ООО "РТ МИС"

ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА.МИС 3.0

(ЕЦП.МИС 3.0)

Руководство администратора

Подсистема "Администрирование" 3.0.4_1

Модуль "Учетные записи пользователей" 3.0.4

Содержание

Перечень терминов, сокращений и обозначений

В настоящем документе применяют следующие термины с соответствующими определениями, сокращения и обозначения:

base64	–	Стандарт кодирования двоичных данных при помощи 64 символов ASCII
DSE	–	DSA Specific Entry – запись управления или контроля на LDAP-сервере
LDAP	–	Lightweight Directory Access Protocol – протокол быстрого доступа к каталогам
LDAP-сервер	–	Сервер, где хранится база каталогов с предоставлением доступа к базе данных, информация в которой хранится в иерархической структуре
LDIF	–	LDAP Data Interchange Forma – формат обмена данными с LDAP-сервера, представляющий записи сервера каталогов или их изменения в текстовой форме
SASL	–	Simple Authentication and Security Layer – механизм аутентификации пользователей LDAP-сервера
VLV-индексы	–	Virtual List View – индекс виртуального представления списка на LDAP-сервере
Кэши LDAP	–	Буферы для быстрого сохранения в памяти информации: запросов, ответов и данных идентификации пользователей
Отличительные имена (DN, Distinguished Names)	–	Описание содержимого атрибутов в дереве (путь навигации), требуемое для доступа к конкретной записи или базовой (стартовой) записи поиска. DN состоит из пар вида "атрибут=значение", разделенных запятыми
Относительное уникальное имя (RDN, Relative Distinguished Names)	–	Описание элемента в дереве
Публикация	–	Создание и обновление записей, соответствующих различным типам данных, на LDAP-сервере

Расширенные операции	–	Вид операций на LDAP-сервере, при которых стандартные операции сервера каталогов возможно объединить как набор операций в единую транзакцию
Схема	–	Набор правил, определяющих допустимые типы данных записей, а также структуру и синтаксис их атрибутов, которые можно хранить в каталоге
Транзакция	–	Группа операций с каталогом на LDAP-сервере, объединенных в единое целое
Управляющие элементы	–	Дополнительная информация, которая определяет способ интерпретации сервером полученного запроса

1 Введение

1.1 Область применения

Настоящий документ описывает порядок работы с модулем "Учетные записи пользователей" 3.0.4 подсистемы "Администрирование" 3.0.4_1 (далее – Подсистема, подсистема), являющейся частью Единой информационной системы здравоохранения (далее– Система, система).

1.2 Краткое описание возможностей

Подсистема "Администрирование" 3.0.4_1 предназначена для настройки функционирования программных компонент и данных в составе Системы, работы с учетными записями пользователя, настройки доступа пользователей к функциям системы, работы с функциями Системы.

Модуль "Учетные записи пользователей" 3.0.4 предназначен для хранения и управления сведениями о пользователях и группах пользователей Системы. Хранение сведений организовано в иерархической каталогизированной структуре с обеспечением доступа к данным по протоколу LDAP.

1.3 Уровень подготовки администратора

К администраторам Подсистемы предъявляются следующие требования:

- глубокое понимание Подсистемы на уровне технологий работы;
- знание основ администрирования;
- знание основ администрирования реляционных баз данных, поддерживающих клиент-серверный режим;
- навыки реализации различных режимов работы операционных систем;
- навыки администрирования учетных записей пользователей Системы.

1.4 Перечень эксплуатационной документации, с которым необходимо ознакомиться администратору

Перед началом работы администраторам рекомендуется ознакомиться с положениями данного Руководства администратора в части своих функциональных обязанностей.

2 Общие сведения

Хранение сведений о пользователях и группах пользователей Системы в модуле "Учетные записи пользователей" осуществляется в нереляционной форме с использованием каталогизированной иерархической структуры.

В рамках LDAP-сервера выполняется хранение учетных данных пользователя. В процессе авторизации по пользователю формируется сессия, хранение которой выполняется в MongoDB.

2.1 Описание процесса

Описание процесса использования модуля "Учетные записи пользователей" в составе Системы приведен на примере процесса авторизации пользователя.

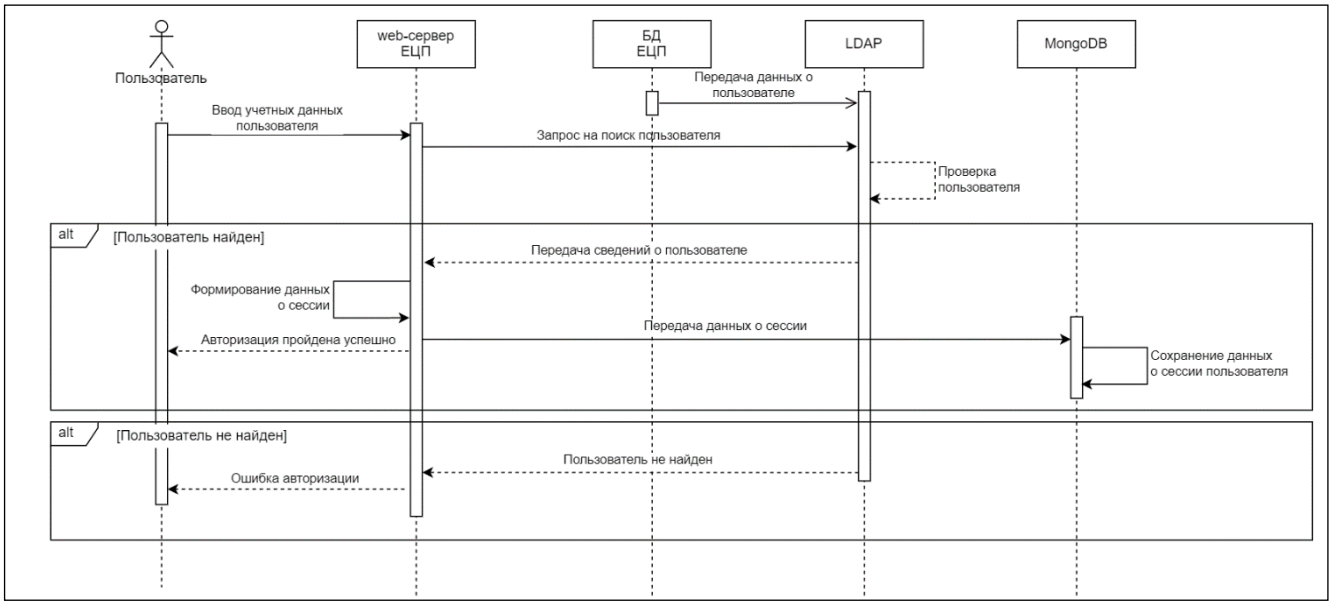


Рисунок 1 – Описание процесса

2.2 Состав экранных форм

Модуль "Учетные записи пользователей" не имеет графического интерфейса. Управление модулем осуществляется текстовыми командами в режиме командной строки.

2.3 Функции модуля

Модуль "Учетные записи пользователей" выполняет следующие группы функций:

- функции конфигурации:
  - создание и удаление критериев фильтрации для журналов доступа сервера каталогов;

- создание и удаление обработчиков уведомлений о статусах аккаунта;
- создание и удаление обработчиков оповещений;
- создание индексов для серверных компонентов сервера каталогов;
- создание и удаление VLV-индексов для серверных компонентов сервера каталогов;
- создание и удаление правил сопоставления сертификатов;
- создание и удаление обработчиков подключений к серверу каталогов;
- создание и удаление точек для отладки;
- создание и удаление кэша для записей в сервере каталогов;
- создание и удаление обработчиков расширенных операций;
- создание и удаление реализаций для групп в сервере каталогов;
- создание и удаление механизмов авторизации по протоколу HTTP;
- создание и удаление точек доступа к функциям сервера каталогов по протоколу HTTP;
- создание и удаление правил сравнения идентификаторов на сервере каталогов;
- создание и удаление провайдеров управления ключами;
- создание и удаление публикаций о выполняемых операциях в журналах;
- создание и удаление политики хранения журналов;
- создание и удаление политики ротации журналов;
- создание и удаление провайдеров мониторинга;
- создание и удаление генераторов паролей;
- создание и удаление политики аутентификации;
- создание и удаление схем хранения паролей;
- создание и удаление валидаторов паролей;
- создание и удаление плагинов;
- создание и удаление доменов репликации;
- создание и удаление серверов репликации;
- создание и удаление обработчиков механизмов SASL;
- создание и удаление провайдеров схем;
- создание и удаление механизмов обнаружения сервисов;
- создание и удаление провайдеров синхронизации;
- создание и удаление провайдеров управления доверием;
- создание и удаление виртуальных атрибутов;
- отображение свойств обработчика контроля доступа;

- отображение свойств критериев фильтрации для журналов доступа сервера каталогов;
- отображение свойств обработчиков уведомлений о статусах аккаунта;
- отображение свойств подключения администратора;
- отображение свойств обработчиков оповещений;
- отображение свойств индексов для серверных компонентов сервера каталогов;
- отображение свойств серверных компонентов;
- отображение свойств VLV-индексов для серверных компонентов сервера каталогов;
- отображение свойств для правил сопоставления сертификатов;
- отображение свойств обработчиков подключений к серверу каталогов;
- отображение свойств менеджера криптографии;
- отображение свойств для точек отладки;
- отображение свойств кэша для записей в сервере каталогов;
- отображение свойств для обработчиков расширенных операций;
- отображение свойств внешнего домена журнала изменений;
- отображение свойств глобальной конфигурации сервера каталогов;
- отображение свойств для реализации для групп в сервере каталогов;
- отображение свойств для механизмов авторизации по протоколу HTTP;
- отображение свойств для точки доступа к функциям сервера каталогов по протоколу HTTP;
- отображение свойств для правил сравнения идентификаторов на сервере каталогов;
- отображение свойств для провайдеров управления ключами;
- отображение свойств для публикаций о выполняемых операциях в журналах;
- отображение свойств для политик хранения журналов;
- отображение свойств для политик ротации журналов;
- отображение свойств для провайдеров мониторинга;
- отображение свойств для генераторов паролей;
- отображение свойств для политик аутентификации;
- отображение свойств для схем хранения паролей;
- отображение свойств для валидаторов паролей;
- отображение свойств для плагинов;
- отображение свойств корневого компонента плагина;
- отображение свойств для доменов репликации;

