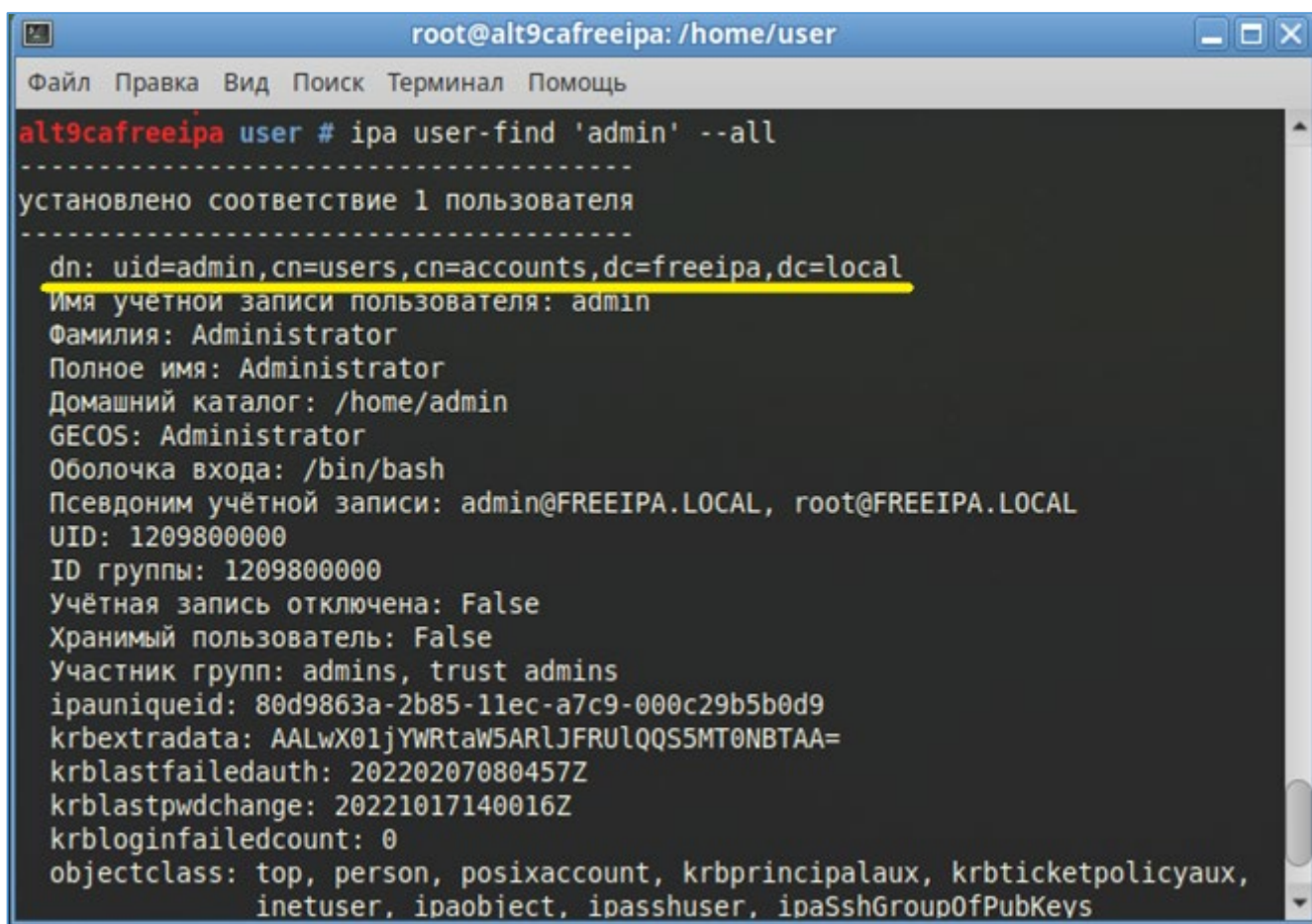
Значение «host» было получено из конфигурационного файла сервера FreeIPA

```
/etc/ipa/default.conf
```

Как было описано в п. 5.14.1 (см. рис. 5.64).

«UID» администратора сервера FreeIPA получается выполнением команды в терминале от имени и с правами «root»:

```
ipa user-find 'admin' --all
```

```
root@alt9cafreeipa: /home/user
Файл Правка Вид Поиск Терминал Помощь
alt9cafreeipa user # ipa user-find 'admin' --all
-----
установлено соответствие 1 пользователя
-----
dn: uid=admin,cn=users,cn=accounts,dc=freeipa,dc=local
Имя учетной записи пользователя: admin
Фамилия: Administrator
Полное имя: Administrator
Домашний каталог: /home/admin
GECOS: Administrator
Оболочка входа: /bin/bash
Псевдоним учётной записи: admin@FREEIPA.LOCAL, root@FREEIPA.LOCAL
UID: 1209800000
ID группы: 1209800000
Учётная запись отключена: False
Хранимый пользователь: False
Участник групп: admins, trust admins
ipauniqueid: 80d9863a-2b85-11ec-a7c9-000c29b5b0d9
krbextradata: AALwX01jYWRtaW5ARlJFRUlQQS5MT0NBTA=
krblastfailedauth: 20220207080457Z
krblastpwdchange: 20221017140016Z
krbloginfailedcount: 0
objectclass: top, person, posixaccount, krbprincipalaux, krbticketpolicyaux,
            inetuser, ipaobject, ipasshuser, ipaSshGroupOfPubKeys
```

Рисунок 5.73 – «UID» администратора сервера FreeIPA

В результате получена строка «UID» администратора сервера FreeIPA, которая имеет следующий вид:

```
uid=admin,cn=users,cn=accounts,dc=FreeIPA,dc=local
```

В зависимости от конкретной конфигурации сервера FreeIPA полученные значения будут отличаться.

Профиль синхронизации создается на сервере СУБД с установленным расширением «ja_sync_ldap» SQL-командой с синтаксисом:

```
select ja_sync_ldap.set_sync_profile(in_profile_id int,
in_profile_name text, in_host_ip text, in_port text, in_login
text, in_pswd text, in_domain_type text);
```

В таблице 5.5 приведены параметры, используемые для создания профиля для сервера FreeIPA.

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

Таблица 5.7 – Параметры и обозначения для создания профиля для сервера FreeIPA

Параметр	Тип данных	Обозначение
in_profile_id	int	идентификатор профиля
in_profile_name	text	имя профиля
in_host_ip	text	IP-адрес (или доменное имя) сервера FreeIPA
in_port	text	порт (по умолчанию 389)
in_login	text	UID администратора FreeIPA
in_pswd	text	пароль от учетной записи администратора FreeIPA
in_domain_type	text	Тип службы каталогов

Для параметра «in_domain_type» при создании профиля синхронизации сервера FreeIPA используется обязательное значение «FreeIPA».

В конкретном примере выполняется SQL-команда:

```
select
ja_sync_ldap.set_sync_profile(null,'user_db','10.72.9.12','389'
,'uid=admin,cn=users,cn=accounts,dc=FreeIPA,dc=local',
'12345678', 'FreeIPA');
```

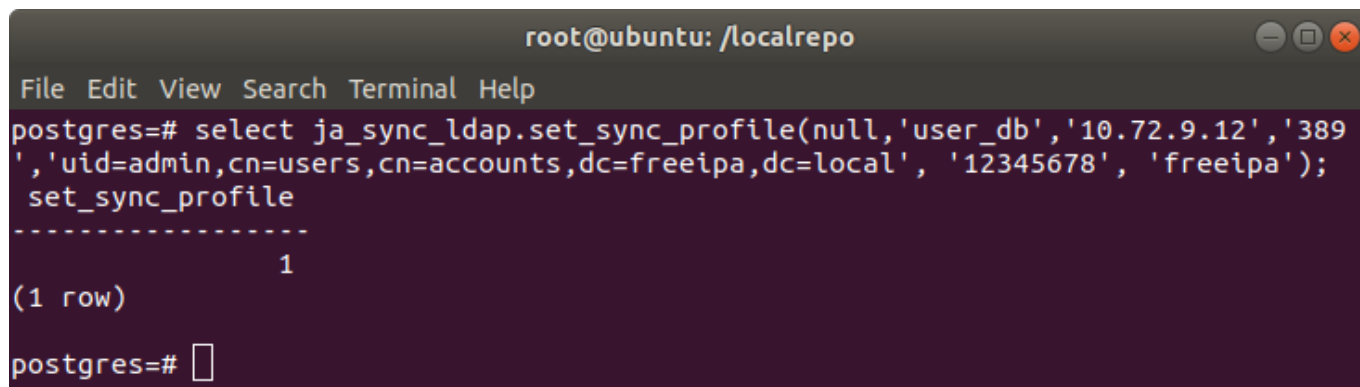


Рисунок 5.74 – Создание профиля синхронизации для сервера FreeIPA

5.14.4. Установка параметров SSL для профиля

Для установления SSL-соединения между сервером активного каталога FreeIPA и сервером СУБД, выполняются следующие действия:

- копирование сертификата с сервера FreeIPA;

На сервере FreeIPA сертификат «CA» находится в каталоге:

```
/etc/ipa/ca.crt
```



Рисунок 5.75 – Расположение файла сертификата на сервере FreeIPA

Для ОС GNU/Linux

Полученный сертификат копируется в любую директорию СУБД, на которую есть права у пользователя «postgres».

Например, в директорию:

```
/var/lib/jatoba/<версия>/
```

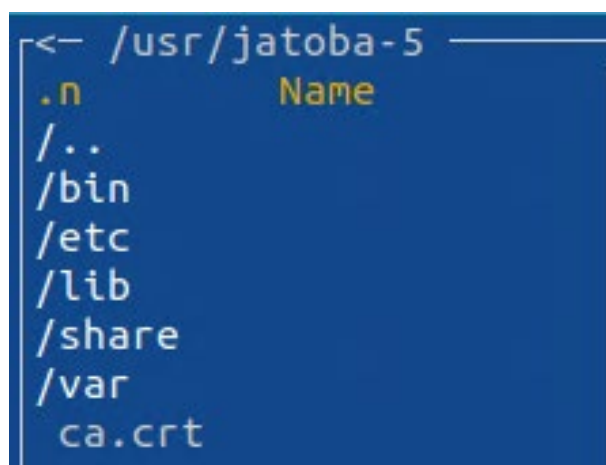


Рисунок 5.76 – Расположение файла сертификата на сервере СУБД

Назначить владельцем сертификата пользователя «postgres», выполнив команду в терминале:

```
chown postgres:postgres /путь/до/ca.crt
```

```

root@ubuntu: /usr/jatoba-5
File Edit View Search Terminal Help
root@ubuntu:/usr/jatoba-5# chown postgres:postgres /usr/jatoba-5/ca.crt
root@ubuntu:/usr/jatoba-5#

```

Рисунок 5.77 – Команда установки прав для пользователя «postgres»

Сертификат может быть добавлен к существующему профилю синхронизации, для чего в SQL-команде потребуется указать «Profile_ID», т.е. идентификатор профиля.

Выведите список профилей SQL-командой:

```
select * from ja_sync_ldap.get_sync_profiles();
```

Получив «Profile_ID», добавить к профилю синхронизации путь до сертификата SQL-командой, имеющей синтаксис:

```
select ja_sync_ldap.set_ca_cert_profile(<Profile_ID>,
'<путь/до/ca.crt>');
```

В рассматриваемом примере SQL-команда будет следующей:

```
select ja_sync_ldap.set_ca_cert_profile(1, '/usr/jatoba-5/ca.crt');
```

```

root@ubuntu: /localrepo
File Edit View Search Terminal Help
postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl | ca_cert
-----+-----+-----+-----+-----+-----+-----+-----+-----
  1 | user_db      | 10.72.9.12 | 389 | uid=admin,cn=users,cn=accounts,dc=freeipa,dc=local | 12345678 | freeipa | f |
(1 row)

postgres=# select ja_sync_ldap.set_ca_cert_profile(1, '/usr/jatoba-5/ca.crt');
 set_ca_cert_profile
-----
                1
(1 row)

postgres=#

```

Рисунок 5.78 – SQL-команда добавления сертификата к профилю синхронизации

При этом функция SSL-соединения останется выключенной. В поле «SSL» останется значение «f», т.е. «false».

```

root@ubuntu: /localrepo
File Edit View Search Terminal Help
postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl | ca_cert
-----+-----+-----+-----+-----+-----+-----+-----+-----
  1 | user_db      | 10.72.9.12 | 389 | uid=admin,cn=users,cn=accounts,dc=freeipa,dc=local | 12345678 | freeipa | f | 
(1 row)

postgres=# select ja_sync_ldap.set_ca_cert_profile(1, '/usr/jatoba-5/ca.crt');
 set_ca_cert_profile
-----
 1
(1 row)

postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl | ca
-----+-----+-----+-----+-----+-----+-----+-----+-----
  1 | user_db      | 10.72.9.12 | 389 | uid=admin,cn=users,cn=accounts,dc=freeipa,dc=local | 12345678 | freeipa | f | /usr/jato
ba-5/ca.crt>
(1 row)

postgres=#

```

Рисунок 5.79 – Вывод состояния SSL-соединения

5.14.5. Включение SSL-соединения для профиля синхронизации

Включение SSL-соединения для профиля синхронизации выполняется SQL-командой, имеющей синтаксис:

```
select ja_sync_ldap.set_ssl_profile(<Profile_ID>, true);
```

В рассматриваемом примере выполняется SQL-команда:

```
select ja_sync_ldap.set_ssl_profile(1, true);
```

```

root@ubuntu: /localrepo
File Edit View Search Terminal Help
postgres=# select ja_sync_ldap.set_ssl_profile(1, true);
 set_ssl_profile
-----
 1
(1 row)

postgres=# select * from ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl | ca
-----+-----+-----+-----+-----+-----+-----+-----+-----
  1 | user_db      | 10.72.9.12 | 389 | uid=admin,cn=users,cn=accounts,dc=freeipa,dc=local | 12345678 | freeipa | t | /usr/jato
ba-5/ca.crt>
(1 row)

postgres=#

```

Рисунок 5.80 – Включение SSL- соединения

При просмотре профилей синхронизации, функция SSL-соединения станет включенной. В поле «SSL» установится значение «t», т.е. «true».

Для выполнения синхронизации по SSL необходимо изменить порт в профиле на 636.

5.14.6. Отключение SSL-соединения для профиля синхронизации

Отключить SSL-соединение для профиля синхронизации возможно SQL-командой:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

```
select ja_sync_ldap.set_ssl_profile(<Profile_ID>, false);
```

5.14.7. Добавление соответствия групп

Добавление соответствия групп описано в п. 4.2 настоящего документа.

5.14.8. Выполнение синхронизации УЗ с сервером FreeIPA

Синхронизация учетных записей активного каталога с СУБД описана в п. 4.3 настоящего документа.

5.15. Синхронизация с сервером Samba

В качестве примера используется сервер под управлением RED OS release MUROM (7.3.4) DESKTOP Standard Edition с установленным активным каталогом Samba и сервер СУБД «Jatoba» под управление ОС Ubuntu 22.04. Сервера имеют IP-адреса, приведенные в таблице 5.8.

Таблица 5.8 – Сетевая адресация серверов стенда Samba

№	Имя сервера	IP-адрес	Маска подсети	DNS	Роль
1	Samba	10.116.101.114	255.255.255.0	10.116.101.2	Контролер домена
2	ldap	10.116.102.47	255.255.255.0	10.116.102.2	СУБД

Сервер СУБД «Jatoba» под управление ОС Ubuntu 22.04 с IP 10.116.102.47 использовался в примерах синхронизации в пунктах 5.1, 5.2 и 5.3 настоящего документа.

