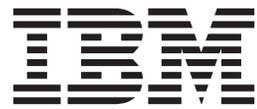


IBM Security Directory Server
версия 6.3.1.5

*Руководство по установке и
настройке*



IBM Security Directory Server
версия 6.3.1.5

*Руководство по установке и
настройке*



Примечание

Перед тем, как начать работу с данной информацией и описанным в ней продуктом, ознакомьтесь с общими сведениями, приведенными в разделе “Примечания” на стр. 263.

Примечания к изданию

Примечание: Данное издание относится к версии 6.3.1.5 *IBM Security Directory Server* (номер продукта 5724-J39) и всем последующим выпускам и модификациям этого продукта, если в следующих изданиях не будет указано иное.

© Copyright IBM Corporation 1998, 2014.

Содержание

Общая информация о публикации . . . vii	
Доступ к публикациям и терминологии vii	
Специальные возможности ix	
Техническое обучение ix	
Информация о поддержке ix	
Заявление о эффективных мерах безопасности ix	
Глава 1. Планирование установки . . . 1	
Глава 2. Обзор установки 3	
Требования к дисковой памяти 3	
Подготовка носителя установки 6	
Загрузка программного обеспечения из Passport Advantage 6	
Структура каталогов загруженных файлов. 7	
Предварительные требования для установки 14	
Предварительно требуемые пакеты в различных операционных системах 15	
Предварительно необходимое требование для клиента LDAP в PowerPC LE 16	
Пользователь и группа <code>idsldap</code> 17	
Методы установки 18	
Глава 3. Установка с помощью IBM Installation Manager 21	
IBM Installation Manager - Обзор 21	
Поддерживаемые операционные системы. 21	
Типы пакетов установки IBM Security Directory Server 22	
Рекомендации по установке 23	
Компоненты IBM Security Directory Server 24	
Настройка установки IBM Security Directory Server 26	
Установочные расположения по умолчанию 27	
Установочные хранилища 27	
Запуск установки. 28	
Запуск установки из панели запуска. 28	
Запуск установки путем задания параметров хранилища. 29	
Установка с помощью IBM Installation Manager 30	
Неинтерактивный режим установки 35	
Установка без вывода сообщений с помощью файла ответов 36	
Глава 4. Изменение с помощью IBM Installation Manager 39	
Изменение компонентов с помощью IBM Installation Manager. 39	
Глава 5. Протоколы IBM Installation Manager 45	
Глава 6. Запрос пакетов IBM Security Directory Server. 47	
Глава 7. Внутренняя установка и настройка с помощью сценариев . . . 49	
Путеводитель по установке 49	
Установка пакетов IBM Security Directory Server в системах Linux, Solaris и HP-UX 49	
Проверка протоколов установки 52	
Глава 8. Установка IBM DB2 53	
Глава 9. IBM Java Development Kit для IBM Security Directory Server 55	
Глава 10. Установка IBM Global Security Kit. 57	
Установка IBM Global Security Kit с помощью <code>installp</code> 58	
Установка IBM Global Security Kit с помощью утилит Linux 59	
Установка IBM Global Security Kit с помощью утилит Solaris 60	
Установка IBM Global Security Kit с помощью утилит HP-UX 61	
Установка IBM Global Security Kit в системе Windows 61	
Установка IBM Global Security Kit в системе Windows без вывода сообщений 62	
Глава 11. Установка языковых пакетов 65	
Языковые пакеты для установки 66	
Установка языковых пакетов с помощью утилит операционной системы. 67	
Глава 12. Установка с помощью утилит командной строки операционной системы 69	
Установка с помощью утилит AIX 69	
Пакеты для установки в системе AIX 69	
Установка с помощью SMIT 71	
Установка с помощью <code>installp</code> 73	
Установка с помощью утилит Linux 74	
Пакеты для установки в системе Linux. 75	
Установка с помощью утилит Linux 77	
Установка с помощью утилит Solaris 78	
Пакеты для установки в системе Solaris 79	
Установка с помощью утилит Solaris 81	
Установка с помощью утилит HP-UX 82	

Пакеты для установки в системе HP-UX Itanium	82
Установка с помощью утилит HP-UX	83

Глава 13. Проверка компонентов IBM Security Directory Server 85

Проверка компонентов IBM Security Directory Server с помощью IBM Installation Manager	85
Проверка компонентов IBM Security Directory Server в Windows	85
Проверка пакетов IBM Security Directory Server	86
Проверка версии Веб-инструмента администрирования	87
Проверка установки IBM Global Security Kit в Windows	88
Проверка установки IBM Global Security Kit в AIX, Linux, Solaris и HP-UX	88

Глава 14. Обновление экземпляра предыдущей версии 89

Настройка среды перед обновлением экземпляра	90
Обновление экземпляра предыдущей версии с помощью команды <code>idsimigr</code>	92
Обновление экземпляра предыдущей версии на другом компьютере	93
Поддерживаемые операционные системы для обновления удаленного экземпляра	94
Обновление удаленного экземпляра предыдущей версии с помощью команды <code>idsimigr</code>	94
Ссылки на утилиты клиента и сервера	96

Глава 15. Миграция данных и решений из экземпляра предыдущей версии 97

Миграция экземпляра с базой данных DB2 ESE к экземпляру с базой данных DB2 WSE	98
Перенос решения управления протоколами	99
Перенос решения SNMP	100
Перенос решения синхронизации Active Directory в новую версию	101
Миграция конфигурации предыдущей версии Web Administration Tool	102
<code>idswmigr</code>	103
Миграция Web Administration Tool вручную	104

Глава 16. Развертывание Web Administration Tool вручную 109

Установка встроенного WebSphere Application Server вручную	109
Порты по умолчанию для веб-инструмента администрирования	110
Развертывание Веб-инструмента администрирования во встроенном WebSphere Application Server	111
Развертывание Веб-инструмента администрирования в WebSphere Application Server	112
Запуск встроенного WebSphere Application Server для использования Веб-инструмента администрирования	114
Получение доступа к Web Administration Tool	115
Завершение работы сервера веб-приложений	116

HTTPS со встроенным WebSphere Application Server	117
Свертывание Веб-инструмента администрирования во встроенном WebSphere Application Server	118

Глава 17. Планирование конфигурации экземпляра 121

Пользователи и группы, связанные с экземпляром сервера каталогов	121
Правила присваивания имен	122
Требования к созданию пользователей и групп	123
Планирование настройки	125
Поддержка UTF-8	126
Использование UTF-8 на сервере каталогов	126
Создание файла LDIF со значениями UTF-8 с помощью утилит сервера	127
Поддерживаемые наборы символов IANA	128
Символы ASCII с кодом от 33 до 126	129

Глава 18. Создание и администрирование экземпляра . . . 131

Запуск Инструмента администрирования экземпляра	132
Запуск Инструмента администрирования экземпляра для обновления экземпляра	133
Создание экземпляра сервера каталогов	133
Создание экземпляра с помощью инструмента администрирования экземпляра	134
Создание экземпляра сервера каталогов по умолчанию	134
Создание экземпляра сервера каталогов с пользовательскими параметрами	136
Создание экземпляра сервера прокси с пользовательскими параметрами	143
Создание экземпляра с помощью утилиты командной строки	146
Обновление экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра	148
Обновление удаленного экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра	150
Создание экземпляра на основе существующего экземпляра	152
Создание копии существующего экземпляра с помощью Инструмента администрирования экземпляра	154
Создание копии существующего экземпляра с помощью утилиты командной строки	157
Запуск и остановка сервера каталогов и сервера администрирования	157
Запуск и завершение работы сервера каталогов и административного сервера	158
Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки	159
Управление конфигурацией экземпляра сервера каталогов	159
Открытие Инструмента настройки из Инструмента администрирования экземпляра	160
Изменение параметров TCP/IP экземпляра	160

Изменение параметров TCP/IP экземпляра с помощью Инструмента администрирования экземпляра	160
Изменение параметров TCP/IP экземпляра с помощью утилит командной строки	161
Просмотр информации об экземпляре	162
Просмотр сведений об экземпляре с помощью Инструмента администрирования экземпляра	163
Просмотр сведений об экземпляре с помощью утилиты командной строки	163
Удаление экземпляра сервера каталогов	163
Удаление экземпляра с помощью Инструмента администрирования экземпляра	164
Удаление экземпляра с помощью утилиты командной строки	165

Глава 19. Проверка структуры каталогов 167

Глава 20. Настройка экземпляра . . . 169

Запуск Инструмента настройки	170
Запуск и остановка сервера каталогов и сервера администрирования с помощью Инструмента настройки	170
Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки	171
Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки	171
Управление DN главного администратора для экземпляра	172
Настройка отличительного имени (DN) главного администратора с помощью Инструмента настройки	172
Настройка отличительного имени (DN) главного администратора с помощью утилиты командной строки	173
Управление паролем главного администратора для экземпляра	174
Настройка пароля главного администратора с помощью Инструмента настройки	174
Настройка пароля главного администратора с помощью утилиты командной строки	175
Настройка базы данных для экземпляра сервера каталогов	175
Настройка базы данных экземпляра с помощью Инструмента настройки	176
Настройка базы данных экземпляра с помощью утилиты командной строки	180
Управление паролем администратора базы данных DB2	182
Изменение пароля администратора базы данных DB2 с помощью Инструмента настройки	182
Изменение пароля администратора базы данных DB2 с помощью утилиты командной строки	183
Удаление конфигурации базы данных из экземпляра сервера каталогов	184
Отключение базы данных DB2 от экземпляра с помощью Инструмента настройки	185

Отключение базы данных DB2 от экземпляра с помощью утилиты командной строки	186
Оптимизация базы данных	186
Оптимизация базы данных с помощью Инструмента настройки	187
Оптимизация базы данных с помощью утилиты командной строки	187
Обслуживание базы данных	188
Обслуживание базы данных с помощью Инструмента настройки	188
Обслуживание базы данных с помощью утилиты командной строки	189
Резервное копирование сервера каталогов	190
Резервное копирование базы данных сервера каталогов с помощью Configuration Tool	190
Резервное копирование экземпляра прокси-сервера с помощью Configuration Tool	192
Восстановление сервера каталогов	193
Восстановление базы данных сервера каталогов с помощью Инструмента настройки	193
Восстановление экземпляра сервера проху с помощью Инструмента настройки	194
Настройка сервера каталогов для повышения производительности	195
Настройка сервера каталогов для тонкой настройки производительности с помощью Configuration Tool	196
Настройка сервера каталогов для тонкой настройки производительности с помощью командной строки	199
Управление протоколом изменений для экземпляра сервера каталогов	200
Настройка протокола изменений с помощью Инструмента настройки	200
Настройка протокола изменений с помощью утилиты командной строки	201
Отключение протокола изменений с помощью Инструмента настройки	202
Отключение протокола изменений с помощью утилиты командной строки	203
Настройка суффикса	204
Добавление суффикса с помощью Configuration Tool	204
Добавление суффикса с помощью командной строки	205
Удаление суффикса с помощью Инструмента настройки	206
Удаление суффикса с помощью командной строки	206
Управление схемой	207
Управление файлом схемы с помощью Configuration Tool	208
Управление файлом схемы с помощью командной строки	209
Настройка проверки правильности схемы с помощью Инструмента настройки	210
Управление данными LDIF	210
Импорт данных LDIF с помощью Инструмента настройки	212
Проверка данных LDIF с помощью Инструмента настройки	213

Экспорт данных LDIF с помощью Инструмента настройки	214
Синхронизация Active Directory	215
Настройка и запуск синхронизации Active Directory	217
Настройка синхронизации Active Directory с помощью Configuration Tool.	217
Настройка синхронизации Active Directory с помощью командной строки	219

**Глава 21. Автоматический запуск
экземпляров сервера каталогов при
запуске операционной системы. 221**

Настройка автоматического запуска экземпляра сервера каталогов в системе Windows.	221
Настройка автоматического запуска экземпляра сервера каталогов в системе UNIX	223

**Глава 22. Стратегия пакетов
исправлений 225**

Установка пакетов исправлений с помощью IBM Installation Manager.	225
Установка пакетов исправлений без вывода сообщений	227
Установка пакетов исправлений с помощью стандартных сценариев	228

**Глава 23. Удаление IBM Security
Directory Server: обзор 229**

**Глава 24. Удаление из системы IBM
Security Directory Server и
сопутствующего программного
обеспечения 231**

Удаление из системы с помощью IBM Installation Manager	232
Удаление с помощью IBM Installation Manager Удаление без вывода сообщений с помощью файла ответов	233
Удаление в режиме без вывода сообщений с помощью команды <code>imcl uninstall</code>	235
Удаление из системы IBM Security Directory Server с помощью утилит операционной системы	235

Удаление из системы с помощью утилит AIX	236
Удаление из системы с помощью утилит Linux	238
Удаление из системы с помощью утилит Solaris	239
Удаление из системы с помощью утилит HP-UX	240
Удаление из системы IBM DB2 с помощью команд DB2	240
Удаление из системы IBM Global Security Kit с помощью утилит операционной системы	241
Удаление IBM Global Security Kit с помощью SMIT	241
Удаление IBM Global Security Kit с помощью <code>installp</code>	241
Удаление IBM Global Security Kit с помощью утилит Linux.	242
Удаление IBM Global Security Kit с помощью утилит Solaris	242
Удаление IBM Global Security Kit с помощью утилит HP-UX	243
Удаление IBM Global Security Kit в операционной системе Windows	243
Удаление из системы языковых пакетов	244
Удаление языковых пакетов с помощью утилит операционной системы	244

**Приложение А. Язык описания
служб каталогов. 247**

**Приложение В. Загрузка примера
базы данных и запуск сервера 249**

**Приложение С. Обновление файла
Idapdb.properties вручную 251**

**Приложение D. Специальные
возможности для Security Directory
Server 253**

Индекс 255

Примечания. 263

Общая информация о публикации

IBM® Security Directory Server (предыдущее название - IBM Tivoli Directory Server) представляет собой реализацию протокола LDAP, разработанную IBM, для следующих операционных систем:

- Microsoft Windows
- AIX
- Linux (System x, System z, System p и System i)
- Solaris
- Hewlett-Packard UNIX (HP-UX) (Itanium)

Руководство по установке и настройке IBM Security Directory Server содержит инструкции по установке, настройке и удалению IBM Security Directory Server. Кроме того, они содержат сведения об обновлении предыдущих версий.

Доступ к публикациям и терминологии

В этом разделе приведена следующая информация:

- Список публикаций в “Библиотека IBM Security Directory Server”.
- Ссылки на “Публикации в Интернете” на стр. viii.
- Ссылка на “Веб-сайт терминологии IBM” на стр. viii.

Библиотека IBM Security Directory Server

В библиотеке IBM Security Directory Server доступны следующие документы:

- *IBM Security Directory Server версии 6.3.1.5 - Обзор продукта, GC27-6212-01*

Содержит информацию о продукте IBM Security Directory Server, включая описание новых функций в текущем выпуске и сведения о системных требованиях.

- *IBM Security Directory Server версии 6.3.1.5 - Краткое руководство по началу работы, GI11-9351-02*

Предоставляет справку по началу работы с IBM Security Directory Server. Включает в себя краткое описание продукта, диаграмму архитектуры, а также ссылку на веб-сайт документации по продукту и инструкции по установке продукта.

- *Руководство по установке и настройке IBM Security Directory Server версии 6.3.1.5, SC27-2747-02*

Содержит полное описание и инструкции по установке, настройке и удалению IBM Security Directory Server. Содержит сведения об обновлении предыдущих версий IBM Security Directory Server.

- *IBM Security Directory Server версии 6.3.1.5 - Руководство администратора, SC27-2749-02*

Содержит инструкции по выполнению административных задач с помощью веб-инструмента администрирования или командной строки.

- *IBM Security Directory Server версии 6.3.1.5 - Руководство по созданию отчетов, SC27-6531-00*

Содержит описание инструментов и программного обеспечения для создания отчетов IBM Security Directory Server.

- *IBM Security Directory Server версии 6.3.1.5 - Справочник по командам, SC27-2753-02*

Содержит описание синтаксиса и формата утилит, запускаемых из командной строки, поставляемых в составе IBM Security Directory Server.

- *IBM Security Directory Server версии 6.3.1.5 - Справочник по модулям сервера, SC27-2750-02*

Содержит информацию о создании встраиваемых модулей сервера.

- *IBM Security Directory Server версии 6.3.1.5 - Справочник по программированию, SC27-2754-02*

Содержит информацию о разработке приложений клиента упрощенного протокола доступа на языках C и Java™.

- *IBM Security Directory Server версии 6.3.1.5 - Руководство по установке и настройке, SC27-2748-02*

Содержит информацию по настройке сервера каталогов для повышения его производительности. Описывает требования к дискам и другие требования для каталогов различных размеров и скоростей чтения и записи. Описывает известные рабочие сценарии для каждого из этих уровней каталога и используемых дисков и памяти; также приводит ряд самых общих правил.

- *IBM Security Directory Server версии 6.3.1.5 - Руководство по устранению неполадок, GC27-2752-02*

Содержит информацию о возможных неполадках и действиях по их устранению, которые можно выполнить перед обращением в службу поддержки IBM.

- *IBM Security Directory Server версии 6.3.1.5 - Справочник по сообщениям об ошибках, GC27-2751-02*

Содержит полный список предупреждений и сообщений об ошибках, относящихся к продукту IBM Security Directory Server.

Публикации в Интернете

IBM размещает публикации в момент выпуска продуктов, а также при обновлении публикаций в следующих расположениях:

Веб-сайт документации IBM Security Directory Server

На веб-странице <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm> показана начальная страница продукта.

IBM Security Systems Documentation Central и начальная страница

IBM Security Systems Documentation Central содержит список всех публикаций о продуктах IBM Security Systems, упорядоченный по алфавиту. Кроме того, приведены ссылки на документацию для различных версий продуктов.

Начальная страница документации по IBM Security Systems содержит общие сведения о продуктах и ссылки на документацию по IBM Security Systems.

IBM Publications Center

Веб-страница <http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss> предлагает настроенные функции поиска, помогающие найти необходимые публикации IBM.

Веб-сайт терминологии IBM

Веб-сайт терминологии IBM объединяет терминологию для библиотек продуктов в одном расположении. Адрес веб-сайта терминологии: <http://www.ibm.com/software/globalization/terminology>.

Специальные возможности

Специальные возможности позволяют успешно работать с программными продуктами пользователям с физическими ограничениями, например ограниченной подвижностью или слабым зрением. С данным продуктом можно применять технологии озвучивания команд и пунктов меню. Кроме того, для работы с графическим пользовательским интерфейсом вместо мыши можно использовать клавиатуру.

Дополнительная информация приведена в приложении Специальные возможности в разделе *Обзор продукта IBM Security Directory Server*.

Техническое обучение

За информацией о техническом обучении обратитесь к следующему веб-сайту IBM Education: <http://www.ibm.com/software/tivoli/education>.

Информация о поддержке

Служба поддержки IBM помогает в устранении неполадок, связанных с кодом, а также найти ответы на вопросы по установке или использованию. Веб-сайт службы поддержки IBM: <http://www.ibm.com/software/support/probsub.html>.

Руководство по устранению неполадок IBM Security Directory Server содержит следующие сведения:

- Информация, которую необходимо собрать перед обращением в службу поддержки IBM.
- Различные способы обращения в службу поддержки IBM.
- Работа с IBM Support Assistant.
- Инструкции и ресурсы по определению неполадок для изоляции и устранения неполадок своими силами.

Примечание: Вкладка **Сообщество и поддержка** в справочной системе Information Center содержит список дополнительных ресурсов поддержки.

Заявление о эффективных мерах безопасности

Обеспечение безопасности информационных систем предусматривает защиту систем и информации путем предотвращения, обнаружения и блокирования несанкционированного доступа в пределах и за пределами организации. Несанкционированный доступ может привести к изменению, уничтожению, неправомерному присваиванию или несанкционированному использованию информации либо может привести к несанкционированному использованию систем, включая организацию с их помощью атак на другие системы. Никакие информационные системы и продукты нельзя считать полностью безопасными; отдельные продукты, службы или меры безопасности не могут обеспечивать полную защиту от несанкционированного доступа или использования. Системы, продукты и службы IBM входят в состав комплексного подхода по обеспечению безопасности, который включает в себя дополнительные рабочие процедуры и может потребовать применения других систем, продуктов и служб для обеспечения максимальной эффективности. **IBM НЕ ГАРАНТИРУЕТ, ЧТО КАКИЕ-ЛИБО СИСТЕМЫ, ПРОДУКТЫ ИЛИ СЛУЖБЫ ПОЛНОСТЬЮ ЗАЩИЩЕНЫ ИЛИ СМОГУТ СДЕЛАТЬ ВАШУ ОРГАНИЗАЦИЮ ЗАЩИЩЕННОЙ ОТ ЗЛОНАМЕРНЫХ ИЛИ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ ЛЮБЫХ СТОРОН.**

Глава 1. Планирование установки

Необходимо выбрать аппаратное обеспечение, программное обеспечение, роли пользователей, параметры защиты и другие требования для среды сервера каталогов, перед тем как устанавливать IBM Security Directory Server.

Схема планирования

Справочная таблица, приведенная в этом разделе, применяется для установки сервера.

При установке поверх предыдущего выпуска не используйте эту таблицу. Вместо нее используйте инструкции, приведенные в главе Глава 14, “Обновление экземпляра предыдущей версии”, на стр. 89.

Для установки сервера выполните следующие действия:

1. Ознакомьтесь с обзором продукта, в котором приведено краткое описание доступных для установки компонентов IBM Security Directory Server:
2. Убедитесь, что у вас есть все необходимое аппаратное и программное обеспечение. Дополнительная информация о требованиях приведена в разделе “Требования к дисковой памяти” на стр. 3.
3. Установите IBM Security Directory Server с помощью IBM Installation Manager.
4. В Windows после перезагрузки системы войдите в систему с именем пользователя, начавшего установку.
5. Для управления экземплярами серверов каталогов применяется программа Instance Administration Tool.
6. Дополнительно можно проверить правильность установки и настройки, загрузив пример файла LDIF в базу данных. Дополнительная информация приведена в разделе Приложение B, “Загрузка примера базы данных и запуск сервера”, на стр. 249.
7. Запустите экземпляр сервера каталогов и Web Administration Tool (если он установлен).
8. Дополнительная информация о настройке сервера и Web Administration Tool приведена в разделе Администрирование документации по IBM Security Directory Server.

Инструкции по планированию организации базы данных для полного сервера каталогов приведены в разделе “Планирование настройки” на стр. 125.

Глава 2. Обзор установки

Необходимо подготовить компьютер и выбрать подходящий режим установки IBM Security Directory Server, допустимый для используемой среды.

Программа установки на основе IBM Installation Manager доступна для Windows, Linux64 и AIX. Внешние программы установки доступны для IBM Security Directory Server в системах UNIX за исключением Linux 64 и AIX. Программа установки на основе Installation Manager позволяет установить IBM Security Directory Server V6.3.1 с помощью графического пользовательского интерфейса или в режиме без вывода сообщений.

Требования к дисковой памяти

Для успешной установки IBM Security Directory Server и сопутствующего программного обеспечения на компьютере должен быть доступен требуемый объем дисковой памяти. Требования к дисковой памяти зависят от операционной системы, компонента IBM Security Directory Server и сопутствующего программного обеспечения, выбранного для установки.

Требования к дисковой памяти в Windows

Примечание: В случае установки прокси-сервера или полного сервера каталогов добавьте размеры для SDK клиента, IBM Java Development Kit и клиента Java.

Таблица 1. Требования к дисковой памяти для компонентов IBM Security Directory Server и сопутствующего программного обеспечения в Windows

Устанавливаемый компонент	Дисковая память для установки (в МБ)
Software Development Kit клиента	25 МБ
IBM Java Development Kit	200 МБ
Java Client	124 МБ
Развернутый Web Administration Tool (включая встроенный WebSphere Application Server и Web Administration Tool на сервере встроенный WebSphere Application Server)	440 МБ
Развертывание Web Administration Tool на существующем встроенном сервере WebSphere Application Server или сервере WebSphere Application Server	260 МБ
Базовый сервер	23 МБ
Прокси-сервер (без учета памяти, необходимой для установки SDK клиента, клиента Java и базового сервера).	40 МБ
Полный сервер каталогов (без учета памяти, необходимой для установки SDK клиента, клиента Java и базового сервера).	8 МБ
IBM DB2	763 МБ
IBM Global Security Kit	11 МБ

Требования к дисковой памяти в AIX

Примечание: В случае установки прокси-сервера или полного сервера каталогов добавьте размеры для SDK клиента, IBM Java Development Kit и клиента Java.

Таблица 2. Требования к дисковой памяти для компонентов IBM Security Directory Server и сопутствующего программного обеспечения в AIX

Устанавливаемый компонент	Дисковая память для установки (в МБ)
Software Development Kit клиента	8 МБ
IBM Java Development Kit	200 МБ
Java Client	91 МБ
Развернутый Web Administration Tool (включая встроенный WebSphere Application Server и Web Administration Tool на сервере встроенный WebSphere Application Server)	443 МБ
Развертывание Web Administration Tool на существующем встроенном сервере WebSphere Application Server или сервере WebSphere Application Server	500 МБ
Web Administration Tool, SSL	51 МБ
Базовый сервер	39 МБ
Прокси-сервер (без учета памяти, необходимой для установки SDK клиента, клиента Java и базового сервера).	4 МБ
Полный сервер каталогов (без учета памяти, необходимой для установки SDK клиента, клиента Java и базового сервера).	12 МБ
IBM DB2	1250 МБ
IBM Global Security Kit	16 МБ

Требования к дисковой памяти в Linux

Примечание: В случае установки прокси-сервера или полного сервера каталогов добавьте размеры для SDK клиента, IBM Java Development Kit и клиента Java.