- отображение свойств для серверов репликации;
- отображение свойств для корневого отличительного имени (DN);
- отображение свойств серверного компонента корневого DSE;
- отображение свойств для обработчиков механизмов SASL;
- отображение свойств для провайдеров схем;
- отображение свойств для механизмов обнаружения сервисов;
- отображение свойств для провайдеров синхронизации;
- отображение свойств для провайдеров управления доверием;
- отображение свойств для виртуальных атрибутов;
- отображение свойств для очередей задач;
- вывод списка существующих критериев фильтрации для журналов доступа сервера каталогов;
- вывод списка существующих обработчиков уведомлений о статусах аккаунта;
- вывод списка существующих обработчиков оповещений;
- вывод списка существующих индексов для серверных компонентов сервера каталогов;
- вывод списка существующих VLV-индексы для серверных компонентов сервера каталогов;
- вывод списка существующих серверов каталогов;
- вывод списка существующих правил сопоставления сертификатов;
- вывод списка существующих обработчиков подключений к серверу каталогов;
- вывод списка существующих точек для отладки;
- вывод списка существующих кэшей для записей в сервере каталогов;
- вывод списка существующих обработчиков расширенных операций;
- вывод списка существующих реализаций для групп в сервере каталогов;
- вывод списка существующих механизмов авторизации по протоколу HTTP;
- вывод списка существующих точек доступа к функциям сервера каталогов по протоколу HTTP;
- вывод списка существующих правил сравнения идентификаторов на сервере каталогов;
- вывод списка существующих провайдеров управления ключами;
- вывод списка существующих публикаций о выполняемых операциях в журналах;
- вывод списка существующих политик хранения журналов;
- вывод списка существующих политик ротации журналов;

- вывод списка существующих провайдеров мониторинга;
- вывод списка существующих генераторов паролей;
- вывод списка существующих политик аутентификации;
- вывод списка существующих схем хранения паролей;
- вывод списка существующих валидаторов паролей;
- вывод списка существующих плагинов
- вывод сведений об управляемых объектах и их свойствах;
- вывод списка существующих доменов репликации;
- вывод списка существующих серверов репликации;
- вывод списка существующих обработчиков механизмов SASL;
- вывод списка существующих провайдеров схем;
- вывод списка существующих механизмов обнаружения сервисов;
- вывод списка существующих провайдеров синхронизации;
- вывод списка существующих провайдеров управления доверием;
- вывод списка существующих виртуальные атрибуты;
- редактирование свойств обработчика контроля доступа;
- изменение свойств для критериев фильтрации в журналах доступа сервера каталогов;
- изменение свойств для обработчиков уведомлений о статусах аккаунта;
- изменение свойств подключения администратора;
- изменение свойств обработчиков оповещений;
- изменение свойств для индексов серверных компонентов сервера каталогов;
- изменение свойств серверных компонентов;
- изменение свойств VLV-индексов для серверных компонентов сервера каталогов;
- изменение свойств для правил сопоставления сертификатов;
- изменение свойств обработчиков подключений к серверу каталогов;
- изменение свойств менеджера криптографии;
- изменение свойств для точек отладки;
- изменение свойств кэша для записей в сервере каталогов;
- изменение свойств для обработчиков расширенных операций;
- изменение свойств внешнего домена журнала изменений;
- изменение свойств глобальной конфигурации сервера каталогов;
- изменение свойств для реализации групп в сервере каталогов;
- изменение свойств для механизмов авторизации по протоколу HTTP;

  - изменение свойств для точки доступа к функциям сервера каталогов по протоколу HTTP;
  - изменение свойств для правил сравнения идентификаторов на сервере каталогов;
  - изменение свойств для провайдеров управления ключами;
  - изменение свойств для публикаций о выполняемых операциях в журналах;
  - изменение свойств для политик хранения журналов;
  - изменение свойств для политик ротации журналов;
  - изменение свойств для провайдеров мониторинга;
  - изменение свойств для генераторов паролей;
  - изменение свойств для политик аутентификации;
  - изменение свойств для схем хранения паролей;
  - изменение свойств для валидаторов паролей;
  - изменение свойств для плагинов;
  - изменение свойств корневого компонента плагина;
  - изменение свойств для доменов репликации;
  - изменение свойств для серверов репликации;
  - изменение свойств для корневого отличительного имени (DN);
  - изменение свойств серверного компонента корневого DSE;
  - изменение свойств для обработчиков механизмов SASL;
  - изменение свойств для провайдеров схем;
  - изменение свойств для механизмов обнаружения сервисов;
  - изменение свойств для провайдеров синхронизации;
  - изменение свойств для провайдеров управления доверием;
  - изменение свойств для виртуальных атрибутов;
  - изменение свойств для очередей задач;
- функции работы с данными:
  - кодирование информации о пользователях и группах пользователей в каталогах сервера с использованием стандарта base64;
  - декодирование информации о пользователях и группах пользователей в каталогах сервера с использованием стандарта base64;
  - шифрование паролей пользователей на сервере каталогов;
  - сравнение данных на сервере каталогов;
  - удаление данных на сервере каталогов;
  - изменение паролей пользователей на сервере каталогов;

  - поиск данных с использованием протокола LDAP на сервере каталогов;
- функции работы с файлами:
  - экспорт данных с сервера каталогов в формате LDIF;
  - импорт данных в формате LDIF с сервера каталогов;
  - просмотр DN-файлов на сервере каталогов;
  - добавление DN-файлов на сервере каталогов;
  - удаление DN-файлов на сервере каталогов;
  - изменение DN-файлов на сервере каталогов;
  - сравнение двух файлов в формате LDIF;
  - изменение записей в файлах формата LDIF;
  - добавление записей в файлах формата LDIF;
  - удаление записей в файлах формата LDIF;
  - поиск данных по записям, содержащимся в файле LDIF;
  - формирование данных в формате LDIF на основе правил определения в файле шаблона;
  - создание файла шаблона в формате LDIF;
- функции управления модулем:
  - отображение сведения о состоянии серверного компонента;
  - формирование резервные копии данных серверных каталогов;
  - создание сценариев RC для выполнения следующих действий над сервером каталогов;
  - отображение сведений о конфигурации сервера каталогов;
  - изменение значения аргументов java на сервере каталогов;
  - репликация данных между несколькими серверами каталогов;
  - составление списков серверных систем и базовых отличительных имен (DN), настроенных на сервере каталогов;
  - извлечение значений переменных состояния политики паролей;
  - формирование списка задач, запланированных к выполнению на сервере каталогов;
  - перестройка индексов в индексированной внутренней базе данных сервера каталогов;
  - восстановление резервной копии серверной части сервера каталогов;
  - настройки сервера каталогов;
  - запуск сервера каталогов;
  - отображение основной информации о функционировании сервера каталогов;

- остановка сервера каталогов;
- удаление сервера каталогов;
- обновление конфигурации и данных серверного компонента модуля и сервера каталогов.
- проверка корректности индексов в индексированной внутренней базе данных сервера каталогов;
- запуск сервера каталогов в качестве службы Windows.

2.4 Состав атрибутов

Хранение сведений о пользователях на LDAP-сервере выполняется согласно следующей структуры:

Наименование поля	**Описание**	**Тип данных**	**Комментарий**
dn	Идентификатор пользователя в LDAP	string	Пример: "uid=login,ou=users,dc=swan,dc=perm,dc=ru"
uid	Логин пользователя	string	
userpassword	Хэш пароля пользователя	string	
cn	Имя пользователя (составное)	string	
sn	Фамилия пользователя	string	
givenname	Имя пользователя	string	
secname	Отчество пользователя	string	
email	Адрес электронной почты пользователя	string	
phone	Номер телефона пользователя	string	
phone_act	Статус активации телефона	string	
phone_act_code	Код подтверждения для телефона	string	
marshserial	Идентификатор МАРШ	string	

Наименование поля	Описание	Тип данных	Комментарий
swtoken	Токен	string	
swtoken_enddate	Дата окончания действия токена	string	
about	Информация о пользователе	string	
avatar	Аватар пользователя	string	
description	Описание записи в LDAP.	string	
employeenumber	Идентификатор врача.	string	Идентификатор медицинского работника из БД ЕЦП - MedPersonal_id
orgid	Список организаций пользователя	string	Поле представлено в виде массива строк с хранением идентификаторов организаций пользователя. Идентификатор организации из БД ЕЦП - Org_id
certs	Сертификаты пользователя	string	
pseudonym	Настройки пользователя	string	Используется сериализованный массив
uidnumber	Идентификатор пользователя в ЕЦП	string	Идентификатор медицинского работника из БД ЕЦП - pmUser_id
blocked	Признак блокировки учетной записи пользователя	string	
medsvidgrantadd	Признак права выписывать медицинские свидетельства	string	

Наименование поля	Описание	Тип данных	Комментарий
deniedarms	Матрица запретов доступа к АРМ в ЕЦП	string	
password_temp	Признак временного пароля	string	
password_last	Последний временный пароль пользователя	string	Поле представлено в виде массива строк с хранением последних 4 временных паролей. Пример: ["{MD5}Az8bh0hPSTi2xfP0Liooew==","{MD5}pZopfz1D+lsvXaFDPBHykg==","{MD5}y1EkNQfdkETA5Os6pJHIzw==","1","{MD5}FpRNiCNPgNAJnXj22c2wuA=="]
password_date	Дата задания пароля	string	Формат даты - unix time
shown_armlist	Перечень АРМ с настроенными уведомлениями	string	JSON-массив АРМ, в которых пользователь получает уведомления. Пример: {"Date":"2020-01-15","Arms":["polka"]}
organizationalstatus	Признак активности пользователя	string	
lis	Настройки ЛИС	string	Перечень настроек пользователя в ЛИС
parallelsessions	Количество параллельных сеансов для пользователя	string	

Наименование поля	**Описание**	**Тип данных**	**Комментарий**
loginemias	Логин пользователя в ЕМИАС	string	

3 Интерфейсы и инструменты администрирования модуля "Учетные записи пользователей" 3.0.4

Программное обеспечение модуля устанавливается с кроссплатформенной панелью управления на основе Java Swing для решения множества повседневных задач.

Программное обеспечение модуля также устанавливает инструменты командной строки для задач настройки и управления.

Панель управления модуля предлагает графический интерфейс для управления как локальными, так и удаленными серверами.

Версия панели управления модуля должна совпадать с целевой версией сервера каталогов модуля. Запустите панель управления модуля, выполнив control-panel команду:

- Linux, Solaris – запустите /path/to/opendj/bin/control-panel;
- Windows – дважды нажмите C:\path\to\opendj\bat\control-panel.bat;
- Mac OS X – дважды нажмите /path/to/opendj/bin/ControlPanel.app.

При входе в панель управления модулем пройдите аутентификацию через LDAP.

3.1 Данные каталога

Подготовка данных каталога обычно не является тем, что выполняется вручную в большинстве развертываний. Обычно записи создаются, изменяются и удаляются через определенные клиентские приложения каталога.

Окно "Управление записями" может быть полезным при проектировании и тестировании данных каталога, а также при изменении отдельных ACI или отладке проблем с определенными записями.