5.15.1. Настройка сервера СУБД

Настройка синхронизации учетных записей пользователей состоит из следующих шагов:

- выполнить установку компонента (п. 3.1);
- настроить конфигурационный файл «postgresql.conf» (п. 3.2);
- создать расширение ja_Sync_LDAP:

```
CREATE EXTENSION ja_sync_ldap;
```

- открыть файл hosts:

Для Linux выполнить команду:

```
gedit /etc/hosts
```

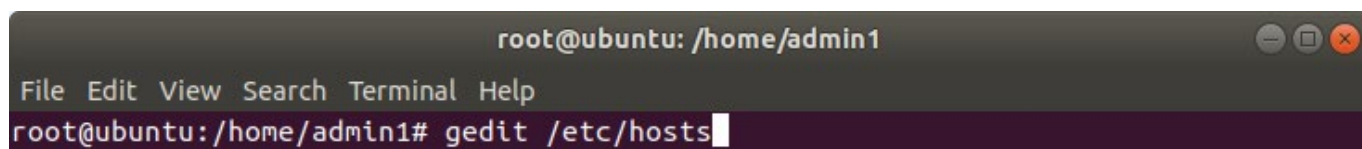


Рисунок 5.81 – Команда открытия конфигурационного файла /etc/hosts

Внести в строку два значения и сохранить изменения.

```
10.116.101.114 dc.domain.test dc
```

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

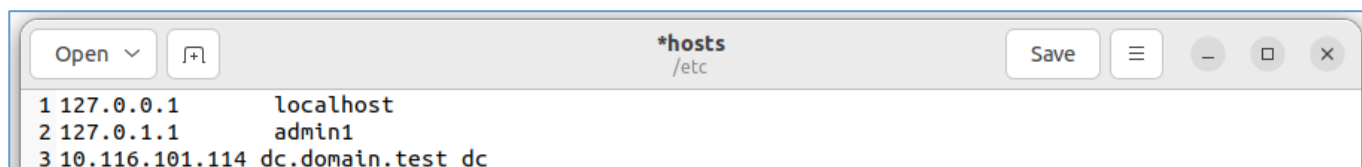


Рисунок 5.82 – Файл /etc/hosts сервера СУБД

Значения необходимо взять из файла «hosts» сервера Samba, расположенного по пути:

/etc/hosts

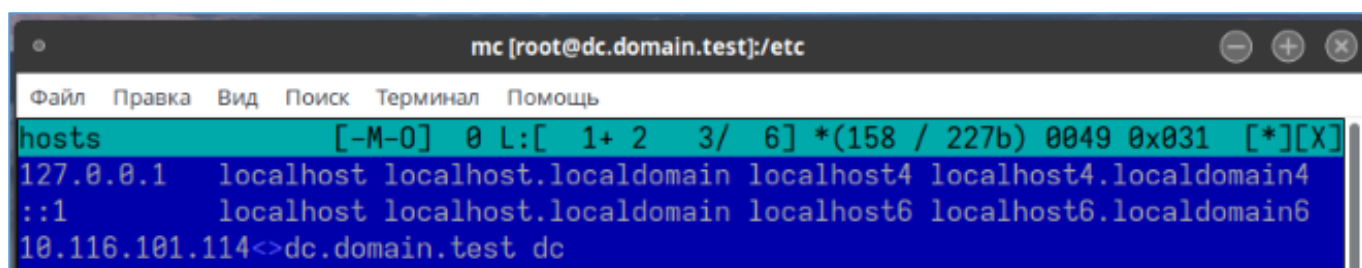


Рисунок 5.83 – Содержание файла «hosts» сервера Samba

5.15.2. Создание группы и пользователей группы в активном каталоге Samba

Предварительная настройка сертификатов на сервере Samba и проверка их работоспособности описана в Приложении 3 настоящего документа.

В созданном активном каталоге Samba требуется создать доменную группу «db_users» в терминале, от имени и с правами привилегированного пользователя ОС:

```
samba-tool group add db_users
```

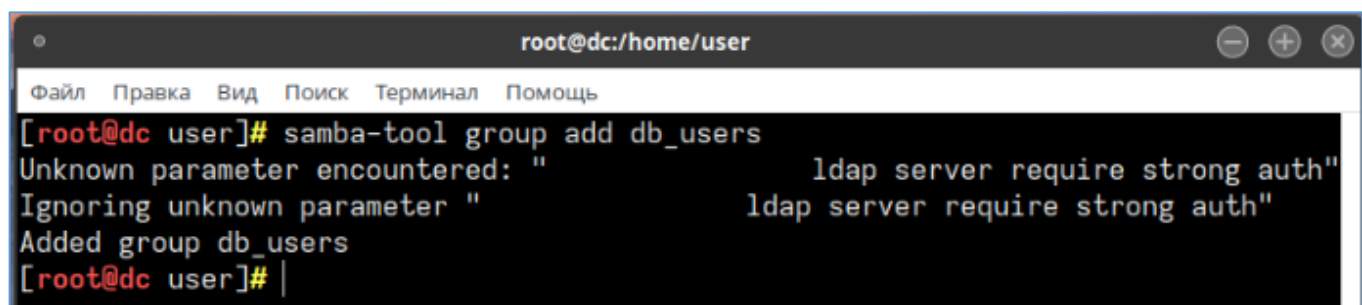
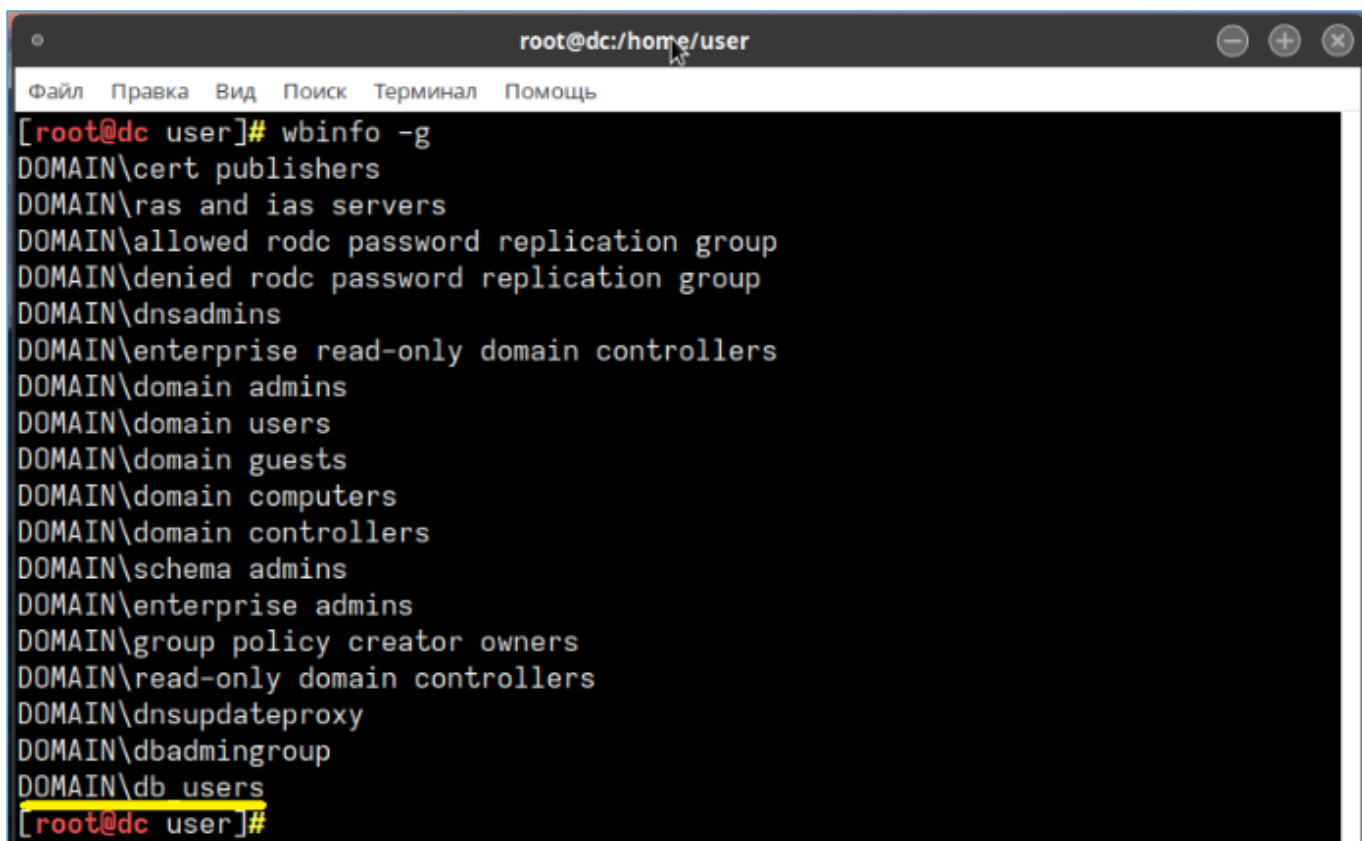


Рисунок 5.84 – Создание доменной группы «db_users»

Вывод доменных групп осуществляется командой:

```
wbinfo -g
```



```
root@dc:/home/user
Файл Правка Вид Поиск Терминал Помощь
[root@dc user]# wbinfo -g
DOMAIN\cert publishers
DOMAIN\ras and ias servers
DOMAIN\allowed rodc password replication group
DOMAIN\denied rodc password replication group
DOMAIN\dnsadmins
DOMAIN\enterprise read-only domain controllers
DOMAIN\domain admins
DOMAIN\domain users
DOMAIN\domain guests
DOMAIN\domain computers
DOMAIN\domain controllers
DOMAIN\schema admins
DOMAIN\enterprise admins
DOMAIN\group policy creator owners
DOMAIN\read-only domain controllers
DOMAIN\dnsupdateproxy
DOMAIN\dbadmingroup
DOMAIN\db users
[root@dc user]#
```

Рисунок 5.85 – Вывод списка доменных групп

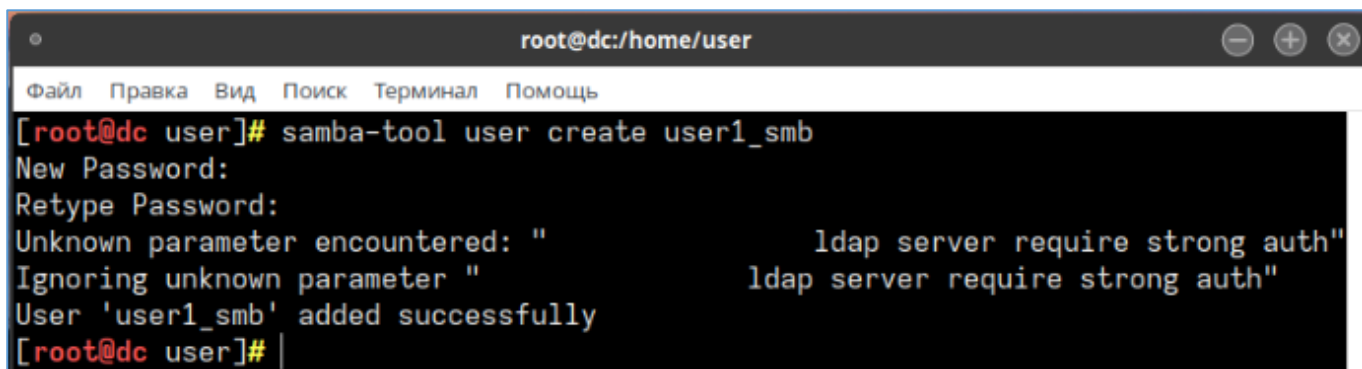
В полученном списке присутствует созданная группа «db_users».

Для последующей синхронизации УЗ с СУБД требуется создать тестовых пользователей:

- user1_smb;
- user2_smb;

выполнив следующие команды:

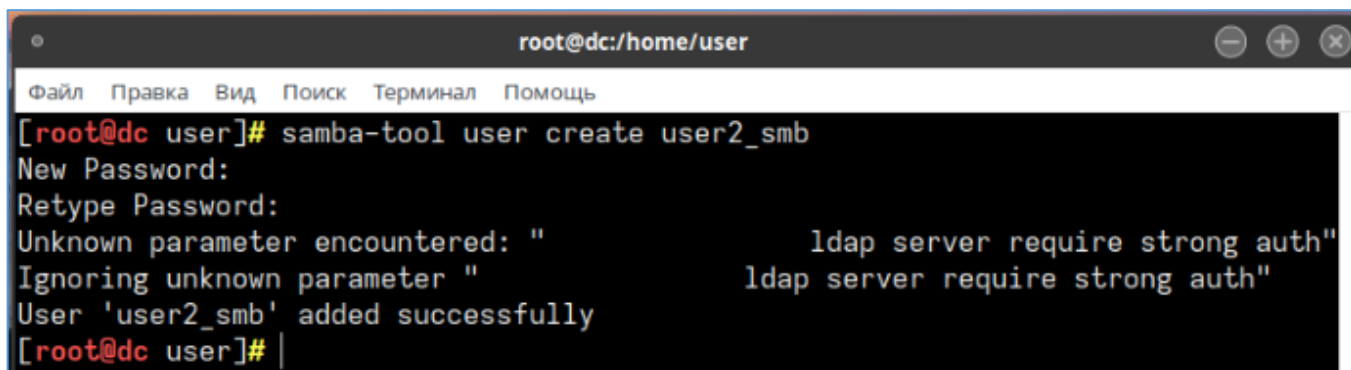
```
samba-tool user create user1_smb
```



```
root@dc:/home/user
Файл Правка Вид Поиск Терминал Помощь
[root@dc user]# samba-tool user create user1_smb
New Password:
Retype Password:
Unknown parameter encountered: " ldap server require strong auth"
Ignoring unknown parameter " ldap server require strong auth"
User 'user1_smb' added successfully
[root@dc user]# |
```

Рисунок 5.86 – Создание пользователя user1_smb


```
samba-tool user create user2_smb
```

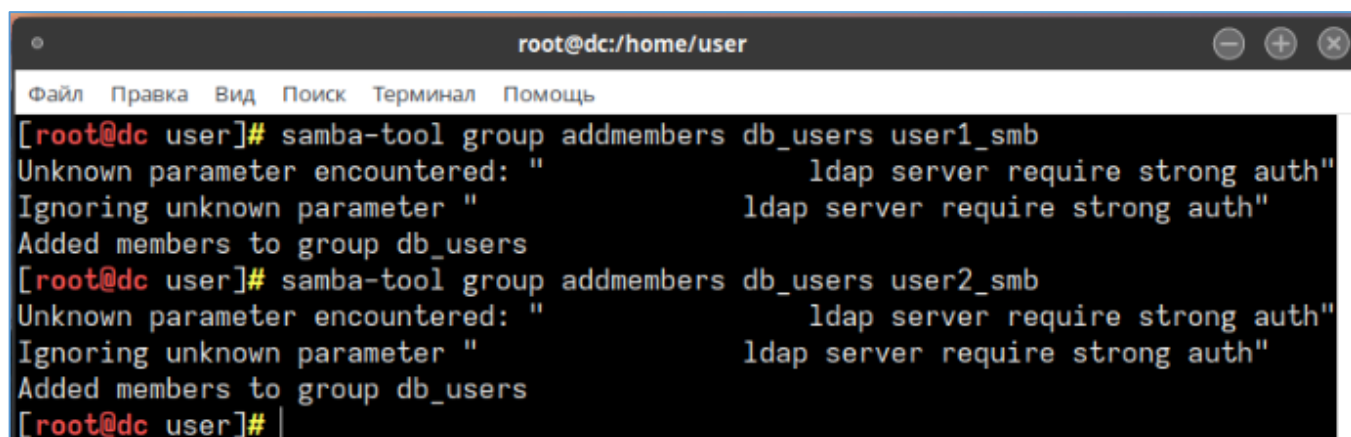


```
root@dc:/home/user
Файл Правка Вид Поиск Терминал Помощь
[root@dc user]# samba-tool user create user2_smb
New Password:
Retype Password:
Unknown parameter encountered: "                ldap server require strong auth"
Ignoring unknown parameter "                ldap server require strong auth"
User 'user2_smb' added successfully
[root@dc user]# |
```

Рисунок 5.87– Создание пользователя user2_smb

После создания пользователей потребуется добавить их в доменную группу, выполнив команды:

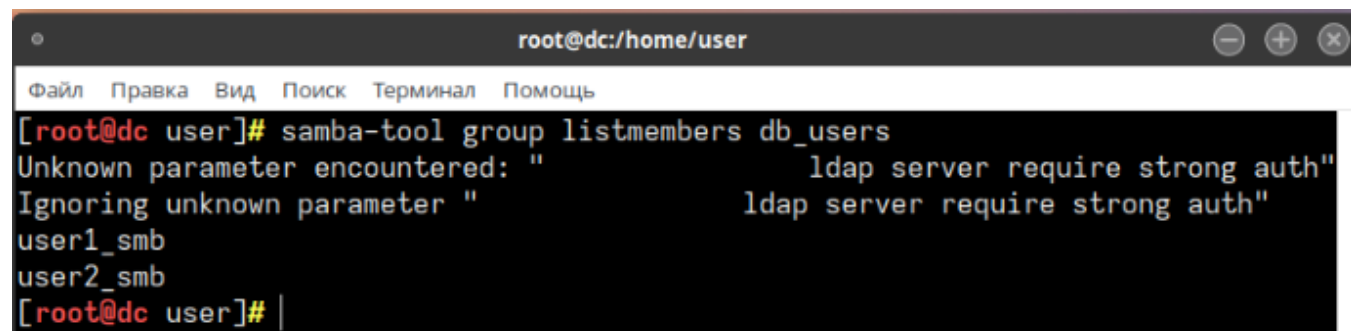
```
samba-tool group addmembers db_users user1_smb
samba-tool group addmembers db_users user2_smb
```



```
root@dc:/home/user
Файл Правка Вид Поиск Терминал Помощь
[root@dc user]# samba-tool group addmembers db_users user1_smb
Unknown parameter encountered: "                ldap server require strong auth"
Ignoring unknown parameter "                ldap server require strong auth"
Added members to group db_users
[root@dc user]# samba-tool group addmembers db_users user2_smb
Unknown parameter encountered: "                ldap server require strong auth"
Ignoring unknown parameter "                ldap server require strong auth"
Added members to group db_users
[root@dc user]# |
```

Рисунок 5.88 – Добавление пользователей в группу

```
samba-tool group listmembers db_users
```



```
root@dc:/home/user
Файл Правка Вид Поиск Терминал Помощь
[root@dc user]# samba-tool group listmembers db_users
Unknown parameter encountered: "                ldap server require strong auth"
Ignoring unknown parameter "                ldap server require strong auth"
user1_smb
user2_smb
[root@dc user]# |
```

Рисунок 5.89 – Просмотр состава группы

5.15.3. Создание профиля синхронизации

При создании профиля синхронизации потребуются два уникальных значения:

- Host;
- UID администратора сервера Samba.