Таблица 3. Требования к дисковой памяти для компонентов IBM Security Directory Server и сопутствующего программного обеспечения в Linux

Устанавливаемый компонент	Дисковая память для установки (в МБ)
Software Development Kit клиента	9 МБ
IBM Java Development Kit	200 МБ
Java Client	166 МБ
Развернутый Web Administration Tool (включая встроенный WebSphere Application Server и Web Administration Tool на сервере встроенный WebSphere Application Server)	443 МБ
Развертывание Web Administration Tool на существующем встроенном сервере WebSphere Application Server или сервере WebSphere Application Server	375 МБ
Базовый сервер	32 МБ

Таблица 3. Требования к дисковой памяти для компонентов IBM Security Directory Server и сопутствующего программного обеспечения в Linux (продолжение)

Устанавливаемый компонент	Дисковая память для установки (в МБ)
Прокси-сервер (без учета памяти, необходимой для установки SDK клиента, клиента Java и базового сервера).	40 МБ
Полный сервер каталогов (без учета памяти, необходимой для установки SDK клиента, клиента Java и базового сервера).	8 МБ
IBM DB2 (System x Linux)	460 МБ
IBM DB2 (System zLinux)	670 МБ
IBM DB2 (System i и System p Linux)	520 МБ
IBM DB2 (AMD64/EM64T Linux)	1300 МБ
IBM Global Security Kit	40 МБ

Примечание: (Применимо для программы установки на основе Installation Manager). Каталог общих ресурсов должен содержать 200 МБ свободной дисковой памяти. В установочном каталоге IBM Security Directory Server требуются дополнительные 200 МБ свободной дисковой памяти.

Требования к памяти для временного каталога по умолчанию: если база данных DB2 выбрана для установки, то временный каталог должен содержать 2048 МБ + 500 МБ свободной памяти. Если установка DB2 не выполняется, то временный каталог должен содержать 500 МБ свободной памяти.

Требования к дисковой памяти в Solaris

Примечание: В случае установки сервера и прокси-сервера добавьте размеры для клиента C, IBM Java Development Kit и клиента Java.

Таблица 4. Требования к дисковой памяти для компонентов IBM Security Directory Server и сопутствующего программного обеспечения в Solaris

Устанавливаемый компонент	Дисковая память для установки (в МБ)	Примечания
C Client	11 МБ	
IBM Java Development Kit		
Java Client	145 МБ	
Сервер	47 МБ	Добавьте размеры для клиентов C и Java
Proxy Server	40 МБ	Добавьте размеры для клиентов C и Java
Веб-инструмент администрирования	470 МБ	Содержит встроенный WebSphere Application Server и Web Administration Tool, который развертывается на этом сервере
IBM DB2	1155 МБ	
IBM Global Security Kit	34 МБ	

Требования к дисковой памяти в HP-UX

Таблица 5. Требования к дисковой памяти для компонентов IBM Security Directory Server и сопутствующего программного обеспечения в HP-UX

Устанавливаемый компонент	Дисковая память для установки (в МБ)
C Client	26 МБ
IBM Java Development Kit	
Java Client	172 МБ
IBM Global Security Kit	41 МБ

Подготовка носителя установки

Пакет продукта IBM Security Directory Server включает в себя IBM Security Directory Server, сопутствующее программное обеспечение и программу установки. Носитель установки можно получить с установочных DVD или с веб-сайта Passport Advantage.

Продукт IBM Security Directory Server поставляется в виде файлов в трех форматах: .zip, .tar и .iso. Файл .iso содержит несколько файлов в форматах .zip или .tar.

Таблица 6. Продукт IBM Security Directory Server доступен в следующем формате в различных операционных системах

AIX, Linux, Solaris и Windows	AIX, Linux, Solaris и HP-UX	Windows
Образ ISO (файл .iso)	Файлы архивов на ленте (.tar)	Файлы архивов (.zip)

Для того чтобы использовать DVD в качестве носителя установки, необходимо выполнить одну из следующих задач:

- Создать образ DVD из образа продукта IBM Security Directory Server для своей операционной системы.
- Сохранить образ продукта IBM Security Directory Server на жестком диске компьютера и смонтировать его, если требуется.

При загрузке файлов архива продукта должны быть выполнены следующие требования:

1. Загрузите все требуемые файлы архива в один и тот же каталог. Не загружайте файлы архива в расположение каталога, которое содержит пробелы в имени пути.
2. Разархивируйте все файлы архива в один и тот же каталог, который не содержит пробелов в имени пути. Путь к каталогу, из которого будет выполняться установка, не должен содержать пробелов.

Для загрузки продукта IBM Security Directory Server из Passport Advantage обратитесь к разделу “Загрузка программного обеспечения из Passport Advantage”.

После подготовки носителя установки необходимо обеспечить соблюдение требований к необходимому программному обеспечению для данной операционной системы. Обратитесь к разделу “Предварительные требования для установки” на стр. 14.

Загрузка программного обеспечения из Passport Advantage

Для установки программного обеспечения IBM Security Directory Server его необходимо загрузить из IBM Passport Advantage.

Прежде чем начать

Для доступа к программе IBM Passport Advantage необходимо зарегистрироваться и получить номер счета клиента.

Процедура

1. Перейдите на веб-сайт IBM Passport Advantage по адресу http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
2. Щелкните на ссылке **Customer sign in**.
3. В поле **IBM ID** введите свой ИД IBM.
4. В поле **Password** введите свой пароль.
5. Нажмите кнопку **Sign in**.
6. Следуйте инструкциям по загрузке программного обеспечения IBM Security Directory Server.

Структура каталогов загруженных файлов

После загрузки установочных файлов для IBM Security Directory Server с сервера необходимо проверить структуру каталогов.

Структура каталогов для пакетов Windows

Пакеты Security Directory Server 6.3.1 для Windows имеют следующие имена:

Образ DVD: sds631-win.iso

Файлы .zip:

- sds631-win-base.zip (Security Directory Server 6.3.1 Client и Server)
- sds631-win-db2.zip (DB2 V9.7)
- sds631-win-ewas.zip (встроенный WebSphere Application Server 7.0.0.29)
- sds631-win-gskit.zip (GSKit 8.0)
- sds631-win-jdk.zip (IBM Java Development Kit)
- sds631-win-IM.zip (IBM Installation Manager)

После создания дисков DVD или распаковки файлов .zip структура каталогов будет следующей:

- \sdsV6.3.1 (главный каталог распакованных файлов)
 - ibm_gskit\ (GSKit)
 - license\ (лицензии для Security Directory Server и других продуктов)
 - quickstart\ (Краткие руководства по началу работы на английском и других языках)
 - entitlement\ (файлы entitlement для прокси-сервера)
 - entitlement.txt
 - tools\ (инструменты, включая migbkup)
 - migbkup.bat
 - ibm_db2_32bit\ (DB2)
 - ibm_db2_64bit\ (DB2)
 - ibm_ewas_32bit\ (встроенный WebSphere Application Server)
 - ibm_ewas_64bit\ (встроенный WebSphere Application Server)
 - ibm_im_32bit\ (IBM Installation Manager)
 - ibm_im_64bit\ (IBM Installation Manager)
 - ibm_jdk\ (IBM Java Development Kit)
 - ibm_sds\ (файлы программы установки)
 - atoc
 - files
 - native

- Offerings
- plugins
- ShareableEntities
- build.properties
- repository.config
- repository.xml
- launchpad\
- SilentInstallScripts\ (файлы ответов для установки без вывода сообщений)
- autorun.inf
- imLauncherWindows.bat
- launchpad.exe
- launchpad.ini
- launchpad64.exe
- launchpad64.ini
- sds_install.xml
- write_sds_path.bat

Пакет клиента Windows

Файл .zip:

- sds631-win-client.zip (Security Directory Server 6.3.1 Client)

После распаковки файла .zip структура каталогов будет следующей:

- \sdsV6.3.1 (главный каталог распакованных файлов)
 - ibm_gskit\ (GSKit 8)
 - jdk\ (IBM Java Development Kit)
 - ibm_im_32bit (IBM Installation Manager)
 - ibm_im_64bit (IBM Installation Manager)
 - ibm_sds\ (файлы программы установки)
 - launchpad\
 - SilentInstallScripts\
 - autorun.inf
 - license\ (лицензии для Security Directory Server и других продуктов)
 - quickstart\ (Краткие руководства по началу работы на английском и других языках)
 - ibm_im_32bit\ (IBM Installation Manager)
 - ibm_im_64bit\ (IBM Installation Manager)
 - imLauncherWindows.bat
 - launchpad.exe
 - launchpad.ini
 - launchpad64.exe
 - launchpad64.ini
 - sds_install.xml
 - write_sds_path.bat

Структура каталогов для пакетов сервера AIX

Пакеты Security Directory Server 6.3.1 для AIX имеют следующие имена:

Образ DVD: sds631-aix-ppc64.iso

Файлы .tar:

- tds63-aix-ppc64-base.tar (Security Directory Server 6.3.1 Client и Server)
- sds631-aix-ppc64-db2.tar (DB2 V9.7)
- sds631-aix-ppc64-ewas.tar (встроенный WebSphere Application Server 7.0.0.29)
- sds631-aix-ppc64-gskit.tar (GSKit 8.0)

- sds631-aix-ppc64-jdk.tar (IBM Java Development Kit)
- sds631-aix-ppc64-IM.tar (IBM Installation Manager)

После создания дисков DVD или распаковки файлов .tar структура каталогов будет следующей:

- /sdsV6.3.1 (главный каталог распакованных файлов)
 - license/ (лицензии для Security Directory Server и других продуктов)
 - quickstart/ (Краткие руководства по началу работы на английском и других языках)
 - ibm_im (IBM Installation Manager)
 - ibm_db2/ (DB2)
 - ibm_ewas/ (встроенный WebSphere Application Server)
 - ibm_gskit/ (GSKit 8)
 - ibm_jdk/ (IBM Java Development Kit)
 - ibm_sds/ (файлы программы установки)
 - atoc/
 - files/
 - native/
 - Offerings/
 - plugins/
 - ShareableEntities
 - build.properties
 - repository.config
 - repository.xml
- tools/ (инструменты, включая migbkup)
- launchpad/
- SilentInstallScripts/
- launchpad.sh
- sds_install.xml
- write_sds_path.sh
- entitlement/ (файлы entitlement для прокси-сервера)
- native / (внутренние пакеты)

Пакет клиента AIX

Файл .zip:

- sds631-aix-ppc64-client.tar (Security Directory Server 6.3.1 Client)

После распаковки файла .zip структура каталогов будет следующей:

- \sdsV6.3.1 (главный каталог распакованных файлов)
 - ibm_gskit\ (GSKit 8)
 - ibm_jdk\ (IBM Java Development Kit)
 - ibm_im\ (IBM Installation Manager)
 - ibm_sds\ (файлы программы установки)
 - launchpad\
 - SilentInstallScripts\
 - autorun.inf
 - license\ (лицензии для Security Directory Server и других продуктов)
 - quickstart\ (Краткие руководства по началу работы на английском и других языках)
 - ibm_im\ (IBM Installation Manager)
 - imLauncherWindows.bat
 - launchpad.exe

- launchpad.ini
- sds_install.xml
- write_sds_path.bat

Структура каталогов для пакетов сервера Linux x86_64

Пакеты Security Directory Server 6.3.1 для Linux x86_64 имеют следующие имена:

Образ DVD: sds631-linux-x86-64.iso

Файлы .tar:

- sds631-linux-x86-64-base.tar (IBM Security Directory Server 6.3.1 Client и Server)
- sds631-linux-x86-64-IM.tar (IBM Installation Manager)
- sds631-linux-x86-64-gskit.tar (GSKit 8)
- sds631-linux-x86-64-db2.tar (DB2 vV9.7)
- sds631-linux-x86-64-ewas.tar (встроенный WebSphere Application Server 7.0.0.29)
- sds631-linux-x86-64-jdk.tar (IBM Java Development Kit)

После создания дисков DVD или распаковки файлов .tar структура каталогов будет следующей:

/sdsV6.3.1 (главный каталог распакованных файлов)

- license/ (лицензии для Security Directory Server и других продуктов)
- quickstart/ (Краткие руководства по началу работы на английском и других языках)
- ibm_im (IBM Installation Manager)
- ibm_db2/ (DB2)
- ibm_ewas/ (встроенный WebSphere Application Server)
- ibm_gskit/ (GSKit 8)
- ibm_jdk/ (IBM Java Development Kit)
- ibm_sds/ (файлы программы установки)
- atoc/
- files/
- native/
- Offerings/
- plugins/
- ShareableEntities
- build.properties
- repository.config
- repository.xml
- tools/ (инструменты, включая migbkup)
- launchpad/
- SilentInstallScripts/
- launchpad.sh
- sds_install.xml
- write_sds_path.sh
- entitlement/ (файлы entitlement для прокси-сервера)
- native / (внутренний пакет)

Пакет клиента Linux x86_64

Файл .zip:

- sds631-linux-x86-64-client.tar (Security Directory Server 6.3.1 Client)

После распаковки файла .zip структура каталогов будет следующей:

- \sdsV6.3.1 (главный каталог распакованных файлов)
- ibm_jdk\ (IBM Java Development Kit)
- ibm_im (IBM Installation Manager)
- ibm_sds\ (файлы программы установки)
- launchpad\
- SilentInstallScripts\
- autorun.inf
- license\ (Лицензии для Security Directory Server и других продуктов)
- quickstart\ (Краткие руководства по началу работы на английском и других языках)
- ibm_im\ (IBM Installation Manager)
- imLauncherWindows.bat
- launchpad.exe
- launchpad.ini
- sds_install.xml
- write_sds_path.bat

Структура каталогов для пакетов сервера Linux x86

Пакеты Security Directory Server 6.3.1 для Linux x86 имеют следующие имена:

Образ DVD: sds631-linux-x86.iso

Файлы .tar:

- sds631-linux-x86-base.tar (IBM Security Directory Server 6.3.1 Client и Server)
- sds631-linux-x86-gskit.tar (GSKit 8)
- sds631-linux-x86-db2.tar (DB2 v9.7)
- sds631-linux-x86-ewas.tar (встроенный WebSphere Application Server 7.0.0.29)
- sds631-linux-x86-jdk.tar (IBM Java Development Kit)

После создания дисков DVD или распаковки файлов .tar структура каталогов будет следующей:

- /sdsV6.3.1 (главный каталог распакованных файлов)
- appsrv/ (встроенный WebSphere Application Server)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids_detectGskitVersion
- idsinstall_i
- idsNativeInstall.sh
- images/ (внутренние образы)
- license (лицензии для Security Directory Server и других продуктов)
- responseFile.txt (файл ответов)

Пакет клиента Linux x86

Файл .zip:

- sds631-linux-x86-client.tar (Security Directory Server 6.3.1 Client)

После распаковки файла .zip структура каталогов будет следующей:

- \sdsV6.3.1 (главный каталог распакованных файлов)
- gskit/(GSKit 8)
- image/
- license/ (лицензии для Security Directory Server и других продуктов)
- jdk (IBM Java Development Kit)

Структура каталогов для пакетов сервера Linux ppc

Пакеты Security Directory Server 6.3.1 для Linux ppc имеют следующие имена:

Образ DVD: sds631-linux-ppc64.iso

Файлы .tar:

- sds631-linux-ppc64-base.tar (IBM Security Directory Server 6.3.1 Client и Server)
- sds631-linux-ppc64-gskit.tar (GSKit 8)
- sds631-linux-ppc64-db2.tar (DB2 V9.7)
- sds631-linux-ppc64-ewas.tar (встроенный WebSphere Application Server 7.0.0.29)
- sds631-linux-ppc64-jdk.tar (IBM Java Development Kit)

После создания дисков DVD или распаковки файлов .tar структура каталогов будет следующей:

/sdsV6.3.1 (главный каталог распакованных файлов)

- appsrv/ (встроенный WebSphere Application Server)
- db2 (DB2)
- gskit/ (GSKit 8)
- jdk/ (IBM Java Development Kit)
- ids_detectGskitVersion
- idsinstall_i
- idsNativeInstall.sh
- images/ (внутренние образы)
- license (лицензии для Security Directory Server и других продуктов)
- responseFile.txt (файл ответов)

Пакет клиента Linux ppc

Файл .zip:

- sds631-linux-ppc64-client.tar (Security Directory Server 6.3.1 Client)

После распаковки файла .zip структура каталогов будет следующей:

\sdsV6.3.1 (главный каталог распакованных файлов)

- gskit/(GSKit 8)
- image/
- license/ (лицензии для Security Directory Server и других продуктов)
- jdk (IBM Java Development Kit)

Структура каталогов для пакетов сервера Linux s390

Пакеты Security Directory Server 6.3.1 для Linux s390 имеют следующие имена:

Образ DVD: sds631-linux-s390x.iso

Файлы .tar:

- sds631-linux-s390x-base.tar (IBM Security Directory Server 6.3.1 Client и Server)
- sds631-linux-s390x-gskit.tar (GSKit 8)
- sds631-linux-s390x-db2.tar (DB2 V9.7)
- sds631-linux-s390x-ewas.tar (встроенный WebSphere Application Server 7.0.0.29)
- sds631-linux-s390x-jdk.tar (IBM Java Development Kit)

После создания дисков DVD или распаковки файлов .tar структура каталогов будет следующей:

/sdsV6.3.1 (главный каталог распакованных файлов)
– appsrv/ (встроенный WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (внутренние образы)
– license (лицензии для Security Directory Server и других продуктов)
– responseFile.txt (файл ответов)

Пакет клиента Linux s390

Файл .zip:

– sds631-linux-s390x-client.tar (Security Directory Server 6.3.1 Client)

После распаковки файла .zip структура каталогов будет следующей:

\sdsV6.3.1 (главный каталог распакованных файлов)
– gskit/(GSKit 8)
– image/
– license/ (лицензии для Security Directory Server и других продуктов)
– jdk (IBM Java Development Kit)

Структура каталогов для пакетов сервера Solaris x86_64

Пакеты Security Directory Server 6.3.1 для Solaris x86_64 имеют следующие имена:

Образ DVD: sds631-solaris-x86-64.iso

Файлы .tar:

– sds631-solaris-x86-64-base.tar (IBM Security Directory Server 6.3.1 Client и Server)
– sds631-solaris-x86-64-gskit.tar (GSKit 8)
– sds631-solaris-x86-64-db2.tar(DB2 v9.7)
– sds631-solaris-x86-64-ewas.tar (встроенный WebSphere Application Server 7.0.0.29)
– sds631-solaris-x86-64-jdk.tar (IBM Java Development Kit)

После создания дисков DVD или распаковки файлов .tar структура каталогов будет следующей:

/sdsV6.3.1 (главный каталог распакованных файлов)
– appsrv/ (встроенный WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (внутренние образы)
– license (лицензии для Security Directory Server и других продуктов)
– responseFile.txt (файл ответов)

Пакет клиента Solaris x86_64

Файл .zip:

– sds631-solaris-x86-64-client.tar (Security Directory Server 6.3.1 Client)

После распаковки файла .zip структура каталогов будет следующей:

```
\sdsV6.3.1 (главный каталог распакованных файлов)
– gskit/(GSKit 8)
– image/
– license/ (лицензии для Security Directory Server и других продуктов)
– jdk (IBM Java Development Kit)
```

Структура каталогов для пакетов сервера Solaris sparc

Пакеты Security Directory Server 6.3.1 для Solaris sparc имеют следующие имена:

Образ DVD:

Файлы .tar:

```
– sds631-solaris-sparc.iso
– sds631-solaris-sparc-base.tar (IBM Security Directory Server 6.3.1 Client и Server)
– sds631-solaris-sparc-gskit.tar (GSKit 8)
– sds631-solaris-sparc-db2.tar (DB2 v9.7)
– sds631-solaris-sparc-ewas.tar (встроенный WebSphere Application Server 7.0.0.29)
– sds631-solaris-sparc-jdk.tar (IBM Java Development Kit)
```

После создания дисков DVD или распаковки файлов .tar структура каталогов будет следующей:

```
/sdsV6.3.1 (главный каталог распакованных файлов)
– appsrv/ (встроенный WebSphere Application Server)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (внутренние образы)
– license (лицензии для Security Directory Server и других продуктов)
– responseFile.txt (файл ответов)
```

Пакет клиента Solaris Sparc

Файл .zip:

```
– sds631-solaris-sparc-client.tar (Security Directory Server 6.3.1 Client)
```

После распаковки файла .zip структура каталогов будет следующей:

```
\sdsV6.3.1 (главный каталог распакованных файлов)
– gskit/ (GSKit 8)
– image/
– license/ (лицензии для Security Directory Server и других продуктов)
– jdk (IBM Java Development Kit)
```

Предварительные требования для установки

Для установки IBM Security Directory Server и сопутствующего программного обеспечения может потребоваться предварительная установка необходимого программного обеспечения для данной операционной системы. Необходимое программное обеспечение следует установить перед установкой IBM Security Directory Server и сопутствующего программного обеспечения.

Предварительно требуемые пакеты в различных операционных системах

Необходимо обновить свой компьютер с помощью предварительно требуемых пакетов перед установкой продуктов IBM Security Directory Server и сопутствующего программного обеспечения.

Оболочка Korn требуется в операционных системах AIX, Linux, Solaris и HP-UX (Itanium). На SuSE Linux Enterprise Server требуется PDKSH.

Следующие пакеты требуются перед установкой IBM Security Directory Server в следующих операционных системах:

AIX Для установки пакетов rpm в системе AIX загрузите администратор пакетов rpm для систем AIX с веб-сайта <ftp://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte>.

Таблица 7. Предварительно требуемые пакеты в операционных системах AIX

Пакеты	Причина	Адрес загрузки
Веб-браузер Mozilla Firefox для AIX	Для открытия панели запуска в AIX должна существовать поддерживаемая версия браузера.	Более подробная информация о веб-браузерах для AIX находится на веб-сайте http://www.ibm.com/systems/power/software/aix/browsers/ .
gtk+ RPM (gtk2-2.10.6-4.aix5.2.ppc.rpm)	Eclipse изменил требования к системе окон с motif на gtk в операционных системах UNIX. Для AIX это изменение системы окон Eclipse требует установки библиотек gtk для поддержки графического пользовательского интерфейса. Для IBM Installation Manager графический пользовательский интерфейс используется в режиме мастера.	Более подробная информация об установке библиотек gtk находится в технической статье Требуемые библиотеки gtk для Installation Manager в системе AIX на веб-сайте http://www.ibm.com/support/docview.wss?uid=swg21631478 .

Таблица 7. Предварительно требуемые пакеты в операционных системах AIX (продолжение)

Пакеты	Причина	Адрес загрузки
GNU tar	Для того чтобы разархивировать сжатые файлы, предоставленные с IBM Security Directory Server в системах AIX, требуется архиватор GNU. Необходимо установить путь программы tar GNU перед программой tar, предоставленной с операционной системой. Программа tar GNU устанавливается в каталоге /opt/freeware/bin, а программа tar, которая предоставлена с операционной системой, в каталоге /usr/bin. Для того чтобы установить путь /opt/freeware/bin, выполните следующую команду: export PATH=/opt/freeware/bin:\$PATH.	Для того чтобы загрузить файл архива tar GNU (tar), откройте веб-сайт http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html .
Набор файлов X11.adt.lib	Набор файлов X11.adt.lib требуется для установки пакетов idsldap.cltjava631 и idsldap.webadmin631 в системах AIX.	
x1C.rte 8.0.0.6 и x1C.aix50.rte 8.0.0.6 или более высоких уровней	IBM C++ Runtime Environment Components for AIX требует уровней среды выполнения x1C.rte 8.0.0.6 и x1C.aix50.rte 8.0.0.6 или выше.	
bos.loc.iso.en_US 5.3.0.0	IBM Security Directory Server версии 6.3.1 требует минимальный уровень набора файлов локали системы bos.loc.iso.en_US 5.3.0.0.	

Предварительно необходимые требования для клиента LDAP в PowerPC LE

Для запуска клиента IBM Security Directory Server в PowerPC LE (в начале младший байт) в системе PowerPC LE необходимо установить IBM Advance Toolchain версии 7.1.

Установите IBM Advance Toolchain версии 7.1, если планируется работать с клиентом LDAP или создавать собственные клиенты путем подключения предоставленных библиотек.

Инструкции по загрузке и установке IBM Advanced Toolchain версии 7.1 приведены в документации по IBM Advance Toolchain.

Пользователь и группа `idsldap`

Если для установки выбран компонент Proxy Server, то программа установки может создать пользователя и группу `idsldap`.

Программа установки создает пользователя и группу `idsldap`, если они еще не созданы.

Примечание: В AIX, Linux и Solaris установка с помощью утилит операционной системы создает пользователя `idsldap`, если он еще не создан. Однако при наличии каталога `/home/idsldap` в Linux и AIX или каталога `/export/home/idsldap` в Solaris, возможно, пользователя `idsldap` создать не удастся. Поэтому необходимо убедиться, что домашний каталог для `idsldap` не существует, если не создан пользователь `idsldap`.

Если в соответствии с требованиями среды вы должны управлять пользователем и группой `idsldap`, то их можно создать до установки. Пользователь и группа `idsldap` должны отвечать следующим требованиям:

- Пользователь `idsldap` должен входить в группу `idsldap`.
- В AIX, Linux и Solaris пользователь `root` должен входить в группу `idsldap`. В Windows, администратор должен входить в группу `idsldap`.
- Для пользователя `idsldap` должен быть предусмотрен домашний каталог.
- В AIX, Linux и Solaris оболочкой по умолчанию для пользователя `idsldap` должна быть оболочка Korn.
- Для пользователя `idsldap` можно (но необязательно) задать пароль.
- Пользователь `idsldap` может быть владельцем экземпляра сервера каталогов.

Перед установкой IBM Security Directory Server необходимо выполнить все требования. Если пользователь `idsldap` существует, но не отвечает перечисленным требованиям, компонент Proxy Server может быть установлен неправильно.

Примечание: Дополнительная информация о требованиях к ИД пользователя для экземпляра, экземпляра каталога, владельца базы данных приведена в разделе “Пользователи и группы, связанные с экземпляром сервера каталогов” на стр. 121.

С помощью инструмента администрирования экземпляра можно создать пользователей и группы при создании экземпляра сервера каталогов. Можно также воспользоваться утилитами операционной системы, чтобы создать пользователя и группу `idsldap` и правильно их настроить.

Примеры

Запустите следующие утилиты операционной системы, чтобы создать группу `idsldap`, пользователя `idsldap`, пароль и добавить пользователя в группу `idsldap`.