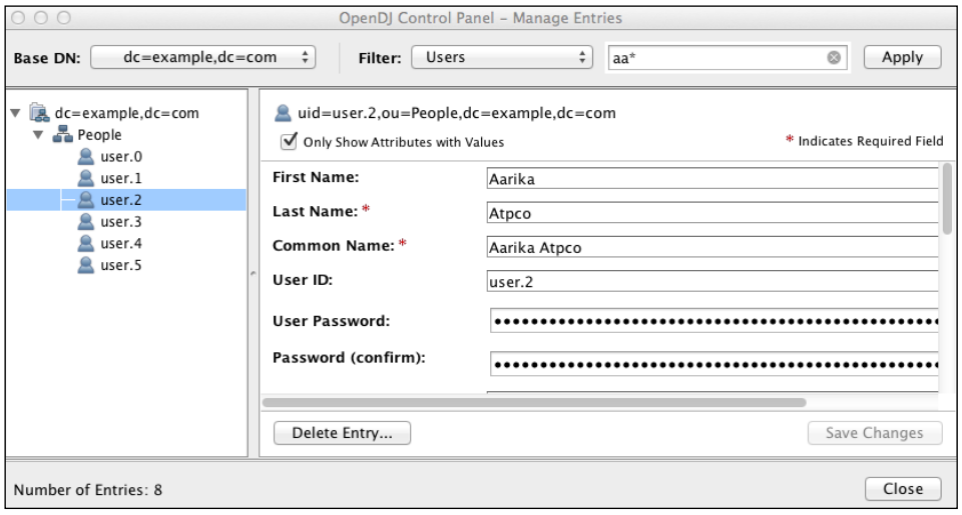


Рисунок 2 – Окно "Управление записями"

Список Directory Data упрощает создание нового базового DN, а затем импорт пользовательских данных для нового базового DN из файлов LDAP Data Interchange Format (LDIF). Доступно использование инструментов в списке для экспорта пользовательских данных в LDIF, а также для резервного копирования и восстановления пользовательских данных.

3.2 Схема

Окно Manage Schema позволяет просматривать и изменять правила, определяющие, как данные хранятся в каталоге. Доступно добавление новых схем определения: новые типы атрибутов и новые классы объектов.

При работе модуля внесенные изменения сразу применяются.

3.3 Индексы

В окне Manage Indexes доступен краткий обзор всех индексов, которые в настоящее время поддерживаются для атрибутов каталога. Чтобы защитить ресурсы каталога от поглощения дорогостоящими поисками по неиндексированным атрибутам, доступно сохранение поведения по умолчанию, предотвращая неиндексированные поиски, вместо этого добавляя индексы, требуемые определенными приложениями.

Панель управления модулем также позволяет проверять и перестраивать существующие индексы, что может потребоваться после операции обновления или при повреждении индекса.

3.4 Мониторинг

Список мониторинга предназначен для просмотра информации о системе, используемой виртуальной машине Java (JVM) и указания о том, как используется кэш, заполняется ли очередь работ, а также сведения о базе данных. Доступен просмотр количества и типов запросов, поступающих через обработчики соединений, а также текущие задачи в процессе выполнения.

3.5 Параметры выполнения

Если не заданы соответствующие параметры среды выполнения JVM во время процесса установки, это доступно сделать через панель управления.

3.6 Инструменты командной строки

Инструменты установки и обновления: setup, upgrade и uninstall, находятся в родительском каталоге других инструментов, поскольку эти инструменты не используются для

повседневного администрирования. Например, если путь к большинству инструментов – /path/to/opendj/bin, вы можете найти эти инструменты в /path/to/opendj.

Все инструменты командной строки поддерживают эту --help опцию.

Все команды вызывают программы Java и подразумевают запуск JVM.

Инструменты и ограничения сервера:

Команды	**Ограничения**
backendstat create-rc-script dsjavaproperties encode-password list-backends setup start-ds upgrade windows-service	Команды необходимо использовать с локальным сервером каталогов модуля в той же установке, что и инструменты
control-panel dsconfig export-ldif import-ldif manage-account manage-tasks rebuild-index restore status stop-ds uninstall verify-index	Команды необходимо использовать с сервером каталогов модуля той же версии, что и команда
dsreplication	Команда может использоваться с текущей и предыдущей версиями сервера каталогов модуля. Единственным исключением является dsreplication reset-change-number подкоманда, которая требует версию сервера каталогов

Команды	Ограничения
make-ldif	Команда зависит от файлов шаблонов. Файлы шаблонов могут использовать файлы конфигурации, установленные с сервером каталогов модуля в config/MakeLDIF/
base64 ldapcompare ldapdelete ldapmodify ldappasswordmodify ldapsearch ldif-diff ldifmodify ldifsearch	Команды можно использовать независимо от сервера каталогов модуля, они не привязаны к конкретной версии

В следующем списке используются имена команд UNIX. В Windows все инструменты командной строки имеют расширение .bat:

- backendstat – отладка баз данных для подключаемых бэкэндов;
- backup – резервное копирование или планирование резервного копирования данных каталога;
- base64 – кодирование и декодирование данных в формате base64. Кодировка Base64 представляет двоичные данные в формате ASCII и может использоваться, например, для кодирования строк символов в формате LDIF;
- create-rc-script (UNIX) – создание скрипта, который можно использовать для запуска, остановки и перезапуска сервера либо напрямую, либо при загрузке и завершении работы системы. Используйте create-rc-script -f script-file;
- dsconfig – является основным инструментом командной строки для просмотра и редактирования конфигурации модуля. При запуске без аргументов dsconfig запрашивает информацию об административном подключении. После подключения предоставляет интерфейс на основе меню для конфигурации сервера. При передаче информации о соединении, подкоманд и дополнительных параметров dsconfig команда выполняется в режиме скрипта и поэтому не является интерактивной;
- dsjavaproperties – применение внесенных изменений opendj/config/java.properties, которые задают параметры среды выполнения Java;

- dsreplication – настройка репликации данных между серверами каталогов, чтобы синхронизировать их содержимое;
- encode-password – шифрование открытого пароля в соответствии с одной из доступных схем хранения;
- export-ldif – экспорт данных каталога в LDIF в стандартное, переносимое, текстовое представление содержимого каталога;
- import-ldif – загрузка содержимого LDIF в каталог, перезаписав существующие данные. Его нельзя использовать для добавления данных в базу данных бэкэнда;
- ldapcompare – сравнение указанных значений атрибутов со значениями, хранящимися в записях в каталоге;
- ldapdelete – удаление одной записи или целой ветви подчиненных записей в справочнике;
- ldapmodify – изменение указанных значений атрибутов для указанных записей. Используйте ldapmodify команду с -a возможностью добавления новых записей;
- ldappasswordmodify – изменение паролей пользователей;
- ldapsearch – поиск в ветви данных каталога записей, соответствующих указанному фильтру LDAP;
- ldif-diff – отображение различий между двумя файлами LDIF с получением выходных данных в формате LDIF;
- ldifmodify – аналогично ldapmodify команде измените указанные значения атрибутов для указанных записей в файле LDIF;
- ldifsearch – аналогично ldapsearch команде выполните поиск в ветви данных в LDIF на предмет записей, соответствующих указанному фильтру LDAP;
- list-backends – список бэкэндов и базовых DN, обслуживаемых сервером каталогов модуля;
- make-ldif – генерация данных каталога в формате LDIF на основе шаблонов, определяющих, как должны отображаться данные. Команда make-ldif предназначена для создания тестовых данных;
- manage-account –блокировка и разблокировка учетных записей пользователей, а также просмотр и изменение информации о состоянии политики паролей;
- manage-tasks – просмотр информации о задачах, запланированных к запуску на сервере, и отмена указанных задач;
- rebuild-index – перестроить индекс, хранящийся в индексированном бэкэнде;
- restore – восстановление данных из резервной копии;

- start-ds – запуск сервера каталогов модуля;
- status – отображение информации о сервере;
- stop-ds – остановка сервера каталогов модуля;
- verify-index – убедитесь, что индекс, хранящийся в индексированном бэкэнде, не поврежден;
- windows-service (Windows) – регистрация модуля как службы Windows.

4 Управление процессами сервера

4.1 Запуск сервера

Используйте один из следующих методов:

- используйте start-ds команду:

```
start-ds
```

В качестве альтернативы вы можете указать --no-detach опцию запуска сервера на переднем плане.

- Linux – если сервер каталогов модуля был установлен из пакета .deb или .rpm, то скрипты управления службами создавались во время установки. Используйте service opendj start команду:

```
centos# service opendj start
Starting opendj (via systemctl):                           [  OK  ]


ubuntu$ sudo service opendj start
$Starting opendj: > SUCCESS.
```

- UNIX – создайте сценарий RC с помощью create-rc-script команды, а затем используйте сценарий для запуска сервера. Если вы не запускаете модуль в Linux от имени пользователя root, используйте --userName userName опцию, чтобы указать пользователя, установившего модуль:

```
sudo create-rc-script \
 --outputFile /etc/init.d/opendj \
 --userName mark
 sudo /etc/init.d/opendj start
```

Если вы запускаете модуль в Linux как пользователь root, вы можете использовать скрипт RC для запуска сервера при загрузке системы и остановки сервера при завершении работы системы:

```
sudo update-rc.d opendj defaults
update-rc.d: warning: /etc/init.d/opendj missing LSB information
update-rc.d: see <http://wiki.debian.org/LSBInitScripts>
 Adding system startup for /etc/init.d/opendj ...
   /etc/rc0.d/K20opendj -> ../init.d/opendj
   /etc/rc1.d/K20opendj -> ../init.d/opendj
   /etc/rc6.d/K20opendj -> ../init.d/opendj
   /etc/rc2.d/S20opendj -> ../init.d/opendj
   /etc/rc3.d/S20opendj -> ../init.d/opendj
   /etc/rc4.d/S20opendj -> ../init.d/opendj
   /etc/rc5.d/S20opendj -> ../init.d/opendj
```

- Windows – зарегистрируйте модуль как службу Windows с помощью windows-service команды, а затем управляйте службой с помощью инструментов администрирования Windows:

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

По умолчанию модуль сохраняет сжатую версию конфигурации сервера, используемую при успешном запуске. Это гарантирует, что сервер предоставит последнюю известную хорошую конфигурацию, которую можно использовать в качестве справочной или скопировать в активную конфигурацию, если сервер не запустится с текущей активной конфигурацией.

4.2 Остановка сервера

Сервер каталогов модуля рассчитан на восстановление после сбоев и несанкционированного завершения работы, безопаснее завершить работу сервера корректно, поскольку корректное завершение работы сокращает задержки запуска, в течение которых сервер модуля пытается восстановить состояние базы данных, и предотвращает ситуации, когда сервер модуль не может восстановиться автоматически.

Чтобы корректно завершить работу сервера модуля, выполните следующие действия:

- если вы окончательно останавливаете реплицированный сервер, удалите сервер из топологии репликации:

```
dsreplication \
 disable \
 --disableAll \
 --port 4444 \
 --hostname opendj.example.com \
 --adminUID admin \
 --adminPassword password \
 --trustAll \
 --no-prompt
```

Этот шаг отменяет регистрацию сервера в топологии репликации, эффективно удаляя его конфигурацию репликации с других серверов. Этот шаг необходимо выполнить до того, как вы выведете систему из эксплуатации, поскольку сервер должен подключиться к своим одноранговым узлам в топологии репликации.