Значение «host» было получено из файла /etc/hosts сервера Samba, как было описано в п. 5.15.1 (см. рис. 5.83).

«UID» администратора сервера Samba получается выполнением команды в терминале от имени и с правами «root»:

```
samba-tool user show administrator
```

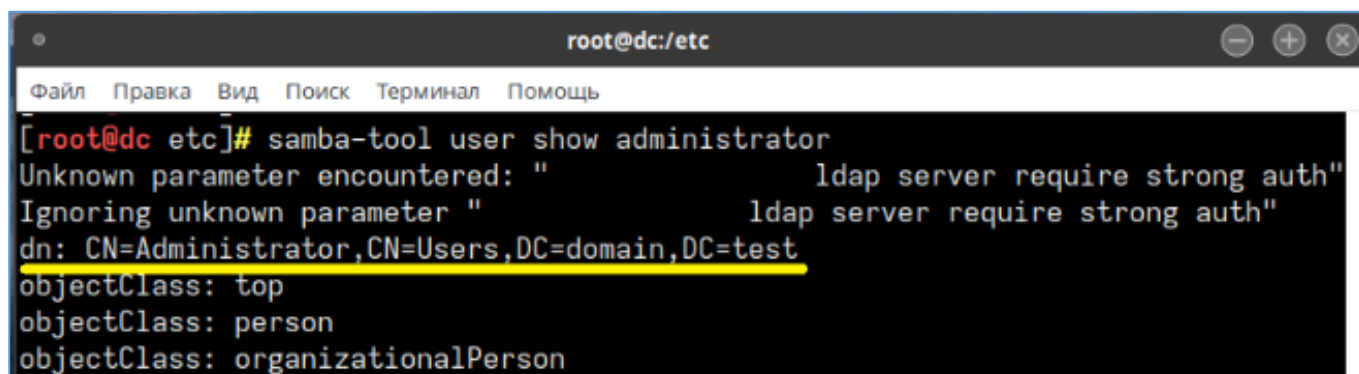


Рисунок 5.90 – «UID» администратора сервера Samba

В результате получена строка «UID» администратора сервера Samba, которая имеет следующий вид:

```
CN=Administrator,CN=Users,DC=domain,DC=test
```

В зависимости от конкретной конфигурации сервера Samba полученные значения будут отличаться.

Профиль синхронизации создается на сервере СУБД с установленным расширением «ja_sync_ldap» SQL-командой с синтаксисом:

```
select ja_sync_ldap.set_sync_profile(in_profile_id int,  
in_profile_name text, in_host_ip text, in_port text, in_login  
text, in_pswd text, in_domain_type text);
```

В таблице 5.9 приведены параметры, используемые для создания профиля для сервера Samba.

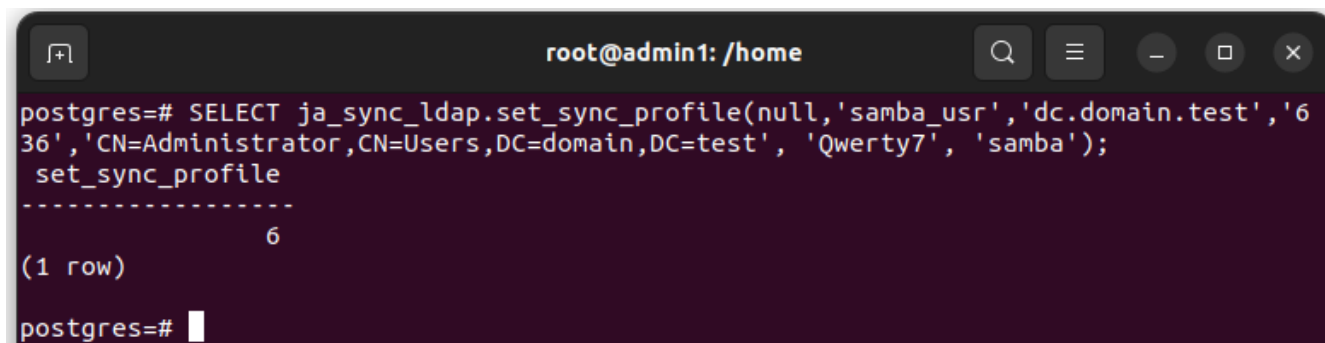
Таблица 5.9 – Параметры и обозначения для создания профиля для сервера Samba

Параметр	Тип данных	Значения в примере	Обозначение
in_profile_id	int	null	идентификатор профиля
in_profile_name	text	samba_usr	имя профиля
in_host_ip	text	10.116.101.114 или dc.domain.test	IP-адрес (или доменное имя) сервера Samba
in_port	text	636	порт (по умолчанию 389, для LDAPS 636)
in_login	text	CN=Administrator,CN=Users,DC=domain,DC=test	UID администратора Samba
in_pswd	text	Qwerty7	пароль от учетной записи администратора Samba
in_domain_type	text	samba	Тип службы каталогов

Для параметра «in_domain_type» при создании профиля синхронизации сервера Samba используется обязательное значение «samba».

В конкретном примере выполняется SQL-команда:

```
SELECT
ja_sync_ldap.set_sync_profile(null,'samba_usr','dc.domain.test',
'636','CN=Administrator,CN=Users,DC=domain,DC=test',
'Qwerty7','samba');
```



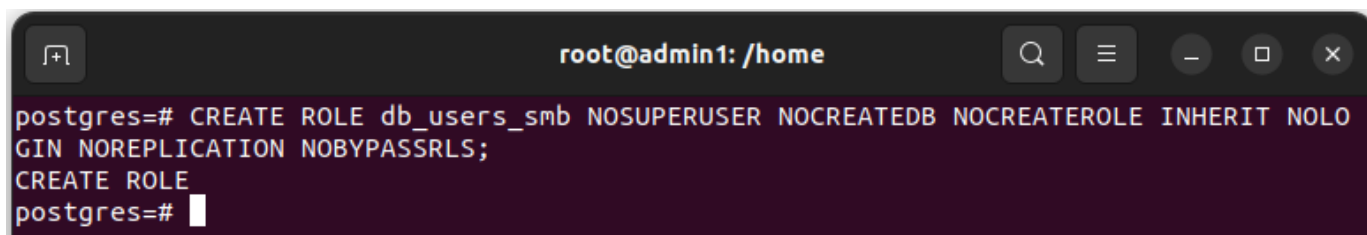
```
root@admin1: /home
postgres=# SELECT ja_sync_ldap.set_sync_profile(null,'samba_usr','dc.domain.test','6
36','CN=Administrator,CN=Users,DC=domain,DC=test','Qwerty7','samba');
set_sync_profile
-----
6
(1 row)
postgres=#
```

Рисунок 5.91 – Создание профиля синхронизации для сервера Samba

5.15.4. Добавление соответствия групп по атрибуту 'sAMAccountName'

Добавление к профилю синхронизации соответствия групп требует создания групповой роли в СУБД. В представляемом примере в СУБД создается роль «db_users_smb» SQL-командой:

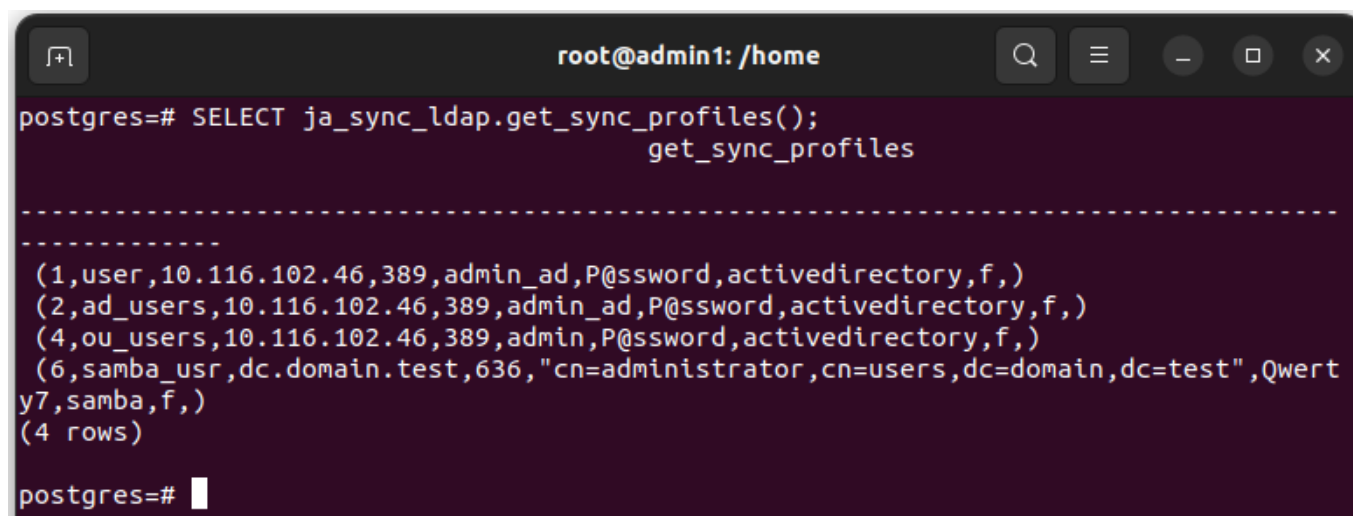
```
CREATE ROLE db_users_smb NOSUPERUSER NOCREATEDB NOCREATEROLE  
INHERIT NOLOGIN NOREPLICATION NOBYPASSRLS;
```



```
root@admin1: /home  
postgres=# CREATE ROLE db_users_smb NOSUPERUSER NOCREATEDB NOCREATEROLE INHERIT NOLO  
GIN NOREPLICATION NOBYPASSRLS;  
CREATE ROLE  
postgres=#
```

Рисунок 5.92 – Создание групповой роли «db_users_smb»

Ранее был создан профиль синхронизации «samba_usr» с ID-6

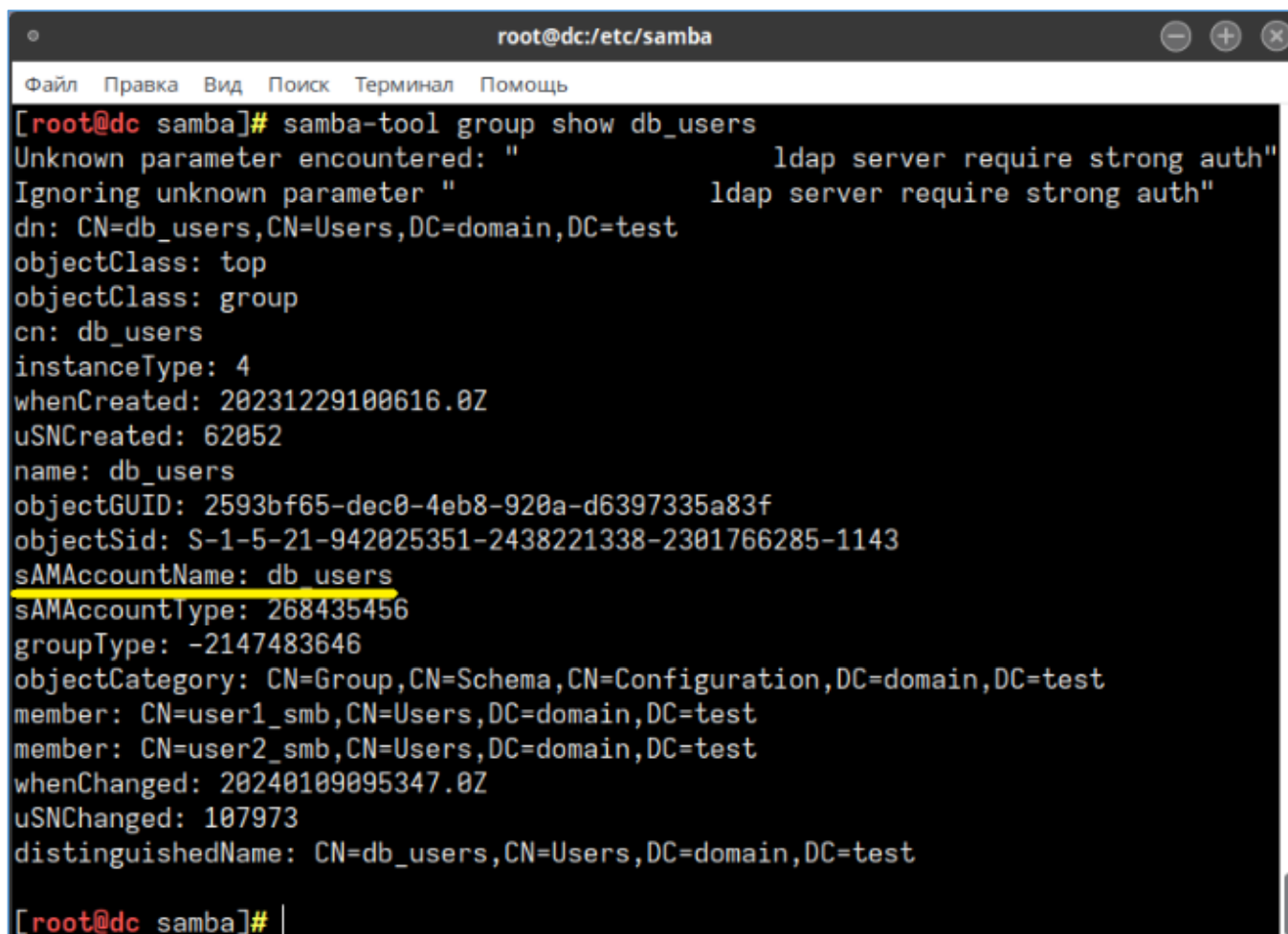


```
root@admin1: /home  
postgres=# SELECT ja_sync_ldap.get_sync_profiles();  
get_sync_profiles  
  
-----  
  
(1,user,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)  
(2,ad_users,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)  
(4,ou_users,10.116.102.46,389,admin,P@ssword,activedirectory,f,)  
(6,samba_usr,dc.domain.test,636,"cn=administrator,cn=users,dc=domain,dc=test",Qwert  
y7,samba,f,)  
(4 rows)  
postgres=#
```

Рисунок 5.93 – Вывод списка профилей синхронизации

Атрибут 'sAMAccountName' получается из вывода свойств группы пользователей на сервере активного каталога Samba командой:

```
samba-tool group show db_user
```



```
root@dc:/etc/samba
Файл Правка Вид Поиск Терминал Помощь
[root@dc samba]# samba-tool group show db_users
Unknown parameter encountered: "          ldap server require strong auth"
Ignoring unknown parameter "          ldap server require strong auth"
dn: CN=db_users,CN=Users,DC=domain,DC=test
objectClass: top
objectClass: group
cn: db_users
instanceType: 4
whenCreated: 20231229100616.0Z
uSNCreated: 62052
name: db_users
objectGUID: 2593bf65-dec0-4eb8-920a-d6397335a83f
objectSid: S-1-5-21-942025351-2438221338-2301766285-1143
sAMAccountName: db users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=domain,DC=test
member: CN=user1_smb,CN=Users,DC=domain,DC=test
member: CN=user2_smb,CN=Users,DC=domain,DC=test
whenChanged: 20240109095347.0Z
uSNChanged: 107973
distinguishedName: CN=db_users,CN=Users,DC=domain,DC=test

[root@dc samba]#
```

Рисунок 5.94 – Вывод свойства группы

В параметре «in_domain_group» указывается строка значений «DistinguishedName», полученная из глобальной группы безопасности пользователей «db_admins»

Для атрибута «sAMAccountName» используется значение «DistinguishedName»:

```
CN=db_users,CN=Users,DC=domain,DC=test
```

Добавление соответствия групп описано в п. 4.2 настоящего документа.

Для создания соответствия групп используется команда:

```
select ja_sync_ldap.set_sync_profile_map(in_map_id int,
in_profile_id int, in_role_bd text, in_domain_group text,
in_attribute text);
```

Синтаксис SQL-команды описан в п. 4.2.1.

Учитывая вышеизложенное, SQL-команда будет следующей:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

```
SELECT
ja_sync_ldap.set_sync_profile_map(null,6,'db_users_smb','CN=db_
users,CN=Users,DC=domain,DC=test','sAMAccountName');
```

```
root@admin1: /home
postgres=# SELECT ja_sync_ldap.set_sync_profile_map(null,6,'db_users_smb','CN=db_
rs,CN=Users,DC=domain,DC=test','sAMAccountName');
set_sync_profile_map
-----
6
(1 row)
postgres=#
```

Рисунок 5.95 – SQL-команда добавления соответствия групп

Для выполнения команды потребуются параметры, приведенные в таблице 5.10.

Таблица 5.10 – Параметры и значения для создания соответствия групп

Параметр	Значение	Обозначение
in_map_id	null	идентификатор соответствия групп
in_profile_id	6	идентификатор профиля синхронизации
in_role_bd	db_users_smb	групповая роль СУБД
in_domain_group	CN=db_users,CN=Users,DC=domain,DC=test	группа в службе каталогов
in_attribute	sAMAccountName	имя атрибута записи в службе каталогов, которое содержит имя пользователя

В идентификаторе соответствия групп указывается значение «null», т.к. ID назначается автоматически.