В системах AIX:

Для создания группы `idsldap` введите следующую команду:

```
mkgroup idsldap
```

Для того чтобы создать ИД пользователя `idsldap` как участника группы `idsldap` и задать оболочку Korn в качестве оболочки по умолчанию, введите следующую команду:

```
mkuser pgrp=idsldap home=/home/idsldap shell=/bin/ksh idsldap
```

Для того чтобы задать пароль для пользователя `idsldap`, введите следующую команду:

```
passwd idsldap
```

Для того чтобы добавить ИД пользователя root в группу idsldap введите следующую команду:

```
/usr/bin/chgrpmem -m + root idsldap
```

В системах Linux:

Для создания группы idsldap введите следующую команду:

```
groupadd idsldap
```

Для того чтобы создать ИД пользователя idsldap как участника группы idsldap и задать оболочку Korn в качестве оболочки по умолчанию, введите следующую команду:

```
useradd -g idsldap -d /home/idsldap -m -s /bin/ksh idsldap
```

Для того чтобы задать пароль для пользователя idsldap, введите следующую команду:

```
passwd idsldap
```

Для того чтобы добавить ИД пользователя root в группу idsldap введите следующую команду:

```
usermod -G idsldap,rootgroups root
```

Можно получить значения *rootgroups* для своего компьютера с помощью команды `groups root`.

В системах Solaris:

Для создания группы idsldap введите следующую команду:

```
groupadd idsldap
```

Для того чтобы создать ИД пользователя idsldap как участника группы idsldap и задать оболочку Korn в качестве оболочки по умолчанию, введите следующую команду:

```
useradd -g idsldap -d /export/home/idsldap -m -s /bin/ksh idsldap
```

Для того чтобы задать пароль для пользователя idsldap, введите следующую команду:

```
passwd idsldap
```

Для того чтобы добавить ИД пользователя root в группу idsldap введите следующую команду:

```
usermod -G idsldap,root idsldap
```

Для того чтобы изменить ИД пользователя root, с тем чтобы включить пользователя root в группу idsldap, воспользуйтесь подходящим инструментом.

Дополнительная информация о команде добавления пользователя и группы приведена в документации по операционной системе.

Методы установки

Для установки IBM Security Directory Server и сопутствующего программного обеспечения необходимо выбрать подходящий метод установки для среды.

Можно использовать следующие методы установки IBM Security Directory Server и сопутствующего программного обеспечения:

- Установка с помощью IBM Installation Manager

- Установка с помощью утилит командной строки операционной системы

ОСТОРОЖНО:

- **Нельзя использовать разные методы установки на одном и том же компьютере. Необходимо выполнять установку IBM Security Directory Server либо с помощью IBM Installation Manager, либо с помощью утилит командной строки операционной системы. В случае применения обоих режимов установки могут быть установлены не все необходимые для компонента правильные пакеты.**
- **Следует избегать установки вручную DB2 и встроенного WebSphere Application Server в соответствующих установочных расположениях по умолчанию, используемых программой IBM Installation Manager. Подобная установка вручную может стать причиной сбоев установки, изменения или удаления из системы, когда эти операции будут выполняться из IBM Installation Manager. Дополнительная информация об установочном расположении по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.**

Глава 3. Установка с помощью IBM Installation Manager

IBM Installation Manager - это инструмент, с помощью которого можно устанавливать и обслуживать IBM Security Directory Server и сопутствующее программное обеспечение.

IBM Installation Manager - Обзор

IBM Installation Manager - это мастер установки, помогающий пройти пошаговую процедуру установки, изменения, обновления, отката или удаления продуктов IBM. Для установки он может использовать удаленные или локальные хранилища программного обеспечения.

С помощью IBM Installation Manager можно также управлять приложениями и пакетами IBM, которые он установил на компьютере. Для этого он выполняет следующее:

- Ведет запись установленных компонентов
- Определяет и показывает пакеты, доступные для установки
- Проверяет предварительные требования и взаимозависимости

IBM Installation Manager включает в себя шесть мастеров, помогающих обслуживать пакеты:

- Мастер **Установить** помогает выполнить этапы процесса установки. За один раз можно установить один или несколько пакетов. Можно оставить значения по умолчанию или изменить параметры, чтобы создать настраиваемую установку, где это возможно. Перед установкой выводится полный обзор выбранных в мастере параметров.
- Мастер **Обновить** выполняет поиск доступных обновлений для пакетов, установленных в системе. Сведения о содержании обновления отображаются в мастере. Предоставляется выбор: нужно ли установить обновление.
- Мастер **Изменить** помогает изменить определенные элементы пакета, который уже установлен. Во время первой установки пакета можно выбрать компоненты, которые требуется установить. Если в дальнейшем потребуются другие компоненты, можно воспользоваться мастером изменения пакетов и добавить компоненты в свой пакет. Также можно удалять компоненты.
- Мастер **Управление лицензиями** помогает настроить лицензии для пакетов. С помощью этого мастера можно изменить пробную лицензию на полноценную лицензию, настроить на сервера нефиксированные лицензии и выбрать для каждого пакета тип лицензии для использования.
- Мастер **Откат** помогает восстановить прежнюю версию пакета.
- Мастер **Удалить из системы** удаляет пакет из системы. За один раз можно удалить несколько пакетов.

Поддерживаемые операционные системы

Можно использовать IBM Installation Manager для установки IBM Security Directory Server в системах AIX (ppc64), Linux (архитектура AMD64/EM64T) и Microsoft Windows.

Следующие разделы перечисляют версии операционных систем, поддерживаемых для установки IBM Security Directory Server с помощью IBM Installation Manager.

Если вы хотите установить IBM Security Directory Server в операционной системе, которая не указана в следующих разделах:

1. Проверьте, поддерживается ли версия операционной системы для IBM Security Directory Server. Список всех поддерживаемых операционных систем приведен в *Обзоре продукта IBM Security Directory Server*.
2. Если она поддерживается, можно использовать утилиты командной строки операционной системы для установки IBM Security Directory Server.

AIX (ppc64)

- AIX версии 6.1
- AIX версии 7.1

Linux (AMD64/EM64T)

- Red Hat Enterprise Linux 5, Advanced Platform
- Red Hat Enterprise Linux 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11

Microsoft Windows (x64)

- Microsoft Windows Server 2008 R2, Enterprise Edition
- Microsoft Windows Server 2008 R2, Standard Edition
- Microsoft Windows Server 2008, Enterprise Edition
- Microsoft Windows Server 2008, Standard Edition
- Microsoft Windows Server 2012, Standard Edition

Типы пакетов установки IBM Security Directory Server

Для того чтобы выбрать правильный пакет установки IBM Security Directory Server, необходимо знать доступные типы пакетов установки.

Следующие типы пакетов установки IBM Security Directory Server доступны для установки с помощью IBM Installation Manager:

Таблица 8. Тип пакета установки IBM Security Directory Server и доступные компоненты для установки

Все компоненты	Компоненты в программе установки полного продукта	Компоненты в программе установки только клиента
IBM DB2	Да	Нет
IBM Global Security Kit	Да	Да
C Client	Да	Да
IBM Java Development Kit	Да	Да
Java Client	Да	Да
Сервер	Да	Нет
Proxy Server	Да	Нет
Веб-инструмент администрирования	Да	Нет

Примечание: Если Web Administration Tool выбран для установки, IBM Installation Manager предоставляет опцию установки встроенного WebSphere Application Server.

Рекомендации по установке

Перед началом установки IBM Security Directory Server с помощью IBM Installation Manager необходимо учесть некоторые ограничения.

Метод установки

При установке IBM Security Directory Server можно выбрать установку с помощью IBM Installation Manager или с помощью утилит командной строки операционной системы. В дальнейшем установку или удаление пакетов, комплектов и пакетов исправлений IBM Security Directory Server необходимо будет выполнять в системе тем же методом установки. Например, если IBM Security Directory Server был установлен с помощью IBM Installation Manager, нельзя использовать утилиты командной строки для установки комплектов или удаления продукта из системы. При такой попытке установка IBM Security Directory Server может выполняться неправильно или с продуктом будет невозможно работать.

Версия IBM Installation Manager

IBM Installation Manager версии 1.7.0 и выше поддерживаются для установки IBM Security Directory Server. В следующих сценариях на странице Установка пакетов программы IBM Installation Manager отображается ошибка, не позволяющая продолжить установку:

- Предпринята попытка начать установку IBM Security Directory Server с помощью предыдущей версии IBM Installation Manager.
- Выявлена предыдущая версия IBM Installation Manager при запуске установки IBM Security Directory Server из программы Панель запуска.

Установка нескольких экземпляров

Нельзя устанавливать несколько копий одной и той же версии IBM Security Directory Server в одной и той же системе. При повторном выборе пакета установки для той же версии программа IBM Installation Manager выдаст предупреждение, не позволяющее продолжить установку. Однако в одной системе могут сосуществовать разные версии IBM Security Directory Server.

Установочное расположение в системах AIX и Linux:

IBM Security Directory Server можно установить в системах AIX и Linux только в стандартном расположении. Путь указан по умолчанию в поле **Установочный каталог** в IBM Installation Manager. Это поле в IBM Installation Manager допускает изменение, но если изменить путь, указанный по умолчанию, перестанет быть доступной кнопка **Далее** и нельзя будет продолжить установку. Потребуется восстановить путь к установке по умолчанию для IBM Security Directory Server.

Это ограничение не распространяется на операционные системы Microsoft Windows. IBM Security Directory Server можно установить в операционных системах Microsoft Windows в любом удобном расположении. Даже при выборе пользовательского установочного расположения для IBM Security Directory Server каталог `idsinstinfo` и находящийся в нем файл `idsinstances.ldif` всегда создаются в разделе, указанном в `%SystemDrive%`. Если IBM Security Directory Server установлен на диске E:, а операционная система на диске C:, то наблюдаются следующие изменения:

- Каталог `idsinstinfo` создается на диске C: (`C:\idsinstinfo`), а не в каталоге `E:\Program Files\IBM\ldap`.

Дополнительная информация об установочных расположениях по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.

Компоненты IBM Security Directory Server

При установке IBM Security Directory Server с помощью IBM Installation Manager можно выбрать компоненты, которые требуется установить. IBM Installation Manager показывает зависимости каждого выбранного компонента.

Для установки доступны следующие компоненты IBM Security Directory Server:

IBM DB2

Можно установить IBM DB2 как компонент. Если установлена поддерживаемая версия IBM DB2, не требуется устанавливать DB2, поставляемую с пакетом IBM Security Directory Server. Информация о поддерживаемых версиях DB2 для различных операционных систем приведена в разделе *IBM Security Directory Server - Обзор продукта*.

Продукт IBM DB2 необходим для хранения данных полного сервера каталогов в базе данных DB2. IBM DB2 не требуется для прокси-сервера.

IBM Global Security Kit

Можно установить IBM Global Security Kit (GSKit) как компонент вместе с другими компонентами IBM Security Directory Server. GSKit является необязательным компонентом, который требуется только в том случае, если будет применяться протокол связи Secure Sockets Layer (SSL) или Transport Layer Security (TLS). Для того чтобы можно было устанавливать и использовать защищенные соединения, GSKit необходимо установить как на сервере, так и в системе клиента.

C Client

Можно установить C Client как компонент отдельно или вместе с другими компонентами IBM Security Directory Server. Компонент C Client не зависит от других компонентов. Но компоненты сервер и прокси-сервер зависят от C Client. При установке компонента сервер или прокси-сервер компонент C Client автоматически выбирается для установки.

C Client - это клиентская часть Software Development Kit (SDK), предоставляющая инструменты, необходимые для разработки приложений LDAP на языке C. Пакет C Client содержит следующие файлы и приложения:

- Библиотеки клиента, предоставляющие набор интерфейсов прикладных программ (API) на языке C
- Заголовочные файлы C для компиляции и компоновки приложений LDAP
- Утилиты сервера и клиента C
- Примеры исходного кода программ

IBM Java Development Kit

Можно установить IBM Java Development Kit как компонент отдельно или вместе с другими компонентами IBM Security Directory Server. Если выбрана установка IBM Java Development Kit, IBM Installation Manager извлекает файлы данных со сжатием в каталог java установочного расположения IBM Security Directory Server. IBM Java Development Kit предоставляет IBM Java SDK и Java 1.6 SR 14. IBM Java Development Kit необходим для компилирования примеров программ на Java и для запуска программ на Java, таких как Инструмент администрирования экземпляра (**idsxinst**) и Инструмент настройки (**idsxcfg**).

Java Client

Можно установить Java Client как компонент отдельно или вместе с другими компонентами IBM Security Directory Server. Компонент Java Client не зависит от других компонентов. Но компоненты сервер и прокси-сервер зависят от

Java Client. При установке компонента сервер или прокси-сервер компонент Java Client автоматически выбирается для установки.

Java Client включает в себя IBM Security Directory Server JNDI toolkit и утилиты клиента Java.

Сервер Можно установить Server как компонент вместе с другими компонентами IBM Security Directory Server. Компонент Server зависит от компонентов C Client и Java Client. Если для установки выбран компонент Server, то для установки будут выбраны компоненты C Client и Java Client.

Server является обязательным компонентом для создания полноценного сервера каталогов или сервера LDAP. Полноценный сервер каталогов необходимо настроить с экземпляром базы данных. Он обрабатывает запросы клиентов на доступ к записям, хранящимся в базе данных. Полный сервер каталогов работает совместно с DB2.

Proxy Server

Можно установить Proxy Server как компонент вместе с другими компонентами IBM Security Directory Server. Компонент Proxy Server зависит от компонентов C Client и Java Client. Если для установки выбран компонент Proxy Server, то для установки будут выбраны компоненты C Client и Java Client.

Прокси-сервер - это сервер LDAP, действующий по отношению к каталогу как промежуточный сервер. Он выполняет идентификацию запросов клиента на уровне каталога и перенаправляет запросы полным серверам каталогов. Прокси-сервер может также использоваться как промежуточный сервер кластера или распределенного каталога для обеспечения автоматического переноса ресурсов или распределения нагрузки.

Веб-инструмент администрирования

Можно установить Веб-инструмент администрирования как компонент отдельно или вместе с другими компонентами IBM Security Directory Server. Веб-инструмент администрирования является необязательным компонентом, который необходим только в том случае, если требуется удаленное управление сервером каталогов. Для работы с веб-инструментом администрирования необходимо развернуть его в поддерживаемой версии встроенного WebSphere Application Server или WebSphere Application Server.

При установке веб-инструмента администрирования файлы DSML (язык описания служб каталогов) также копируются на компьютер. Дополнительная информация о DSML приведена в разделе Приложение А, “Язык описания служб каталогов”, на стр. 247.

Можно использовать Веб-инструмент администрирования как консоль для управления серверами каталогов, которые могут быть следующих типов:

- IBM Security Directory Server версии 6.3.1
- IBM Security Directory Server версии 6.3
- IBM Security Directory Server версии 6.2
- IBM Security Directory Server версии 6.1
- IBM Security Directory Server версии 6.0
- i5/OS V5 R4
- z/OS V1 R6 Integrated Security Services
- z/OS V1 R8 Integrated Security Services
- z/OS V1 R8 IBM Tivoli Directory Server
- z/OS V1 R9 IBM Tivoli Directory Server

- z/OS V1 R10 IBM Tivoli Directory Server

Важное замечание: В z/OS поддерживается управление данными каталога; администрирование сервера недоступно.

Embedded WebSphere Application Server

Можно установить встроенный WebSphere Application Server, если выбрана установка веб-инструмента администрирования. Встроенный WebSphere Application Server необходим только в том случае, если предполагается развертывание и запуск веб-инструмента администрирования. Если в системе установлена поддерживаемая версия WebSphere Application Server, можно отказаться от установки встроенного WebSphere Application Server. Можно развернуть Веб-инструмент администрирования на существующем WebSphere Application Server или на встроенном WebSphere Application Server, который установлен в системе.

Настройка установки IBM Security Directory Server

Можно настроить установку IBM Security Directory Server для удобства использования продукта.

Можно разбить по следующим категориям назначений установку IBM Security Directory Server:

- Полный продукт
- Полный сервер каталогов
- Прокси-сервер
- Клиент
- Удаленное управление сервером с помощью Web Administration Tool

Таблица 9. Устанавливаемые компоненты IBM Security Directory Server основаны на использовании продукта

Все компоненты	Полный сервер каталогов	Прокси-сервер	Клиент	Удаленное управление сервером с помощью Web Administration Tool
IBM DB2	Да	Нет	Нет	Нет
IBM Global Security Kit	Да	Да	Да	Нет
C Client	Да	Да	Да	Нет
IBM Java Development Kit	Да	Да	Да	Нет
Java Client	Да	Да	Да	Нет
Сервер	Да	Нет	Нет	Нет
Proxy Server	Нет	Да	Нет	Нет
Веб-инструмент администрирования	Необязательный	Необязательный	Нет	Да

Примечание: Если Web Administration Tool выбран для установки, IBM Installation Manager предоставляет опцию установки встроенного WebSphere Application Server.

Можно выбрать встроенный WebSphere Application Server и Web Administration Tool для установки с Полным сервером каталогов и Прокси-сервером.

Установочные расположения по умолчанию

Если для установки запущен IBM Installation Manager, то IBM Security Directory Server и сопутствующее программное обеспечение устанавливается в стандартное установочное расположение.

Таблица 10. Установочное расположение по умолчанию для IBM Security Directory Server, IBM DB2, встроенного WebSphere Application Server и IBM Java Development Kit.

Операционная система	IBM Security Directory Server	IBM DB2	Встроенный WebSphere Application Server	IBM Java Development Kit
Linux	/opt/ibm/ldap/V6.3.1	/opt/ibm/sdsV6.3.1db2	/opt/ibm/ldap/V6.3.1/appsrv	/opt/ibm/ldap/V6.3.1/java
AIX	/opt/IBM/ldap/V6.3.1	/opt/IBM/sdsV6.3.1db2	/opt/IBM/ldap/V6.3.1/appsrv	/opt/IBM/ldap/V6.3.1/java
Microsoft Windows	C:\Program Files\IBM\ldap\V6.3.1	C:\Program Files\IBM\sdsV6.3.1db2	C:\Program Files\IBM\ldap\V6.3.1\appsrv	C:\Program Files\IBM\ldap\V6.3.1\java

IBM Security Directory Server можно установить в системах AIX и Linux только в стандартном расположении. Путь указан по умолчанию в поле **Установочный каталог** в IBM Installation Manager. Это поле в IBM Installation Manager допускает изменение, но если изменить путь, указанный по умолчанию, перестанет быть доступной кнопка **Далее** и нельзя будет продолжить установку. Потребуется восстановить путь к установке по умолчанию для IBM Security Directory Server.

Это ограничение не распространяется на операционные системы Microsoft Windows. IBM Security Directory Server можно установить в операционных системах Microsoft Windows в любом удобном расположении. Даже при выборе пользовательского установочного расположения для IBM Security Directory Server каталог `idsinstinfo` и находящийся в нем файл `idsinstances.ldif` всегда создаются в разделе, указанном в `%SystemDrive%`. Если IBM Security Directory Server установлен на диске E:, а операционная система на диске C:, то наблюдаются следующие изменения:

- Каталог `idsinstinfo` создается на диске C: (C:\idsinstinfo), а не в каталоге E:\IBM\ldap.

Установочные хранилища

Установочное хранилище - это расположение, в котором находятся пакеты IBM Security Directory Server, доступные для установки.

Можно установить IBM Security Directory Server из одного из следующих расположений:

- Диск установки продукта
- Удаленный общий диск или локальный каталог с электронным образом установочного пакета

С помощью хранилища можно начать установку следующими способами:

- Использовать Панель запуска для запуска установки из следующих расположений:

- Диск установки продукта
- Электронный образ пакета установки на удаленном общем диске или в локальном каталоге

В случае использования панели запуска процесс установки уже настроен с расположением хранилища, содержащего установочный пакет.

- Запустить IBM Installation Manager непосредственно и указать параметры хранилища вручную. Например:
 - URL хранилища на веб-сервере
 - Путь к удаленному общему диску, содержащему пакет продукта

Запуск установки

Вы можете запустить установку IBM Security Directory Server либо с помощью панели запуска, либо с помощью IBM Installation Manager с заданными параметрами хранилища.

Запуск установки из панели запуска

Панель запуска предоставляет единую точку для запуска процесса установки.

Об этой задаче

Из панели запуска вы можете запустить установку в следующих сценариях:

- Установка с установочного диска продукта.
- Установка из локального каталога или с удаленного общего диска, содержащего электронный образ пакета продукта.

Когда вы запускаете установку из панели запуска, IBM Installation Manager автоматически устанавливается, если в системе нет его поддерживаемой версии.

Процедура

1. Перейдите в корневой каталог установочного пакета.
 - Если вы применяете установочный диск продукта IBM Security Directory Server, вставьте диск в дисковод.
 - Если вы устанавливаете из электронного образа установочного пакета продукта, перейдите в каталог, в котором находится образ.
2. Откройте панель запуска.

Примечание: В операционной системе Windows щелкните правой кнопкой мыши на файле `.exe` для панели запуска и выберите **Выполнить от имени администратора**.

Операционная система	Выполняемая команда:
Windows, 32-разрядная версия	<code>!launchpad.exe</code>
Windows, 64-разрядная версия	<code>!launchpad64.exe</code>
AIX и Linux	<code>./!launchpad.sh</code>

Откроется панель запуска IBM Security Directory Server и появится страница Приветствие.

3. На странице **Приветствие** выберите язык в списке **Выбрать язык** и нажмите **ОК**.
4. В левой панели навигации выберите **Установка IBM Security Directory Server**.

5. На странице **Установка** щелкните на ссылке **Запустить программу установки IBM Security Directory Server**. Будет запущена программа IBM Installation Manager.
6. Убедитесь, что следующие пакеты выбраны для установки:
 - IBM Installation Manager (указывается, только если поддерживаемая версия еще не установлена в системе.)
 - IBM Security Directory Server
7. Продолжите установку IBM Security Directory Server. См. раздел “Установка с помощью IBM Installation Manager” на стр. 30.
8. По окончании установки нажмите **Выход**.

Результаты

Когда вы используете панель запуска для запуска установки IBM Security Directory Server, панель запуска создает временный файл, `sds631.tmp`, содержащий путь к носителю. Файл `sds631.tmp` создается в следующем каталоге операционной системы:

AIX и Linux
/tmp

Microsoft Windows

Временный каталог по умолчанию системы, указанной в переменной *TEMP*.

Нельзя устанавливать несколько копий одной и той же версии IBM Security Directory Server в одной и той же системе. При повторном выборе пакета установки для той же версии программа IBM Installation Manager выдаст предупреждение, не позволяющее продолжить установку. Однако в одной системе могут сосуществовать разные версии IBM Security Directory Server.

Дальнейшие действия

Продолжите установку IBM Security Directory Server. См. раздел “Установка с помощью IBM Installation Manager” на стр. 30.

Запуск установки путем задания параметров хранилища

Если в системе установлена поддерживаемая версия IBM Installation Manager, то вы можете запустить ее напрямую и указать параметры хранилища.

Прежде чем начать

IBM Installation Manager версии 1.7.0 и выше поддерживаются для установки IBM Security Directory Server. В следующих сценариях на странице Установка пакетов программы IBM Installation Manager отображается ошибка, не позволяющая продолжить установку:

- Предпринята попытка начать установку IBM Security Directory Server с помощью предыдущей версии IBM Installation Manager.
- Выявлена предыдущая версия IBM Installation Manager при запуске установки IBM Security Directory Server из программы Панель запуска.

Если система содержит IBM Installation Manager версии ниже 1.7.0, то вы должны обновить его до уровня 1.7.0 или выше. Установить требуемую версию IBM Installation Manager можно одним из следующих способов.

- Запустите установку IBM Installation Manager из панели запуска. Дополнительная информация приведена в разделе “Запуск установки из панели запуска” на стр. 28.

- Загрузите IBM Installation Manager версии 1.7.0 или выше для применяемой операционной системы. Дополнительная информация об установке IBM Installation Manager без вывода сообщений приведена в документации по IBM Installation Manager: <http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>.

Об этой задаче

Вы можете запустить установку, задав параметры хранилища в следующих сценариях установки:

- Установка из локального каталога или с удаленного общего диска, содержащего пакет продукта, загруженный из IBM Passport Advantage.
- Установка с URL хранилища на веб-сервере.

Процедура

1. Запустите IBM Installation Manager.

Windows

В меню **Пуск** выберите **Программы > IBM Installation Manager > IBM Installation Manager**.

AIX и Linux

Введите в командной строке следующую команду. Измените указанный стандартный путь, если IBM Installation Manager установлен в другом расположении.

```
/opt/IBM/InstallationManager/eclipse/IBMIM
```

2. На странице Запуск продукта IBM Installation Manager выберите **Файл > Параметры**.
3. На странице Хранилища выберите **Добавить хранилище**.
4. На странице Добавить хранилище введите URL расположения хранилища или выберите его в окне обзора и задайте путь к файлу.
5. Нажмите **ОК**. Если вы указали HTTPS или расположение хранилища с ограниченным доступом, то вам будет предложено ввести ИД пользователя и пароль. Будет указано новое или изменившееся расположение хранилища.
6. Для проверки доступа к хранилищу выберите **Проверить соединения**.
7. Нажмите **ОК**, чтобы завершить работу со страницей Хранилища.

Результаты

Нельзя устанавливать несколько копий одной и той же версии IBM Security Directory Server в одной и той же системе. При повторном выборе пакета установки для той же версии программа IBM Installation Manager выдаст предупреждение, не позволяющее продолжить установку. Однако в одной системе могут сосуществовать разные версии IBM Security Directory Server.

Дальнейшие действия

Продолжите установку IBM Security Directory Server. См. раздел “Установка с помощью IBM Installation Manager”.

Установка с помощью IBM Installation Manager

В этом разделе описываются действия по установке IBM Security Directory Server с помощью IBM Installation Manager.

Прежде чем начать

Запустите установку.