- перед завершением работы системы, на которой работает сервер модуля, и перед отключением любого хранилища, используемого для данных каталога, остановите сервер, используя один из следующих методов:
  - используйте stop-ds команду:

```
stop-ds
```

  - Linux – если сервер каталогов модуля был установлен из пакета .deb или .rpm, то скрипты управления службами создавались во время установки. Используйте service opendj stop команду:

```
centos# service opendj stop
Stopping opendj (via systemctl):                           [  OK  ]


ubuntu$ sudo service opendj stop
$Stopping opendj: ... > SUCCESS.
```

  - UNIX – создайте скрипт RC, а затем используйте его для остановки сервера:

```
sudo create-rc-script \
 --outputFile /etc/init.d/opendj \
 --userName mark
 sudo /etc/init.d/opendj stop
```

  - Windows – зарегистрируйте модуль как службу Windows, а затем управляйте службой с помощью инструментов администрирования Windows:

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

Не завершайте намеренно процесс сервера модуля, если только сервер полностью не перестает отвечать.

При корректной остановке сервер записывает информацию о состоянии в бэкэнды базы данных и снимает блокировки, которые он удерживает в файлах базы данных.

4.3 Перезапуск сервера

Используйте один из следующих методов:

- используйте stop-ds команду:

```
stop-ds --restart
```

- Linux – если сервер каталогов модуля был установлен из пакета .deb или .rpm, то скрипты управления службами создавались во время установки. Используйте service opendj restart команду:

```
centos# service opendj restart
Restarting opendj (via systemctl):                         [  OK  ]


ubuntu$ sudo service opendj restart
$Stopping opendj: ... > SUCCESS.

$Starting opendj: > SUCCESS.
```

- UNIX – создайте скрипт RC, а затем используйте его для остановки сервера:

```
sudo create-rc-script \
 --outputFile /etc/init.d/opendj \
 --userName mark
 /etc/init.d/opendj restart
```

- Windows – зарегистрируйте модуль как службу Windows, а затем управляйте службой с помощью инструментов администрирования Windows:

```
C:\path\to\opendj\bat> windows-service.bat --enableService
```

4.4 Восстановление сервера

Модулю может потребоваться повторно воспроизвести последние несколько записей в журнале транзакций. Обычно модуль быстро возвращается к работе.

Сообщения о восстановлении базы данных находятся в файле журнала базы данных, например /path/to/opendj/db/userRoot/dj.log.

Примеры сообщений из журнала восстановления:

- записано в начале процесса восстановления:

```
111104 10:23:48:967 CONFIG [/path/to/opendj/db/userRoot]Recovery
 underway, found end of log
...
```

- записано в конце процесса:

```
111104 10:23:49:015 CONFIG [/path/to/opendj/db/userRoot]Recovery finished:
 Recovery Info ...
```

5 Управление данными каталога

5.1 Импорт и экспорт данных

Вы можете использовать панель управления модулем для импорта данных (Directory Data > Import LDIF) и экспорта данных (Directory Data > Export LDIF).

Наиболее эффективным методом импорта данных LDIF является отключение сервера модуля от сети.

Импорт из LDIF перезаписывает все данные в целевом бэкэнде записями из данных LDIF.

Если вы не хотите использовать userRoot бэкэнд по умолчанию, создайте новый бэкэнд для своих данных.

В примере dc=example, dc=org данные импортируются в userRoot бэкэнд, перезаписывая существующие данные:

- если вы хотите ускорить процесс, сначала выключите сервер, а затем выполните import-ldif команду:

```
stop-ds
 import-ldif \
 --offline \
 --includeBranch dc=example,dc=org \
 --backendID userRoot \
 --ldifFile /path/to/generated.ldif
```

- если не нужно ускорять процесс, запланируйте задачу по импорту данных в режиме онлайн:

```
import-ldif \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --includeBranch dc=example,dc=org \
 --backendID userRoot \
 --ldifFile /path/to/generated.ldif \
 --trustAll
```

Если сервер реплицирован с другими серверами, инициализируйте репликацию еще раз после успешного импорта.

Инициализация репликации перезаписывает данные на удаленных серверах таким же образом, как импорт перезаписывает существующие данные данными LDIF.

В примерах экспортируются dc=example, dc=org данные из userRoot бэкэнда:

- чтобы ускорить экспорт, выключите сервер, а затем используйте export-ldif команду:

```
stop-ds
 export-ldif \
 --offline
 --includeBranch dc=example,dc=org \
 --backendID userRoot \
 --ldifFile /path/to/backup.ldif
```

- чтобы экспортировать данные в режиме онлайн, оставьте сервер работающим и запланируйте задачу:

```
export-ldif \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --includeBranch dc=example,dc=org \
 --backendID userRoot \
 --ldifFile /path/to/backup.ldif \
 --start 20111221230000 \
 --trustAll
```

5.2 Создание новой базы данных бэкэнда

Модуль хранит данные каталога в backend. Backend – это репозиторий, к которому сервер каталогов может получить доступ для хранения данных. Сервер каталогов модуля предлагает различные реализации, такие как backend памяти, backend файлов LDIF и backend базы данных. Backend базы данных можно резервировать и восстанавливать. По умолчанию модуль хранит данные в backend базы данных с именем userRoot.

Вы можете создавать новые бэкенды с помощью dsconfig create-backend команды. Сервер каталогов модуля поддерживает различные типы бэкендов, включая бэкенды в памяти, бэкенды, которые хранят данные в файлах LDIF, и бэкенды, которые хранят данные в базах данных "ключ-значение" с индексами для повышения производительности с большими наборами данных. При создании бэкенда выберите тип бэкенда.

Следующий пример создает бэкенд с именем myData. Бэкенд имеет тип pdb, который опирается на базу данных PDB для хранения данных и индексации. В качестве альтернативы вы можете выбрать другой тип бэкенда с другим аргументом для --type опции, как в --type je:

```
dsconfig \
 create-backend \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --type pdb \
 --backend-name myData \
 --set base-dn:dc=example,dc=com \
 --set enabled:true \
 --set db-cache-percent:25 \
 --trustAll \
 --no-prompt
```

После создания бэкэнда вы можете просмотреть настройки:

```
dsconfig \
 get-backend-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backend-name myData \
 --trustAll \
 --no-prompt
Property          : Value(s)
------------------:--------------------
backend-id        : myData
base-dn           : "dc=example,dc=com"
compact-encoding  : true
db-cache-percent  : 25
db-cache-size     : 0 b
db-directory      : db
enabled           : true
index-entry-limit : 4000
writability-mode  : enabled
```

5.3 Шифрование данных каталога

Сервер каталогов модуля может шифровать данные каталога перед их сохранением в базе данных на диске, сохраняя конфиденциальность данных до тех пор, пока к ним не получит доступ клиент каталога.

Шифрование данных полезно как минимум в следующих случаях:

- обеспечение конфиденциальности и целостности – зашифрованные данные каталога являются конфиденциальными и остаются конфиденциальными до тех пор, пока не будут расшифрованы с помощью надлежащего ключа. Шифрование обеспечивает целостность данных в момент доступа к ним. Каталог модуля не может расшифровать поврежденные данные;
- защита в общей инфраструктуре – при развертывании служб каталогов в общей инфраструктуре вы отказываетесь от полного и единоличного контроля над данными каталога.

Конфиденциальность данных и шифрование влекут за собой следующие компромиссы:

- индексы равенства ограничены сопоставлением равенства;
- влияние на производительность;
- конфигурация репликации перед шифрованием.

Сервер каталогов модуля по умолчанию не шифрует данные каталога. Любой пользователь с системным доступом для чтения файлов каталога может потенциально получить доступ к данным каталога в открытом виде:

```
strings /path/to/opendj/db/userRoot/dj* | grep bjensen | sort | uniq
'uid=bjensen,ou=People,dc=example,dc=com
/home/bjensen
bjensen
bjensen@example.com
```

Шифрование хранимых данных каталога не препятствует их отправке по сети в открытом виде.

Включите конфиденциальность бэкэнда с настройками шифрования по умолчанию, который применяется к userRoot бэкэнду:

```
dsconfig \
 set-backend-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backend-name userRoot \
 --set confidentiality-enabled:true \
 --no-prompt \
 --trustAll
```

После включения конфиденциальности записи шифруются при следующей записи. Сервер каталогов модуля не перезаписывает автоматически все записи в зашифрованном виде. Вместо этого он шифрует каждую запись при обновлении. Настройки конфиденциальности данных зависят от возможностей шифрования JVM.

Вы можете принять настройки по умолчанию или указать следующее:

- алгоритм шифрования, определяющий, как шифруется и расшифровывается открытый текст;
- режим работы шифра, определяющий, как алгоритм блочного шифрования должен преобразовывать данные, размер которых превышает один блок;
- заполнение шифра определяет, как заполнять открытый текст, чтобы достичь подходящего для алгоритма размера;
- длина ключа шифрования. Более длинные ключи усиливают шифрование за счет большего влияния на производительность.

Сервер каталогов модуля шифрует данные с помощью симметричного ключа, который хранится в конфигурации сервера. Симметричный ключ в свою очередь шифруется открытым ключом сервера, который также хранится в конфигурации сервера.

Избегайте использования чувствительных атрибутов в индексах VLV. Конфиденциальность не может быть включена для индексов VLV.

Шифрование и дешифрование данных сопряжено с расходами в плане криптографической обработки, которая снижает пропускную способность, и дополнительного пространства для больших зашифрованных значений.

6 Настройка обработчиков соединений

Настройте доступ клиента LDAP с помощью инструмента командной строки dsconfig. По умолчанию модуль настраивается на прослушивание LDAP при установке.

Стандартный номер порта для доступа клиента LDAP – 389. Если вы устанавливаете сервер каталогов модуля как пользователь, который может использовать порт 389, и порт еще не используется, то 389 – это номер порта по умолчанию, представленный во время установки. Если вы устанавливаете как пользователь, который не может использовать порт < 1024, то номер порта по умолчанию, представленный во время установки, – 1389.

Чтобы изменить номер порта LDAP:

- измените номер порта с помощью dsconfig команды:

```
dsconfig \
 set-connection-handler-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --handler-name "LDAP Connection Handler" \
 --set listen-port:11389 \
 --trustAll \
 --no-prompt
```

В этом примере номер порта в конфигурации изменяется на 11389.

- перезапустите обработчик соединений, чтобы изменения вступили в силу.