5.15.5. Установка параметров SSL для профиля

Подготовительные действия по копированию сертификата на сервер СУБД приведены в Приложении 4.

Для установления SSL-соединения между сервером активного каталога Samba и сервером СУБД, выполняются следующие действия:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

- Скопировать сертификат из директории:

```
/usr/local/share/ca-certificates/
```

в любую директорию СУБД, на которую есть права у пользователя «postgres».

Например, в директорию:

```
/var/lib/jatoba/<версия>/
```

На сервере СУБД выполняются следующие команды:

```
cd /usr/local/share/ca-certificates/  
cp rootCA.crt /var/lib/jatoba/5/  
cd /var/lib/jatoba/5/  
ls -l
```

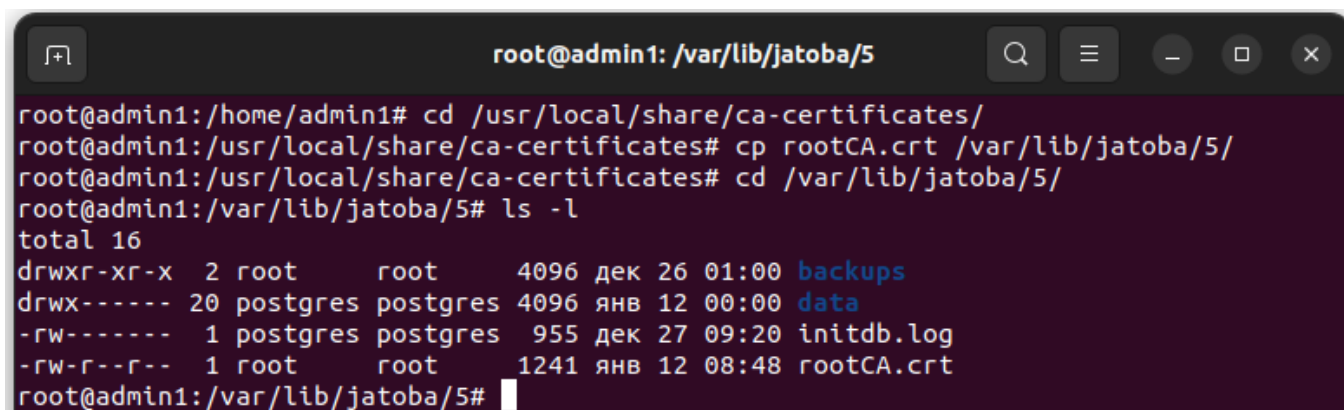


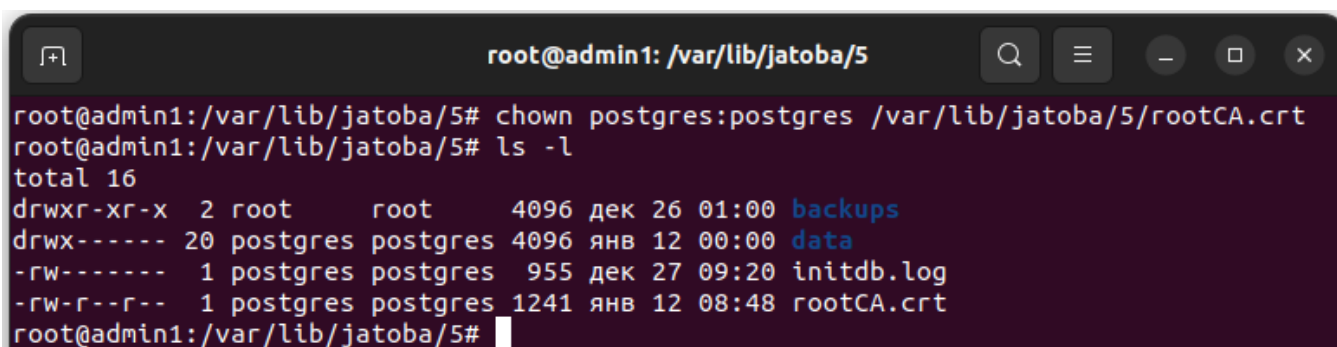
Рисунок 5.96 – Копирование сертификата

- Назначить владельцем сертификата пользователя «postgres», выполнив команду в терминале:

```
chown postgres:postgres /путь/до/са.crt
```

В рассматриваемом примере выполняются команды:

```
chown postgres:postgres /var/lib/jatoba/5/rootCA.crt  
ls -l
```

```
root@admin1: /var/lib/jatoba/5
root@admin1:/var/lib/jatoba/5# chown postgres:postgres /var/lib/jatoba/5/rootCA.crt
root@admin1:/var/lib/jatoba/5# ls -l
total 16
drwxr-xr-x  2 root      root      4096 дек 26 01:00 backups
drwx----- 20 postgres postgres 4096  янв 12 00:00 data
-rw-----  1 postgres postgres  955 дек 27 09:20 initdb.log
-rw-r--r--  1 postgres postgres 1241  янв 12 08:48 rootCA.crt
root@admin1:/var/lib/jatoba/5#
```

Рисунок 5.97 – Назначение прав на файл сертификата и проверка их

Сертификат может быть добавлен к существующему профилю синхронизации, для чего в SQL-команде потребуется указать «Profile_ID», т.е. идентификатор профиля.

Выведите список профилей SQL-командой:

```
select * from ja_sync_ldap.get_sync_profiles();
```

Получив «Profile_ID», добавить к профилю синхронизации путь до сертификата SQL-командой, имеющей синтаксис:

```
select ja_sync_ldap.set_ca_cert_profile(<Profile_ID>,
'<путь/до/ca.crt>');
```

В рассматриваемом примере SQL-команда будет следующей:

```
select ja_sync_ldap.set_ca_cert_profile(6,
'/var/lib/jatoba/5/rootCA.crt');
```



```
root@admin1: /home
postgres=# select ja_sync_ldap.set_ca_cert_profile(6, '/var/lib/jatoba/5/rootCA.crt');
set_ca_cert_profile
-----
(1 row)

postgres=# SELECT ja_sync_ldap.get_sync_profiles();
get_sync_profiles
-----
(1,user,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)
(2,ad_users,10.116.102.46,389,admin_ad,P@ssword,activedirectory,f,)
(4,ou_users,10.116.102.46,389,admin,P@ssword,activedirectory,f,)
(6,samba_usr,dc.domain.test,636,"cn=administrator,cn=users,dc=domain,dc=test",Qwert
y7,samba,f,/var/lib/jatoba/5/rootCA.crt)
(4 rows)

postgres=#
```

Рисунок 5.98 – Установка и проверка параметров SSL для профиля синхронизации

5.15.6. Включение SSL-соединения для профиля синхронизации

По умолчанию режим SSL-соединения не включается и в столбце «ssl» имеет значение «f», т.е. «false», как показано на рисунке 5.98.

Включение SSL-соединения для профиля синхронизации выполняется SQL-командой, имеющей синтаксис:

```
select ja_sync_ldap.set_ssl_profile(<Profile_ID>, true);
```

В рассматриваемом примере выполняется SQL-команда:

```
select ja_sync_ldap.set_ssl_profile(6, true);
```

```

root@admin1: /home
postgres=# select ja_sync_ldap.set_ssl_profile(6, true);
set_ssl_profile
-----
6
(1 row)

postgres=# SELECT * FROM ja_sync_ldap.get_sync_profiles();
 id | profile_name | host_ip | port | login | pswd | domain_type | ssl |
-----+-----+-----+-----+-----+-----+-----+-----+
  1 | user         | 10.116.102.46 | 389 | admin_ad | P@ssword | activedirectory | f |
  2 | ad_users     | 10.116.102.46 | 389 | admin_ad | P@ssword | activedirectory | f |
  4 | ou_users     | 10.116.102.46 | 389 | admin    | P@ssword | activedirectory | f |
  6 | samba_usr    | dc.domain.test | 636 | cn=administrator,cn=users,dc=domain,dc=test | Qwerty7 | samba | t | /var/l
ib/jatoba/5/rootCA.crt
(4 rows)

postgres=#

```

Рисунок 5.99 – Включение режима SSL и вывод статуса режима SSL

Для выполнения синхронизации по SSL необходимо изменить порт в профиле на 636.

5.15.7. Выполнение синхронизации УЗ с сервером Samba по атрибуту 'sAMAccountName'

Синхронизация учетных записей активного каталога с СУБД описана в п. 4.3 настоящего документа. Синхронизация осуществляется командой с синтаксисом:

```
select ja_sync_ldap.ldap_synchronize_jds(prof_id int);
```

В рассматриваемом примере выполняется SQL-команда:

```
select ja_sync_ldap.ldap_synchronize_jds(6);
```

```

root@admin1: /home
postgres=# select ja_sync_ldap.ldap_synchronize_jds(6);
ldap_synchronize_jds
-----
0
(1 row)

postgres=#

```

Рисунок 5.100 – Выполнение синхронизации с активным каталогом Samba

В результате пользователи, созданные в группе «db_users» на сервере активного каталога Samba, синхронизированы с сервером СУБД и находятся в групповой роли «db_users_smb».

```

root@admin1: /home
postgres=#
postgres=# \du

          List of roles
Role name |          Attributes          | Member of
-----+-----+-----
ad_users  | Cannot login                  | {}
admin     | Superuser, Cannot login      | {}
admin1    |                               | {admin}
admin2    |                               | {admin}
admin3    |                               | {admin}
db_users_smb | Cannot login                | {}
ou_users  | Cannot login                  | {}
postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}
user1_smb |                               | {db_users_smb}
user2_smb |                               | {db_users_smb}
user_1    |                               | {ad_users}
user_2    |                               | {ad_users}
user_3    |                               | {ad_users}
postgres=#

```

Рисунок 5.101 – Вывод списка пользователей

5.15.8. Авторизация после синхронизации по атрибуту 'sAMAccountName'

Настройка авторизации пользователей аналогична настройке для MS Active Directory и описана в п. 5.1.5 настоящего документа.

5.15.9. Выполнение синхронизации УЗ с сервером Samba по атрибуту 'cn'

Настройка синхронизации УЗ с сервером Samba по атрибуту 'cn' аналогична настройке для MS Active Directory и описана в п. 5.2 настоящего документа.

5.15.10. Отключение SSL-соединения для профиля синхронизации

Отключить SSL-соединение для профиля синхронизации возможно SQL-командой:

```
select ja_sync_ldap.set_ssl_profile(<Profile_ID>, false);
```

6. ОБНОВЛЕНИЕ И УДАЛЕНИЕ КОМПОНЕНТА

Обновление компонента в ОС GNU/Linux выполняется следующими шагами:

- получить новую версию пакета `jatoba<версия>-ja-sync-ldap`;
- перезаписать им старый пакет, находящийся в директории локального репозитория;
- проиндексировать обновленное состояние/обновить кэш репозитория;
- выполнить обновление пакета:

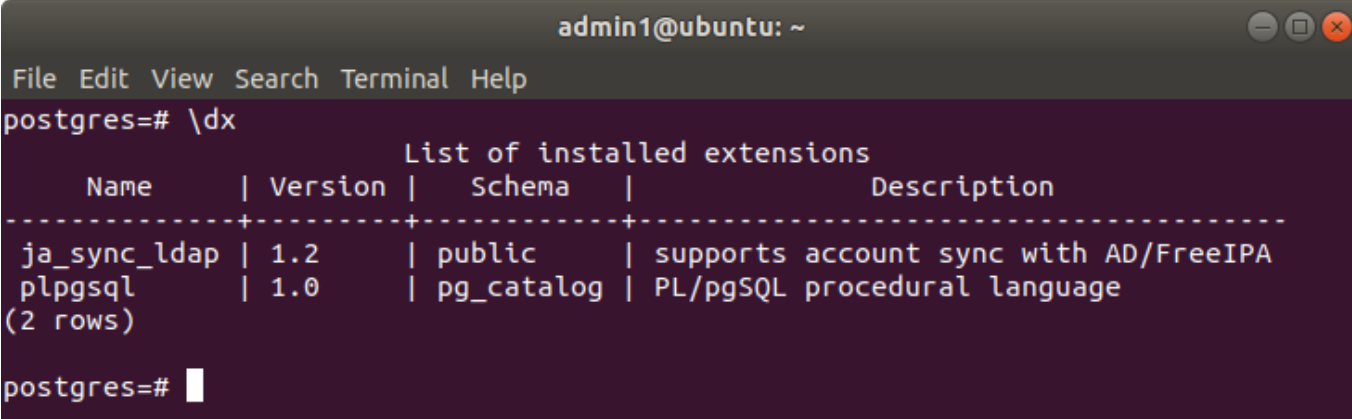
```
apt-get install --only-upgrade jatoba<версия>-ja-sync-ldap
```

- выполнить перезагрузку СУБД;
- авторизоваться в СУБД под суперпользователем;
- выполнить обновление:

```
alter extension ja_sync_ldap update
```

- вывести текущую версию компонентов SQL-командой:

```
\dx
```



```
admin1@ubuntu: ~
File Edit View Search Terminal Help
postgres=# \dx
List of installed extensions
  Name      | Version | Schema  | Description
-----+-----+-----+-----
ja_sync_ldap | 1.2     | public  | supports account sync with AD/FreeIPA
plpgsql     | 1.0     | pg_catalog | PL/pgSQL procedural language
(2 rows)
postgres=#
```

Рисунок 6.1 – Просмотр версий компонентов

Удаление компонента происходит с помощью команды:

```
drop extension ja_sync_ldap;
```

7. ДЕЙСТВИЯ ПОСЛЕ СБОЕВ И ОШИБОК ЭКСПЛУАТАЦИИ

При выполнении синхронизации может возникнуть ошибка соединения с сервером домена, при том, что аутентификационные параметры были верными.

Для устранения возникшей ошибки, убедитесь, что:

- пользователь MS AD имеет достаточные привилегии;
- заполнены поля в карточке пользователя «Имя» и «Выводимое имя».

The image shows a Windows XP-style dialog box titled 'Свойства: admin'. It has several tabs at the top: 'Опубликованные сертификаты', 'Член групп', 'Репликация паролей', 'Удаленное управление', 'Профиль служб удаленных рабочих столов', 'COM+', 'Редактор атрибутов', 'Входящие звонки', 'Объект', 'Безопасность', 'Среда', 'Сеансы', 'Общие', 'Адрес', 'Учетная запись', 'Профиль', 'Телефоны', and 'Организация'. The 'Общие' (General) tab is selected. It displays a user icon and the name 'admin'. Below this, there are several text input fields. The 'Имя:' (Name) field contains 'admin' and is highlighted with a yellow box. The 'Инициалы:' (Initials) field is empty. The 'Фамилия:' (Surname) field is empty. The 'Выводимое имя:' (Display name) field contains 'admin' and is also highlighted with a yellow box. Below this are fields for 'Описание:' (Description) and 'Комната:' (Room), both empty. At the bottom, there are fields for 'Номер телефона:' (Phone number), 'Эл. почта:' (E-mail), and 'Веб-страница:' (Web page), each with a 'Другой...' (Other...) button next to it. At the very bottom of the dialog are four buttons: 'ОК', 'Отмена', 'Применить', and 'Справка'.