Процедура

1. На начальной странице IBM Installation Manager выберите **Установить**.
2. На странице Установить пакеты выберите пакет IBM Security Directory Server для установки.
3. Нажмите кнопку **Далее**. IBM Installation Manager проверит наличие предварительно необходимых пакетов на компьютере.
4. Если для компьютера не выполнены предварительные требования, они будут показаны на странице **Результаты проверки**.
 - a. Для того чтобы проверить, выполнены ли предварительные требования после установки предварительно необходимых пакетов, нажмите кнопку **Повторно проверить состояние**. Дополнительная информация о предварительных требованиях содержится в разделе “Предварительно требуемые пакеты в различных операционных системах” на стр. 15.
 - b. Если все предварительные требования выполнены, нажмите кнопку **Далее**.
5. Нажмите кнопку **Я согласен с условиями лицензионного соглашения**, затем кнопку **Далее**. Будет показано расположение каталога общих ресурсов.
6. Необязательно: Используйте каталог по умолчанию или укажите каталог в поле **Каталог общих ресурсов**. Каталог общих ресурсов - это каталог, в котором хранятся артефакты установки, доступные для использования одному или нескольким группам пакетов продукта. Каталог общих ресурсов можно указать только в том случае, если пакет устанавливается впервые.
7. Нажмите кнопку **Далее**. Будет показано имя группы пакетов и установочное расположение по умолчанию. По умолчанию выбрана опция **Создать группу пакетов**; это единственная опция, которая поддерживается для установки IBM Security Directory Server. Группа пакетов представляет каталог, в котором пакеты из одной и той же группы совместно используют ресурсы. Имя группе пакетов присваивается автоматически.

Ограничение:

IBM Security Directory Server можно установить в системах AIX и Linux только в стандартном расположении. Путь указан по умолчанию в поле **Установочный каталог** в IBM Installation Manager. Это поле в IBM Installation Manager допускает изменение, но если изменить путь, указанный по умолчанию, перестанет быть доступной кнопка **Далее** и нельзя будет продолжить установку. Потребуется восстановить путь к установке по умолчанию для IBM Security Directory Server.

Список установочных расположений по умолчанию в различных операционных системах приведен в разделе “Установочные расположения по умолчанию” на стр. 27.

Это ограничение не распространяется на операционные системы Microsoft Windows. IBM Security Directory Server можно установить в операционных системах Microsoft Windows в любом удобном расположении. Даже при выборе пользовательского установочного расположения для IBM Security Directory Server каталог `idsinstinfo` и находящийся в нем файл `idsinstances.ldif` всегда создаются в разделе, указанном в `%SystemDrive%`. Если IBM Security Directory Server установлен на диске E:, а операционная система на диске C:, то наблюдаются следующие изменения:

- Каталог `idsinstinfo` создается на диске `C:` (`C:\idsinstinfo`), а не в каталоге `E:\Program Files\IBM\ldap`.
8. Нажмите кнопку **Далее**.
 9. На странице **Установить пакеты** выберите требуемые компоненты. Для просмотра объектов, связанных с выбранным компонентом, или взаимосвязей компонента с другими компонентами включите переключатель **Показать взаимосвязи**.

Таблица 11. Компоненты IBM Security Directory Server, доступные для установки в полном пакете продукта или в клиентском пакете

Все компоненты	Зависимости установки	Компоненты в полном пакете продукта	Компоненты в клиентском пакете
IBM DB2	Нет	Да	Нет
IBM Global Security Kit	Нет	Да	Да
C Client	Нет	Да	Да
IBM Java Development Kit	Нет	Да	Да
Java Client	Нет	Да	Да
Сервер	C Client Java Client	Да	Нет
Proxy Server	C Client Java Client	Да	Нет
Веб-инструмент администрирования	Нет	Да	Нет

10. Нажмите кнопку **Далее**.
11. Если для установки выбирается компонент IBM DB2, щелкните на **IBM DB2**, а затем выполните одно из следующих действий:
 - Для установки IBM DB2 выполните следующие действия:
 - a. Выберите **Установить DB2**.
 - b. В поле **Каталог устанавливаемого компонента DB2** укажите каталог устанавливаемого компонента DB2. Для выбора каталога нажмите кнопку **Обзор**.
 - c. В системе Windows в поле **Имя пользователя** введите ИД пользователя системы, который должен входить в состав группы DB2ADMNS или DB2USERS. Этот ИД пользователя можно использовать для запуска локальных приложений и инструментов DB2 на компьютере. Если этот ИД пользователя не существует, программа установки создаст соответствующую учетную запись.
 - d. В системе Windows введите пароль пользователя с указанным ИД в поле **Пароль**. Если пароль не удовлетворяет настроенной на компьютере стратегии управления паролями, то установка может завершиться неудачно.
 - e. В системе Windows введите пароль пользователя с указанным ИД в поле **Подтверждение пароля**.
 - f. Нажмите кнопку **Далее**.
 - Если на компьютере установлена поддерживаемая версия IBM DB2, выполните одно из следующих действий:
 - a. Для продолжения установки при наличии существующей версии IBM DB2 выберите опцию **Продолжить при существующей DB2**.

Важное замечание: Если выбрано продолжение установки при наличии существующей базы данных DB2, IBM Installation Manager обновит свой реестр с записью компонента DB2.

- b. Выберите в списке поддерживаемую версию DB2, которая должна использоваться с IBM Security Directory Server.
 - c. Нажмите кнопку **Далее**.
12. Если для установки выбирается компонент IBM Global Security Kit, щелкните на **IBM Global Security Kit**, а затем выполните одно из следующих действий:
- Если на компьютере не установлен GSKit версии 8.0 или выше, выполните следующие действия:
 - a. Выберите **Установить GSKit**.
 - b. В поле **Каталог устанавливаемого компонента GSKit** укажите каталог устанавливаемого компонента GSKit. Для выбора каталога нажмите кнопку **Обзор**.

Примечание: В указанном каталоге должна содержаться как 64-разрядная, так и 32-разрядная версия устанавливаемого компонента GSKit.

- c. Нажмите кнопку **Далее**.
- Если на компьютере установлен GSKit версии 8.0 или выше, выполните одно из следующих действий:
 - a. Для продолжения установки при наличии существующей версии GSKit выберите опцию **Продолжить при существующей версии GSKit**.

Важное замечание: Если выбрано продолжение установки при наличии существующей версии GSKit, IBM Installation Manager обновит свой реестр с записью компонента GSKit.

- b. Нажмите кнопку **Далее**.
13. Если для установки выбирается компонент IBM Java Development Kit, щелкните на **IBM Java Development Kit** и выполните следующие действия:
- a. В поле **IBM Java Development Kit** укажите полное имя сжатого файла JDK. Для выбора каталога нажмите кнопку **Обзор**.
 - b. Нажмите кнопку **Далее**.
14. Если для установки выбирается компонент Веб-инструмент администрирования, щелкните на элементе **Веб-инструмент администрирования** и выполните следующие действия:
- a. Для установки встроенного WebSphere Application Server выполните следующие действия:
 - 1) Выберите **Установить встроенный WebSphere Application Server**.
 - 2) В поле **Каталог устанавливаемого встроенного WebSphere Application Server** укажите каталог устанавливаемого встроенного WebSphere Application Server. Для выбора каталога нажмите кнопку **Обзор**.
 - b. Для развертывания Веб-инструмента администрирования выполните одно из следующих действий:
 - Для развертывания во встроенном WebSphere Application Server, расположенном в установочном каталоге по умолчанию, выберите опцию **Развернуть во встроенном WebSphere Application Server по умолчанию**.

Примечание: Если существует предыдущая версия Веб-инструмента администрирования, то при выполнении перечисленных ниже условий программа установки выполнит миграцию к текущей версии:

- 1) Предыдущая версия Веб-инструмента администрирования и встроенный WebSphere Application Server установлены в установочном каталоге по умолчанию.
 - 2) Предыдущая версия Веб-инструмента администрирования развернута во встроенном WebSphere Application Server, расположенном в установочном каталоге по умолчанию.
 - 3) Миграция поддерживается для Веб-инструмента администрирования, поставляемого с IBM Security Directory Server версии 6.1, 6.2 и 6.3.
- Для развертывания в WebSphere Application Server или во встроенном WebSphere Application Server, расположенном в пользовательском установочном каталоге, выберите опцию **Развернуть в существующем WebSphere Application Server**.
 - 1) В поле **Установочный каталог WebSphere Application Server или встроенного WebSphere Application Server** укажите установочный каталог существующего сервера веб-приложений.
 - Для того чтобы развернуть Веб-инструмент администрирования позже на поддерживаемом сервере веб-приложений, выберите **Развернуть вручную позже**.
15. Нажмите кнопку **Далее**. Будет показана сводная информация для предварительного этапа установки, содержащая установочное расположение, список пакетов и сведения о хранилище.
 16. Проверьте обзорную информацию и нажмите кнопку **Установить**. Начнется установка и появится индикатор состояния. После установки будет открыта страница обзора заключительного этапа установки.
 17. Щелкните на ссылке **Просмотреть файл протокола**, чтобы проверить, успешно ли выполнена установка. Дополнительная информация приведена в разделе Глава 5, “Протоколы IBM Installation Manager”, на стр. 45.
 18. Для запуска одной из следующих программ выполните одно из следующих действий:
 - Для запуска Инструмента администрирования экземпляра выберите **Инструмент администрирования экземпляра (idsxinst)**.
 - Если никакие программы запускать не требуется, выберите **Нет**.
 19. Нажмите кнопку **Готово**.
 20. Выберите **Файл > Выход**.

Результаты

В случае успешной установки, IBM Security Directory Server будет установлен в установочном каталоге. Информация об установочном каталоге по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27. В случае неудачной установки любого из выбранных компонентов, установка пакетов IBM Security Directory Server будет аннулирована.

Дальнейшие действия

После установки IBM Security Directory Server необходимо выполнить следующие действия:

- Для того чтобы использовать IBM Security Directory Server в качестве полного сервера каталогов, создайте экземпляр сервера каталогов. Дополнительная информация приведена в разделе “Создание экземпляра сервера каталогов по умолчанию” на стр. 134.

- Для того чтобы использовать IBM Security Directory Server в качестве сервера прокси, создайте экземпляр сервера прокси. Дополнительная информация приведена в разделе “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.

Неинтерактивный режим установки

Можно использовать неинтерактивный режим для установки IBM Security Directory Server в нескольких системах без участия оператора.

Для установки в неинтерактивном режиме необходимо выполнить следующие действия:

1. Установить IBM Installation Manager, если он не установлен.
2. Использовать файл ответов по умолчанию или записать пользовательский файл ответов.
3. Установить пакеты.

Файл ответов для неинтерактивной установки

При установке в неинтерактивном режиме пользовательский интерфейс не доступен. Входом для установки служит файл ответов. Файл ответов — это файл XML, который содержит данные, требуемые для выполнения неинтерактивной установки.

Запись пользовательского файла ответов

Можно записать файл ответов для следующих задач:

- Установка пакетов
- Изменение пакетов
- Удаление пакетов из системы

Для того чтобы записать файл ответов, необходимо записать параметры и действия установки с помощью IBM Installation Manager в пользовательском интерфейсе. При первой записи файла ответов для неинтерактивной установки можно выбрать не устанавливать пакеты с помощью опции **-skipInstall** параметра *agentDataLocation*.

Расположение *agentDataLocation* хранит данные для установки продукта. Для того чтобы записать файл ответов для неинтерактивного изменения или удаления из системы продукта, необходимо использовать то же расположение *agentDataLocation* с параметром **-skipInstall**.

Для нескольких сценариев установок необходимо записать различные файлы ответов с различными расположениями *agentDataLocation* для каждого из сценариев.

Дополнительная информация о записи файла ответов для установки без вывода сообщений приведена в документации по IBM Installation Manager: <http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>.

Проверка неинтерактивной установки

После завершения установки необходимо ее проверить. установку можно проверить одним из следующих способов:

- Анализ кода возврата
- Просмотр файла протокола
- Проверка пакетов

Установка без вывода сообщений с помощью файла ответов

Установка без вывода сообщений IBM Security Directory Server позволяет установить необходимые пакеты без вмешательства вручную.

Прежде чем начать

IBM Installation Manager версии 1.7.0 или выше необходим для установки пакетов IBM Security Directory Server без вывода сообщений.

Об этой задаче

Вы можете воспользоваться файлом ответов по умолчанию или записать свой файл ответов и использовать его в качестве входного файла для установки без вывода сообщений.

Процедура

1. Войдите в систему как администратор.
2. Откройте команду **IBMIM** в установочном каталоге IBM Installation Manager.

Операционная система	Каталог по умолчанию команды IBMIM :
Microsoft Windows	C:\Program Files\IBM\InstallationManager\eclipse
AIX и Linux	/opt/IBM/InstallationManager/eclipse

3. Необязательно: Выполните команду **IBMIM** для записи файла ответов, предназначенного для процедуры установки.

Совет: Вы можете использовать пример файла ответов для процедуры установки. См. каталог по умолчанию примера файла ответов - “Неинтерактивный режим установки” на стр. 35.

- a. Для того чтобы записать процедуру установки, не устанавливая продукт, выполните одну из следующих команд, в зависимости от операционной системы:

Microsoft Windows

```
IBMIM.exe -record путь\responseFile.xml -skipInstall  
каталог_данных_агента
```

AIX и Linux

```
./IBMIM -record путь/responseFile.xml -skipInstall  
каталог_данных_агента
```

Команда откроет IBM Installation Manager.

- b. Задайте хранилище IBM Security Directory Server. Дополнительная информация приведена в разделе 2 на стр. 30.
 - c. Закончите запись процедуры установки IBM Security Directory Server. Дополнительная информация приведена в разделе “Установка с помощью IBM Installation Manager” на стр. 30.
4. Выполните команду **imc1**, чтобы запустить установку без вывода сообщений с использованием файла ответов в качестве входного. Команда **imc1** расположена в каталоге <каталог-IBM-Installation-Manager>/eclipse/tools.

Операционная система	Выполняемая команда:
Microsoft Windows	<code>imcl.exe input путь\responseFile.xml -acceptLicense -showProgress</code>
AIX и Linux	<code>./imcl input путь/responseFile.xml -acceptLicense -showProgress</code>

Примечание: В команде **imcl** можно указать много других параметров. За дополнительной информацией обратитесь к справке по команде **imcl**.

5. Просмотрите итоговый отчет об установке и файлы протокола.

Операционная система	Путь к протоколу по умолчанию:
Microsoft Windows	<code>C:\ProgramData\IBM\InstallationManager\ logs</code>
AIX и Linux	<code>/var/ibm/InstallationManager/logs/</code>

6. Убедитесь, что пакеты IBM Security Directory Server установлены на требуемом уровне.

Операционная система	Проверка пакетов:
Microsoft Windows	См. раздел “Проверка компонентов IBM Security Directory Server с помощью IBM Installation Manager” на стр. 85.
AIX и Linux	См. раздел “Проверка компонентов IBM Security Directory Server с помощью IBM Installation Manager” на стр. 85.

Результаты

В случае успешной установки, IBM Security Directory Server будет установлен в каталоге IBM Security Directory Server. Информация об установочном каталоге по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27. В случае неудачной установки любого из выбранных компонентов, установка пакетов IBM Security Directory Server будет аннулирована.

Дальнейшие действия

Примечание: Если вы выбрали открытие Инструмента администрирования экземпляра во время записи файла ответов для процедуры установки, то Инструмент администрирования экземпляра не откроется после окончания установки IBM Security Directory Server без вывода сообщений.

Если вы выбрали установку компонента Сервер или Сервер проху, то откройте Инструмент администрирования экземпляра, чтобы создать экземпляр сервера каталогов или экземпляр сервера проху. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.

Глава 4. Изменение с помощью IBM Installation Manager

Можно установить компоненты IBM Security Directory Server, которые не были установлены ранее, и/или удалить из системы уже установленные компоненты с помощью IBM Installation Manager.

Невозможно удалить компонент, если он требуется для других установленных компонентов. Можно удалить зависимость, только если все зависимые компоненты выбраны для удаления или удалены.

Важное замечание: Если вы хотите продолжить работу с существующей версией DB2 или GSKit в процессе установки, IBM Installation Manager обновляет свой реестр с помощью записи компонента. При удалении компонента, который был установлен с помощью опции **Продолжить работу с существующей версией**, Installation Manager выполняет следующие действия:

- Удаляет запись компонента из реестра IBM Installation Manager.
- Не удаляет компонент из системы.

Изменение компонентов с помощью IBM Installation Manager

В этом разделе объясняется, как изменить компоненты IBM Security Directory Server с помощью IBM Installation Manager.

Прежде чем начать

Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Пользовательские приложения LDAP

При наличии активных процессов удалить программы и библиотеки нельзя.

Процедура

1. Запустите IBM Installation Manager.
 - AIX и Linux:
 - a. Откройте окно командной строки и перейдите в каталог, содержащий IBM Installation Manager. Следующий каталог служит установочным каталогом по умолчанию IBM Installation Manager:
`opt/IBM/InstallationManager/eclipse`
 - b. Введите следующую команду:
`./IBMIM`
 - Microsoft Windows:
 - a. Выберите **Пуск > Все программы > IBM Installation Manager > IBM Installation Manager**.
2. Нажмите кнопку **Изменить**.
3. Выберите **IBM Security Directory Server** и нажмите кнопку **Далее**.
4. На странице **Изменить пакеты** необходимо выполнить следующие действия:

- a. Выберите компоненты, которые требуется установить.
- b. Отмените выбор компонентов, которые требуется удалить из системы.

Таблица 12. Компоненты IBM Security Directory Server, доступные для изменения в полном или клиентском пакете

Все компоненты	Зависимости установки	Компоненты в полном пакете продукта	Компоненты в клиентском пакете
IBM DB2	Нет	Да	Нет
IBM Global Security Kit	Нет	Да	Да
C Client	Нет	Да	Да
IBM Java Development Kit	Нет	Да	Да
Java Client	Нет	Да	Да
Сервер	C Client Java Client	Да	Нет
Proxy Server	C Client Java Client	Да	Нет
Веб-инструмент администрирования	Нет	Да	Нет

Важное замечание: Если вы хотите продолжить работу с существующей версией DB2 или GSKit в процессе установки, IBM Installation Manager обновляет свой реестр с помощью записи компонента. При удалении компонента, который был установлен с помощью опции **Продолжить работу с существующей версией**, Installation Manager выполняет следующие действия:

- Удаляет запись компонента из реестра IBM Installation Manager.
- Не удаляет компонент из системы.

Если существуют экземпляры DB2, созданные на основе копии DB2, установленной с помощью IBM Installation Manager, то IBM DB2 удалить нельзя. В этом случае необходимо вручную удалить экземпляры DB2 и повторить операцию. Перед удалением экземпляров DB2 рекомендуется создать резервную копию базы данных.

- c. Нажмите кнопку **Далее**.
5. Если для установки выбирается компонент IBM DB2, щелкните на **IBM DB2**, а затем выполните одно из следующих действий:
 - Для установки IBM DB2 выполните следующие действия:
 - a. Выберите **Установить DB2**.
 - b. В поле **Каталог устанавливаемого компонента DB2** укажите каталог устанавливаемого компонента DB2. Для выбора каталога нажмите кнопку **Обзор**.
 - c. В системе Windows в поле **Имя пользователя** введите ИД пользователя системы, который должен входить в состав группы DB2ADMNS или DB2USERS. Этот ИД пользователя можно использовать для запуска локальных приложений и инструментов DB2 на компьютере. Если этот ИД пользователя не существует, программа установки создаст соответствующую учетную запись.

- d. В системе Windows введите пароль пользователя с указанным ИД в поле **Пароль**. Если пароль не удовлетворяет настроенной на компьютере стратегии управления паролями, то установка может завершиться неудачно.
 - e. В системе Windows введите пароль пользователя с указанным ИД в поле **Подтверждение пароля**.
 - f. Нажмите кнопку **Далее**.
- Если на компьютере установлена поддерживаемая версия IBM DB2, выполните следующие действия:
 - a. Для продолжения установки при наличии существующей версии IBM DB2 выберите опцию **Продолжить при существующей DB2**.

Важное замечание: Если выбрано продолжение установки при наличии существующей базы данных DB2, IBM Installation Manager обновит свой реестр с записью компонента DB2.
 - b. Выберите в списке поддерживаемую версию DB2, которая должна использоваться с IBM Security Directory Server.
 - c. Нажмите кнопку **Далее**.
6. Если для установки выбирается компонент IBM Global Security Kit, щелкните на **IBM Global Security Kit**, а затем выполните одно из следующих действий:
- Если на компьютере не установлен GSKit версии 8.0 или выше, выполните следующие действия:
 - a. Выберите **Установить GSKit**.
 - b. В поле **Каталог устанавливаемого компонента GSKit** укажите каталог устанавливаемого компонента GSKit. Для выбора каталога нажмите кнопку **Обзор**.

Примечание: В указанном каталоге должна содержаться как 64-разрядная, так и 32-разрядная версия устанавливаемого компонента GSKit.
 - c. Нажмите кнопку **Далее**.
 - Если на компьютере установлен GSKit версии 8.0 или выше, выполните следующие действия:
 - a. Для продолжения установки при наличии существующей версии GSKit выберите опцию **Продолжить при существующей версии GSKit**.

Важное замечание: Если выбрано продолжение установки при наличии существующей версии GSKit, IBM Installation Manager обновит свой реестр с записью компонента GSKit.
 - b. Нажмите кнопку **Далее**.
7. Если для установки выбирается компонент IBM Java Development Kit, щелкните на **IBM Java Development Kit** и выполните следующие действия:
- a. В поле **IBM Java Development Kit** укажите полное имя сжатого файла JDK. Для выбора каталога нажмите кнопку **Обзор**.
 - b. Нажмите кнопку **Далее**.
8. Если для установки выбирается компонент Веб-инструмент администрирования, щелкните на элементе **Веб-инструмент администрирования** и выполните следующие действия:
- a. Для установки встроенного WebSphere Application Server выполните следующие действия:
 - 1) Выберите **Установить встроенный WebSphere Application Server**.

- 2) В поле **Каталог устанавливаемого встроенного WebSphere Application Server** укажите каталог устанавливаемого встроенного WebSphere Application Server. Для выбора каталога нажмите кнопку **Обзор**.
- б. Для развертывания Веб-инструмента администрирования выполните одно из следующих действий:
 - Для развертывания во встроенном WebSphere Application Server, расположенном в установочном каталоге по умолчанию, выберите опцию **Развернуть во встроенном WebSphere Application Server по умолчанию**.

Примечание: Если существует предыдущая версия Веб-инструмента администрирования, то при выполнении перечисленных ниже условий программа установки выполнит миграцию к текущей версии:

- 1) Предыдущая версия Веб-инструмента администрирования и встроенный WebSphere Application Server установлены в установочном каталоге по умолчанию.
 - 2) Предыдущая версия Веб-инструмента администрирования развернута во встроенном WebSphere Application Server, расположенном в установочном каталоге по умолчанию.
 - 3) Миграция поддерживается для Веб-инструмента администрирования, поставляемого с IBM Security Directory Server версии 6.1, 6.2 и 6.3.
- Для развертывания в WebSphere Application Server или во встроенном WebSphere Application Server, расположенном в пользовательском установочном каталоге, выберите опцию **Развернуть в существующем WebSphere Application Server**.
 - 1) В поле **Установочный каталог WebSphere Application Server или встроенного WebSphere Application Server** укажите установочный каталог существующего сервера веб-приложений.
 - Для того чтобы развернуть Веб-инструмент администрирования позже на поддерживаемом сервере веб-приложений, выберите **Развернуть вручную позже**.
9. Нажмите кнопку **Далее**.

Важное замечание: Если вы хотите продолжить работу с существующей версией DB2 или GSKit в процессе установки, IBM Installation Manager обновляет свой реестр с помощью записи компонента. При удалении компонента, который был установлен с помощью опции **Продолжить работу с существующей версией**, Installation Manager выполняет следующие действия:

- Удаляет запись компонента из реестра IBM Installation Manager.
 - Не удаляет компонент из системы.
10. Проверьте сводную информацию и нажмите кнопку **Изменить**.
 11. Необязательно: Если во время изменения произошли ошибки, выберите **Просмотреть файл протокола**, чтобы просмотреть подробные сведения. Дополнительная информация приведена в разделе Глава 5, “Протоколы IBM Installation Manager”, на стр. 45.
 12. Нажмите кнопку **Готово**.
 13. Выберите **Файл > Выход**.

Результаты

Если изменение выполнено успешно, вы увидите следующие изменения:

- Компоненты IBM Security Directory Server, выбранные для добавления, будут установлены в установочном расположении. Информация об установочном расположении по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.
- Компоненты IBM Security Directory Server, выбранные для удаления, будут удалены из системы.

Глава 5. Протоколы IBM Installation Manager

Для проверки установки, изменения или удаления IBM Security Directory Server и его компонентов можно проверить протокол, создаваемый IBM Installation Manager.

Если при установке, изменении или удалении IBM Security Directory Server и его компонентов произойдет ошибка, необходимо проверить протоколы. IBM Installation Manager создает протоколы в расположении по умолчанию.

Таблица 13. Стандартное расположение протоколов IBM Installation Manager в различных операционных системах

Операционная система	Стандартное расположение протокола IBM Installation Manager
AIX и Linux	/var/ibm/InstallationManager/logs
Microsoft Windows	C:\ProgramData\IBM\InstallationManager\ logs

Расположения по умолчанию применимы ко всем поддерживаемым версиям AIX, Linux и Microsoft Windows.

Глава 6. Запрос пакетов IBM Security Directory Server

Для проверки пакетов IBM Security Directory Server можно запросить пакеты IBM Security Directory Server на поддерживаемых платформах.

Об этой задаче

После установки IBM Security Directory Server следует убедиться, что все пакеты имеют требуемый уровень. Эта задача помогает получить номер версии пакетов установленных IBM Security Directory Server.

Процедура

Войдите в систему, в которой установлены пакеты IBM Security Directory Server, и выполните следующие команды от имени пользователя root.

- Системы AIX: выполните команду **ls1pp**. Например:

```
ls1pp -l 'idsldap*'
```
- Системы Linux: выполните команду **rpm**. Пример:

```
rpm -qa | grep idsldap
```
- В системах Solaris:
 1. Для просмотра списка установленных пакетов, выполните команду **pkginfo**.
Пример:

```
pkginfo | grep IDS1
```
 2. Для запроса версии конкретного пакета IBM Security Directory Server выполните команду **pkgparam**. Пример:

```
pkgparam IDS1bc63 VERSION
```
- Системы HP-UX (Itanium): выполните команду **swlist**. Пример:

```
swlist | grep idsldap
```

Глава 7. Внутренняя установка и настройка с помощью сценариев

Для установки и настройки можно использовать сценарии IBM Security Directory Server.