Чтобы перезапустить обработчик соединений, отключите его, а затем включите снова:

```
dsconfig \
 set-connection-handler-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --handler-name "LDAP Connection Handler" \
 --set enabled:false \
 --trustAll \
 --no-prompt
 dsconfig \
 set-connection-handler-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --handler-name "LDAP Connection Handler" \
 --set enabled:true \
 --trustAll \
 --no-prompt
```

6.1 Доступ к файлам LDIF

Обработчик соединений LDIF позволяет вносить изменения в данные каталога, помещая LDIF в каталог файловой системы, который сервер модуля регулярно опрашивает на предмет изменений. После использования LDIF удаляется.

Доступ к файлу LDIF настраивается с помощью инструмента командной строки dsconfig.

Чтобы настроить доступ к файлу LDIF:

- активируйте доступ к файлу LDIF:

```
dsconfig \
 set-connection-handler-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --handler-name "LDIF Connection Handler" \
 --set enabled:true \
 --trustAll \
 --no-prompt
```

Изменение вступает в силу немедленно.

- добавьте каталог, в который вы поместили LDIF для обработки:

```
mkdir /path/to/opendj/config/auto-process-ldif
```

В этом примере используется значение свойства по умолчанию ldif-directory для обработчика соединений LDIF.

7 Индексация значений атрибутов

Настроить стандартные индексы можно из панели управления, а также в командной строке с помощью dsconfig команды. После завершения настройки индекса необходимо перестроить индекс, чтобы изменения вступили в силу.

Чтобы предотвратить появление индексированных значений в открытом тексте в бэкенде, можно включить конфиденциальность по индексу бэкенда.

Создать новый индекс:

```
dsconfig \
 create-backend-index \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backend-name myData \
 --index-name cn \
 --set index-type:equality \
 --trustAll \
 --no-prompt
```

Настроить приблизительный индекс:

```
dsconfig \
 set-backend-index-prop \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backend-name myData \
 --index-name cn \
 --set index-type:approximate \
 --trustAll \
 --no-prompt
```

Настроить расширяемый индекс соответствия:

```
dsconfig \
 create-backend-index \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backend-name myData \
 --set index-type:extensible \
 --set index-extensible-matching-rule:1.3.6.1.4.1.26027.1.4.5 \
 --set index-extensible-matching-rule:1.3.6.1.4.1.26027.1.4.6 \
 --index-name lastLoginTime \
 --trustAll \
 --no-prompt
```

7.1 Настройка индекса виртуального списка просмотра

На панели управления модуля выберите "Управление индексами" – "Новый индекс VLV", а затем настройте индекс VLV с помощью окна "Новый индекс VLV".

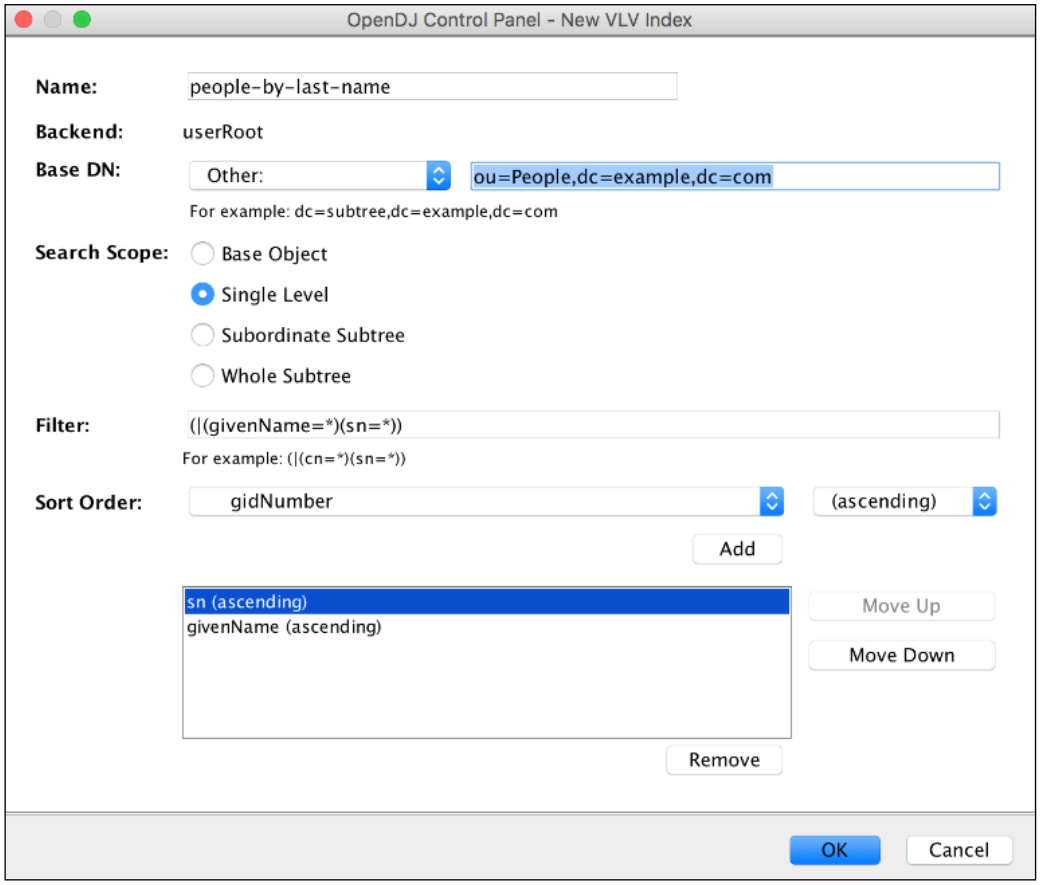


Рисунок 3 – Окно "Новый индекс VLV"

После настройки индекса и нажмете кнопку "ОК". Панель управления предложит внести дополнительные изменения, необходимые для завершения настройки индекса VLV, а затем построить индекс.

Вы также можете создать эквивалентную конфигурацию индекса с помощью dsconfig команды.

В следующем примере показано, как создать индекс VLV для бэкэнда с pdb именем типа myData:

```
dsconfig \
 create-backend-vlv-index \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDn "cn=Directory Manager" \
 --bindPassword password \
 --backend-name myData \
 --index-name people-by-last-name \
 --set base-dn:ou=People,dc=example,dc=com \
 --set filter:"(|(givenName=*)(sn=*))" \
 --set scope:single-level \
 --set sort-order:"+sn +givenName" \
 --trustAll \
 --no-prompt
```

8 Управление репликацией данных

Модуль использует расширенную репликацию данных с автоматическим разрешением конфликтов, чтобы гарантировать, что службы каталогов остаются доступными во время административных операций, которые переводят отдельный сервер в автономный режим, или в случае сбоя сервера или выхода сети из строя.

Запустить процесс репликации можно с помощью dsreplication enable команды:

```
dsreplication \
 enable \
 --adminUID admin \
 --adminPassword password \
 --baseDN dc=example,dc=com \
 --host1 opendj.example.com \
 --port1 4444 \
 --bindDN1 "cn=Directory Manager" \
 --bindPassword1 password \
 --replicationPort1 8989 \
 --host2 opendj2.example.com \
 --port2 4444 \
 --bindDN2 "cn=Directory Manager" \
 --bindPassword2 password \
 --replicationPort2 8989 \
 --trustAll \
 --no-prompt

Establishing connections ..... Done.
Checking registration information ..... Done.
Updating remote references on server opendj.example.com:4444 ..... Done.
Configuring Replication port on server opendj2.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
 opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN dc=example,dc=com on server
 opendj2.example.com:4444 ..... Done.
Updating registration configuration on server
 opendj.example.com:4444 ..... Done.
Updating registration configuration on server
 opendj2.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
 opendj.example.com:4444 ..... Done.
Updating replication configuration for baseDN cn=schema on server
 opendj2.example.com:4444 ..... Done.
Initializing registration information on server opendj2.example.com:4444 with
 the contents of server opendj.example.com:4444 ..... Done.
Initializing schema on server opendj2.example.com:4444 with the contents of
 server opendj.example.com:4444 ..... Done.

Replication has been successfully enabled.  Note that for replication to
 work you must initialize the contents of the base DN's that are being
```

```
  replicated (use dsreplication initialize to do so).

See
/var/.../opends-replication-7958637258600693490.log
for a detailed log of this operation.
```

Чтобы включить безопасные соединения для репликации, используйте параметры --secureReplication1 и --secureReplication2, которые эквивалентны выбору параметра. Настройте как безопасный на экране параметров топологии репликации мастера настройки.

В выводе команды видно, что репликация настроена на работу после включения. Для запуска процесса необходимо инициализировать репликацию.

При написании сценария конфигурации для настройки нескольких реплик в быстрой последовательности используйте один и тот же начальный сервер репликации каждый раз при запуске команды. Передайте параметры --host1, --port1, --bindDN1, --bindPassword1, и --replicationPort1 для каждой из других реплик, которые настроили в своем сценарии.

Если необходимо добавить еще один сервер каталогов модуля для участия в репликации, используйте dsreplication enable новый сервер в качестве второго сервера.

9 Резервное копирование и восстановление данных

Модуль позволяет создавать резервные копии и восстанавливать данные в сжатом двоичном формате или в формате LDIF.

9.1 Резервное копирование данных каталога

При установке модуля предоставляется каталог в качестве места для сохранения бинарных резервных копий. При создании резервной копии в нем содержится bak/backup.info информация об архиве.

Если у вас более одного бэкенда, используйте отдельный каталог резервного копирования для каждого бэкенда, чтобы иметь отдельные backup.info файлы для каждого идентификатора бэкенда.

Архивы, созданные командой backup, содержат резервные копии только данных каталога. Резервные копии конфигурации сервера находятся в config/archived-configs/.

Для выполнения резервного копирования в режиме онлайн запустите резервное копирование как задачу, подключившись к административному порту и пройдя аутентификацию как пользователь с соответствующими backend-backup привилегиями, а также установите время начала задачи с помощью –start параметра.

Чтобы выполнить автономное резервное копирование, когда сервер каталогов модуля остановлен, выполните backup команду без подключения к серверу, аутентификации или запроса задачи резервного копирования.

Используйте один из следующих вариантов:

- создайте резервную копию только базы данных Example.com, где данные хранятся в бэкэнде с именем userRoot.

В следующем примере запрашивается задача онлайн-резервного копирования, которая запускается немедленно и создает резервную копию только userRoot внутреннего хранилища:

```
backup \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backendID userRoot \
 --backupDirectory /path/to/opendj/bak/userRoot \
 --start 0
Backup task 20110613143715983 scheduled to start Jun 13, 2011 2:37:15 PM CEST
```

- остановите сервер для резервного копирования данных Example.com в автономном режиме.