Рисунок 7.1 – Карточка пользователя MS AD

ПРИЛОЖЕНИЕ 1

Пример установки СУБД «Jatoba» из локального репозитория для ОС Ubuntu

Установка СУБД «Jatoba» из локального репозитория для ОС Ubuntu проводится в следующем порядке:

- 1) В терминале войти в режим суперпользователя, выполнив команду:

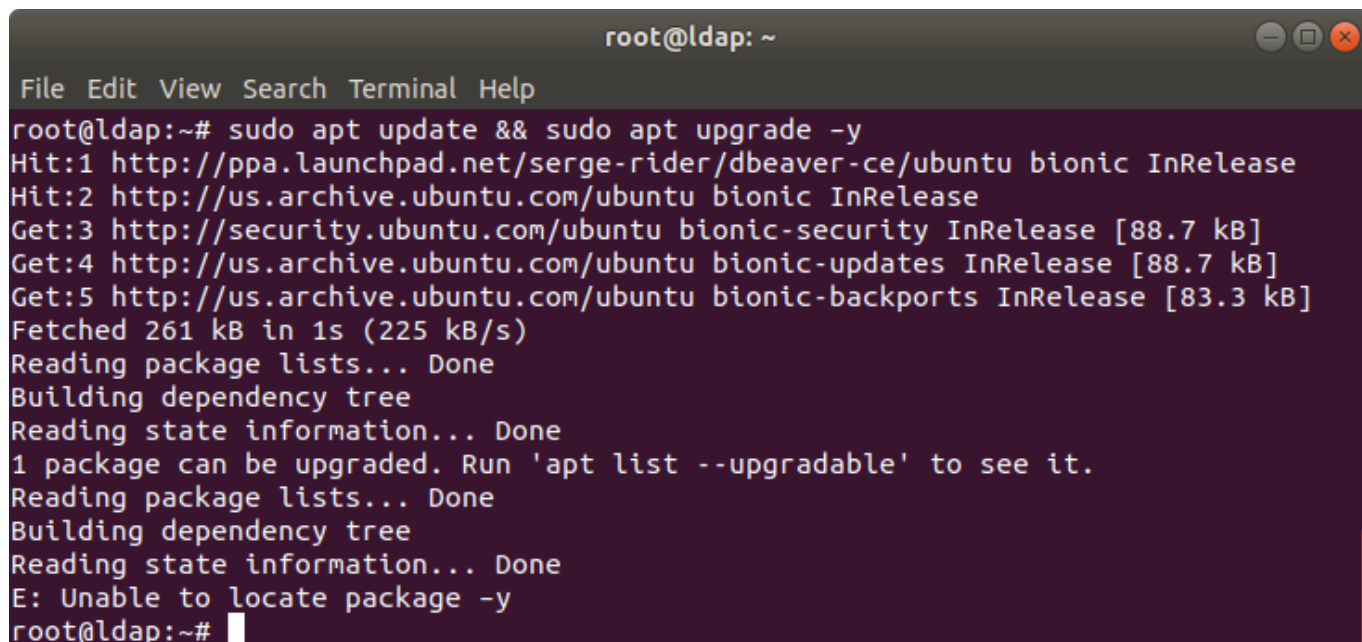
```
sudo su
```

- 2) Если команды sudo не существует – установить:

```
su -l  
apt-get install sudo -y
```

- 3) Выполнить обновление системы:

```
sudo apt update && sudo apt upgrade -y  
sudo apt -s dist-upgrade  
sudo apt dist-upgrade
```



The screenshot shows a terminal window titled 'root@ldap: ~'. The terminal output displays the execution of 'sudo apt update && sudo apt upgrade -y'. It lists several package sources being updated, including security updates and backports. The output indicates that 1 package can be upgraded. The terminal ends with the prompt 'root@ldap:~# '.

Рисунок 1.1 – Обновление системы

- 4) Создать папку localrepo в корневом каталоге:

```
mkdir /localrepo
```

- 5) В созданную папку скопировать:

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

- а) каталог <pool>
- б) каталог <dist>
- в) файл <DEB-GPG-KEY-Jatoba>

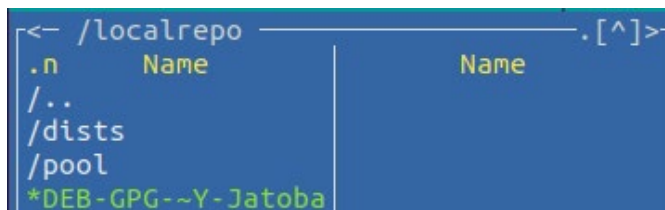


Рисунок 1.2 – Структура каталога «localrepo»

- 6) Установить открытый ключ репозитория:

```
apt-key add /localrepo/DEB-GPG-KEY-Jatoba
```

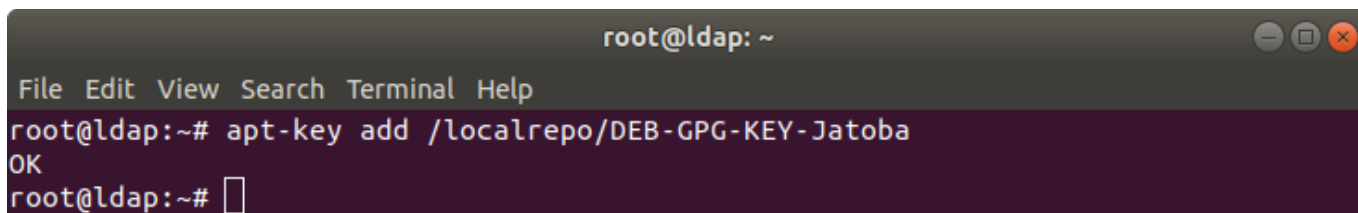


Рисунок 1.3 – Установка открытого ключа репозитория

- 7) Добавить описание локального репозитория в систему:

```
nano /etc/apt/sources.list.d/jatoba-4.list
```

- 8) Вставить в файл следующее содержимое и сохранить:

```
deb file:///localrepo stable non-free
```

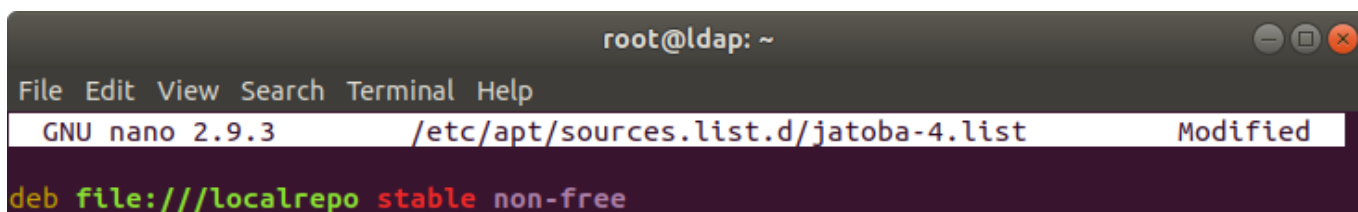
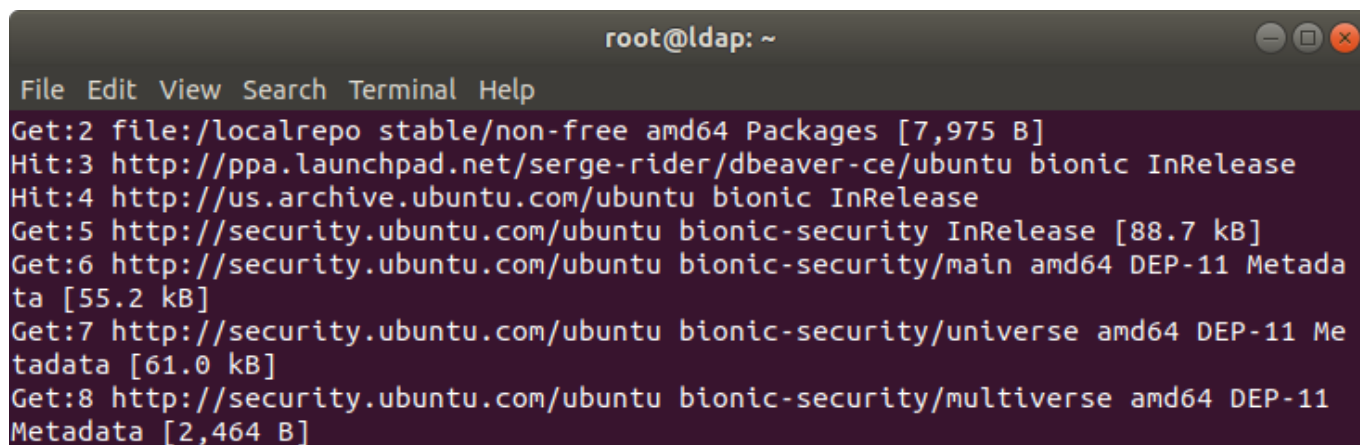


Рисунок 1.4 – Содержание файла «jatoba-4.list»

- 9) Проиндексировать обновленное состояние репозитория:

```
apt-get update
```

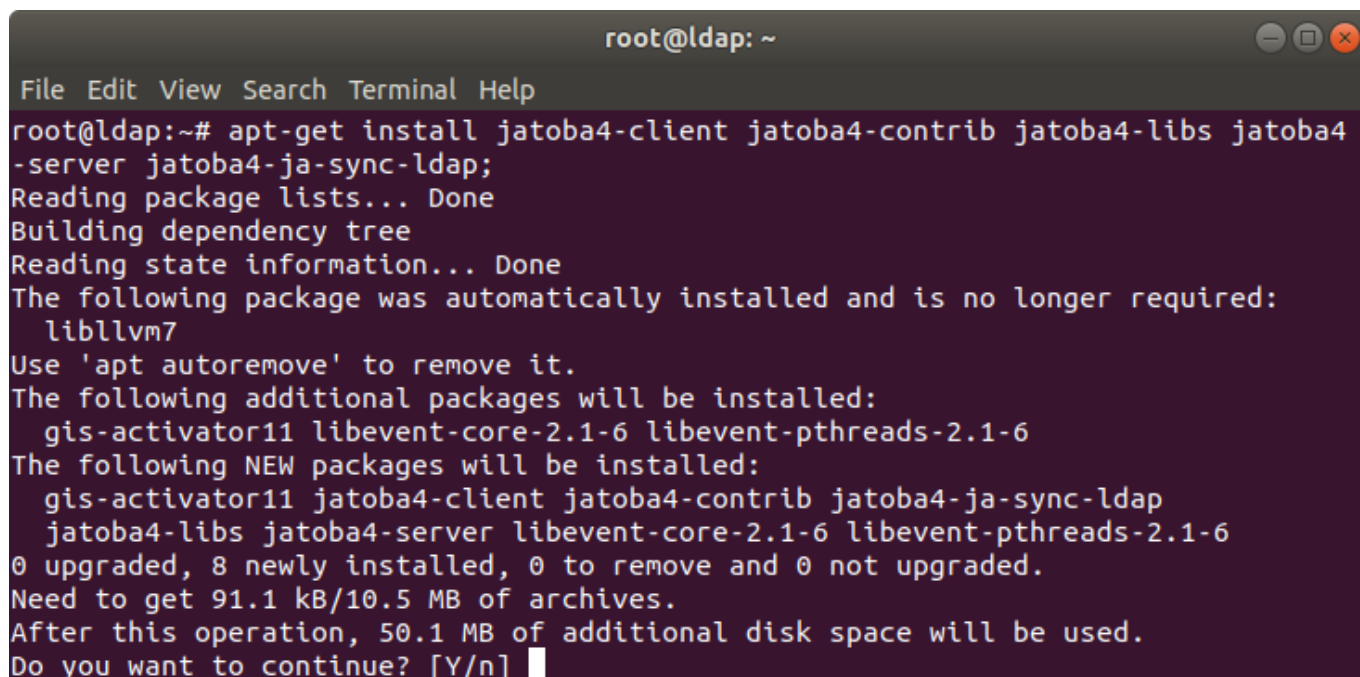


```
root@ldap: ~  
File Edit View Search Terminal Help  
Get:2 file:/localrepo stable/non-free amd64 Packages [7,975 B]  
Hit:3 http://ppa.launchpad.net/serge-rider/dbeaver-ce/ubuntu bionic InRelease  
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic InRelease  
Get:5 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]  
Get:6 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Meta-  
data [55.2 kB]  
Get:7 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 Me-  
tadata [61.0 kB]  
Get:8 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11  
Metadata [2,464 B]
```

Рисунок 1.5 – Индексация репозитория

- 10) Установить СУБД Jatoba при помощи команды:

```
apt-get install jatoba4-client jatoba4-contrib jatoba4-libs  
jatoba4-server jatoba4-ja-sync-ldap;
```

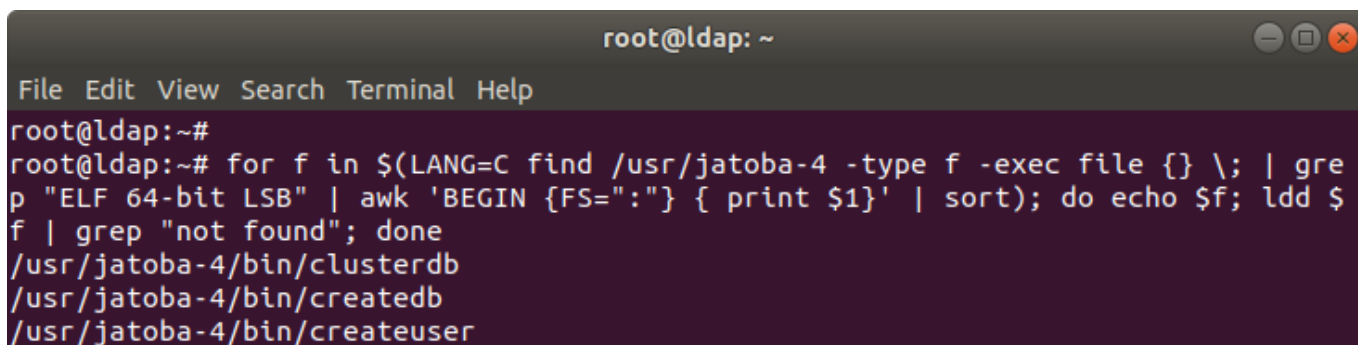


```
root@ldap: ~  
File Edit View Search Terminal Help  
root@ldap:~# apt-get install jatoba4-client jatoba4-contrib jatoba4-libs jatoba4-  
-server jatoba4-ja-sync-ldap;  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following package was automatically installed and is no longer required:  
  libllvm7  
Use 'apt autoremove' to remove it.  
The following additional packages will be installed:  
  gis-activator11 libevent-core-2.1-6 libevent-pthreads-2.1-6  
The following NEW packages will be installed:  
  gis-activator11 jatoba4-client jatoba4-contrib jatoba4-ja-sync-ldap  
  jatoba4-libs jatoba4-server libevent-core-2.1-6 libevent-pthreads-2.1-6  
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.  
Need to get 91.1 kB/10.5 MB of archives.  
After this operation, 50.1 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

Рисунок 1.6 – Установка пакетов

- 11) Убедиться, что отсутствуют ошибки зависимостей:

```
for f in $(LANG=C find /usr/jatoba-4 -type f -exec file {} \; |  
grep "ELF 64-bit LSB" | awk 'BEGIN {FS=":"} { print $1}' |  
sort); do echo $f; ldd $f | grep "not found"; done
```

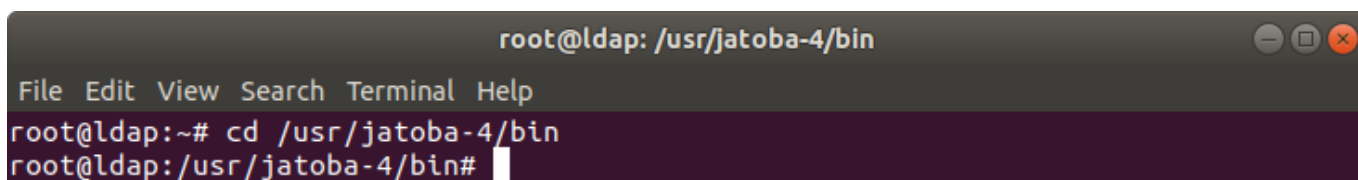



```
root@ldap: ~  
File Edit View Search Terminal Help  
root@ldap:~#  
root@ldap:~# for f in $(LANG=C find /usr/jatoba-4 -type f -exec file {} \; | gre  
p "ELF 64-bit LSB" | awk 'BEGIN {FS=":"} { print $1}' | sort); do echo $f; ldd $  
f | grep "not found"; done  
/usr/jatoba-4/bin/clusterdb  
/usr/jatoba-4/bin/createdb  
/usr/jatoba-4/bin/createuser
```

Рисунок 1.7 – Проверка отсутствия ошибок зависимостей

- 12) Перейти в директорию исполняемых файлов СУБД:

```
cd /usr/jatoba-4/bin
```

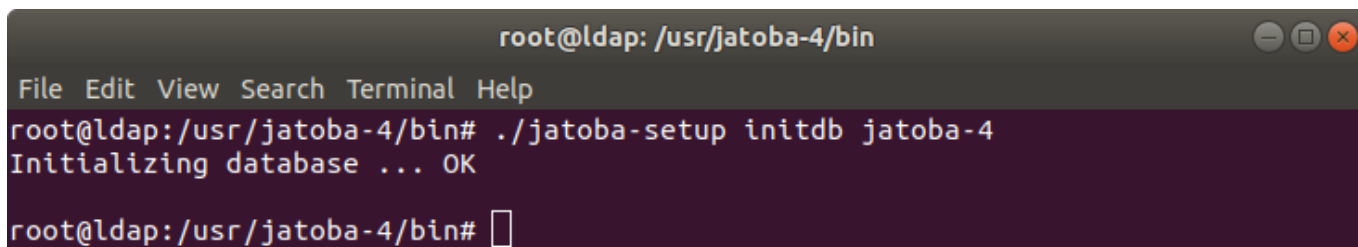


```
root@ldap: /usr/jatoba-4/bin  
File Edit View Search Terminal Help  
root@ldap:~# cd /usr/jatoba-4/bin  
root@ldap:/usr/jatoba-4/bin#
```

Рисунок 1.8 – Переход в каталог

- 13) Инициализировать каталог данных СУБД при помощи команды:

```
./jatoba-setup initdb jatoba-4
```

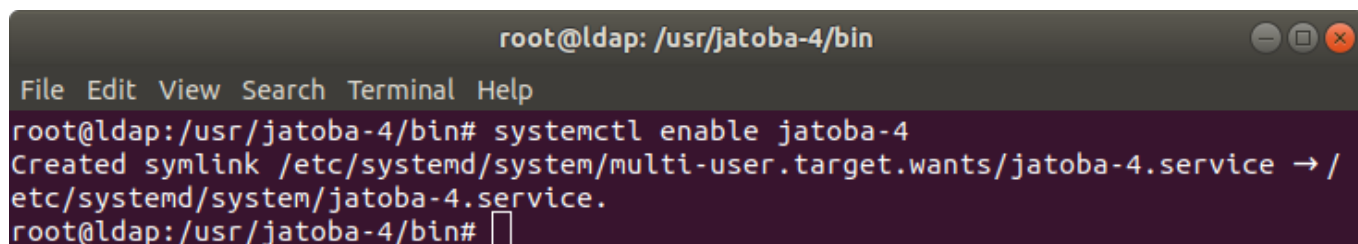


```
root@ldap: /usr/jatoba-4/bin  
File Edit View Search Terminal Help  
root@ldap:/usr/jatoba-4/bin# ./jatoba-setup initdb jatoba-4  
Initializing database ... OK  
root@ldap:/usr/jatoba-4/bin#
```

Рисунок 1.9 – Инициализация СУБД

- 14) Добавить сервис в список автозапуска:

```
systemctl enable jatoba-4
```



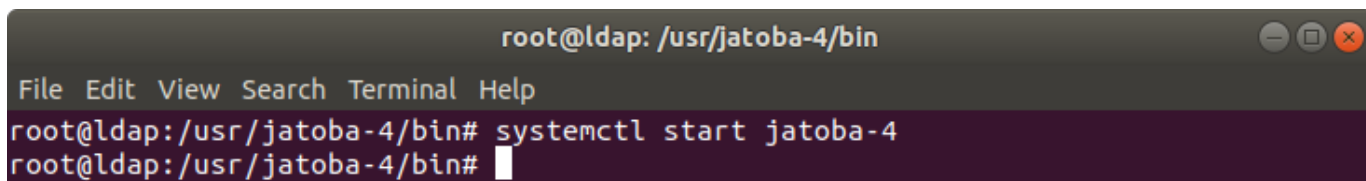
```
root@ldap: /usr/jatoba-4/bin  
File Edit View Search Terminal Help  
root@ldap:/usr/jatoba-4/bin# systemctl enable jatoba-4  
Created symlink /etc/systemd/system/multi-user.target.wants/jatoba-4.service → /  
etc/systemd/system/jatoba-4.service.  
root@ldap:/usr/jatoba-4/bin#
```

Рисунок 1.10 – Добавление сервиса jatoba-4 а автозагрузку ОС

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

15) Запустить службу:

```
systemctl start jatoba-4
```

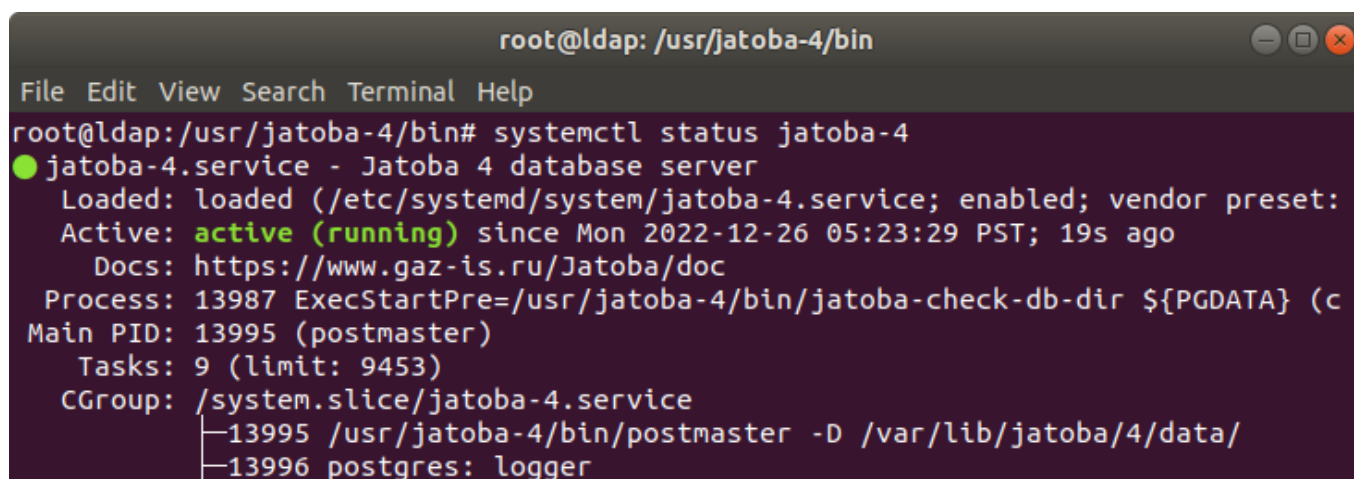


A terminal window titled 'root@ldap: /usr/jatoba-4/bin'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command 'systemctl start jatoba-4' has been entered and executed, with the prompt returning to 'root@ldap: /usr/jatoba-4/bin# '.

Рисунок 1.11 – Запуск службы jatoba-4

16) Проверить статус службы:

```
systemctl status jatoba-4
```



A terminal window titled 'root@ldap: /usr/jatoba-4/bin'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command 'systemctl status jatoba-4' has been entered and executed. The output shows that the 'jatoba-4.service' is active and running. Key details include: Loaded: loaded (/etc/systemd/system/jatoba-4.service; enabled; vendor preset: Active: active (running) since Mon 2022-12-26 05:23:29 PST; 19s ago; Docs: https://www.gaz-is.ru/Jatoba/doc; Process: 13987 ExecStartPre=/usr/jatoba-4/bin/jatoba-check-db-dir \${PGDATA} (c Main PID: 13995 (postmaster); Tasks: 9 (limit: 9453); CGroup: /system.slice/jatoba-4.service. The CGroup details show two processes: 13995 /usr/jatoba-4/bin/postmaster -D /var/lib/jatoba/4/data/ and 13996 postgres: logger.

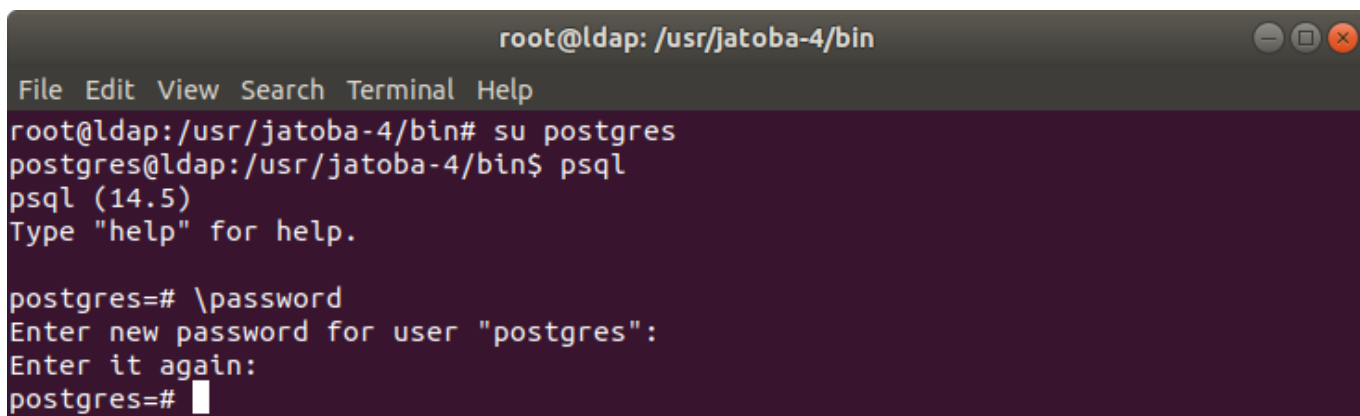
Рисунок 1.12 – Проверка статуса службы jatoba-4

17) Авторизоваться в psql:

```
su postgres  
psql
```

18) Установить пароль для пользователя СУБД «postgres»:

```
\password
```



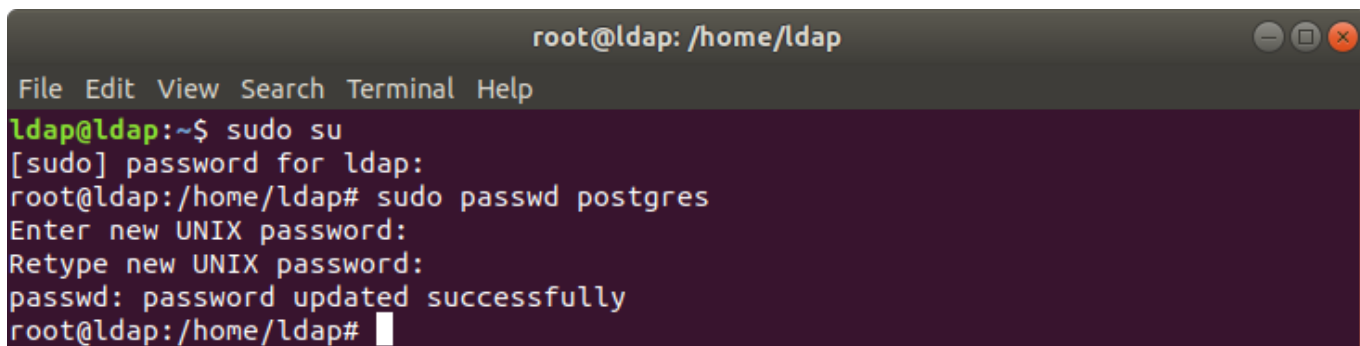
```
root@ldap: /usr/jatoba-4/bin
File Edit View Search Terminal Help
root@ldap:/usr/jatoba-4/bin# su postgres
postgres@ldap:/usr/jatoba-4/bin$ psql
psql (14.5)
Type "help" for help.

postgres=# \password
Enter new password for user "postgres":
Enter it again:
postgres=#
```

Рисунок 1.13 – Установка пароля для пользователя ОС

- 19) Установить пароль для системного пользователя ОС «postgres»:

```
sudo passwd postgres
```



```
root@ldap: /home/ldap
File Edit View Search Terminal Help
ldap@ldap:~$ sudo su
[sudo] password for ldap:
root@ldap:/home/ldap# sudo passwd postgres
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ldap:/home/ldap#
```

Рисунок 1.14 – Установка пароля для пользователя СУБД

На этом этапе установку СУБД с компонентом «ja_Sync_LDAP» можно считать завершенной.

ПРИЛОЖЕНИЕ 2

Пример создания Organizational Unit (OU) в MS AD

Создать такую сущность как, «Подразделение» в MS AD возможно в следующем порядке:

1) Запустить консоль «Центр администрирования Active Directory» через исполняемый файл:

dsac.exe

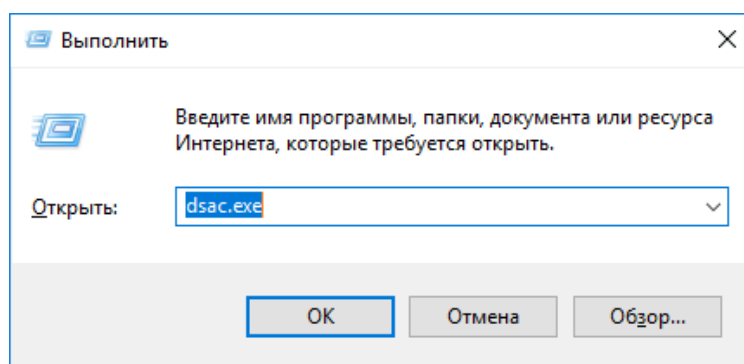


Рисунок 2.1 – Запуск исполняемого файла dsac.exe

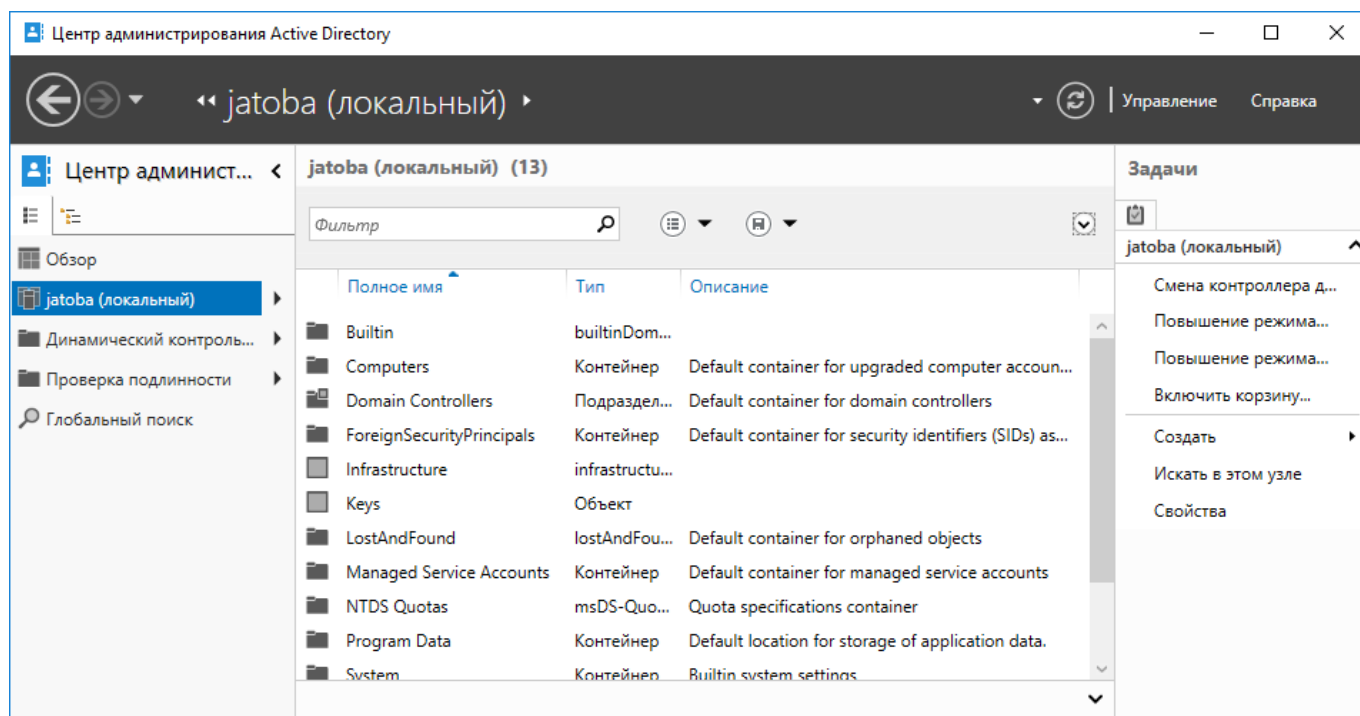


Рисунок 2.2 - Вид консоли «Центр администрирования Active Directory»

2) Выбрав домен, через контекстное меню, перейти по опциям «Создать» → «Подразделение»;

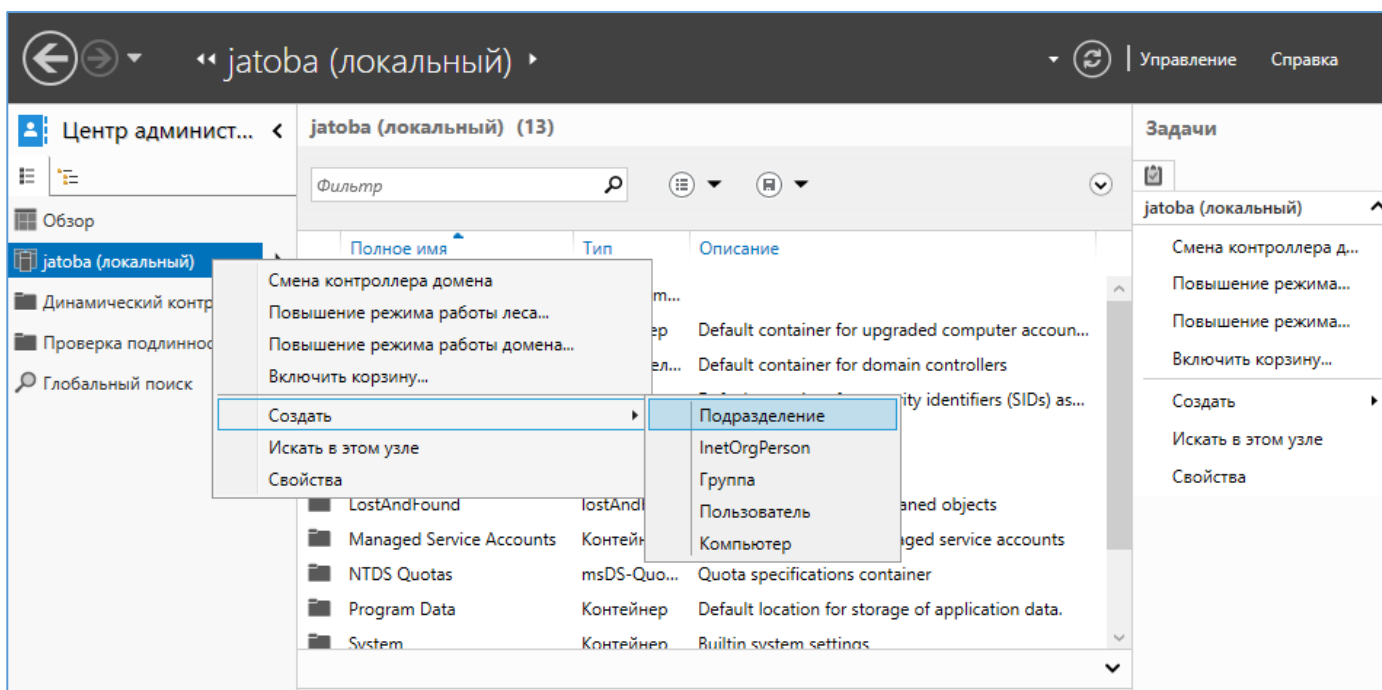


Рисунок 2.3 – Контекстное меню создания подразделения

3) В открывшемся окне «Создать Подразделение» заполнить обязательное поле «Имя» и установить в поле «Управляется» пользователя или группу пользователей, которая будет иметь права на администрирование создаваемого подразделения.

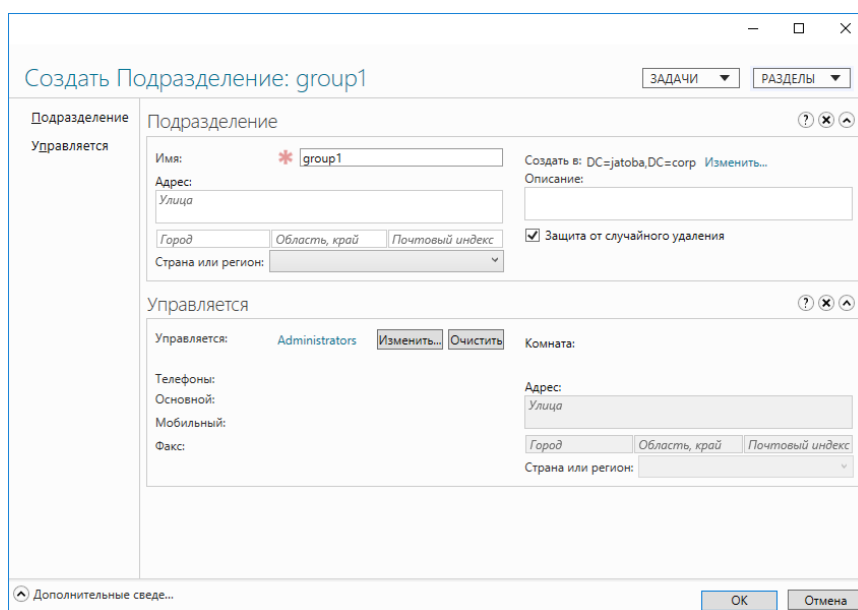


Рисунок 2.4 – Окно «Создать Подразделение»

ПРИЛОЖЕНИЕ 3

Пример настройки сертификатов на сервере Samba

Настройку сертификатов на сервере Samba возможно выполнить в следующем порядке:

1. В терминале перейти в режим привилегированного пользователя:

```
sudo su
```

2. Установить пакет openssl:

```
dnf install openssl-gost-engine
```

3. Сгенерировать корневую пару ключ-сертификат:

```
openssl genrsa -out rootCA.key 2048  
openssl req -x509 -new -key rootCA.key -days 10000 -out  
rootCA.crt
```

Все поля можно оставить пустыми.

4. Сгенерировать приватный ключ и сертификат, подписанный корневым сертификатом:

```
openssl genrsa -out lnx-dc11.alt.test.key 2048  
openssl req -new -key lnx-dc11.alt.test.key -out lnx-  
dc11.alt.test.csr
```

Здесь в поле «Common Name» важно указать FQDN имя хоста. Можно узнать с помощью команды «hostname -f». Остальные поля можно оставить пустыми.

5. Подписать корневым сертификатом:

```
openssl x509 -req -in lnx-dc11.alt.test.csr -CA rootCA.crt -  
CAkey rootCA.key -CAcreateserial -out lnx-dc11.alt.test.crt -  
days 5000
```

6. Скопировать сгенерированные ключи в рабочий каталог Samba (от имени суперпользователя):

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------

```
# cp lnx-dc11.alt.test.crt /var/lib/samba/private/tls/  
# cp lnx-dc11.alt.test.key /var/lib/samba/private/tls/  
# cp rootCA.crt /var/lib/samba/private/tls/
```

7. В секцию Global в /etc/samba/smb.conf добавить следующие параметры:

```
ldap server require strong auth = yes  
tls enabled = yes  
tls keyfile = tls/lnx-dc11.alt.test.key  
tls certfile = tls/lnx-dc11.alt.test.crt
```

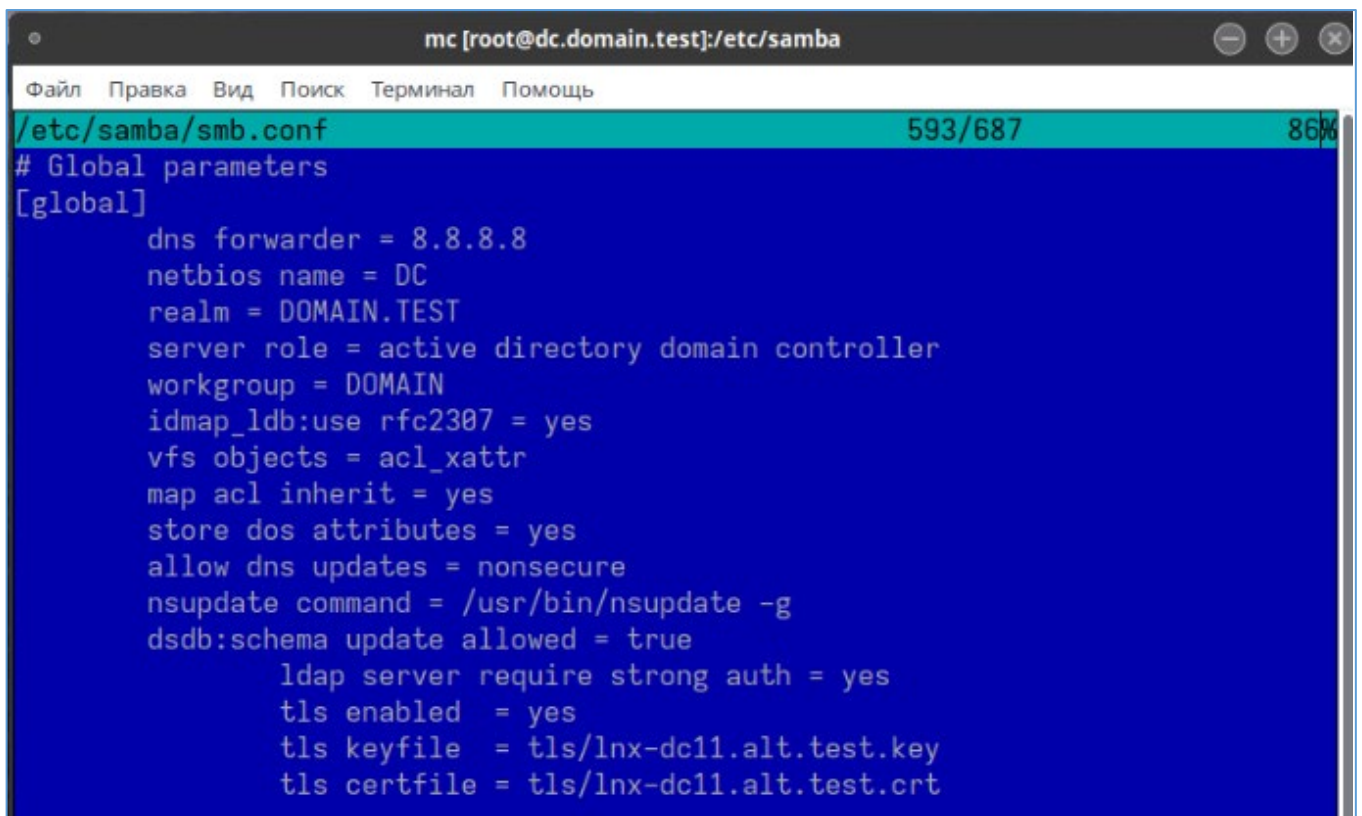


Рисунок 3.1 – Содержание файла /etc/samba/smb.conf

8. Перезапустить сервис Samba:

```
# systemctl restart samba
```

Проверка работы сертификатов локально на сервере Samba

Работоспособность сертификатов на сервере Samba выполняется следующими шагами:

1. Добавить в системный репозиторий сертификатов наш корневой сертификат:

```
# cp rootCA.crt /etc/pki/ca-trust/source/anchors/  
# update-ca-trust
```

2. Выполнить команду `ldapsearch` для проверки соединения к активному каталогу:

```
ldapsearch -H ldaps://dc.domain.test:636 -b  
"CN=Users,DC=domain,DC=test" -D  
"CN=Administrator,CN=Users,DC=domain,DC=test" -W
```

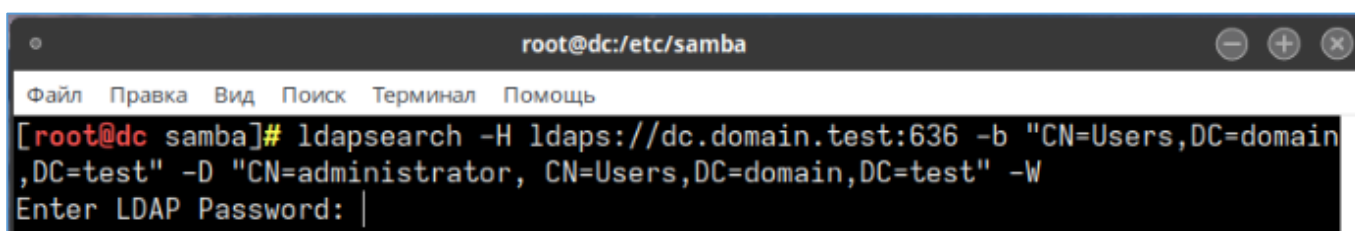


Рисунок 3.2 – Команда проверки соединения

В случае, если сертификаты отработали верно, выведется длинный список вывода. Это дает понять работоспособность.

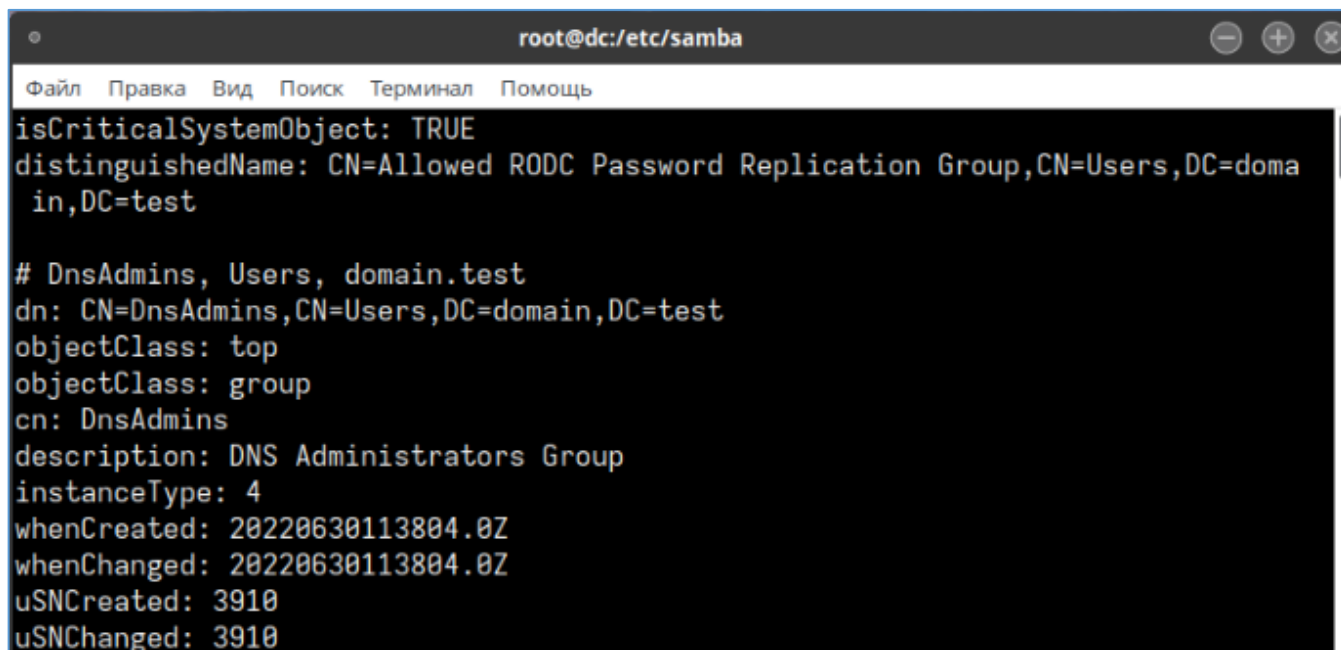


Рисунок 3.3 – Вывод проверки соединения

ПРИЛОЖЕНИЕ 4

Пример настройки сертификатов на клиенте (сервере СУБД)

Настройка сертификатов на сервере Samba можно выполнить в следующем порядке:

1. Внести изменения в конфигурационный файл /etc/hosts сервера СУБД.

В файл вносится IP-адрес сервера Samba и FQDN.

Значения необходимо взять из файла «hosts» сервера Samba, расположенного по пути:

```
/etc/hosts
```

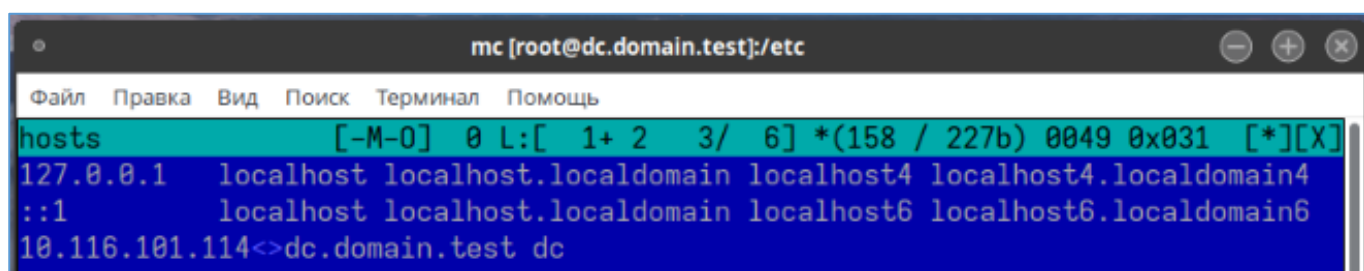


Рисунок 4.1 – Содержание файла «hosts» сервера Samba

Отдельно получить FQDN сервера Samba можно выполнив команду на нем:

```
hostname -f
```

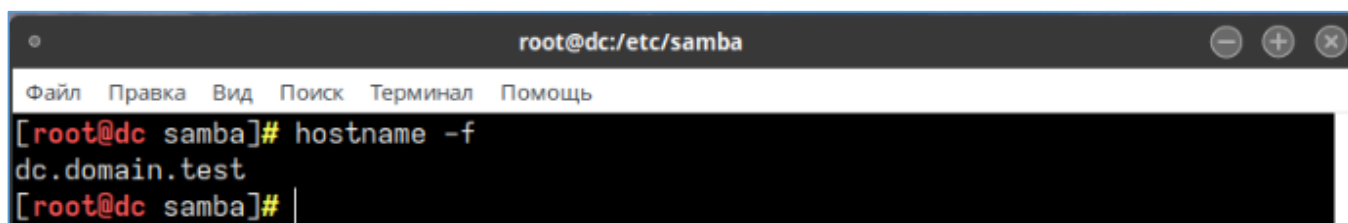


Рисунок 4.2 – Вывод FQDN

В результате в конфигурационном файле /etc/hosts сервера СУБД, должна появиться строка, аналогичная представленной ниже на рисунке 4.3.

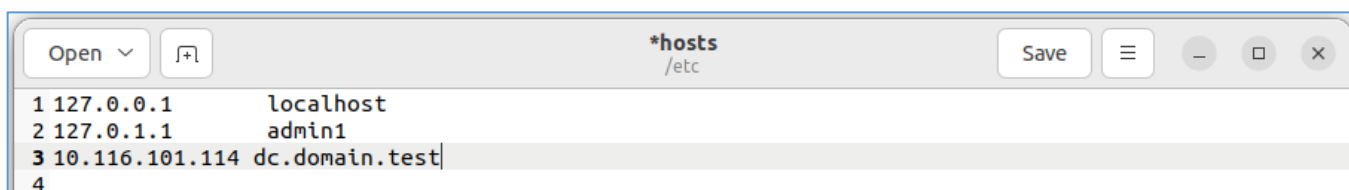
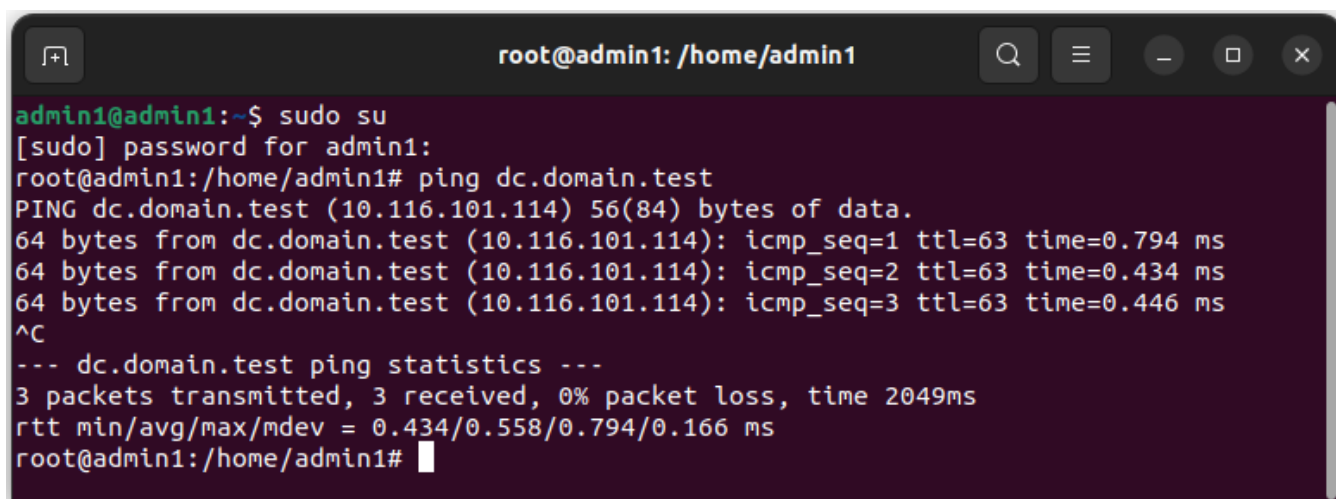


Рисунок 4.3 – Содержание файла /etc/hosts сервера СУБД

Обращаться к серверу активного каталога можно только по FQDN, которое было указано при создании сертификатов.

Для проверки связи между серверами используем команду `ping <FQDN>`, в рассматриваемом примере команда будет иметь следующий вид:

```
ping dc.domain.test
```



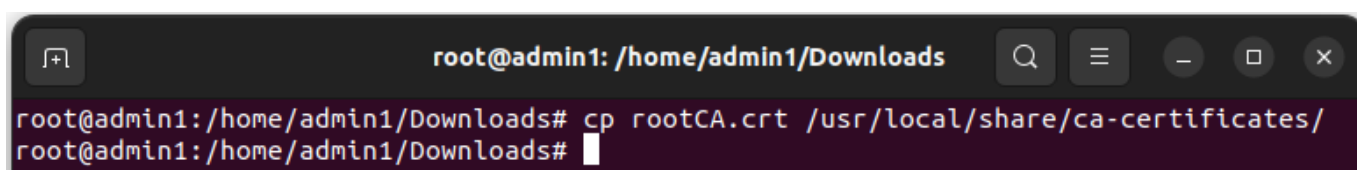
The screenshot shows a terminal window titled 'root@admin1: /home/admin1'. The user 'admin1' has executed 'sudo su' to become root. The root user then runs 'ping dc.domain.test'. The output shows three successful ping requests to 10.116.101.114 with varying times. Finally, it shows ping statistics: 3 packets transmitted, 3 received, 0% packet loss, and an average round-trip time of 0.558 ms.

```
admin1@admin1:~$ sudo su
[sudo] password for admin1:
root@admin1:/home/admin1# ping dc.domain.test
PING dc.domain.test (10.116.101.114) 56(84) bytes of data.
64 bytes from dc.domain.test (10.116.101.114): icmp_seq=1 ttl=63 time=0.794 ms
64 bytes from dc.domain.test (10.116.101.114): icmp_seq=2 ttl=63 time=0.434 ms
64 bytes from dc.domain.test (10.116.101.114): icmp_seq=3 ttl=63 time=0.446 ms
^C
--- dc.domain.test ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2049ms
rtt min/avg/max/mdev = 0.434/0.558/0.794/0.166 ms
root@admin1:/home/admin1#
```

Рисунок 4.4 – Тестирование соединения сервера СУБД с сервером Samba через команду ping

2. Скопировать с сервера Samba на сервер СУБД корневой сертификат rootCA.crt.
3. Скопировать корневой сертификат rootCA.crt в хранилище:

```
cp rootCA.crt /usr/local/share/ca-certificates/
```



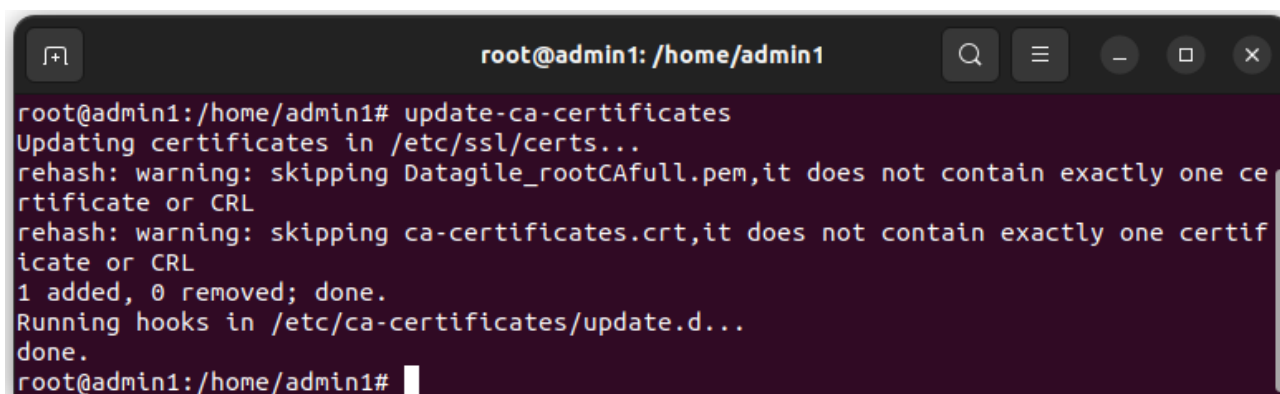
The screenshot shows a terminal window titled 'root@admin1: /home/admin1/Downloads'. The user runs the command 'cp rootCA.crt /usr/local/share/ca-certificates/'. The command is executed successfully, and the prompt returns to the user's home directory.

```
root@admin1:/home/admin1/Downloads# cp rootCA.crt /usr/local/share/ca-certificates/
root@admin1:/home/admin1/Downloads#
```

Рисунок 4.5 – Команда копирования сертификата

4. Обновить содержание репозитория

```
update-ca-certificates
```

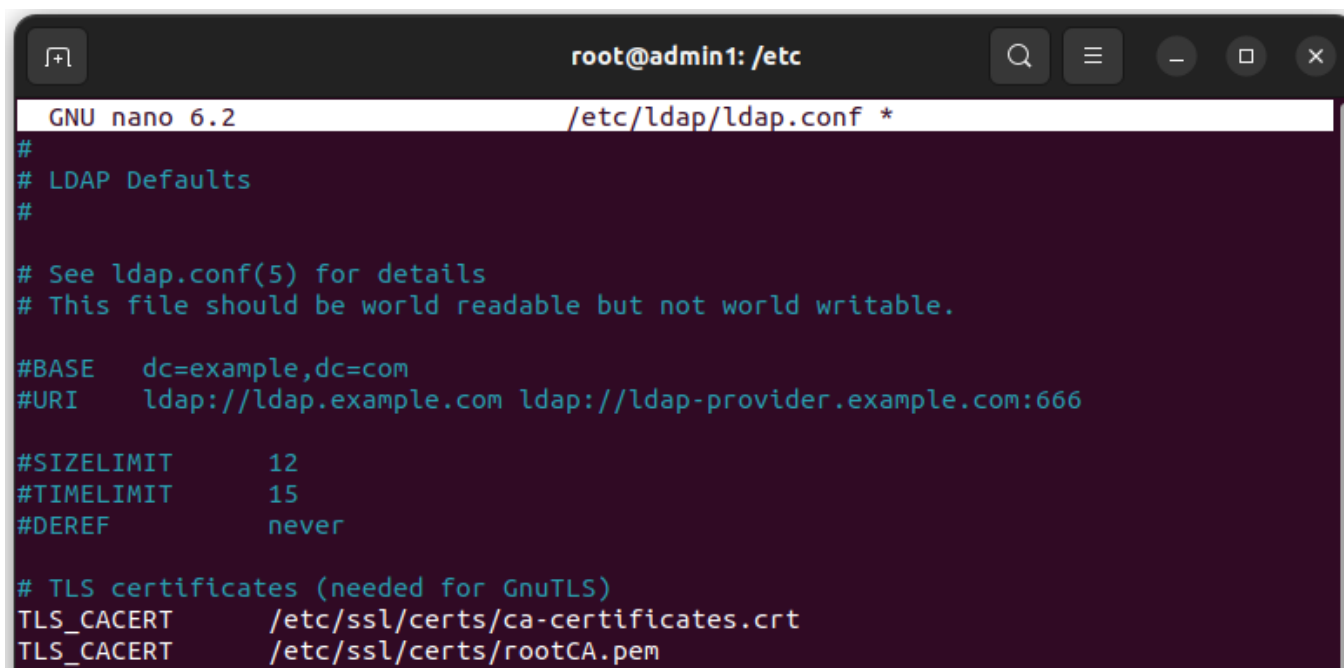


```
root@admin1: /home/admin1
root@admin1:/home/admin1# update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping Datagile_rootCAfull.pem,it does not contain exactly one certificate or CRL
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
root@admin1:/home/admin1#
```

Рисунок 4.6 – Обновление содержания репозитория

5. Отредактировать конфигурационный файл `/etc/ldap/ldap.conf`, внося дополнительную строку в конец файла:

```
TLS_CACERT      /etc/ssl/certs/rootCA.pem
```



```
GNU nano 6.2 /etc/ldap/ldap.conf *
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
#BASE    dc=example,dc=com
#URI      ldap://ldap.example.com ldap://ldap-provider.example.com:666
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never
# TLS certificates (needed for GnuTLS)
TLS_CACERT    /etc/ssl/certs/ca-certificates.crt
TLS_CACERT    /etc/ssl/certs/rootCA.pem
```

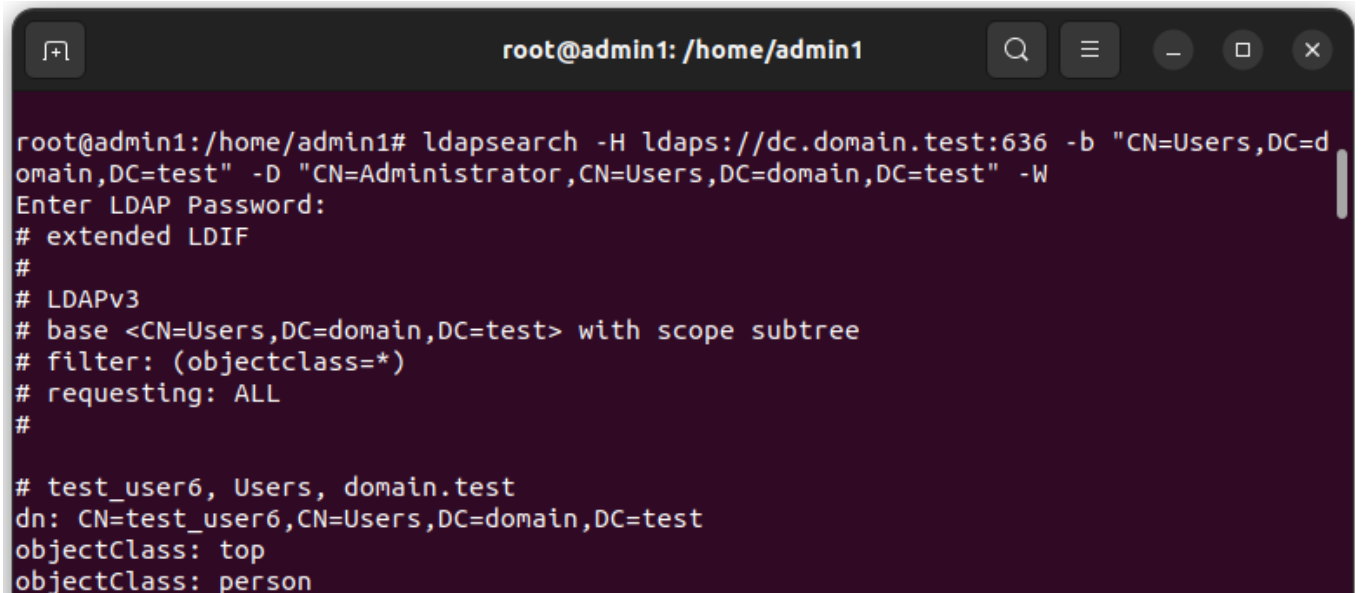
Рисунок 4.7 - Конфигурационный файл `/etc/ldap/ldap.conf`

6. Установить пакет `ldap-utils`

```
apt install ldap-utils
```

7. Выполнить команду `ldapsearch` для проверки соединения к активному каталогу с сервера СУБД:

```
ldapsearch -H ldaps://dc.domain.test:636 -b  
"CN=Users,DC=domain,DC=test" -D  
"CN=Administrator,CN=Users,DC=domain,DC=test" -W
```



```
root@admin1: /home/admin1  
root@admin1:/home/admin1# ldapsearch -H ldaps://dc.domain.test:636 -b "CN=Users,DC=d  
omain,DC=test" -D "CN=Administrator,CN=Users,DC=domain,DC=test" -W  
Enter LDAP Password:  
# extended LDIF  
#  
# LDAPv3  
# base <CN=Users,DC=domain,DC=test> with scope subtree  
# filter: (objectclass=*)  
# requesting: ALL  
#  
# test_user6, Users, domain.test  
dn: CN=test_user6,CN=Users,DC=domain,DC=test  
objectClass: top  
objectClass: person
```

Рисунок 4.8 – Команда и вывод проверки соединения

Если ранее выполненные действия были верны, то команда осуществит вывод.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификационная информация — информация, используемая при аутентификации субъекта доступа или объекта доступа.

Аутентификация – действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации (ГОСТ Р 58833-2020).

Идентификация доступа – присвоение субъектам и объектам доступа идентификаторов и сравнение предъявленного идентификатора с утвержденным перечнем.

Идентификатор – признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию (ГОСТ Р 58833-2020).

Пароль – конфиденциальная аутентификационная информация, обычно состоящая из строки знаков (ГОСТ Р 58833-2020).

Профиль – совокупность параметров для доступа к учетным записям AD.

Соответствие групп (mapping) – совокупность параметров, описывающих какие учетные записи AD будут синхронизированы с учетными записями СУБД.

Учетная запись – совокупность данных о пользователе, на основании которых происходит отличие одного пользователя от другого.

Служебный идентификатор – последовательность символов (буквенно-цифровая), по которой УЗ является уникальной в рамках каталога.

Сервисы управления УЗ – системное программное обеспечение, предоставляющее средства добавления/изменения/удаления УЗ.

Внешняя система аутентификации – сетевая служба, осуществляющая аутентификацию пользователей.

FreeIPA (акроним от англ. Free Identity, Policy and Audit) – открытое программное обеспечение, специализированная служба каталогов, предназначенная для создания в

ОС Linux среды, позволяющей централизованно управлять аутентификацией пользователей, устанавливать политики доступа и аудита.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

AD	–	Active Directory — службы каталогов корпорации Microsoft для операционных систем семейства Windows Server
DEB	–	сокращение от Debian — расширение имен файлов «бинарных» пакетов для распространения и установки программного обеспечения в операционной системе проекта Debian
GSSAPI	–	Generic Security Services Application Programming Interface — программный интерфейс сервисов безопасности
IP	–	Internet Protocol — маршрутизируемый протокол сетевого уровня стека TCP/IP
IT	–	Information technology — информационные технологии
LDAP	–	Lightweight Directory Access Protocol — протокол прикладного уровня для доступа к каталогам
RPM	–	RPM Package Manager — формат пакетов программного обеспечения, в операционной системе проекта Red Hat
SQL	–	Structured Query Language — язык структурированных запросов
SSPI	–	Security Support Provider Interface — программный интерфейс в Microsoft Windows между приложениями и провайдерами безопасности
SSSD	–	System Security Services Daemon - демон или служба, которая обеспечивает доступ к службам аутентификации, авторизации и аккаунтинга для приложений и сервисов в системе. SSSD работает на Linux и других Unix-подобных системах и предоставляет унифицированный интерфейс для различных источников данных, таких как PAM (Pluggable Authentication Modules), Kerberos, LDAP (Lightweight Directory Access Protocol) и другие. SSSD улучшает безопасность, производительность и упрощает управление сервисами безопасности в системе.
FQDN	–	Fully Qualified Domain Name - полное доменное имя, уникальное имя, идентифицирующее хост (компьютер или устройство) в сети Интернет или в локальной сети. FQDN состоит из двух частей: относительного имени (часто это название самой организации или домена, например, example.com) и корневого домена (www, org, net, com и т.д.). FQDN позволяет точно идентифицировать устройство и обеспечивает связь с другими устройствами или ресурсами в сети.
СУБД	–	Система управления базами данных
УЗ	–	Учетная запись

[illegible]

№ изменения: _____	Подпись отв. лица: _____	Дата внесения изм: _____
--------------------	--------------------------	--------------------------