Путеводитель по установке

Обзор установки IBM Security Directory Server в системах Linux x86, Linux i/pSeries, Linux s390, Solaris и HP-UX.

1. Убедитесь, что у вас есть все необходимое аппаратное и программное обеспечение. Дополнительная информация приведена в разделе *Системные требования* в главе Обзор продукта документации по IBM Security Directory Server.
2. Установите предварительно необходимое программное обеспечение, такое как DB2. Если оно еще не установлено, проверьте наличие необходимых прав доступа к установочному файлу DB2.
3. Если планируется использовать следующие функции, то необходимо установить дополнительное предварительно необходимое программное обеспечение. Если оно еще не установлено, проверьте наличие необходимых прав доступа к каталогу предварительно необходимого программного обеспечения.
 - Для применения Web Administration Tool требуется поддерживаемая версия встроенного сервера WebSphere Application Server или WebSphere Application Server. Кроме того, требуется поддерживаемая версия браузера.
 - Для применения шифрования Secure Socket Layer (SSL) или Transport Layer Security (TLS) требуется поддерживаемая версия IBM Global Security Kit (GSKit).
4. В системах Linux x86, Linux i/pSeries, Linux s390, Solaris и HP-UX для установки пакетов IBM Security Directory Server и другого требуемого программного обеспечения следует использовать программу установки **idsNativeInstall**.
5. После установки IBM Security Directory Server создайте и настройте экземпляр сервера каталогов с помощью команды **idsdefinst**.
6. Запустите экземпляр сервера каталогов.
7. Загрузите пример файла LDIF в базу данных. Дополнительная информация о работе с экземпляром сервера каталогов приведена в разделе Администрирование документации по IBM Security Directory Server.

Примечание: Сценарий установки **idsNativeInstall** недоступен для операционных систем Windows, AIX и Linux x86_64 (64-разрядная версия). В этих операционных системах для установки следует использовать IBM Installation Manager или утилиты командной строки.

Установка пакетов IBM Security Directory Server в системах Linux, Solaris и HP-UX

Приведены инструкции по установке или обновлению пакетов IBM Security Directory Server в системах Linux x86, Linux i/pSeries, Linux s390, Solaris и HP-UX.

Прежде чем начать

Перед тем как приступить к установке пакетов IBM Security Directory Server, выполните следующие действия:

1. Войдите в систему от имени пользователя root.
2. Извлеките содержимое файла архива IBM Security Directory Server версии 6.3.1 в подходящий каталог, например /sdsV6.3.1.
3. Остановите все процессы клиента или сервера IBM Security Directory Server, включая сервер каталогов, сервер администрирования и пользовательские приложения LDAP. Программы и библиотеки нельзя заменить, если они используются. Если включена трассировка, остановите процесс трассировки с помощью команды `ldtrc off`. Инструкции по завершению работы экземпляров сервера каталогов и серверов администрирования приведены в разделах "Основные задачи администрирования сервера" и "Сервер администрирования каталогов" в главе *Администрирование* документации по IBM Security Directory Server.

Об этой задаче

Для установки и обновления пакетов IBM Security Directory Server в системах Linux x86, Linux i/pSeries, Linux s390, Solaris и HP-UX можно использовать команду **idsNativeInstall**. Кроме того, с помощью команды **idsNativeInstall** можно установить DB2, GSKit и встроенный WebSphere Application Server, если они еще не установлены в системе.

Примечание:

- Сценарий установки **idsNativeInstall** недоступен для операционных систем Windows, AIX и Linux x86_64 (64-разрядная версия). В этих операционных системах для установки следует использовать IBM Installation Manager или утилиты командной строки.
- В системах HP-UX для установки и обновления доступны только пакеты клиента IBM Security Directory Server.

Процедура

1. Перейдите в каталог, в котором расположены программа установки **idsNativeInstall** и файл `responseFile.txt`. Кроме того, в этом каталоге должны быть расположены файлы `idsNativeInstall` и `responseFile.txt`.
2. Обновите файл `responseFile.txt` для следующей записей. По умолчанию значения переменных установки содержат значения `false` и соответствующие переменные путей не заданы.
 - Для установки DB2 укажите в переменной `db2FeatureInstall` значение `true`, а в переменной `db2InstallImagePath` - полный путь к каталогу установочного образа DB2. Например:

```
db2FeatureInstall=true
db2InstallImagePath=/sdsV6.3.1/db2
```
 - **Важное замечание:** Для полного сервера каталогов в системе должна быть установлена база данных DB2. Если заданы переменные DB2 (`db2FeatureInstall` и `db2InstallImagePath`), то база данных DB2 устанавливается в каталоге `/opt/ibm/sdsV6.3.1db2` (Linux) или `/opt/IBM/sdsV6.3.1db2` (Solaris). Если версия DB2 уже установлена в указанном расположении, то существующие файлы заменяются новыми.
 - Для установки GSKit укажите в переменной `gskitFeatureInstall` значение `true`, а в переменной `gskitInstallImagePath` - полный путь к каталогу установочного образа GSKit. Например:

```
gskitFeatureInstall=true
gskitInstallImagePath=/sdsV6.3.1/gskit
```

Важное замечание: Для настройки экземпляра сервера каталогов для поддержки SSL или TLS в системе должна быть установлена поддерживаемая версия GSKit.

- Для установки IBM Java Development Kit укажите в переменной *JDKFeatureInstall* значение true, а в переменной *JDKInstallImagePath* - полный путь к каталогу установочного образа IBM Java Development Kit. Например:
JDKFeatureInstall=true
JDKInstallImagePath=/sdsV6.3.1/java/ibm-java-16sr14-linux-i386.tar

IBM Java Development Kit устанавливается в каталоге /opt/ibm/ldap/V6.3.1/java (Linux и Solaris).

- Для установки встроенной версии WebSphere Application Server укажите в переменной *eWasFeatureInstall* значение true, а в переменной *eWasInstallImagePath* - полный путь к каталогу установочного образа WebSphere Application Server. Например:
eWasFeatureInstall=true
eWasInstallImagePath=/sdsV6.3.1/appsrv

Встроенная версия WebSphere Application Server устанавливается в каталоге /opt/ibm/ldap/V6.3/appsrv (Linux и Solaris).

- Для установки IBM Security Directory Server версии 6.3.1 GA укажите в переменной *tdsInstallImagePath* полный путь к каталогу установочного образа IBM Security Directory Server версии 6.3.1 GA. Пример:
tdsInstallImagePath=/sdsV6.3.1

Если в качестве расположения установочного образа IBM Security Directory Server версии 6.3.1 указан каталог /sdsV6.3.1, убедитесь, что он содержит следующие файлы.

```
idsinstall  
idsinstall_i  
ids_detectGskitVersion
```

Пакеты IBM Security Directory Server версии 6.3.1 должны быть доступны в каталоге /sdsV6.3.1/tdsfiles.

3. В командной строке введите команду **idsNativeInstall**.

Результаты

Команда **idsNativeInstall** устанавливает пакеты IBM Security Directory Server 6.3.1. Кроме того, команда **idsNativeInstall** устанавливает DB2, GSKit, IBM Java Development Kit и встроенную версию WebSphere Application Server с учетом значений файла ответов.

Примечание: Если IBM Security Directory Server версии 6.3.1 не установлен, то устанавливаются все компоненты IBM Security Directory Server версии 6.3.1. IBM Security Directory Server версии 6.3.1 устанавливается в каталоге /opt/ibm/lldap/V6.3.1/ (Linux, Solaris и HP-UX).

Дальнейшие действия

После установки IBM Security Directory Server убедитесь, что пакеты IBM Security Directory Server установлены. Дополнительная информация о проверке протоколов приведена в разделе “Проверка протоколов установки” на стр. 52.

Проверка протоколов установки

Определите файл протокола для проверки состояния установки в системе Linux x86, Linux i/pSeries, Linux s390, Solaris или HP-UX.

После завершения установки команда **idsNativeInstall** выдает сообщения, указывающие на состояние установки. Для проверки правильности установки пакетов IBM Security Directory Server обратитесь к файлу протокола установки.

Файл протокола: `/var/idsldap/V6.3/idsNativeInstall_время.log`.

После проверки протокола установки убедитесь, что все пакеты установлены правильным образом и имеют требуемые версии. Дополнительная информация о запросе номеров версий установленных пакетов приведена в разделе Глава 6, “Запрос пакетов IBM Security Directory Server”, на стр. 47.

Глава 8. Установка IBM DB2

Для создания экземпляра IBM Security Directory Server с настроенной базой данных DB2 необходимо, чтобы на компьютере была установлена поддерживаемая версия IBM DB2.

На установочном носителе IBM Security Directory Server содержится поддерживаемая версия IBM DB2. Если установка IBM Security Directory Server выполняется с помощью утилит операционной системы, необходимо установить IBM DB2. При запуске установки IBM Security Directory Server происходит обновление файлов свойств: в них добавляются сведения о поддерживаемой версии IBM DB2. Если на компьютере установлена поддерживаемая версия IBM DB2, можно использовать DB2 и настроить ее для работы с экземпляром сервера каталогов. Дополнительная информация об обновлении файла `ldapdb.properties` приведена в разделе Приложение C, “Обновление файла `ldapdb.properties` вручную”, на стр. 251.

Для установки IBM DB2 откройте установочный носитель IBM Security Directory Server и перейдите в каталог, содержащий установочный файл IBM DB2.

Перед запуском IBM DB2 необходимо убедиться, что соблюдены все предварительные требования для DB2. Для проверки соответствия требованиям DB2 запустите команду **db2prereqcheck**. Если выяснится, что на компьютере отсутствуют необходимые пакеты, необходимо их установить.

В AIX, Linux и Solaris для установки IBM DB2 можно использовать команду **db2_install**. В Windows для установки IBM DB2 следует использовать команду **setup.exe**.

В System x Linux 32-разрядной архитектуры Intel необходимо выбрать Workspace Server Edition путем ввода WSE. В других поддерживаемых операционных системах выберите Enterprise Server Edition путем ввода ESE.

Для того чтобы определить, успешно ли была выполнена установка IBM DB2, проверьте файл `/tmp/db2_install_log.XXXXXX.XXXXXX` - случайное число, связанное с установкой.

Дополнительная информация о предварительных требованиях DB2 и установке IBM DB2 приведена в документации по IBM DB2: <http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>.

Параметры ядра в системах Solaris

В системах Solaris перед установкой IBM DB2 рекомендуется обновить параметры ядра в файле `/etc/system`. Правильные значения параметров ядра для своего компьютера можно определить с помощью команды **db2osconf**. С помощью команды **projmod** можно настроить значения параметров ядра Solaris перед установкой DB2 в Solaris.

В системе Solaris с настроенными областями команду **db2osconf** можно запускать только из глобальной области в Solaris.

Дополнительную информацию о команде **db2osconf** можно найти, задав поиск слова **db2osconf** в документации по IBM DB2: <http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>.

Глава 9. IBM Java Development Kit для IBM Security Directory Server

Для компиляции примеров программ на Java и выполнения программ на Java, таких как Инструмент администрирования экземпляра и Инструмент настройки, необходимо разархивировать IBM Java Development Kit в расположении установки IBM Security Directory Server.

Носитель установки IBM Security Directory Server предоставляет поддерживаемую версию IBM Java Development Kit, IBM Java 1.6 SR 14. При использовании утилит операционной системы для установки IBM Security Directory Server необходимо выполнить установку IBM Java Development Kit.

Для установки IBM Java Development Kit откройте носитель установки IBM Security Directory Server и перейдите в каталог, который содержит сжатый файл IBM Java Development Kit.

Необходимо разархивировать файл архива IBM Java Development Kit в расположение установки IBM Security Directory Server. Файл архива IBM Java Development Kit разархивируется в каталог java. Более подробная информация о расположении установки IBM Security Directory Server находится в разделе “Установочные расположения по умолчанию” на стр. 27.

В системе AIX можно использовать программу tar GNU для разархивирования IBM Java Development Kit в расположение установки IBM Security Directory Server. В противном случае может потребоваться перенести разархивированный каталог java в расположение установки IBM Security Directory Server. Более подробная информация о предварительно требуемых пакетах находится в разделе “Предварительно требуемые пакеты в различных операционных системах” на стр. 15.

Таблица 14. Пакеты IBM Java Development Kit, доступные в различных операционных системах

Операционная система	Имя пакета
AIX	ibm-java-16sr14-aix-ppc-64.tar
System x Linux (Intel 32-bit)	ibm-java-16sr14-linux-i386.tar
System i и System p Linux	ibm-java-16sr14-linux-ppc-64.tar
System z Linux	ibm-java-16sr14-linux-s390-64.tar
Linux в AMD64/EM64T	ibm-java-16sr14-linux-64.tar
HP-UX (Itanium)	ibm-java-16sr14-hp-itanium-64.tar
Solaris в AMD64/EM64T	ibm-java-16sr14-solaris-amd-64.tar
Solaris SPARC	ibm-java-16sr14-solaris-sparc-64.tar
Windows 32-bit	ibm-java-16sr14-win-i386.zip
Windows в AMD64/EM64T	ibm-java-16sr14-win-x86_64.zip

Примеры

Пример 1:

Для того чтобы разархивировать файл IBM Java Development Kit в расположение установки IBM Security Directory Server в системе Linux, выполните следующую команду:

```
tar -xf ibm-java-16sr14-linux-64.tar -C /opt/ibm/ldap/V6.3.1/
```

Глава 10. Установка IBM Global Security Kit

Для того чтобы можно было использовать Secure Sockets Layer (SSL) и Transaction Layer Security (TLS) с IBM Security Directory Server, на компьютере должна быть установлена поддерживаемая версия IBM Global Security Kit (GSKit).

Если используемые операционные системы не поддерживают установку с помощью IBM Installation Manager, то для установки IBM Global Security Kit можно воспользоваться утилитами операционной системы. Для того чтобы можно было устанавливать и использовать защищенные соединения, необходимо установить GSKit как на сервере, так и в системе клиента.

Для поддержки шифрования с низким уровнем надежности необходим пакет GSKit crypt. Пакет GSKit SSL требуется для операций согласования защищенной связи. Наличие пакета GSKit crypt является предварительным требованием для установки пакета GSKit SSL.

Установочный носитель IBM Security Directory Server содержит следующие пакеты GSKit для различных операционных систем:

Примечание: Для архитектур Solaris x64 и SPARC имена пакетов GSKit совпадают.

AIX

Имена пакетов GSKit (64-разрядного)

GSKit8.gskcrypt64.ppc.rte

GSKit8.gskssl64.ppc.rte

Имена пакетов GSKit (32-разрядного)

GSKit8.gskcrypt32.ppc.rte

GSKit8.gskssl32.ppc.rte

System x Linux

Имена пакетов GSKit (32-разрядного)

gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

System z Linux

Имена пакетов GSKit (64-разрядного)

gskcrypt64-8.0.14.26.linux.s390x.rpm

gskssl64-8.0.14.26.linux.s390x.rpm

Имена пакетов GSKit (32-разрядного)

gskcrypt31-8.0.14.26.linux.s390.rpm

gskssl31-8.0.14.26.linux.s390.rpm

System i и System p Linux

Имена пакетов GSKit (64-разрядного)

gskcrypt64-8.0.14.26.linux.ppc.rpm

gskssl64-8.0.14.26.linux.ppc.rpm

Имена пакетов GSKit (32-разрядного)

gskcrypt32-8.0.14.26.linux.ppc.rpm

gkssl32-8.0.14.26.linux.ppc.rpm

Linux IA64 (Itanium) и AMD64/EM64T Linux

Имена пакетов GSKit (64-разрядного)

gskcrypt64-8.0.14.26.linux.x86_64.rpm

gkssl64-8.0.14.26.linux.x86_64.rpm

Имена пакетов GSKit (32-разрядного)

gskcrypt32-8.0.14.26.linux.x86.rpm

gkssl32-8.0.14.26.linux.x86.rpm

Solaris

Имена пакетов GSKit (64-разрядного)

gsk8cry64.pkg

gsk8ssl64.pkg

Имена пакетов GSKit (32-разрядного)

gsk8cry32.pkg

gsk8ssl32.pkg

HP-UX (Itanium)

Имена пакетов GSKit (64-разрядного)

gskcrypt64

gkssl64

Имена пакетов GSKit (32-разрядного)

gskcrypt32

gkssl32

Microsoft Windows

Имена пакетов GSKit (64-разрядного)

gsk8crypt64.exe

gsk8ssl64.exe

Имена пакетов GSKit (32-разрядного)

gsk8crypt32.exe

gsk8ssl32.exe

Установка IBM Global Security Kit с помощью installp

IBM Global Security Kit в системе AIX можно установить с помощью команды **installp**.

Прежде чем начать

Откройте установочный носитель IBM Security Directory Server, чтобы получить устанавливаемый компонент IBM Global Security Kit. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Программа установки **installp** устанавливает IBM Global Security Kit (GSKit) в системе AIX.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Измените текущий каталог на каталог `gskit`, в котором хранится программа установки IBM Global Security Kit.
4. Выполните команду `installp` для установки пакетов IBM Global Security Kit.
 - a. Для установки пакетов 64-разрядной версии GSKit введите следующие команды:

```
installp -acgXd . GSKit8.gskcrypt64.ppc.rte
installp -acgXd . GSKit8.gskssl64.ppc.rte
```
 - b. Для установки пакетов 32-разрядной версии GSKit введите следующие команды:

```
installp -acgXd . GSKit8.gskcrypt32.ppc.rte
installp -acgXd . GSKit8.gskssl32.ppc.rte
```
5. Для того чтобы проверить, успешно ли выполнена установка IBM Global Security Kit, введите следующую команду:

```
lsipp -aL GSKit8*
```

Результаты

Программа установки устанавливает IBM Global Security Kit в системе AIX в следующих расположениях:

64-разрядная версия GSKit
`/usr/opt/ibm/gsk8_64/`

32-разрядная версия GSKit
`/usr/opt/ibm/gsk8/`

Установка IBM Global Security Kit с помощью утилит Linux

IBM Global Security Kit в системе Linux можно установить с помощью команды `rpm`.

Прежде чем начать

Откройте установочный носитель IBM Security Directory Server, чтобы получить устанавливаемый компонент IBM Global Security Kit. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Команда `rpm` устанавливает IBM Global Security Kit (GSKit) в системе Linux. В примере показана установка IBM Global Security Kit в AMD64 Opteron/EM64T Linux. Для System z, System i и System p или System x Linux следует использовать соответствующие имена пакетов.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Измените текущий каталог на каталог `gskit`, в котором хранится программа установки IBM Global Security Kit.
4. Выполните команду `rpm` для установки пакетов IBM Global Security Kit.
 - a. Для установки пакетов 64-разрядной версии GSKit введите следующие команды:

```
rpm -ivh gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -ivh gkssl64-8.0.14.26.linux.x86_64.rpm
```

- b. Для установки пакетов 32-разрядной версии GSKit введите следующие команды:

```
rpm -ivh gskcrypt32-8.0.14.26.linux.x86.rpm
rpm -ivh gkssl32-8.0.14.26.linux.x86.rpm
```

5. Для того чтобы проверить, успешно ли выполнена установка IBM Global Security Kit, введите следующую команду:

```
rpm -qa | grep -i gsk
```

Результаты

Программа установки устанавливает IBM Global Security Kit в системе Linux в следующих расположениях:

64-разрядная версия GSKit

```
/usr/local/ibm/gsk8_64/
```

32-разрядная версия GSKit

```
/usr/local/ibm/gsk8/
```

Установка IBM Global Security Kit с помощью утилит Solaris

Для установки IBM Global Security Kit в системе Solaris используется команда **pkgadd**.

Прежде чем начать

Откройте установочный носитель IBM Security Directory Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Команда **pkgadd** устанавливает IBM Global Security Kit (GSKit) в системе Solaris. Имена пакетов и имена файлов для операционных систем Solaris SPARC и Solaris X64 одинаковы.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Измените текущий каталог на каталог `gskit`, в котором хранится программа установки IBM Global Security Kit.
4. Выполните команду **pkgadd** для установки пакетов IBM Global Security Kit.
 - a. Для установки пакетов 64-разрядной версии GSKit введите следующие команды:

```
pkgadd -d gsk8cry64.pkg
pkgadd -d gsk8ssl64.pkg
```
 - b. Для установки пакетов 32-разрядной версии GSKit введите следующие команды:

```
pkgadd -d gsk8cry32.pkg
pkgadd -d gsk8ssl32.pkg
```
5. Для того чтобы проверить, успешно ли выполнена установка IBM Global Security Kit, введите следующую команду:

```
pkginfo | grep -i gsk
pkgparam имя-пакета VERSION
```

Замените имя-пакета на требуемое имя пакета GSKit для проверки версии.

Установка IBM Global Security Kit с помощью утилит HP-UX

IBM Global Security Kit в системе HP-UX можно установить с помощью команды **swinstall**.

Прежде чем начать

Откройте установочный носитель IBM Security Directory Server, чтобы получить устанавливаемый компонент IBM Global Security Kit. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Измените текущий каталог на каталог `gskit`, в котором хранится программа установки IBM Global Security Kit.
4. Выполните команду **swinstall** для установки пакетов IBM Global Security Kit.

- a. Для установки пакетов 64-разрядной версии GSKit введите следующие команды:

```
swinstall -s полный-путь-к-устанавливаемому-gskit/gskcrypt64 gskcrypt64  
swinstall -s полный-путь-к-устанавливаемому-gskit/gskssl64 gskssl64
```

В параметре **-s** необходимо указать полный путь к устанавливаемому комплекту GSKit.

- b. Для установки пакетов 32-разрядной версии GSKit введите следующие команды:

```
swinstall -s полный-путь-к-устанавливаемому-gskit/gskcrypt32 gskcrypt32  
swinstall -s полный-путь-к-устанавливаемому-gskit/gskssl32 gskssl32
```

5. Для того чтобы проверить, успешно ли выполнена установка IBM Global Security Kit, введите следующую команду:

```
swlist | grep -i gsk
```

Установка IBM Global Security Kit в системе Windows

Для установки IBM Global Security Kit в системе Windows запустите программу установки IBM Global Security Kit.

Прежде чем начать

Откройте установочный носитель IBM Security Directory Server, чтобы получить устанавливаемый компонент IBM Global Security Kit. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

В примере показана установка 64-разрядной версии GSKit `crypt` и 64-разрядной версии GSKit `SSL`. Для установки 32-разрядной версии используйте соответствующие пакеты. В операционной системе Windows 64-разрядной версии можно устанавливать пакеты как 64-разрядной, так и 32-разрядной версии GSKit.

Процедура

1. Войдите как участник группы администраторов.

2. Измените текущий каталог на каталог `gskit`, в котором хранится программа установки IBM Global Security Kit.
3. Для установки пакетов 64-разрядной версии GSKit запустите программу установки GSKit.
 - a. Запустите пакет установки GSKit8 crypt: `gsk8crypt64.exe`.
 - b. В окне установки GSKit8 crypt выполните следующие действия:
 - 1) Укажите установочный каталог для GSKit8 crypt.
 - 2) Нажмите кнопку **Далее**.
 - 3) Нажмите кнопку **Установить**.
 - 4) Нажмите кнопку **Готово**.
 - c. Запустите пакет установки GSKit8 SSL: `gsk8ssl64.exe`.
 - d. В окне установки GSKit8 SSL выполните следующие действия:
 - 1) Укажите установочный каталог для GSKit8 SSL.
 - 2) Нажмите кнопку **Далее**.
 - 3) Нажмите кнопку **Установить**.
 - 4) Нажмите кнопку **Готово**.
4. Для запуска команд GSKit в командной строке укажите в переменной *PATH* каталоги `bin` и `lib64` в системе Windows x86_64.

Примечание: В 32-разрядной версии Windows укажите в переменной *PATH* каталоги `bin` и `lib`.

Если GSKit устанавливается в каталоге `C:\Program Files\IBM\gsk8`, то укажите в переменной *PATH* следующие значения:

```
set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
```

Установка IBM Global Security Kit в системе Windows без вывода сообщений

Запустите команду установки IBM Global Security Kit в командной строке для установки IBM Global Security Kit в системе Windows в режиме без вывода сообщений.

Прежде чем начать

Откройте установочный носитель IBM Security Directory Server, чтобы получить устанавливаемый компонент IBM Global Security Kit. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

В примере показана установка 64-разрядной версии GSKit crypt и 64-разрядной версии GSKit SSL. Для установки 32-разрядной версии используйте соответствующие пакеты. В операционной системе Windows 64-разрядной версии можно устанавливать пакеты как 64-разрядной, так и 32-разрядной версии GSKit.

Процедура

1. Войдите как участник группы администраторов.
2. Откройте окно ввода команд.
3. Измените текущий каталог на каталог `gskit`, в котором хранится программа установки IBM Global Security Kit.

4. Для установки пакетов 64-разрядной версии GSKit в режиме без вывода сообщений введите следующие команды:

```
gsk8crypt64.exe /s /v"/quiet"  
gsk8ssl64.exe /s /v"/quiet"
```
5. Для запуска команд GSKit в командной строке укажите в переменной *PATH* каталоги *bin* и *lib64* в системе Windows x86_64.

Примечание: В 32-разрядной версии Windows укажите в переменной *PATH* каталоги *bin* и *lib*.

Если GSKit устанавливается в каталоге *C:\Program Files\IBM\gsk8*, то укажите в переменной *PATH* следующие значения:

```
set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%  
set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
```


Глава 11. Установка языковых пакетов

Для генерации сообщений сервера каталогов не на английском, а на других языках, необходимо установить нужные языковые пакеты.

IBM Installation Manager может установить все языковые пакеты, которые доступны для операционной системы, если выбран компонент установки из программы полной установки. Языковые пакеты устанавливаются в подкаталог `nls` в расположении установки IBM Security Directory Server.

Примечание: Для клиента не требуется устанавливать языковые пакеты. Можно установить языковые пакеты для клиента, если вы хотите генерировать сообщения на отличном от английского языке для команд `idslink` и `idsrmlink`. Информация о командах `idslink` и `idsrmlink` приведена в *Справочнике по командам*.

Языковые пакеты можно установить с помощью IBM Installation Manager или с помощью утилит операционной системы в системах AIX и Linux. Установка языкового пакета с помощью IBM Installation Manager предоставляется в программе установки полного продукта IBM Security Directory Server.