В следующем примере останавливается модуль, запускается автономное резервное копирование и запускается сервер после завершения резервного копирования:

```
stop-ds
Stopping Server...

[13/Jun/2011:14:31:00 +0200] category=BACKEND severity=NOTICE msgID=9896306
 msg=The backend userRoot is now taken offline
[13/Jun/2011:14:31:00 +0200] category=CORE severity=NOTICE msgID=458955
 msg=The Directory Server is now stopped
 backup --backendID userRoot -d /path/to/opendj/bak
[13/Jun/2011:14:33:48 +0200] category=TOOLS severity=NOTICE msgID=10944792
 msg=Starting backup for backend userRoot
...
[13/Jun/2011:14:33:48 +0200] category=TOOLS severity=NOTICE msgID=10944795
 msg=The backup process completed successfully
 start-ds
... The Directory Server has started successfully
```

- резервное копирование всех пользовательских данных на сервере.

В следующем примере запрашивается задача онлайн-резервного копирования, которая запускается немедленно и создает резервные копии всех внутренних процессов:

```
backup \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backUpAll \
 --backupDirectory /path/to/opendj/bak/userRoot \
 --start 0
Backup task 20110613143801866 scheduled to start Jun 13, 2011 2:38:01 PM CEST
```

9.2 Восстановление данных каталога из резервной копии

При восстановлении данных процедура, которую необходимо выполнить, зависит от того, реплицирован ли сервер каталогов модуля.

Чтобы восстановить модуль, когда сервер находится в сети, запустите задачу восстановления, подключившись к административному порту и пройдя аутентификацию как пользователь с backend-restore привилегиями, а также установите время начала задачи с помощью –start параметра.

Чтобы восстановить данные при остановленном сервере каталогов модуля, выполните restore команду без подключения к серверу, аутентификации или запроса задачи восстановления.

Используйте один из следующих вариантов:

- остановите сервер, чтобы восстановить данные для Example.com.

В следующем примере останавливается модуль, восстанавливаются данные в автономном режиме из одной из доступных резервных копий, а затем после завершения восстановления запускается сервер:

```
stop-ds
Stopping Server...

[13/Jun/2011:15:44:06 +0200] category=BACKEND severity=NOTICE msgID=9896306
 msg=The backend userRoot is now taken offline
[13/Jun/2011:15:44:06 +0200] category=CORE severity=NOTICE msgID=458955
 msg=The Directory Server is now stopped
 restore --backupDirectory /path/to/opendj/bak/userRoot --listBackups
Backup ID:          20110613080032
Backup Date:        13/Jun/2011:08:00:45 +0200
Is Incremental:     false
Is Compressed:      false
Is Encrypted:       false
Has Unsigned Hash:  false
Has Signed Hash:    false
Dependent Upon:     none
 restore     --backupDirectory     /path/to/opendj/bak/userRoot     --backupID
20110613080032
[13/Jun/2011:15:47:41 +0200] ... msg=Restored: 00000000.jdb (size 341835)
 start-ds
... The Directory Server has started successfully
```

- запланируйте восстановление как задачу, которая должна начаться немедленно.

В следующем примере запрашивается задача восстановления в режиме онлайн, запуск которой запланирован на немедленный период:

```
restore \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --backupDirectory /path/to/opendj/bak/userRoot \
 --backupID 20110613080032 \
 --start 0
Restore task 20110613155052932 scheduled to start Jun 13, 2011 3:50:52 PM CEST
```

10 Настройка политики паролей

Настройка политики паролей выполняется на основе сервера с помощью dsconfig команды.

Чтобы настроить политику паролей по умолчанию:

- включите соответствующий валидатор пароля:

```
dsconfig \
 set-password-validator-prop \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --validator-name Dictionary \
 --set enabled:true \
 --set check-substrings:true \
 --set min-substring-length:4 \
 --trustAll \
 --no-prompt
```

- примените изменения к политике паролей по умолчанию:

```
dsconfig \
 set-password-policy-prop \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --policy-name "Default Password Policy" \
 --set max-password-age:90d \
 --set min-password-age:4w \
 --set password-history-count:7 \
 --set password-validator:Dictionary \
 --trustAll \
 --no-prompt
```

- проверьте работу:

```
dsconfig \
 get-password-policy-prop \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --policy-name "Default Password Policy"
Property                                  : Value(s)
------------------------------------------:--------------------------
account-status-notification-handler       : -
allow-expired-password-changes            : false
allow-user-password-changes               : true
default-password-storage-scheme           : Salted SHA-1
deprecated-password-storage-scheme        : -
expire-passwords-without-warning          : false
force-change-on-add                       : false
force-change-on-reset                     : false
grace-login-count                         : 0
idle-lockout-interval                     : 0 s
last-login-time-attribute                 : -
last-login-time-format                    : -
lockout-duration                          : 0 s
lockout-failure-count                     : 0
lockout-failure-expiration-interval       : 0 s
max-password-age                          : 12 w 6 d
max-password-reset-age                    : 0 s
min-password-age                          : 4 w
password-attribute                        : userpassword
password-change-requires-current-password : false
password-expiration-warning-interval      : 5 d
password-generator                        : Random Password Generator
password-history-count                    : 7
password-history-duration                 : 0 s
password-validator                        : Dictionary
previous-last-login-time-format           : -
require-change-by-time                    : -
require-secure-authentication             : false
require-secure-password-changes           : false
```

10.1 Настройка генерации пароля

Генераторы паролей используются модулем во время расширенной операции LDAP Password Modify для создания нового пароля для пользователя. Администратор каталога, сбрасывающий пароль пользователя, может заставить сервер каталога модуль сгенерировать новый пароль с помощью ldappasswordmodify команды:

```
ldappasswordmodify \
 --port 1389 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --authzID "u:bjensen"
The LDAP password modify operation was successful
Generated Password:  eak77qdi
```

Политика паролей по умолчанию использует генератор случайных паролей:

```
dsconfig \
 get-password-policy-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --policy-name "Default Password Policy" \
 --property password-generator
Property           : Value(s)
-------------------:-------------------------
password-generator : Random Password Generator
 dsconfig \
 get-password-generator-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --generator-name "Random Password Generator" \
 --property password-generator
 Property               : Value(s)
-----------------------:---------------------------------------------------
enabled                : true
password-character-set : alpha:abcdefghijklmnopqrstuvwxyz, numeric:0123456789
password-format        : "alpha:3,numeric:2,alpha:3"
```

Обратите внимание, что конфигурация по умолчанию для генератора случайных паролей определяет два password-character-set значения, а затем использует эти определения в password-formattак, чтобы сгенерированные пароли имели восемь символов: три из alpha набора, затем два из numeric набора, затем три из alpha набора. password-character-set – имя должно быть ASCII.

Чтобы задать генератор паролей, который модуль использует при создании нового пароля для пользователя, задайте password-generator свойство для политики паролей, применяемой к пользователю.

В следующем примере не изменяется политика паролей, а вместо этого изменяется конфигурация генератора случайных паролей, а затем демонстрируется генерация пароля при сбросе:

```
dsconfig \
 set-password-generator-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --generator-name "Random Password Generator" \
 --remove password-character-set:alpha:abcdefghijklmnopqrstuvwxyz \
 --add \
  password-character-
set:alpha:ABCDEFGHIJKLMNOPQRSTUVWabcdefghijklmnopqrstuvwxyz \
 --add password-character-set:punct:,./\`!@#\$%^&*:\;[]\"\'\(\)+=-_~\\ \
 --set \
  password-format:alpha:3,punct:1,numeric:2,punct:2,numeric:3,alpha:3,punct:2 \
 --no-prompt
 ldappasswordmodify \
 --port 1389 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --authzID "u:bjensen"
The LDAP password modify operation was successful
Generated Password:  pld^06:)529HTq$'
```

10.2 Настройка хранилища паролей

Схемы хранения паролей кодируют новые пароли, предоставляемые пользователями, так что они хранятся в закодированном виде. Это затрудняет или делает невозможным определение паролей в открытом виде из закодированных значений. Схемы хранения паролей также определяют, соответствует ли пароль в открытом виде, предоставленный клиентом, закодированному значению, хранящемуся на сервере.

Модуль предлагает множество как обратимых, так и односторонних схем хранения паролей. Некоторые схемы позволяют легко восстановить пароль в открытом виде, в то время как другие стремятся сделать это вычислительно сложным:

```
dsconfig \
 list-password-storage-schemes \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password

Password Storage Scheme : Type          : enabled
------------------------:---------------:--------
3DES                    : triple-des    : true
AES                     : aes           : true
Base64                  : base64        : true
Bcrypt                  : bcrypt        : true
Blowfish                : blowfish      : true
Clear                   : clear         : true
CRYPT                   : crypt         : true
MD5                     : md5           : true
PBKDF2                  : pbkdf2        : true
PKCS5S2                 : pkcs5s2       : true
RC4                     : rc4           : true
Salted MD5              : salted-md5    : true
Salted SHA-1            : salted-sha1   : true
Salted SHA-256          : salted-sha256 : true
Salted SHA-384          : salted-sha384 : true
Salted SHA-512          : salted-sha512 : true
SHA-1                   : sha1          : true
```

10.3 Настройка проверки пароля

Валидаторы паролей отвечают за определение того, приемлем ли предложенный пароль для использования. Валидаторы могут выполнять проверки, например, чтобы убедиться, что пароль соответствует минимальным требованиям длины, имеет соответствующий диапазон символов или отсутствует в истории недавно использованных паролей. Сервер каталогов модуля предоставляет различные валидаторы паролей:

```
dsconfig \
 list-password-validators \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password
```

```
Password Validator                  : Type                : enabled
------------------------------------:---------------------:--------
Attribute Value                     : attribute-value     : true
Character Set                       : character-set       : true
Dictionary                          : dictionary          : false
Length-Based Password Validator     : length-based        : true
Repeated Characters                 : repeated-characters : true
Similarity-Based Password Validator : similarity-based    : true
Unique Characters                   : unique-characters   : true
```

Политика паролей для пользователя определяет набор валидаторов паролей, которые должны использоваться всякий раз, когда пользователь предоставляет новый пароль. По умолчанию валидаторы паролей не настроены.

В следующем примере показано, как настроить пользовательский валидатор паролей и назначить его политике паролей по умолчанию. Пользовательский валидатор паролей гарантирует, что пароли соответствуют как минимум трем из следующих четырех критериев. Пароли состоят из:

- строчные буквы английского языка (от a до z);
- заглавные английские буквы (от A до Z);
- 10 значная система счисления (от 0 до 9);
- символы (например, !, $, #, %).

Обратите внимание, как character-set построены значения. Начальное значение 0 означает, что набор необязателен, тогда как 1 будет означать, что набор обязателен:

```
dsconfig \
 create-password-validator \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --validator-name "Custom Character Set Password Validator" \
 --set allow-unclassified-characters:true \
 --set enabled:true \
 --set character-set:0:abcdefghijklmnopqrstuvwxyz \
 --set character-set:0:ABCDEFGHIJKLMNOPQRSTUVWXYZ \
 --set character-set:0:0123456789 \
 --set character-set:0:!\"#\$%&\'\(\)*+,-./:\;\\<=\>?@[\\]^_\`{\|}~ \
 --set min-character-sets:3 \
 --type character-set \
 --no-prompt
 dsconfig \
 set-password-policy-prop \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --policy-name "Default Password Policy" \
 --set password-validator:"Custom Character Set Password Validator" \
 --no-prompt
 ldappasswordmodify \
 --port 1389 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --authzID "u:bjensen" \
 --newPassword '!ABcd$%^'
```

В предыдущем примере набор символов пунктуации ASCII, !\"#\$%&\'\(\)*+,-./:\;\<=\>?@[\\]^_`{\|}~, трудно читать из-за всех экранированных символов. На практике может быть проще вводить такие последовательности, используя `dsconfig` в интерактивном режиме и позволяя ему выполнить экранирование. Также доступна опция --commandFilePath {path} сохранения результата интерактивного сеанса в файл для использования в скриптах позже.