Напоминание: Установка языкового пакета с помощью IBM Installation Manager поддерживается только в системах AIX, Linux на архитектуре AMD64/EM64T и Microsoft Windows. В операционных системах, которые поддерживают установку IBM Security Directory Server с помощью IBM Installation Manager, не следует устанавливать языковые пакеты вручную с помощью утилит операционной системы. Если установка языковых пакетов с помощью IBM Installation Manager не поддерживается для вашей операционной системы, воспользуйтесь утилитами операционной системы.

Таблица 15. Список поддерживаемых языков в операционных системах AIX, Linux, Solaris и Windows

Язык	AIX	Linux	Solaris	Microsoft Windows
Чешский	✓			
Французский	✓	✓	✓	✓
Немецкий	✓	✓	✓	✓
Венгерский	✓			
Итальянский	✓	✓	✓	✓
Японский	✓	✓	✓	✓
Корейский	✓	✓	✓	✓
Польский	✓			
Португальский (Бразилия)	✓	✓	✓	✓
Русский	✓			
Словацкий	✓			
Испанский	✓	✓	✓	✓
Китайский (КНР)	✓	✓	✓	✓
Китайский (Тайвань)	✓	✓	✓	✓

Языковые пакеты для установки

Перед установкой языкового пакета необходимо определить имена пакетов, связанные с каждым языком для поддерживаемой операционной системы.

Языки и имена языковых пакетов

Напоминание: Языковые пакеты для Linux поддерживаются в следующих архитектурах:

- System x Linux
- System z Linux
- AMD64 Opteron / Intel EM64T Linux
- System i и System p Linux

Напоминание: Языковые пакеты для Solaris поддерживаются в следующих архитектурах:

- Solaris SPARC
- Solaris X64

Таблица 16. Список поддерживаемых языков с именами языковых пакетов в операционных системах AIX, Linux и Solaris

Языки	AIX	Linux	Solaris
Чешский	idsldap.msg631.cs_CZ		
Французский	idsldap.msg631.fr_FR	idsldap-msg631-fr-6.3.1-0.noarch.rpm	idsldap.msg631.fr.pkg
Немецкий	idsldap.msg631.de_DE	idsldap-msg631-de-6.3.1-0.noarch.rpm	idsldap.msg631.de.pkg
Венгерский	idsldap.msg631.hu_HU		
Итальянский	idsldap.msg631.it_IT	idsldap-msg631-it-6.3.1-0.noarch.rpm	idsldap.msg631.it.pkg
Японский	idsldap.msg631.ja_JP	idsldap-msg631-ja-6.3.1-0.noarch.rpm	idsldap.msg631.ja.pkg
Корейский	idsldap.msg631.ko_KO	idsldap-msg631-ko-6.3.1-0.noarch.rpm	idsldap.msg631.ko.pkg
Польский	idsldap.msg631.pl_PL		
Португальский (Бразилия)	idsldap.msg631.pt_BR	idsldap-msg631-pt_BR-6.3.1-0.noarch.rpm	idsldap.msg631.pt_BR.pkg
Русский	idsldap.msg631.ru_RU		
Словацкий	idsldap.msg631.sk_SK		
Испанский	idsldap.msg631.es_ES	idsldap-msg631-es-6.3.1-0.noarch.rpm	idsldap.msg631.es.pkg
Китайский (КНР)	idsldap.msg631.zh_CN	idsldap-msg631-zh_CN-6.3.1-0.noarch.rpm	idsldap.msg631.zh_CN.pkg
Китайский (Тайвань)	idsldap.msg631.zh_TW	idsldap-msg631-zh_TW-6.3.1-0.noarch.rpm	idsldap.msg631.zh_TW.pkg

Установка языковых пакетов с помощью утилит операционной системы

Если операционная система не поддерживает установку языковых пакетов с помощью IBM Installation Manager, то их можно установить с помощью утилит операционной системы.

Прежде чем начать

Необходимо подготовить установочный носитель IBM Security Directory Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Если требуется, чтобы сообщения сервера каталогов выдавались не на английском, а на других языках, то необходимо установить языковые пакеты для этих языков.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Перейдите в каталог, в котором хранится устанавливаемый IBM Security Directory Server.
4. Перейдите в подкаталог tdsLangpack.
5. Для того чтобы установить нужный языковой пакет, выполните команды установки пакета. В следующем примере показано, как установить пакет для французского языка. Таким же образом можно установить любой пакет, указав соответствующее имя пакета для операционной системы.

Операционная система	Выполняемая команда:
AIX	<code>installp -acgXd . idsldap.msg631.fr_FR</code>
Linux	<code>rpm -ivh idsldap-msg631-fr-6.3.1-0.noarch.rpm</code>
Solaris	<code>pkgadd -d idsldap.msg631.fr.pkg</code>

6. Проверьте, успешно ли выполнено удаление языковых пакетов. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Результаты

Программа установки устанавливает языковые пакеты в следующих каталогах:

Таблица 17. Установочный каталог по умолчанию для языковых пакетов IBM Security Directory Server

Операционная система	Установочный каталог языковых пакетов
Linux	<code>/opt/ibm/ldap/V6.3.1/nls/msg</code>
AIX и Solaris	<code>/opt/IBM/ldap/V6.3.1/nls/msg</code>

Глава 12. Установка с помощью утилит командной строки операционной системы

Можно запустить установку IBM Security Directory Server с помощью утилит командной строки операционной системы, если в системе не поддерживается X11.

ОСТОРОЖНО:

- Нельзя использовать разные методы установки на одном и том же компьютере. Необходимо выполнять установку IBM Security Directory Server либо с помощью IBM Installation Manager, либо с помощью утилит командной строки операционной системы. В случае применения обоих режимов установки могут быть установлены не все необходимые для компонента правильные пакеты.
- Следует избегать установки вручную DB2 и встроенного WebSphere Application Server в соответствующих установочных расположениях по умолчанию, используемых программой IBM Installation Manager. Подобная установка вручную может стать причиной сбоев установки, изменения или удаления из системы, когда эти операции будут выполняться из IBM Installation Manager. Дополнительная информация об установочном расположении по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.

Перед установкой продукта необходимо получить источник установки IBM Security Directory Server. Продукт IBM Security Directory Server доступен в файлах архива или в виде установочного образа. С помощью установочного образа можно создать установочные диски DVD.

Необходимо подготовить установочный носитель. Дополнительная информация приведена в разделе “Подготовка носителя установки” на стр. 6.

Важное замечание: Для того чтобы работать с IBM Security Directory Server как с полноценным сервером каталогов, установите на компьютер поддерживаемую версию IBM DB2, если она еще не установлена. Необходимо настроить файл `ldapdb.properties` так, чтобы в нем были указаны версия и полный путь к IBM DB2.

Установка с помощью утилит AIX

Можно использовать утилиты командной строки AIX для установки IBM Security Directory Server в системе AIX.

Для установки IBM Security Directory Server можно использовать одну из следующих утилит:

SMIT Использование этой утилиты рекомендуется как предпочитаемый метод установки. Дополнительная информация приведена в разделе “Установка с помощью SMIT” на стр. 71.

installp

Дополнительная информация приведена в разделе “Установка с помощью **installp**” на стр. 73.

Пакеты для установки в системе AIX

Для применения IBM Security Directory Server в качестве полного сервера каталогов, прокси-сервера или клиента в системе AIX необходимо установить подходящие пакеты.

Пакеты и наборы файлов

IBM Security Directory Server предлагает пакеты для системы AIX. Каждый пакет содержит один или несколько наборов файлов.

Таблица 18. Пакеты и наборы файлов, входящие в состав пакетов

Пакеты	Наборы файлов, связанные с пакетом
idsldap.license631	idsldap.license631.rte - Лицензия
idsldap.cltbody631	<ul style="list-style-type: none"> idsldap.cltbody631.rte - Среда выполнения базового клиента idsldap.cltbody631.adt - Базовый клиент SDK
idsldap.clt32bit631	idsldap.clt32bit631.rte - 32-разрядный клиент C (без SSL и TLS)
idsldap.clt64bit631	idsldap.clt64bit631.rte - 64-разрядный клиент C (без SSL и TLS)
idsldap.clt_max_crypto32bit631	idsldap.clt_max_crypto32bit631.rte - 32-разрядный клиент C (SSL и TLS)
idsldap.clt_max_crypto64bit631	idsldap.clt_max_crypto64bit631.rte - 64-разрядный клиент C (SSL и TLS)
idsldap.cltjava631	idsldap.cltjava631.rte - Клиент Java
idsldap.srvbase64bit631	idsldap.srvbase64bit631.rte - Базовый сервер
idsldap.srv_max_cryptobase64bit631	idsldap.srv_max_cryptobase64bit631.rte - Базовый сервер (SSL)
idsldap.srvproxy64bit631	idsldap.srvproxy64bit631.rte - Прокси-сервер (64-разрядная версия)
idsldap.srv64bit631	idsldap.srv64bit631.rte - Сервер каталогов (64-разрядная версия)
idsldap.webadmin631	idsldap.webadmin631.rte - Web Administration Tool (без SL и TLS)
idsldap.webadmin_max_crypto631	idsldap.webadmin_max_crypto631.rte - Web Administration Tool (SL и TLS)
idsldap.msg631.en_US	Недоступно
idsldap.ent631	idsldap.ent631.rte - IBM Directory Server Entitlement (доступно только на сайте Passport Advantage)

Последовательность установки

Поддерживается одновременная установка всех компонентов. Если они устанавливаются отдельно, то установку следует выполнять в определенном порядке.

Важное замечание:

- Для применения Secure Socket Layer (SSL) или Transport Layer Security (TLS) необходимо установить поддерживаемую версию IBM Global Security Kit.
- Для поддержки Kerberos в системах AIX требуется поддерживаемая версия служб сетевой идентификации.

Примечание: Если компьютер не поддерживает X11, то установку компонента JDK, входящего в состав IBM JDK, можно пропустить. Если компонент JDK не установлен, то инструменты Instance Administration Tool и Configuration Tool могут быть недоступны.

Таблица 19. Последовательность установки для клиента

32-разрядный клиент (без SSL и TLS)	32-разрядный клиент (SSL и TLS)	64-разрядный клиент (без SSL и TLS)	64-разрядный клиент (SSL и TLS)
1. idsldap.cltbody631	1. idsldap.cltbody631	1. idsldap.cltbody631	1. idsldap.cltbody631
2. idsldap.clt32bit631	2. idsldap.clt32bit631	2. idsldap.clt64bit631	2. idsldap.clt64bit631
3. idsldap.cltjava631	3. idsldap.clt_max_crypto32bit631	3. idsldap.cltjava631	3. idsldap.clt_max_crypto32bit631
	4. idsldap.cltjava631		4. idsldap.cltjava631

Примечание: В случае применения файла архива для клиента и сервера с правами на использование или образа ISO с правами на использование для установки IBM Security Directory Server сначала необходимо принять условия лицензии и установить пакет `idsldap.license631`.

Таблица 20. Последовательность установки для полного сервера каталогов

Полный сервер каталогов, 64-разрядная версия (без SSL и TLS)	Полный сервер каталогов, 64-разрядная версия (SSL и TLS)
1. <code>idsldap.license631</code>	1. <code>idsldap.license631</code>
2. <code>idsldap.cltbase631</code>	2. <code>idsldap.cltbase631</code>
3. <code>idsldap.clt64bit631</code>	3. <code>idsldap.clt64bit631</code>
4. <code>idsldap.cltjava631</code>	4. <code>idsldap.clt_max_crypto64bit631</code>
5. <code>idsldap.srvbase64bit631</code>	5. <code>idsldap.cltjava631</code>
6. <code>idsldap.srv64bit631</code>	6. <code>idsldap.srvbase64bit631</code>
7. <code>idsldap.msg631.en_US</code>	7. <code>idsldap.srv_max_cryptobase64bit631</code>
8. <code>idsldap.ent631</code>	8. <code>idsldap.srv64bit631</code>
	9. <code>idsldap.msg631.en_US</code>
	10. <code>idsldap.ent631</code>

Таблица 21. Последовательность установки для прокси-сервера

Прокси-сервер, 64-разрядная версия (без SSL и TLS)	Прокси-сервер, 64-разрядная версия (SSL и TLS)
1. <code>idsldap.license631</code>	1. <code>idsldap.license631</code>
2. <code>idsldap.cltbase631</code>	2. <code>idsldap.cltbase631</code>
3. <code>idsldap.clt64bit631</code>	3. <code>idsldap.clt64bit631</code>
4. <code>idsldap.cltjava631</code>	4. <code>idsldap.clt_max_crypto64bit631</code>
5. <code>idsldap.srvbase64bit631</code>	5. <code>idsldap.cltjava631</code>
6. <code>idsldap.srvproxy64bit631</code>	6. <code>idsldap.srvbase64bit631</code>
7. <code>idsldap.msg631.en_US</code>	7. <code>idsldap.srv_max_cryptobase64bit631</code>
8. <code>idsldap.ent631</code>	8. <code>idsldap.srvproxy64bit631</code>
	9. <code>idsldap.msg631.en_US</code>
	10. <code>idsldap.ent631</code>

Примечание: Для применения инструмента Web Administration Tool необходимо развернуть его на веб-сервере приложений. Дополнительная информация об установке встроенного WebSphere Application Server приведена в разделе “Установка встроенного WebSphere Application Server вручную” на стр. 109.

Таблица 22. Установочный пакет Web Administration Tool

Web Administration Tool (без SL и TLS)	Web Administration Tool (SL и TLS)
1. <code>idsldap.license631</code>	1. <code>idsldap.license631</code>
2. <code>idsldap.webadmin631</code>	2. <code>idsldap.webadmin_max_crypto631</code>

В случае установки Web Administration Tool на компьютер копируются файлы языка описания служб каталогов (DSML). Дополнительная информация о DSML приведена в разделе Приложение А, “Язык описания служб каталогов”, на стр. 247.

Установка с помощью SMIT

Команда `smit` позволяет установить IBM Security Directory Server в системе AIX.

Прежде чем начать

Подготовьте установочный носитель IBM Security Directory Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Программа установки **smi t** установит IBM Security Directory Server в системе AIX. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл `ldapdb.properties`, добавив в него путь и версию DB2.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Выполните команду **idsLicense**.
`./idsLicense`
4. Если вы принимаете условия Лицензионного соглашения о программном обеспечении, введите 1. Вам доступны следующие опции:
 - 1: Принять условия лицензионного соглашения.
 - 2: Отклонить условия лицензионного соглашения и завершить установку.
 - 3: Напечатать лицензионное соглашение.
 - 4: Ознакомиться с условиями третьих сторон в лицензионном соглашении.
 - 99: Вернуться в предыдущее меню.

После принятия условий лицензионного соглашения файл `LAPID` и папка `license` будут созданы в установочном каталоге IBM Security Directory Server. Папка `license` содержит файлы лицензии на IBM Security Directory Server на всех поддерживаемых языках.

Важное замечание: Не изменяйте и не удаляйте файл `LAPID` и файлы лицензии в папке `license`.

5. Выполните команду **smi t install**. Откроется окно **Установка и обслуживание программного обеспечения**.
6. Выберите **Установить и обновить программное обеспечение > Установить и обновить на основе всего доступного программного обеспечения**.
7. Выберите установочный носитель.
 - Если вы устанавливаете с DVD, выполните следующие действия:
 - a. Нажмите **Список**, чтобы открыть устройство, содержащее образы IBM Security Directory Server.
 - Если вы устанавливаете из несжатого архивного файла, введите `.` в поле **Устройство или каталог с программным обеспечением**.
8. Нажмите **Выполнить**.
9. Переместите курсор в окно **Устанавливаемое программное обеспечение** и выполните следующие действия:
 - a. Для установки набора файлов `idsldap` введите `idsldap`.
 - b. Нажмите **Список**, чтобы просмотреть все наборы файлов, и выберите наборы файлов, которые вы хотите установить.
 - c. Нажмите **ОК**.
10. Для того чтобы начать установку, нажмите **ОК**.
11. После завершения установки просмотрите итоговый отчет, чтобы убедиться, что все наборы файлов установлены правильно.

12. По окончании установки нажмите **Готово**.
13. Для завершения работы с программой **SMIT** нажмите клавишу F12.
14. Убедитесь, что установка IBM Security Directory Server успешно выполнена. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Результаты

Программа установки устанавливает IBM Security Directory Server в каталоге `/opt/IBM/ldap/V6.3.1` в системе AIX. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл `ldapdb.properties`, добавив в него путь и версию DB2.

Дальнейшие действия

По окончании установки IBM Security Directory Server выполните следующее действие:

- Для того чтобы использовать IBM Security Directory Server в качестве полного сервера каталогов, создайте экземпляр сервера каталогов. См. раздел “Создание экземпляра сервера каталогов по умолчанию” на стр. 134.
- Для того чтобы использовать IBM Security Directory Server в качестве сервера проху, создайте экземпляр сервера проху. См. раздел “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.

Установка с помощью `installp`

Команда `installp` позволяет выполнить установку IBM Security Directory Server в системе AIX.

Прежде чем начать

Необходимо подготовить установочный носитель IBM Security Directory Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Программа установки `installp` устанавливает IBM Security Directory Server в системе AIX. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл `ldapdb.properties` с учетом пути и версии DB2.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Перейдите в каталог, содержащий устанавливаемые пакеты IBM Security Directory Server.
4. Выполните команду `idsLicense`.
`./idsLicense`
5. Если вы принимаете условия Лицензионного соглашения о программном обеспечении, введите 1. Вам доступны следующие опции:
 - 1: Принять условия лицензионного соглашения.
 - 2: Отклонить условия лицензионного соглашения и завершить установку.
 - 3: Напечатать лицензионное соглашение.
 - 4: Ознакомиться с условиями третьих сторон в лицензионном соглашении.

- 99: Вернуться в предыдущее меню.

После принятия условий лицензионного соглашения файл LAPID и папка license будут созданы в установочном каталоге IBM Security Directory Server. Папка license содержит файлы лицензии на IBM Security Directory Server на всех поддерживаемых языках.

Важное замечание: Не изменяйте и не удаляйте файл LAPID и файлы лицензии в папке license.

6. Выберите пакеты IBM Security Directory Server для установки.

```
installp -ld . | grep idsldap
```

Появится список всех пакетов IBM Security Directory Server, доступных для установки.

7. Для установки пакетов введите следующую команду:

```
installp -acgXd . имена-пакетов
```

Для установки всех пакетов IBM Security Directory Server из текущего каталога выполните следующую команду:

```
installp -acgXd . idsldap
```

8. После завершения установки будет показан итоговый отчет.
9. Убедитесь, что установка IBM Security Directory Server успешно выполнена. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Результаты

Программа установки устанавливает IBM Security Directory Server в каталоге /opt/IBM/ldap/V6.3.1 в системе AIX. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл ldapdb.properties, добавив в него путь и версию DB2.

Дальнейшие действия

После установки IBM Security Directory Server необходимо выполнить следующие действия:

- Для того чтобы использовать IBM Security Directory Server в качестве полного сервера каталогов, создайте экземпляр сервера каталогов. Дополнительная информация приведена в разделе “Создание экземпляра сервера каталогов по умолчанию” на стр. 134.
- Для того чтобы использовать IBM Security Directory Server в качестве сервера проху, создайте экземпляр сервера проху. Дополнительная информация приведена в разделе “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.

Установка с помощью утилит Linux

Можно использовать утилиты командной строки Linux для установки IBM Security Directory Server в системе Linux.

IBM Security Directory Server предоставляет отдельные пакеты для компьютеров с различными операционными системами и архитектурой. Необходимо выбрать

подходящие пакеты для установки на своем компьютере. Дополнительная информация об именах пакетов приведена в разделе “Пакеты для установки в системе Linux”.

Пакеты для установки в системе Linux

Для применения IBM Security Directory Server в качестве полного сервера каталогов, прокси-сервера или клиента в системе Linux необходимо установить подходящие пакеты.

Пакеты для различных систем Linux

Таблица 23. Пакеты IBM Security Directory Server для различных систем Linux

Пакеты IBM Security Directory Server	AMD64 Opteron/EM64T Linux	System i или System p	System x	System z
IBM Directory Server - Лицензия	idsldap-license631-6.3.1-0.x86_64.rpm	idsldap-license631-6.3.1-0.ppc.rpm	idsldap-license631-6.3.1-0.i386.rpm	idsldap-license631-6.3.1-0.s390.rpm
IBM Directory Server - Базовый клиент	idsldap-cltbase631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.ppc.rpm	idsldap-cltbase631-6.3.1-0.i386.rpm	idsldap-cltbase631-6.3.1-0.s390.rpm
IBM Directory Server - 32-разрядный клиент	idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-clt32bit631-6.3.1-0.ppc.rpm	idsldap-clt32bit631-6.3.1-0.i386.rpm	idsldap-clt32bit631-6.3.1-0.s390.rpm
IBM Directory Server - 64-разрядный клиент	idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-clt64bit631-6.3.1-0.ppc64.rpm	Недоступно	idsldap-clt64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - клиент Java	idsldap-cltjava631-6.3.1-0.x86_64.rpm	idsldap-cltjava631-6.3.1-0.ppc.rpm	idsldap-cltjava631-6.3.1-0.i386.rpm	idsldap-cltjava631-6.3.1-0.s390.rpm
IBM Directory Server - Базовый сервер	idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	idsldap-srvbase64bit631-6.3.1-0.ppc64.rpm	idsldap-srvbase32bit631-6.3.1-0.i386.rpm	idsldap-srvbase64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Сервер Прoxy	idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	idsldap-srvproxy64bit631-6.3.1-0.ppc64.rpm	idsldap-srvproxy32bit631-6.3.1-0.i386.rpm	idsldap-srvproxy64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - 32-разрядный сервер	Недоступно	Недоступно	idsldap-srv32bit631-6.3.1-0.i386.rpm	Недоступно
IBM Directory Server - 64-разрядный сервер	idsldap-srv64bit631-6.3.1-0.x86_64.rpm	idsldap-srv64bit631-6.3.1-0.ppc64.rpm	Недоступно	idsldap-srv64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Web Administration Tool	idsldap-webadmin631-6.3.1-0.x86_64.rpm	idsldap-webadmin631-6.3.1-0.ppc.rpm	idsldap-webadmin631-6.3.1-0.i386.rpm	idsldap-webadmin631-6.3.1-0.s390.rpm
IBM Directory Server - Сообщения на английском языке (США)	idsldap-msg631-en-6.3.1-0.x86_64.rpm	idsldap-msg631-en-6.3.1-0.ppc.rpm	idsldap-msg631-en-6.3.1-0.i386.rpm	idsldap-msg631-en-6.3.1-0.s390.rpm
IBM Directory Server Entitlement (доступно только на сайте Passport Advantage)	idsldap-ent631-6.3.1-0.x86_64.rpm	idsldap-ent631-6.3.1-0.ppc.rpm	idsldap-ent631-6.3.1-0.i386.rpm	idsldap-ent631-6.3.1-0.s390.rpm

Зависимые пакеты

Перед установкой отдельных пакетов может потребоваться установить зависимости.

Примечание: В случае применения файла архива для клиента и сервера с правами на использование или образа ISO с правами на использование для установки IBM Security Directory Server сначала необходимо принять условия лицензии и установить пакет `idsldap-license631-6.3.1-0.архитектура.rpm`.

В таблице показан зависимый пакет для AMD64 Opteron/EM64T Linux. Для System z, System i или System p или System x Linux следует использовать соответствующие имена пакетов.

Таблица 24. Пакет и зависимые пакеты

Имя пакета	Зависит от
idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	<ol style="list-style-type: none"> idsldap-license631-6.3.1-0.x86_64.rpm idsldap-cltbase631-6.3.1-0.x86_64.rpm idsldap-clt64bit631-6.3.1-0.x86_64.rpm
idsldap-srv64bit631-6.3.1-0.x86_64.rpm	<ol style="list-style-type: none"> idsldap-license631-6.3.1-0.x86_64.rpm idsldap-cltbase631-6.3.1-0.x86_64.rpm idsldap-clt64bit631-6.3.1-0.x86_64.rpm idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm
idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	<ol style="list-style-type: none"> idsldap-license631-6.3.1-0.x86_64.rpm idsldap-cltbase631-6.3.1-0.x86_64.rpm idsldap-clt64bit631-6.3.1-0.x86_64.rpm idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm

Последовательность установки

Поддерживается одновременная установка всех компонентов. Если они устанавливаются отдельно, то установку следует выполнять в определенном порядке.

Важное замечание: Для применения Secure Socket Layer (SSL) или Transport Layer Security (TLS) необходимо установить поддерживаемую версию IBM Global Security Kit.

В примере последовательности установки применяется AMD64 Opteron/EM64T Linux. Для System z, System i или System p или System x Linux следует использовать соответствующие имена пакетов.

Таблица 25. Последовательность установки для клиента

32-разрядный клиент	64-разрядный клиент
1. idsldap-cltbase631-6.3.1-0.x86_64.rpm	1. idsldap-cltbase631-6.3.1-0.x86_64.rpm
2. idsldap-clt32bit631-6.3.1-0.x86_64.rpm	2. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
3. idsldap-cltjava631-6.3.1-0.x86_64.rpm	3. idsldap-cltjava631-6.3.1-0.x86_64.rpm

Таблица 26. Последовательность установки для полного сервера каталогов и прокси-сервера

Полный сервер каталогов, 64-разрядная версия	Прокси-сервер, 64-разрядная версия
1. <code>idsldap-license631-6.3.1-0.x86_64.rpm</code>	1. <code>idsldap-license631-6.3.1-0.x86_64.rpm</code>
2. <code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code>	2. <code>idsldap-cltbase631-6.3.1-0.x86_64.rpm</code>
3. <code>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</code>	3. <code>idsldap-clt64bit631-6.3.1-0.x86_64.rpm</code>
4. <code>idsldap-cltjava631-6.3.1-0.x86_64.rpm</code>	4. <code>idsldap-cltjava631-6.3.1-0.x86_64.rpm</code>
5. <code>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</code>	5. <code>idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm</code>
6. <code>idsldap-srv64bit631-6.3.1-0.x86_64.rpm</code>	6. <code>idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm</code>
7. <code>idsldap-msg631-en-6.3.1-0.x86_64.rpm</code>	7. <code>idsldap-msg631-en-6.3.1-0.x86_64.rpm</code>
8. <code>idsldap-ent631-6.3.1-0.x86_64.rpm</code>	8. <code>idsldap-ent631-6.3.1-0.x86_64.rpm</code>

Примечание: Для работы с Веб-инструментом администрирования его необходимо развернуть на сервере веб-приложений. Дополнительная информация об установке встроенного WebSphere Application Server приведена в разделе “Установка встроенного WebSphere Application Server вручную” на стр. 109.

Таблица 27. Установочный пакет *Web Administration Tool*

Web Administration Tool
1. <code>idsldap-license631-6.3.1-0.x86_64.rpm</code>
2. <code>idsldap-webadmin631-6.3.1-0.x86_64.rpm</code>

В случае установки *Web Administration Tool* на компьютер копируются файлы языка описания служб каталогов (DSML). Дополнительная информация о DSML приведена в разделе Приложение А, “Язык описания служб каталогов”, на стр. 247.

Установка с помощью утилит Linux

Команда **rpm** позволяет выполнить установку IBM Security Directory Server в системе Linux.

Прежде чем начать

Необходимо подготовить установочный носитель IBM Security Directory Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Программа установки **rpm** устанавливает IBM Security Directory Server в системе Linux. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл `ldapdb.properties` с учетом пути и версии DB2.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Перейдите в каталог, в котором хранится устанавливаемый IBM Security Directory Server.
4. Выполните команду **idsLicense**.

./idsLicense

5. Если вы принимаете условия Лицензионного соглашения о программном обеспечении, введите 1. Вам доступны следующие опции:
 - 1: Принять условия лицензионного соглашения.
 - 2: Отклонить условия лицензионного соглашения и завершить установку.
 - 3: Напечатать лицензионное соглашение.
 - 4: Ознакомиться с условиями третьих сторон в лицензионном соглашении.
 - 99: Вернуться в предыдущее меню.

После принятия условий лицензионного соглашения файл LAPID и папка license будут созданы в установочном каталоге IBM Security Directory Server. Папка license содержит файлы лицензии на IBM Security Directory Server на всех поддерживаемых языках.

Важное замечание: Не изменяйте и не удаляйте файл LAPID и файлы лицензии в папке license.

6. Для установки пакета введите следующую команду:

```
rpm -ivh имя-пакета
```

Для установки всех пакетов IBM Security Directory Server выполните следующую команду:

```
rpm -ivh idsldap*
```

7. Убедитесь, что установка IBM Security Directory Server успешно выполнена. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Результаты

Программа установки устанавливает IBM Security Directory Server в каталоге /opt/ibm/ldap/V6.3.1 в системе Linux. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл ldapdb.properties, добавив в него путь и версию DB2.

Дальнейшие действия

По окончании установки IBM Security Directory Server выполните следующее действие:

- Для того чтобы использовать IBM Security Directory Server в качестве полного сервера каталогов, создайте экземпляр сервера каталогов. Дополнительная информация приведена в разделе “Создание экземпляра сервера каталогов по умолчанию” на стр. 134.
- Для того чтобы использовать IBM Security Directory Server в качестве сервера проxy, создайте экземпляр сервера проxy. Дополнительная информация приведена в разделе “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.

Установка с помощью утилит Solaris

Можно использовать утилиты командной строки Solaris для установки IBM Security Directory Server в системе Solaris.

IBM Security Directory Server предоставляет одинаковый набор пакетов для компьютеров с различной архитектурой. Имеются пакеты для операционных систем Sun SPARC Solaris и AMD64 Opteron/EM64T Solaris. Имена пакетов и файлов

одинаковые для обеих операционных систем. Дополнительная информация об именах пакетов приведена в разделе “Пакеты для установки в системе Solaris”.

При установке пакетов IBM Security Directory Server нельзя применять системное значение по умолчанию для всех пакетов (ALL). При выборе всех пакетов система устанавливает пакеты в неправильной последовательности, поэтому установка не будет выполнена.

Пакеты для установки в системе Solaris

Для применения IBM Security Directory Server в качестве полного сервера каталогов, прокси-сервера или клиента в системе Solaris необходимо установить подходящие пакеты.

Пакеты для систем Solaris

Важное замечание: Имена пакетов и файлов одинаковые для операционных систем Solaris SPARC и AMD64 Opteron/EM64T Solaris.

Таблица 28. Пакеты IBM Security Directory Server для различных систем Solaris

Пакеты IBM Security Directory Server	Имена пакетов	Имя файла
IBM Directory Server - Лицензия	IDSlicense631	idsldap-license631.pkg
IBM Directory Server - Базовый клиент	IDS1bc631	idsldap.clbase631.pkg
IBM Directory Server - 32-разрядный клиент	IDS132c631	idsldap.clt32bit631.pkg
IBM Directory Server - 64-разрядный клиент	IDS164c631	idsldap.clt64bit631.pkg
IBM Directory Server - клиент Java	IDS1jc631	idsldap.cltjava631.pkg
IBM Directory Server - Базовый сервер	IDS1bs631	idsldap.srvbase64bit631.pkg
IBM Directory Server - Сервер Прoxy	IDS164p631	idsldap.srvproxy64bit631.pkg
IBM Directory Server - 64-разрядный сервер	IDS164s631	idsldap.srv64bit631.pkg
IBM Directory Server - Web Administration Tool	IDS1web631	idsldap.webadmin631.pkg
IBM Directory Server - Сообщения на английском языке (США)	IDS1en631	idsldap.msg631.en.pkg
IBM Directory Server Entitlement (доступно только на сайте Passport Advantage)	IDS1ent631	idsldap.ent631.pkg

Зависимые пакеты

Перед установкой отдельных пакетов может потребоваться установить зависимости.

Таблица 29. Пакет и зависимые пакеты

Имя пакета	Зависит от
idsldap.clt32bit631.pkg	idsldap.clbase631.pkg
idsldap.clt64bit631.pkg	idsldap.clbase631.pkg
idsldap.srvbase64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.clbase631.pkg 3. idsldap.clt64bit631.pkg
idsldap.srv64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.clbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg

Таблица 29. Пакет и зависимые пакеты (продолжение)

Имя пакета	Зависит от
idsldap.srvproxy64bit631.pkg	<ol style="list-style-type: none"> 1. idsldap-license631.pkg 2. idsldap.cltbody631.pkg 3. idsldap.cltbody64bit631.pkg 4. idsldap.srvbase64bit631.pkg

Последовательность установки

Установку пакетов в системе Solaris следует выполнять в определенном порядке.

Важное замечание: Для применения Secure Socket Layer (SSL) или Transport Layer Security (TLS) необходимо установить поддерживаемую версию IBM Global Security Kit.

Таблица 30. Последовательность установки для клиента

32-разрядный клиент	64-разрядный клиент
1. idsldap.cltbody631.pkg	1. idsldap.cltbody631.pkg
2. idsldap.cltbody32bit631.pkg	2. idsldap.cltbody64bit631.pkg
3. idsldap.cltbodyjava631.pkg	3. idsldap.cltbodyjava631.pkg

Примечание: В случае применения файла архива для клиента и сервера с правами на использование или образа ISO с правами на использование для установки IBM Security Directory Server сначала необходимо принять условия лицензии и установить пакет `idsldap-license631.pkg`.

Таблица 31. Последовательность установки для полного сервера каталогов и прокси-сервера

Полный сервер каталогов, 64-разрядная версия	Прокси-сервер, 64-разрядная версия
1. idsldap-license631.pkg	1. idsldap-license631.pkg
2. idsldap.cltbody631.pkg	2. idsldap.cltbody631.pkg
3. idsldap.cltbody64bit631.pkg	3. idsldap.cltbody64bit631.pkg
4. idsldap.cltbodyjava631.pkg	4. idsldap.cltbodyjava631.pkg
5. idsldap.srvbase64bit631.pkg	5. idsldap.srvbase64bit631.pkg
6. idsldap.srv64bit631.pkg	6. idsldap.srvproxy64bit631.pkg
7. idsldap.msg631.en.pkg	7. idsldap.msg631.en.pkg
8. idsldap.ent631.pkg	8. idsldap.ent631.pkg

Примечание: Для работы с Веб-инструментом администрирования его необходимо развернуть на сервере веб-приложений. Дополнительная информация об установке встроенного WebSphere Application Server приведена в разделе “Установка встроенного WebSphere Application Server вручную” на стр. 109.

Таблица 32. Установочный пакет Web Administration Tool

Web Administration Tool
1. idsldap-license631.pkg
2. idsldap.webadmin631.pkg

В случае установки Web Administration Tool на компьютер копируются файлы языка описания служб каталогов (DSML). Дополнительная информация о DSML приведена в разделе Приложение А, “Язык описания служб каталогов”, на стр. 247.

Установка с помощью утилит Solaris

Команда **pkgadd** позволяет выполнить установку IBM Security Directory Server в системе Solaris.

Прежде чем начать

Откройте установочный носитель IBM Security Directory Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Программа установки **pkgadd** устанавливает IBM Security Directory Server в системе Solaris. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл `ldapdb.properties` с учетом пути и версии DB2.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Перейдите в каталог, содержащий устанавливаемый пакет IBM Security Directory Server.
4. Выполните команду **idsLicense**.
`./idsLicense`
5. Если вы принимаете условия Лицензионного соглашения о программном обеспечении, введите 1. Вам доступны следующие опции:
 - 1: Принять условия лицензионного соглашения.
 - 2: Отклонить условия лицензионного соглашения и завершить установку.
 - 3: Напечатать лицензионное соглашение.
 - 4: Ознакомиться с условиями третьих сторон в лицензионном соглашении.
 - 99: Вернуться в предыдущее меню.

После принятия условий лицензионного соглашения в установочном каталоге IBM Security Directory Server создаются файл `LAPID` и папка `license`. Папка `license` содержит файлы лицензий IBM Security Directory Server на всех поддерживаемых языках.

Важное замечание: Файл `LAPID` и файлы лицензий из папки `license` не следует изменять и удалять.

6. Для установки пакета введите следующую команду:

Примечание: Установку пакетов IBM Security Directory Server в системе Solaris следует выполнять в определенном порядке. Дополнительная информация приведена в разделе “Пакеты для установки в системе Solaris” на стр. 79.

```
pkgadd -d имя-пакета
```

7. Проверьте правильность установки IBM Security Directory Server. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Результаты

Программа установки устанавливает IBM Security Directory Server в каталоге /opt/IBM/ldap/V6.3.1 в системе Solaris. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл ldapdb.properties с учетом пути и версии DB2.

Дальнейшие действия

После установки IBM Security Directory Server необходимо выполнить следующее действие:

- Для применения IBM Security Directory Server в качестве полного сервера каталогов создайте экземпляр сервера каталогов. Дополнительная информация приведена в разделе “Создание экземпляра сервера каталогов по умолчанию” на стр. 134.
- Для того чтобы использовать IBM Security Directory Server в качестве сервера прокси, создайте экземпляр сервера прокси. Дополнительная информация приведена в разделе “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.

Установка с помощью утилит HP-UX

Можно использовать утилиты командной строки HP-UX для установки IBM Security Directory Server в системе HP-UX.

IBM Security Directory Server только клиентские пакеты для HP-UX в системах Itanium (серверы на основе процессора Intel IA64). Дополнительная информация приведена в разделе “Пакеты для установки в системе HP-UX Itanium”.

Пакеты для установки в системе HP-UX Itanium

Для применения IBM Security Directory Server в качестве клиента в системе HP-UX необходимо установить подходящие пакеты.

Пакеты для систем HP-UX

IBM Security Directory Server предлагает только пакет клиента для HP-UX в системах Itanium (серверы на основе процессоров Intel IA64).

Таблица 33. Пакеты IBM Security Directory Server для систем HP-UX

Пакеты IBM Security Directory Server	Имена пакетов
IBM Directory Server - Базовый клиент	idsldap.clbase631.depot
IBM Directory Server - 32-разрядный клиент	idsldap.clt32bit631.depot
IBM Directory Server - 64-разрядный клиент	idsldap.clt64bit631.depot
IBM Directory Server - клиент Java	idsldap.cltjava631.depot
IBM Directory Server - Лицензия	idsldap.license631.depot

Зависимые пакеты

Перед установкой отдельных пакетов может потребоваться установить зависимости.

Таблица 34. Пакет и зависимые пакеты

Имя пакета	Зависит от
idsldap.clt32bit631.depot	idsldap.clbase631.depot
idsldap.clt64bit631.depot	idsldap.clbase631.depot

Последовательность установки

Установку пакетов в системе HP-UX следует выполнять в определенном порядке.

Важное замечание: Для применения Secure Socket Layer (SSL) или Transport Layer Security (TLS) необходимо установить поддерживаемую версию IBM Global Security Kit.

Таблица 35. Последовательность установки для клиента

32-разрядный клиент	64-разрядный клиент
1. idsldap.cltbodybase631.depot	1. idsldap.cltbodybase631.depot
2. idsldap.cltbody32bit631.depot	2. idsldap.cltbody64bit631.depot
3. idsldap.cltbodyjava631.depot	3. idsldap.cltbodyjava631.depot

Установка с помощью утилит HP-UX

Команда **swinstall** позволяет выполнить установку IBM Security Directory Server в системе HP-UX.

Прежде чем начать

Необходимо подготовить установочный носитель IBM Security Directory Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Программа установки **pkgadd** устанавливает IBM Security Directory Server в системе Solaris. Если в системе установлена поддерживаемая версия IBM DB2, то процесс установки обновит файл `ldapdb.properties` с учетом пути и версии DB2.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Перейдите в каталог, в котором хранится устанавливаемый IBM Security Directory Server.
4. Для установки пакетов введите следующую команду:

```
swinstall -s каталог-sds/idsldap.cltbodybase631.depot \  
swinstall -s каталог-sds/idsldap.cltbody32bit631.depot \  
swinstall -s каталог-sds/idsldap.cltbody64bit631.depot \  
swinstall -s каталог-sds/idsldap.cltbodyjava631.depot \*
```
5. Убедитесь, что установка IBM Security Directory Server успешно выполнена. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Результаты

Программа установки устанавливает IBM Security Directory Server в каталоге `/opt/IBM/ldap/V6.3.1` в системе HP-UX.

Глава 13. Проверка компонентов IBM Security Directory Server

После установки, изменения или удаления из системы IBM Security Directory Server необходимо проверить, были ли компоненты IBM Security Directory Server правильно установлены, изменены или удалены.

Можно использовать IBM Installation Manager или утилиты операционной системы для проверки успешности установки, изменения или удаления из системы.

Проверка компонентов IBM Security Directory Server с помощью IBM Installation Manager

Используйте IBM Installation Manager для проверки компонентов IBM Security Directory Server и связанных продуктов, установленных с помощью IBM Installation Manager.

Процедура

1. Запустите IBM Installation Manager.

Windows

В меню **Пуск** выберите **Программы > IBM Installation Manager > IBM Installation Manager**.

AIX и Linux

Введите в командной строке следующую команду. Измените указанный стандартный путь, если IBM Installation Manager установлен в другом расположении.

```
/opt/IBM/InstallationManager/eclipse/IBMIM
```

2. На странице **IBM Installation Manager** выберите **Файл > Просмотреть установленные пакеты**.
3. В списке **Установленные пакеты и исправления** на странице **Установленные пакеты** разверните **IBM Security Directory Server**.
4. В списке **Установленные пакеты и исправления** выберите версию IBM Security Directory Server, компоненты которой требуется просмотреть.
5. В области **Сведения** проверьте установку компонентов и связанных продуктов.
6. Для закрытия страницы **Установленные пакеты** нажмите кнопку **Закрыть**.
7. Для закрытия **IBM Installation Manager** воспользуйтесь меню **Файл > Выход**.

Проверка компонентов IBM Security Directory Server в Windows

Для проверки успешности установки, изменения или удаления IBM Security Directory Server можно проверить реестр Microsoft Windows.

Об этой задаче

Microsoft Windows использует записи в реестре для отслеживания программного обеспечения, установленного в системе Windows. После успешной установки, изменения или удаления компонентов IBM Security Directory Server записи в реестре отражают последнее обновление системы. Пример записей реестра демонстрирует успешную установку компонентов IBM Security Directory Server. Во время изменения

или удаления компонентов IBM Security Directory Server изменяются записи реестра, отслеживающие компоненты - в них записывается самое новое состояние. Записи реестра показаны для Microsoft Windows на архитектуре AMD64/EM64T.

Процедура

1. Войдите в систему Windows с правами доступа администратора.
2. Откройте командную строку и запустите следующую команду:
regedit
3. В окне **Редактор реестра** выберите **Мой компьютер > HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432NODE > IBM > IDSLDAP > 6.3.1**

Примечание: Для проверки установки IBM Security Directory Server в системах Microsoft Windows на архитектуре Intel x86 (IA32) разверните **Компьютер > HKEY_LOCAL_MACHINE > SOFTWARE > IBM > IDSLDAP > 6.3.1**.
Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1 содержит основные версии компонентов IBM Security Directory Server, установленных в системе.

BaseServerMajorVersion	6.3.1
BitMode	64
ClientMajorVersion	6.3.1
JavaClientMajorVersion	6.3.1
LDAPHome	<i>расположение-установки</i>
ProxyServerMajorVersion	6.3.1
ServerMajorVersion	6.3.1
WebadminMajorVersion	6.3.1
WebSphereAppSrvMajorVersion	7.0

Вспомогательные версии компонентов IBM Security Directory Server, установленных в системе, показаны в разделе Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1. Пример:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\BaseServer\  
BaseServerMinorVersion 1.0
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Client\  
ClientMinorVersion 1.0
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\JavaClient\  
JavaClientMinorVersion 1.0
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\ProxyServer\  
ProxyServerMinorVersion 1.0
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Server\  
ServerMinorVersion 1.0
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Webadmin\  
WebadminMinorVersion 1.0
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\WebSphereAppSrv\  
WebSphereAppSrvMinorVersion 0.25
```

4. Для закрытия окна **Редактор реестра** воспользуйтесь меню **Файл > Выход**.

Проверка пакетов IBM Security Directory Server

Для проверки успешности установки IBM Security Directory Server можно проверить наличие в системе пакетов IBM Security Directory Server.

Об этой задаче

После установки IBM Security Directory Server следует убедиться, что пакеты имеют требуемый уровень. Можно получить номер версии пакетов IBM Security Directory Server.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте командную строку и запустите следующую команду:

Операционная система	Команда для опроса пакетов:
AIX	lspp -l 'idsldap*'
Linux	rpm -qa grep -i idsldap
Solaris	pkginfo grep IDS1 pkgparam пакет VERSION
HP-UX	swlist grep -i idsldap

Результаты

Команда перечисляет пакеты IBM Security Directory Server, установленные в системе.

Проверка версии Веб-инструмент администрирования

Для проверки успешности установки или обновления Веб-инструмента администрирования требуется проверить версию Веб-инструмента администрирования.

Процедура

1. Войдите в систему с правами доступа администратора.
2. Откройте каталог *каталог-установки-ds/idstools*. *каталог-установки-ds* - это расположение установки IBM Security Directory Server. В различных операционных системах используются следующие расположения по умолчанию:

Таблица 36. Стандартное расположение установки IBM Security Directory Server в различных операционных системах

Операционные системы	Стандартное расположение установки:
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX и Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Введите следующую команду:

Операционные системы	Выполняемая команда:
Microsoft Windows	deploy_IDSWebApp.bat -v
AIX, Linux и Solaris	deploy_IDSWebApp -v

Команда выводит следующую информацию:

- Версию и дату команды **deploy_IDSWebApp**.
- Версию и дату установленного файла **IDSWebApp.war**.
- Версию и дату текущего развертывания файла **IDSWebApp.war**.

Дальнейшие действия

Необходимо проверить следующие значения:

1. Если значения версии и даты установленного файла `IDSWebApp.war` отличаются от версии и даты текущего развернутого файла `IDSWebApp.war`.
2. Если значения не совпадают, разверните последний Веб-инструмент администрирования на сервере веб-приложений.

Проверка установки IBM Global Security Kit в Windows

Проверьте состояние установки IBM Global Security Kit (GSKit) для того чтобы убедиться, что установка в Windows выполнена успешно.

Процедура

1. Откройте файл `gskitinst.log`.

Операционная система	Путь по умолчанию:
Windows	C:\Program Files\IBM\ldap\V6.3.1\var

2. Убедитесь, что создан указанный ниже каталог: `C:\Program Files\IBM\gsk8`
3. Проверьте, содержит ли файл `gskitinst.log` значение `EXIT 0`. Если установка IBM Global Security Kit выполнена успешно, то указывается значение `0`, иначе указывается ненулевое значение.
4. Необязательно: Если установка IBM Global Security Kit не выполнена успешно, сведения об ошибках сохраняются в файле `C:\Program Files\IBM\ldap\V6.3.1\var\gskitinsterr.log`.

Проверка установки IBM Global Security Kit в AIX, Linux, Solaris и HP-UX

Проверьте установку IBM Global Security Kit (GSKit) installation, чтобы убедиться, что установка выполнена успешно.

Об этой задаче

После установки IBM Global Security Kit следует убедиться, что пакеты имеют требуемый уровень. Можно получить номер версии IBM Global Security Kit.

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте командную строку и запустите следующую команду:

Операционная система	Выполняемая команда:
AIX	<code>lspp -al grep -i gsk</code>
Linux	<code>rpm -qa grep -i gsk</code>
Solaris	<code>pkginfo grep gsk</code> <code>pkgparam пакет VERSION</code>
HP-UX	<code>swlist grep -i gsk</code>

Глава 14. Обновление экземпляра предыдущей версии

Для того чтобы преобразовать существующий экземпляр в функциональный экземпляр последнего выпуска и продолжить работу с существующими файлами конфигурации, необходимо обновить экземпляр.

Процедура обновления сохраняет изменения в определениях схем, изменения в файлах конфигурации и данные экземпляра сервера каталогов.

Обновление экземпляра из предыдущей версии требует выполнения следующего процесса:

1. Выполните установку IBM Security Directory Server.
2. Обновите существующий экземпляр из предыдущей версии.

Клиент и сервер IBM Security Directory Server версии 6.3.1 могут сосуществовать с серверами и клиентами версий 6.0, 6.1, 6.2 и 6.3.

Можно непосредственно обновить экземпляры сервера каталогов следующих версий до IBM Security Directory Server версии 6.3.1:

- IBM Security Directory Server версии 6.3
- IBM Security Directory Server версии 6.2
- IBM Security Directory Server версии 6.1

Важное замечание: Непосредственное обновление экземпляров IBM Security Directory Server версии 6.0 до IBM Security Directory Server версии 6.3.1 не поддерживается. Можно обновить экземпляры версии 6.0 до версий 6.1, 6.2 или 6.3, а затем до 6.3.1.

Можно обновить экземпляр предыдущей версии следующими способами:

- Обновление экземпляра, существующего на локальном компьютере, с помощью команды IBM Security Directory Server Инструмента администрирования экземпляра (**idsxinst**) или **idsimigr**. Нельзя удалять экземпляр сервера каталогов, который требуется обновить. Для экземпляра полного сервера каталогов нельзя нарушать конфигурацию базы данных. Обновление не поддерживается, если экземпляр сервера каталогов удален или удалена конфигурация его базы данных.
- Обновление экземпляра на удаленном компьютере с помощью команд **migbkup** и **idsimigr**. Дополнительная информация приведена в разделе “Обновление удаленного экземпляра предыдущей версии с помощью команды **idsimigr**” на стр. 94.

Внимание: Необходимо выполнить резервное копирование схемы, файлов конфигурации и баз данных экземпляра, для восстановления после каких-либо неполадок обновления.

Обновление базы данных DB2

При выполнении обновления экземпляра связанная с ним база данных DB2 также обновляется, если версия DB2 ниже версии, поддерживаемой IBM Security Directory Server версии 6.3.1. Команда **idsdbmigr** выполняется внутренне для обновления базы данных DB2.

Важное замечание: Непосредственное обновление экземпляра сервера каталогов с DB2 версии 9.1 до экземпляра с DB2 версии 10.1.0.2 или выше не поддерживается. Обновить экземпляр сервера каталогов с DB2 версии 9.1 до экземпляра с DB2 версии 10.1.0.2 или выше можно одним из следующих способов:

- Обновите экземпляр с DB2 версии 9.1 до экземпляра с DB2 версии 9.5, а затем до экземпляра с DB2 версии 10.1.0.2 или выше.
- Обновите экземпляр с DB2 версии 9.1 до экземпляра с DB2 версии 9.7, а затем до экземпляра с DB2 версии 10.1.0.2 или выше.

Обновление установки клиента

Если установлены только компоненты клиента с помощью программы установки клиента IBM Security Directory Server, то обновление не требуется. Клиенты версий 6.0, 6.1, 6.2 и 6.3 могут сосуществовать с сервером и клиентом 6.3.1.

Настройка среды перед обновлением экземпляра

Перед обновлением существующего экземпляра необходимо настроить среду сервера каталогов.

Прежде чем начать

Перед настройкой среды вы должны выполнить следующие задачи:

- Откройте установочный носитель IBM Security Directory Server.
- Установите IBM Security Directory Server версии 6.3.1. См. раздел “Запуск установки” на стр. 28.
- Войдите в систему от лица пользователя root при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Процедура

1. Убедитесь, что операционная система, в которой находится предназначенный для обновления экземпляр, поддерживается IBM Security Directory Server, версии 6.3.1.
2. Убедитесь, что экземпляр предыдущей версии, который вы собираетесь обновить, успешно запускается. Если вы хотите обновить экземпляр сервера каталогов, то вы должны настроить базу данных, если она еще не настроена.

Внимание: Обновление сервера проху или сервера каталогов не поддерживается, если сервер не удастся запустить.

3. Создайте резервную копию обновляемого экземпляра в автономном режиме. В случае экземпляра сервера каталогов создайте резервную копию баз данных DB2 и параметров DB2. Дополнительная информация приведена в описании команды **idsdbback** в *Справочнике по командам*.
4. Для создания резервной копии схемы и файлов конфигурации выполните команду **migbkup**:

Операционная система	Выполняемая команда:
Microsoft Windows	migbkup.bat диск\idsslapd-экземпляр резервный-каталог
AIX, Linux и Solaris	migbkup домашний-каталог-пользователя/ idsslapd-экземпляр резервный-каталог

Команда **migbkup** расположена в подкаталоге **tools** установочного носителя IBM Security Directory Server. Если вы выполнили установку IBM Security Directory

Server, то команда **migbkup** находится в папке `sbin` установочного каталога IBM Security Directory Server. Следующие каталоги служат установочными каталогами по умолчанию в соответствующих операционных системах:

Microsoft Windows

`C:\Program Files\IBM\ldap\V6.3.1`

AIX и Solaris

`/opt/IBM/ldap/V6.3.1`

Linux `/opt/ibm/ldap/V6.3.1`

Команда **migbkup** сохраняет резервную копию следующих файлов:

- `ibmslapd.conf`
- `V3.config.at`
- `V3.config.oc`
- `V3.ibm.at`
- `V3.ibm.oc`
- `V3.system.at`
- `V3.system.oc`
- `V3.user.at`
- `V3.user.oc`
- `V3.modifiedschema`
- `V3.ldapsyntaxes`
- `V3.matchingrules`
- `ibmslapdcfg.ksf`
- `ibmslapddir.ksf`
- `perftune_stat.log`
- `perftune_input.conf`
- `ibmdiradmService.cmd` (для Windows)
- `ibmslapdService.cmd` (для Windows)

Команда **migbkup** создает следующие файлы:

- `db2info` содержит путь и версию DB2, используемую экземпляром сервера каталогов. Команда **idsimigr** или Инструмент администрирования экземпляра использует этот файл для обновления экземпляра и базы данных DB2, когда вы обновляете экземпляр сервера каталогов. В случае экземпляра сервера проху этот файл недоступен.
 - `platforminfo` содержит информацию об операционной системе и типе процесса.
5. Если вы вручную изменили файл `V3.modifiedschema` обновляемого экземпляра, то файл не должен содержать повторяющихся идентификаторов объектов (OID) для классов объектов и атрибутов. Если файл содержит повторяющиеся OID, то они не сохраняются во время обновления. Если файлы схемы содержат повторяющиеся OID, то OID в `V3.modifiedschema` сохраняются. Если файлы схемы не содержат атрибутов или классов объектов, то запустить административный сервер и процесс `idsslapd`, возможно, не удастся. В этом случае вы должны вручную добавить недостающие атрибуты и классы объектов в файлы схемы, прежде чем запускать серверы.
 6. Если вы настроили экземпляр с пользовательскими файлами схемы, скопируйте файлы вручную в каталог резервной копии. Когда вы сохраняете файлы схемы и конфигурации, команда **migbkup** сохраняет резервную копию пользовательских файлов схемы. Однако эти файлы схемы нельзя будет использовать, если вы обновите экземпляр.

Дальнейшие действия

После настройки среды запустите команду **idsimigr** или Инструмент администрирования экземпляра, чтобы обновить предыдущую версию экземпляра. Для обновления экземпляра воспользуйтесь одним из следующих способов:

- “Обновление экземпляра предыдущей версии с помощью команды **idsimigr**”
- “Обновление экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра” на стр. 148

Обновление экземпляра предыдущей версии с помощью команды **idsimigr**

Используйте команду **idsimigr** для обновления экземпляра сервера каталогов или экземпляра сервера Proху с предыдущей версии до текущей версии.

Прежде чем начать

Перед обновлением экземпляра с помощью команды **idsimigr** требуется выполнить следующие задачи:

- Выполните установку IBM Security Directory Server. См. раздел “Запуск установки” на стр. 28.
- Настройте среду перед обновлением экземпляра. Обратитесь к разделу “Настройка среды перед обновлением экземпляра” на стр. 90.
- Войдите в систему от лица пользователя root при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Кроме того, имеющийся на компьютере экземпляр можно обновить с помощью Инструмента администрирования экземпляра. Дополнительная информация приведена в разделе “Обновление экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра” на стр. 148.

Об этой задаче

После обновления экземпляра предыдущей версии он преобразуется в полнофункциональный экземпляр IBM Security Directory Server текущей версии.

Процедура

1. Откройте окно ввода команд.
2. Измените текущий рабочий каталог на `sbin`. В различных операционных системах используются следующие расположения по умолчанию:

Microsoft Windows