Попытка установить неверный пароль завершается неудачей, как показано в следующем примере:

```
ldappasswordmodify \
 --port 1389 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --authzID "u:bjensen" \
 --newPassword hifalutin
The LDAP password modify operation failed with result code 19
Error Message:  The provided new password failed the validation checks defined
in the server:  The provided password did not contain characters from at least
3 of the following character sets or ranges: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ',
'!"#$%&'()*+,-./:;<=\>?@[\]^_`{|}~', '0123456789', 'abcdefghijklmnopqrstuvwxyz'
```

Проверка не влияет на существующие пароли, а вступает в силу только при обновлении пароля.

11 Реализация блокировки учетной записи и уведомления

Сервер каталогов модуля поддерживает автоматическую блокировку учетной записи. Цель блокировки учетной записи – защитить каталог от атак, в которых злоумышленник пытается угадать пароль пользователя, многократно пытаясь выполнить привязку до тех пор, пока не будет достигнут успех.

Блокировка учетной записи отключает учетную запись пользователя после определенного количества последовательных неудачных попыток аутентификации. При реализации блокировки учетной записи вы можете выбрать, чтобы сервер каталогов модуля разблокировал учетную запись после определенного интервала времени, или вы можете оставить учетную запись заблокированной до сброса пароля.

11.1 Настройка блокировки учетной записи

Блокировка учетной записи настраивается как часть политики паролей.

Пользователям разрешено три последовательных неудачных попытки, прежде чем они будут заблокированы на пять минут. Сами неудачи также истекают через пять минут.

Измените политику паролей по умолчанию, чтобы активировать блокировку с помощью dsconfig команды. Поскольку политика паролей является частью конфигурации сервера, необходимо вручную применить изменения к каждой реплике в топологии репликации:

```
dsconfig \
 set-password-policy-prop \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --policy-name "Default Password Policy" \
 --set lockout-failure-count:3 \
 --set lockout-duration:5m \
 --set lockout-failure-expiration-interval:5m \
 --trustAll \
 --no-prompt
```

Пользователи, имеющие политику паролей по умолчанию, блокируются после трех неудачных попыток подряд:

```
ldapsearch \
 --port 1389 \
 --bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
 --bindPassword hifalutin \
 --baseDN dc=example,dc=com \
 uid=bjensen \
 mail
dn: uid=bjensen,ou=People,dc=example,dc=com
mail: bjensen@example.com
 ldapsearch \
 --port 1389 \
 --bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
 --bindPassword fatfngrs \
 --baseDN dc=example,dc=com \
 uid=bjensen \
 mail
The simple bind attempt failed
Result Code:  49 (Invalid Credentials)
 ldapsearch \
 --port 1389 \
 --bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
 --bindPassword fatfngrs \
 --baseDN dc=example,dc=com \
 uid=bjensen \
 mail
The simple bind attempt failed
Result Code:  49 (Invalid Credentials)
 ldapsearch \
 --port 1389 \
 --bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
 --bindPassword fatfngrs \
 --baseDN dc=example,dc=com \
 uid=bjensen \
 mail
The simple bind attempt failed
Result Code:  49 (Invalid Credentials)
 ldapsearch \
 --port 1389 \
 --bindDN "uid=bjensen,ou=people,dc=example,dc=com" \
 --bindPassword hifalutin \
 --baseDN dc=example,dc=com \
```

```
 uid=bjensen \
 mail
The simple bind attempt failed
Result Code:  49 (Invalid Credentials)
```

11.2 Управление учетными записями вручную

Чтобы отключить учетную запись, установите статус учетной записи "Отключено" с помощью manage-account команды:

```
manage-account \
 set-account-is-disabled \
 --port 4444 \
 --bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
 --bindPassword bribery \
 --operationValue true \
 --targetDN uid=bjensen,ou=people,dc=example,dc=com \
 --trustAll
Account Is Disabled:  true
```

Чтобы активировать отключенную учетную запись, очистите статус "Отключено" с помощью manage-account команды:

```
manage-account \
 clear-account-is-disabled \
 --port 4444 \
 --bindDN "uid=kvaughan,ou=people,dc=example,dc=com" \
 --bindPassword bribery \
 --targetDN uid=bjensen,ou=people,dc=example,dc=com \
 --trustAll
Account Is Disabled:  false
```

12 Реализация уникальности значений атрибутов

Некоторые значения атрибутов должны оставаться уникальными. Если вы используете uid значения как RDN для различения множества записей пользователей, хранящихся в ou=People, то каталог не должен содержать два или более одинаковых uid значения.

Сервер каталогов модуля использует плагин уникальных атрибутов для обработки уникальности значений атрибутов. Как показано в примерах, вы можете настроить плагин уникальных атрибутов для обработки одного или нескольких атрибутов и для обработки записей под одним или несколькими базовыми DN. Вы также можете настроить несколько экземпляров плагина для одного и того же сервера каталогов модуля.

Модуль предоставляет уникальный плагин атрибутов, который вы настраиваете с помощью dsconfig команды. По умолчанию плагин готов гарантировать, что значения атрибутов являются уникальными для uid атрибутов.

Установите базовое DN, где uid должны быть уникальные значения, и включите плагин:

```
dsconfig \
 set-plugin-prop \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --plugin-name "UID Unique Attribute" \
 --set base-dn:ou=people,dc=example,dc=com \
 --set enabled:true \
 --trustAll \
 --no-prompt
```

Проверьте правильность работы плагина:

```
cat bjensen.ldif
dn: uid=ajensen,ou=People,dc=example,dc=com
changetype: modify
add: uid
uid: bjensen
 ldapmodify \
 --defaultAdd \
 --port 1389 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --filename bjensen.ldif
Processing MODIFY request for uid=ajensen,ou=People,dc=example,dc=com
MODIFY operation failed
Result Code:  19 (Constraint Violation)
Additional Information:  A unique attribute conflict was detected for
 attribute uid:  value bjensen already exists in entry
 uid=bjensen,ou=People,dc=example,dc=com
```

13 Настройка сквозной аутентификации

При настройке сквозной аутентификации вам необходимо знать, к какому удаленному серверу или серверам перенаправлять привязки, а также как сопоставлять записи пользователей в модуле с записями пользователей в удаленном каталоге.

Настройте политики аутентификации с помощью dsconfig команды. Обратите внимание, что политики аутентификации являются частью конфигурации сервера и, следовательно, не реплицируются.

Настройте политику аутентификации для сквозной аутентификации на сервере аутентификации:

```
dsconfig \
 create-password-policy \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --type ldap-pass-through \
 --policy-name "PTA Policy" \
 --set primary-remote-ldap-server:pta-server.example.com:636 \
 --set mapped-attribute:uid \
 --set mapped-search-base-dn:"dc=PTA Server,dc=com" \
 --set mapping-policy:mapped-search \
 --set use-ssl:true \
 --set trust-manager-provider:JKS \
 --trustAll \
 --no-prompt
```

Политика сопоставляет идентификаторы с этой политикой паролей с идентификаторами в dc=PTA Server,dc=com. Пользователи должны иметь одинаковые uid значения на обоих серверах. Политика также использует SSL между модулем и сервером аутентификации.

Проверьте, что ваш полис добавлен в список:

```
dsconfig \
 list-password-policies \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --property use-ssl

Password Policy         : Type              : use-ssl
------------------------:-------------------:--------
Default Password Policy : password-policy   : -
PTA Policy              : ldap-pass-through : true
Root Password Policy    : password-policy   : -
```

Политики аутентификации назначаются так же, как и политики паролей, с помощью ds-pwp-password-policy-dnатрибута.

Пользователям, зависящим от PTA, больше не нужна локальная политика паролей, поскольку они больше не проходят локальную аутентификацию.

Примеры в следующей процедуре работают для этого пользователя. Обратите внимание, что у пользователя нет установленного пароля. Пароль пользователя на сервере аутентификации password:

```
dn: uid=user.0,ou=People,dc=example,dc=com
cn: Aaccf Amar
description: This is the description for Aaccf Amar.
employeeNumber: 0
givenName: Aaccf
homePhone: +1 225 216 5900
initials: ASA
l: Panama City
mail: user.0@maildomain.net
mobile: +1 010 154 3228
objectClass: person
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: top
pager: +1 779 041 6341
postalAddress: Aaccf Amar$01251 Chestnut Street$Panama City, DE  50369
postalCode: 50369
sn: Amar
st: DE
street: 01251 Chestnut Street
telephoneNumber: +1 685 622 6202
uid: user.0
```

Запись этого пользователя на сервере аутентификации также имеет значение uid=user.0, и политика сквозной аутентификации выполняет сопоставление для поиска записи пользователя на сервере аутентификации.

Запретите пользователям изменять собственную политику паролей:

```
cat protect-pta.ldif
dn: ou=People,dc=example,dc=com
changetype: modify
add: aci
aci: (target ="ldap:///uid=*,ou=People,dc=example,dc=com")(targetattr =
 "ds-pwp-password-policy-dn")(version 3.0;acl "Cannot choose own pass
 word policy";deny (write)(userdn = "ldap:///self");)
 ldapmodify \
 --port 1389 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --filename protect-pta.ldif
Processing MODIFY request for ou=People,dc=example,dc=com
MODIFY operation successful for DN ou=People,dc=example,dc=com
```

Обновите атрибут пользователя ds-pwp-password-policy-dn:

```
ldapmodify \
 --port 1389 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password
dn: uid=user.0,ou=People,dc=example,dc=com
changetype: modify
add: ds-pwp-password-policy-dn
ds-pwp-password-policy-dn: cn=PTA Policy,cn=Password Policies,cn=config

Processing MODIFY request for uid=user.0,ou=People,dc=example,dc=com
MODIFY operation successful for DN uid=user.0,ou=People,dc=example,dc=com
```

Проверьте, может ли пользователь пройти аутентификацию на сервере аутентификации:

```
ldapsearch \
 --port 1389 \
 --baseDN dc=example,dc=com \
 --bindDN uid=user.0,ou=People,dc=example,dc=com \
 --bindPassword password \
 uid=user.0 \
 cn sn
dn: uid=user.0,ou=People,dc=example,dc=com
cn: Aaccf Amar
sn: Amar
```

14 Мониторинг, ведение журнала и оповещения

14.1 Мониторинг

Модуль предоставляет информацию мониторинга через LDAP под записью cn=monitor. Предоставляется множество различных типов информации. Следующий пример показывает информацию мониторинга о userRoot бэкэнде, содержащем данные Example.com:

```
ldapsearch --port 1389 --baseDN cn=monitor "(cn=userRoot backend)"
dn: cn=userRoot backend,cn=Disk Space Monitor,cn=monitor
disk-state: normal
objectClass: top
objectClass: ds-monitor-entry
objectClass: extensibleObject
disk-dir: /path/to/opendj/db/userRoot
disk-free: 343039315968
cn: userRoot backend

dn: cn=userRoot Backend,cn=monitor
objectClass: top
objectClass: ds-monitor-entry
objectClass: ds-backend-monitor-entry
cn: userRoot Backend
ds-backend-id: userRoot
ds-backend-base-dn: dc=example,dc=com
ds-backend-is-private: FALSE
ds-backend-entry-count: 176
ds-base-dn-entry-count: 176 dc=example,dc=com
ds-backend-writability-mode: enabled
```

Модуль поставляется с двумя командами для мониторинга процессов и задач сервера:

- status – для чтения конфигурации команда, как и панель управления, требует учетные данные администратора:

```
status --bindDN "cn=Directory Manager" --bindPassword password

          --- Server Status ---
Server Run Status:        Started
Open Connections:         1

          --- Server Details ---
Host Name:                localhost
Administrative Users:     cn=Directory Manager
Installation Path:        /path/to/opendj
Version:                  OpenDJ 3.5.3
Java Version:             version
Administration Connector: Port 4444 (LDAPS)

          --- Connection Handlers ---
Address:Port : Protocol : State
-------------:----------:---------
--           : LDIF     : Disabled
0.0.0.0:636  : LDAPS    : Disabled
0.0.0.0:1389 : LDAP     : Enabled
0.0.0.0:1689 : JMX      : Disabled

          --- Data Sources ---
Base DN:     dc=example,dc=com
Backend ID:  userRoot
Entries:     163
Replication: Disabled
```

- команда manage-tasks подключается через порт администрирования и поэтому может подключаться как к локальным, так и к удаленным серверам:

```
manage-tasks \
 --hostname opendj.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --trustAll \
 --no-prompt

ID                          Type    Status
-------------------------------------------------------
example                     Backup  Recurring
example-20110623030000000   Backup  Waiting on start time
```

14.2 Журналы

По умолчанию модуль хранит журналы доступа и ошибок, а также файл идентификатора процесса сервера в logs/ каталоге. Для службы репликации модуль также хранит журнал репликации. Настройте ведение журнала с помощью dsconfig команды.

Журнал доступа отслеживает операции, обрабатываемые сервером, включая временные метки, информацию о подключении и информацию о самой операции. Журнал доступа может быстро расти, так как каждый запрос клиента приводит как минимум к одному новому сообщению журнала.

Следующий фрагмент журнала доступа демонстрирует операцию поиска с локального хоста, при этом первые три строки перенесены для удобства чтения:

```
[21/Jun/2011:08:01:53 +0200] CONNECT conn=4 from=127.0.0.1:49708
 to=127.0.0.1:1389 protocol=LDAP
[21/Jun/2011:08:01:53 +0200] SEARCH REQ conn=4 op=0 msgID=1
 base="dc=example,dc=com" scope=wholeSubtree filter="(uid=bjensen)" attrs="ALL"
[21/Jun/2011:08:01:53 +0200] SEARCH RES conn=4 op=0 msgID=1
 result=0 nentries=1 etime=3
[21/Jun/2011:08:01:53 +0200] UNBIND REQ conn=4 op=1 msgID=2
[21/Jun/2011:08:01:53 +0200] DISCONNECT conn=4 reason="Client Unbind"
```

Журнал ошибок отслеживает события сервера, состояния ошибок и предупреждения, классифицируя их и идентифицируя по степени серьезности.

В следующем errors фрагменте журнала показаны записи журнала для задачи резервного копирования, строки перенесены для удобства чтения:

```
[06/Oct/2015:16:58:15 +0200] category=... severity=NOTICE msgID=...
 msg=Backup task 20151006165815904 started execution
[06/Oct/2015:16:58:15 +0200] category=TASK severity=NOTICE msgID=...
 msg=Starting backup for backend userRoot
[06/Oct/2015:16:58:16 +0200] category=UTIL severity=NOTICE msgID=...
 msg=Archived backup file: dj
...
[06/Oct/2015:16:58:16 +0200] category=UTIL severity=NOTICE msgID=...
 msg=Archived backup file: tasks.ldif
[06/Oct/2015:16:58:16 +0200] category=TASK severity=NOTICE msgID=...
 msg=The backup process completed successfully
[06/Oct/2015:16:58:16 +0200] category=... severity=NOTICE msgID=...
 msg=Backup task 20151006165815904 finished execution in the state
     Completed successfully
```

14.3 Оповещения

Модуль может отправлять оповещения для предоставления уведомлений о важных событиях сервера. Однако оповещения по умолчанию не включены. Вы можете использовать dsconfig команду для включения оповещений:

```
dsconfig \
 set-alert-handler-prop \
 --port 4444 \
 --hostname opendj.example.com \
 --bindDN "cn=Directory Manager" \
 --bindPassword password \
 --handler-name "JMX Alert Handler" \
 --set enabled:true \
 --trustAll \
 --no-prompt
```

15 Аварийные ситуации

15.1 Описание аварийных ситуаций

Надежность Системы обеспечивается при следующих аварийных ситуациях:

- отказ Системы;
- сбой Системы.

Отказом Системы следует считать событие, состоящее в утрате работоспособности Системы и приводящее к невыполнению или неправильному выполнению контрольных примеров или задач функциональных модулей.

Сбоем Системы следует считать событие, состоящее во временной утрате работоспособности Системы и характеризуемое возникновением ошибки при выполнении контрольных примеров или задач функциональных модулей.

В Системе предусмотрено автоматическое восстановление обрабатываемой информации в следующих аварийных ситуациях:

- программный сбой при операциях записи–чтения;
- разрыв связи с клиентской программой (терминальным устройством) в ходе редактирования/обновления информации.

В Системе предусмотрена возможность ручного восстановления обрабатываемой информации из резервной копии в следующих аварийных ситуациях:

- физический выход из строя дисковых накопителей;
- ошибочные действия обслуживающего персонала.

В Системе предусмотрено автоматическое восстановление работоспособности серверной части Системы в следующих ситуациях:

- штатное и аварийное отключение электропитания серверной части;
- штатная перезагрузка Системы и загрузка после отключения;
- программный сбой общесистемного программного обеспечения, приведший к перезагрузке Системы.

В Системе предусмотрено полуавтоматическое восстановление работоспособности серверной части Системы в следующих аварийных ситуациях:

- физический выход из строя любого аппаратного компонента, кроме дисковых накопителей – после замены компонента и восстановления конфигурации общесистемного программного обеспечения;
- аварийная перезагрузка системы, приведшая к нефатальному нарушению целостности файловой системы – после восстановления файловой системы.

Для восстановления Системы после отказа или сбоя, необходимо сначала устранить причину отказа/сбоя (заменить неисправное оборудование, устранить системные ошибки и др.), а затем предпринять следующие действия:

- установить операционную систему, а затем – соответствующий пакет обновления; проверить правильность работы домена.
- установить СУБД, а затем – соответствующий пакет обновления.
- восстановить базу данных из резервной копии; перезагрузить сервер после восстановления базы данных.
- проверить доступность Системы; чтобы убедиться в правильности работы, запустите сценарий проверки основных функций.
- активировать возможность работы пользователей в штатном режиме.

В случае отказа или сбоя Системы, связанного с неисправностью оборудования, работы проводит Администратор Заказчика.

В случае отказа или сбоя Системы, связанного с системной ошибкой, работы проводит Администратор Исполнителя.

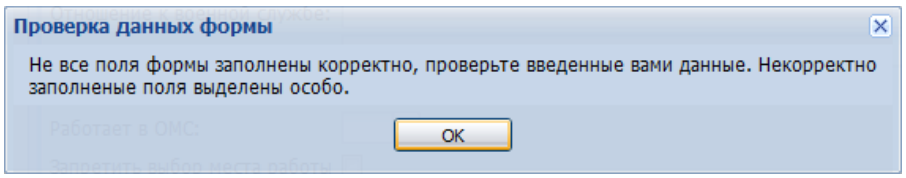
15.2 Действия в случае несоблюдения условий выполнения технологического процесса

При работе с Системой пользователю могут отображаться сообщения нескольких типов:

- сообщение об успешном завершении действия;
- сообщение об ошибке;
- предупреждение;
- сообщение о неисправности системы.

Сообщение об успешном завершении действия содержит краткое резюме операции. Для закрытия сообщения нажмите кнопку "**ОК**".

Сообщение об ошибке отображается в случае, когда дальнейшее выполнение действия в Системе невозможно. Как правило, в таком сообщении содержится краткое описание причины возникновения ошибки. Для закрытия сообщения об ошибке нажмите кнопку "**ОК**".



Предупреждение отображается в том случае, если действия, совершенные оператором, могут повлечь за собой какие–либо особенности в выполнении операции, но не приведут к

ошибке. Например, если оператор укажет у сотрудника ставку менее 0,1, то отобразится сообщение, что такая ставка не будет учитываться при выгрузке. Для того чтобы продолжить выполнение действия, нажмите кнопку "**Да**"/"**Продолжить**". Для того чтобы прекратить действие, нажмите кнопку "**Нет**"/"**Отмена**".

В случае возникновения ошибки о неисправности системы, пользователю системы следует обратиться к администратору системы.

Администратор системы для решения проблем обращается к эксплуатационной документации, настоящему руководству, онлайн справочной системе.

В случае невозможности разрешения ситуации следует обратиться в техническую поддержку.

16 Эксплуатация модуля

Система предназначена для функционирования 24 часа в сутки 7 дней в неделю. Обеспечивается возможность взаимодействия с пользователями в круглосуточном режиме без перерывов, в том числе при доступе пользователей из других по отношению к серверной части временных зон.

Для программного обеспечения Системы определены следующие режимы функционирования:

- штатный режим (режим, обеспечивающий выполнение функций Системы);
- предаварийный режим (режим, предшествующий переходу в аварийный режим);
- аварийный режим (характеризуется отказом одного или нескольких компонентов программного и/или аппаратного обеспечения. В данном режиме функционируют ресурсы, которые в штатном режиме находятся в режиме горячего резерва)
- сервисный режим (режим для проведения реконфигурирования, обновления и профилактического обслуживания).

Информационный обмен со стороны Системы построен через:

- интеграционную шину Системы с соблюдением правил информационной безопасности;
- Сервисы интеграции.

Подробное описание приведено в документе "Регламент эксплуатации".