```
C:\Program Files\IBM\ldap\V6.3.1\sbin
```

AIX и Solaris

```
/opt/IBM/ldap/V6.3.1/sbin
```

Linux /opt/ibm/ldap/V6.3.1/sbin

3. Остановите процесс `ibmslapd` и сервер администрирования экземпляра, который требуется обновить.

```
ibmslapd -I экземпляр -k  
ibmdiradm -I экземпляр -k
```

4. Не удаляйте версию продукта IBM Security Directory Server, связанную с версией, которую требуется обновить.
5. Запустите команду **idsimigr** для обновления экземпляра с предыдущей версии до текущей версии IBM Security Directory Server.
`idsimigr -I экземпляр`
6. Запустите процесс `ibmslapd` и сервер администрирования экземпляра.
`ibmslapd -I экземпляр -n`
`ibmdiradm -I экземпляр`
7. Создайте резервную копию экземпляра без подключения. Обратитесь к разделу “Резервное копирование сервера каталогов” на стр. 190.

Обновление экземпляра предыдущей версии на другом компьютере

Можно обновить существующий экземпляр предыдущей версии, который находится на компьютере, до более поздней версии на другом компьютере.

Может потребоваться обновить существующий экземпляр удаленно по одной из следующих причин:

- Операционная система на компьютере, на котором находится экземпляр предыдущей версии, может не поддерживаться IBM Security Directory Server версии 6.3.1. Вы можете не захотеть обновлять или изменять операционную систему на компьютере.
- Если требуется установить IBM Security Directory Server версии 6.3.1 на компьютере с операционной системой, которая отличается от операционной системы, в которой существует предыдущая версия. Однако, вы хотите создать экземпляр с информацией, совпадающей с существующим экземпляром предыдущей версии. Например, существующий экземпляр предыдущей версии находится в системе AMD64/EM64T Linux, но вы хотите иметь сервер 6.3.1 в системе AIX. В таком случае две операционные системы должны иметь одинаковый тип порядка байтов. Если первый компьютер имеет прямой порядок байтов, вторая система также должна иметь прямой порядок байтов. Тип порядка байтов связан с порядком битов, используемым для представления данных в памяти. Если операционные системы имеют разный тип порядка байтов, обновление экземпляра не поддерживается.

Процедура удаленного обновления аналогична процедуре обновления на том же компьютере. Исключение состоит в том, что необходимо скопировать файлы резервной копии с данного компьютера на тот компьютер, где устанавливается IBM Security Directory Server версии 6.3.1.

Примечание: При обновлении удаленного экземпляра с компьютера, который участвует в репликации, выполните следующие действия:

- Включите репликацию с исходной системой в качестве поставщика.
- Включите репликацию с целевой системой в качестве приемника.

Репликация обеспечивает занесение обновлений в очереди и возможность их копирования после подключения целевой системы. Необходимо включить репликацию перед резервным копированием экземпляра в исходной системе.

Поддерживаемые операционные системы для обновления удаленного экземпляра

Для обновления удаленного экземпляра в целевой операционной системе необходимо определить исходную и целевую операционные системы для экземпляра.

Таблица 37. Поддерживаемые исходные и целевые операционные системы для удаленного обновления экземпляра

ОС: исходная система (IBM Security Directory Server 6.3 или более ранней версии) ↓	Операционная система: целевая система (IBM Security Directory Server 6.3.1)								
	Intel Windows (32-разр. версия)	AMD64/ EM64T Windows	System x Linux (32-разр. версия)	AMD64/ EM64T Linux	System i и System p Linux	System z Linux	AIX	Solaris SPARC	Solaris X64
32-разр. система Windows на базе Intel	✓	✓	✓	✓					✓
AMD/ EM64T Windows	✓	✓	✓	✓					✓
System x Linux (32-разр. версия)	✓	✓	✓	✓					✓
AMD/ EM64T Linux	✓	✓	✓	✓					✓
System i и System p Linux					✓	✓	✓	✓	
System z Linux					✓	✓	✓	✓	
AIX					✓	✓	✓	✓	
Solaris SPARC					✓	✓	✓	✓	
Solaris X64	✓	✓	✓	✓					✓

Обновление удаленного экземпляра предыдущей версии с помощью команды `idsimigr`

Используйте команду `idsimigr` с параметром `-u` для обновления удаленного экземпляра сервера каталогов или сервера Проху с предыдущей версии до версии 6.3.1.

Прежде чем начать

Перед обновлением экземпляра с помощью команды `idsimigr` с указанием параметра `-u` требуется выполнить следующие задачи:

- Настройте среду перед обновлением экземпляра. См. “Настройка среды перед обновлением экземпляра” на стр. 90.

- Войдите в систему от лица пользователя root при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Кроме того, можно обновить удаленный экземпляр с помощью файлов резервного копирования с использованием Инструмента администрирования экземпляров. Дополнительная информация приведена в разделе “Обновление удаленного экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра” на стр. 150.

Об этой задаче

После обновления команда **idsimigr** создаст на компьютере экземпляр 6.3.1 с информацией из удаленного экземпляра.

Процедура

1. Создайте резервную копию экземпляра сервера каталогов, расположенного на удаленном сервере, с помощью команды **idsdb2ldif**.

Важное замечание: Если выполняется обновление экземпляра сервера Proxu, не создавайте резервную копию базы данных. Сервер Proxu не содержит базу данных, которая с ним связана.

```
idsdb2ldif -I экземпляр -o inst_out.ldif
```

Дополнительная информация о команде **idsdb2ldif** приведена в *Справочнике по командам*.

2. Выполните установку IBM Security Directory Server на компьютере, на котором требуется обновить удаленный экземпляр. См. “Запуск установки” на стр. 28.
3. Для резервного копирования файлов схемы и конфигурации удаленного экземпляра запустите команду **migbkup** той версии, до которой требуется провести обновление:

Операционная система	Выполняемая команда:
Microsoft Windows	migbkup.bat диск\idsldapd-экземпляр резервный-каталог
AIX, Linux и Solaris	migbkup домашний-каталог-пользователя/idsldapd-экземпляр резервный-каталог

Команда **migbkup** расположена в подкаталоге **tools** установочного носителя IBM Security Directory Server.

4. Скопируйте резервный каталог резервный-каталог, созданный с помощью **migbkup**, с удаленного компьютера на компьютер с IBM Security Directory Server.
5. Необязательно: Скопируйте файл резервной копии базы данных **inst_out.ldif** с удаленного компьютера на компьютер с IBM Security Directory Server.
6. Запустите команду **idsimigr** с параметром **-u** для создания экземпляра с данными резервной копии удаленного экземпляра.

```
idsimigr -u резервный-каталог
```
7. Укажите базу данных, суффикс, DN и пароль администратора для экземпляра сервера каталогов.

Важное замечание: Если выполняется обновление экземпляра сервера Proxu, не запускайте команду **idscfgdb** для настройки базы данных.

```
idscfgdb -I экземпляр
-a ИД-администратора-базы-данных
-w пароль-администратора-базы-данных
-t база-данных
-l расположение-базы-данных
idscfgsuf -I экземпляр -s суффикс
idsdnpw -I экземпляр -u DN-администратора
-r пароль-администратора
```

8. Необязательно: Выполните команду **idsldif2db** для импорта файла резервной копии базы данных `inst_out.ldif` на обновленный экземпляр сервера каталогов.
9. Запустите процесс `ibmslapd` и сервер администрирования экземпляра.

```
ibmslapd -I экземпляр -n
ibmdiradm -I экземпляр
```
10. Создайте резервную копию экземпляра. Дополнительная информация приведена в разделе “Резервное копирование сервера каталогов” на стр. 190.

Ссылки на утилиты клиента и сервера

С помощью команды **idslink** можно задать ссылки на утилиты командной строки сервера каталогов и на библиотеки.

После установки IBM Security Directory Server можно задать ссылки на утилиты клиента и сервера. Эти ссылки не создаются автоматически во время установки.

Если были настроены ссылки на утилиты предыдущей версии IBM Security Directory Server, эти ссылки продолжают действовать, если только они не были изменены. Для удаления ссылок, заданных с помощью команды `idslink`, воспользуйтесь командой **idsrmlink**.

С помощью команды **idslink** можно задать ссылки на утилиты командной строки, такие как **idsldapmodify** и **idsldapadd**, и на библиотеки, такие как `libibmldap.so`. Эти ссылки указывают на расположение, где хранятся утилиты и библиотеки IBM Security Directory Server.

Дополнительная информация о командах **idslink** и **idsrmlink** приведена в разделе *Справочник по командам*.

Глава 15. Миграция данных и решений из экземпляра предыдущей версии

Можно перенести данные каталога и/или решения, настроенные в экземпляре предыдущей версии, для использования в экземпляре версии 6.3.1.

Миграция данных DB2 из IBM DB2 Enterprise Server Edition (ESE) в IBM DB2 Workspace Server Edition (WSE)

В System x Linux (32-разрядная архитектура Intel), IBM DB2 ESE версии 9.7 или выше не поддерживается. В System x Linux, IBM Security Directory Server использует IBM DB2 WSE версии 9.7 с пакетом исправлений 6 или выше для создания и настройки базы данных.

Когда вы обновляете экземпляр версии 6.1 или 6.2 с данными до версии 6.3.1, может потребоваться выполнить удаленное обновление экземпляра. Можно обновить экземпляр версии 6.3 с DB2 WSE версии 9.7 или выше для экземпляра версии 6.3.1 с DB2 WSE версии 9.7 или выше. В System x Linux непосредственное обновление экземпляра версии 6.1 или 6.2 с DB2 ESE версии 9.1 или выше до экземпляра версии 6.3.1 с DB2 WSE версии 9.7 или выше может привести к ошибке. Более подробная информация о способе выполнения миграции базы данных DB2 ESE в DB2 WSE находится в разделе “Миграция экземпляра с базой данных DB2 ESE к экземпляру с базой данных DB2 WSE” на стр. 98.

Миграция решений сервера каталогов, основанных на IBM Security Directory Integrator

Для использования решений, которые настроены с помощью предыдущей версии экземпляра, в экземпляре 6.3.1, необходимо выполнить миграцию этих решений.

Поддерживаются следующие решения:

- Инструмент управления протоколами
- Простой протокол управления сетью (SNMP)
- Синхронизация Active Directory

Более подробная информация о решениях сервера каталогов приведена в разделе *Администрирование* документации по IBM Security Directory Server.

Для функционирования решения компьютер должен содержать IBM Security Directory Integrator версии 7.1. Более подробная информация об установке и администрировании IBM Security Directory Integrator приведена в разделе *Установка и администрирование*: <http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome>.

Если путь установки IBM Security Directory Integrator отличается от пути установки по умолчанию, установите с помощью переменной *IDS_LDAP_TDI_HOME* расположение установки IBM Security Directory Integrator. Следующие пути установки используются по умолчанию для IBM Security Directory Integrator версии 7.1 в различных операционных системах:

AIX, Linux и Solaris

`/opt/IBM/TDI/V7.1`

Windows

`C:\Program Files\IBM\TDI\V7.1`

Миграция экземпляра с базой данных DB2 ESE к экземпляру с базой данных DB2 WSE

Для миграции экземпляра версии 6.1 или 6.2 с базой данных DB2 ESE к экземпляру версии 6.3.1 с базой данных DB2 WSE необходимо перенести данные из базы данных DB2 ESE в базу данных DB2 WSE.

Прежде чем начать

Перед тем как переносить данные из экземпляра предыдущей версии в экземпляр версии 6.3.1, выполните следующие задачи:

- Установите IBM Security Directory Server версии 6.3.1 с IBM DB2 WSE. См. раздел “Запуск установки” на стр. 28.
- Настройте среду перед обновлением экземпляра. Обратитесь к разделу “Настройка среды перед обновлением экземпляра” на стр. 90.
- Войдите в систему от лица пользователя root при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Процедура

1. Остановите экземпляр сервера каталогов, из которого необходимо перенести данные каталога.
2. С помощью команды **migbkup**, поставляемой с IBM Security Directory Server версии 6.3.1, создайте резервную копию экземпляра. Обратитесь к разделу “Настройка среды перед обновлением экземпляра” на стр. 90. Дополнительная информация о команде **migbkup** приведена в *Справочнике по командам*.
3. Создайте резервную копию базы данных экземпляра сервера каталогов, из которого требуется перенести данные. Для создания резервной копии базы данных экземпляра dsrdbm01 выполните следующие действия:
 - a. Переключите пользовательский контекст на владельца экземпляра DB2.
`su - dsrdbm01`
 - b. Выполните команду `db2profile` для этого пользователя.
`sqllib/db2profile`
 - c. Создайте резервную копию базы данных DB2 для экземпляра.
`db2 backup database dsrdbm01 to каталог-резервной-копии-базы-данных`

У владельца базы данных должны быть права доступа для чтения, записи и выполнения в каталоге `каталог-резервной-копии-базы-данных`.
 - d. Если для экземпляра сервера каталогов настроена база данных протокола изменений, создайте ее резервную копию.
`db2 backup db ldaplog to каталог-резервной-копии-протокола-изменений`

У владельца базы данных должны быть права доступа для чтения, записи и выполнения в каталоге `каталог-резервной-копии-протокола-изменений`.
 - e. Выполните команду `exit` для выхода из пользовательского контекста.
4. Удалите экземпляр сервера каталогов с базой данных. Дополнительная информация об удалении экземпляра с базой данных приведена в разделе “Удаление экземпляра с помощью утилиты командной строки” на стр. 165.
5. Перейдите в подкаталог `sbin` установочного каталога IBM Security Directory Server версии 6.3.1.

6. Для использования каталога резервной копии экземпляра для удаленного обновления версии экземпляра введите команду **idsimigr** следующего формата:


```
idsimigr -I dsrdbm01 -u расположение-резервной-копии-экземпляра
-l каталог-экземпляра -n
```
7. Для настройки экземпляра введите команду **idscfgdb** следующего формата:


```
idscfgdb -I dsrdbm01 -a владелец-базы-данных -w пароль
-t dsrdbm01 -l каталог-экземпляра -n
```
8. Если для экземпляра была настроена база данных протокола изменений, то необходимо настроить базу данных протокола изменений для экземпляра:


```
idscfgchlg -I dsrdbm01 -n
```
9. Восстановите базу данных из образа резервной копии. Для восстановления базы данных экземпляра dsrdbm01 выполните следующие действия:
 - a. Переключите пользовательский контекст на владельца экземпляра DB2.


```
su - dsrdbm01
```
 - b. Восстановите базу данных DB2 для экземпляра.


```
db2 restore database dsrdbm01 from каталог-резервной-копии-базы-данных
replace existing
```
 - c. Если для экземпляра сервера каталогов была настроена база данных протокола изменений, восстановите ее.


```
db2 restore db ldaplog from каталог-резервной-копии-протокола-изменений
```
 - d. Выполните команду `exit` для выхода из пользовательского контекста.
10. Для каталогизации восстановленной базы данных введите следующие команды:


```
su - dsrdbm01
db2 uncatalog database dsrdbm01
db2 catalog database dsrdbm01 as dsrdbm01 authentication server
exit
```
11. Для каталогизации восстановленной базы данных протокола изменений введите следующие команды:


```
su - dsrdbm01
db2 uncatalog database ldaplog
db2 catalog database ldaplog as ldaplog authentication server
exit
```
12. Запустите сервер каталогов и сервер администрирования.


```
ibmslapd -I dsrdbm01 -n -t
ibmdiradm -I dsrdbm01
```

Перенос решения управления протоколами

Решение управления протоколами, настроенное с экземпляром предыдущей версии, можно перенести в экземпляр версии 6.3.1.

Прежде чем начать

Перед тем как переносить решение управления протоколами из экземпляра предыдущей версии в экземпляр версии 6.3.1, выполните следующие задачи:

- Установите IBM Security Directory Server версии 6.3.1. См. раздел “Запуск установки” на стр. 28.
- Установите IBM Security Directory Integrator версии 7.1 (если этот продукт еще не установлен на компьютере).
- Войдите в систему от лица пользователя root при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Процедура

1. Создайте резервную копию файла `solution.properties`, который находится в каталоге *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt* для существующего экземпляра сервера каталогов.
2. Обновите предыдущую версию экземпляра до версии 6.3.1. Обратитесь к разделу Глава 14, “Обновление экземпляра предыдущей версии”, на стр. 89.
3. Удалите все содержимое каталога *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt* для обновленного экземпляра.
4. Если версия IBM Security Directory Integrator ниже чем 7.1, установите IBM Security Directory Integrator версии 7.1.
5. Переключите пользовательский контекст на владельца экземпляра сервера каталогов.
`su - владелец-экземпляра`
6. Скопируйте следующие файлы:
 - a. Скопируйте файлы и подкаталоги из каталога *установочный-каталог-Directory-Integrator-v7.1/etc* в каталог *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt*.
 - b. Скопируйте файлы и подкаталоги из каталога *установочный-каталог-Directory-Integrator-v7.1/serverapi* в каталог *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt*.
 - c. Скопируйте файл *установочный-каталог-Directory-Integrator-v7.1/idisrv.sth* в каталог *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt*.
 - d. Скопируйте файл *установочный-каталог-Directory-Integrator-v7.1/testserver.jks* в каталог *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt*.
7. Создайте каталог с именем `logs` в каталоге *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt*.
8. Добавьте запись `systemqueue.on=false` в конец файла *каталог-экземпляра-DS/idsslapd-экземпляр/etc/logmgt/solutions.properties*.
9. Если установочный каталог IBM Security Directory Integrator версии 7.1 отличается от каталога по умолчанию, то задайте переменную `IDS_LDAP_TDI_HOME`, указав в ней установочный каталог.
10. Запустите решение управления протоколами.

Перенос решения SNMP

Решение Простого протокола управления сетью (SNMP), настроенное с экземпляром предыдущей версии, можно перенести в экземпляр версии 6.3.1.

Прежде чем начать

Перед тем как переносить решение SNMP из экземпляра предыдущей версии в экземпляр версии 6.3.1, выполните следующие задачи:

- Установите IBM Security Directory Server версии 6.3.1. См. раздел “Запуск установки” на стр. 28.
- Установите IBM Security Directory Integrator версии 7.1 (если этот продукт еще не установлен на компьютере).
- Войдите в систему от лица пользователя `root` при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Процедура

1. Создайте резервную копию каталога `snmp`, который находится в установочном каталоге IBM Security Directory Server, связанном с существующим экземпляром предыдущей версии.
2. Обновите предыдущую версию экземпляра до версии 6.3.1. Обратитесь к разделу Глава 14, “Обновление экземпляра предыдущей версии”, на стр. 89.
3. Замените файл `/idstools/snmp/idssnmp.conf`, который находится в установочном каталоге IBM Security Directory Server версии 6.3.1, файлом `/idstools/snmp/idssnmp.conf` из установочного каталога IBM Security Directory Server предыдущей версии.
4. Замените файл `/idstools/snmp/idssnmp.properties`, который находится в установочном каталоге IBM Security Directory Server версии 6.3.1, файлом `/idstools/snmp/idssnmp.properties` из установочного каталога IBM Security Directory Server предыдущей версии.
5. Замените файл `/idstools/snmp/IBM-DIRECTORYSERVER-MIB`, который находится в установочном каталоге IBM Security Directory Server версии 6.3.1, файлом `/idstools/snmp/IBM-DIRECTORYSERVER-MIB` из установочного каталога IBM Security Directory Server предыдущей версии.
6. Замените файл `/idstools/snmp/INET-ADDRESS-MIB`, который находится в установочном каталоге IBM Security Directory Server версии 6.3.1, файлом `/idstools/snmp/INET-ADDRESS-MIB` из установочного каталога IBM Security Directory Server предыдущей версии.
7. Если установочный каталог IBM Security Directory Integrator версии 7.1 отличается от каталога по умолчанию, то задайте переменную `IDS_LDAP_TDI_HOME`, указав в ней установочный каталог.
8. Запустите решение SNMP.

Перенос решения синхронизации Active Directory в новую версию

Решение синхронизации Active Directory, настроенное с экземпляром предыдущей версии, можно перенести в экземпляр версии 6.3.1.

Прежде чем начать

Перед тем как переносить решение синхронизации Active Directory из экземпляра предыдущей версии в экземпляр версии 6.3.1, выполните следующие задачи:

- Установите IBM Security Directory Server версии 6.3.1. См. раздел “Запуск установки” на стр. 28.
- Установите IBM Security Directory Integrator версии 7.1 (если этот продукт еще не установлен на компьютере).
- Войдите в систему от лица пользователя `root` при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Начиная с IBM Security Directory Server версии 6.3.1, решение синхронизации Active Directory устарело. В качестве замены следует использовать решение LDAPSync.

Процедура

1. Обновите предыдущую версию экземпляра до версии 6.3.1. Обратитесь к разделу Глава 14, “Обновление экземпляра предыдущей версии”, на стр. 89.
2. Создайте экземпляр сервера каталогов. Обратитесь к разделу “Создание экземпляра с помощью инструмента администрирования экземпляра” на стр. 134.

3. Настройте экземпляр сервера каталогов для синхронизации Active Directory. Обратитесь к разделу “Синхронизация Active Directory” на стр. 215.
4. Перед тем как обновлять экземпляр, восстановите изменения в файле `каталог-экземпляра-DS/idsslapd-экземпляр/etc/tdisoldir/solution.properties`.

Примечание: Новый файл `solution.properties` нельзя заменить старым файлом, так как в этом случае выполнить синхронизацию Active Directory не удастся. Формат файла `solution.properties`, который создается при выполнении команды `idsadsconf`, отличается от формата старого файла.

5. Запустите решение синхронизации Active Directory. Дополнительная информация о команде `idsadsrun` приведена в *Справочнике по командам*.

Миграция конфигурации предыдущей версии Web Administration Tool

Можно перенести конфигурацию предыдущей версии Web Administration Tool для продолжения использования тех же параметров в более поздней версии Web Administration Tool.

Для того чтобы выполнить миграцию конфигурации Web Administration Tool предыдущей версии с помощью команды `idswmigr`, должны быть выполнены следующие условия:

1. В системе установлена предыдущая версия Web Administration Tool.
2. В системе установлена предыдущая версия встроенного WebSphere Application Server.
3. Предыдущая версия Web Administration Tool развернута в предыдущей версии встроенного WebSphere Application Server.
4. Установите Web Administration Tool, предоставленный с IBM Security Directory Server версии 6.3.1.
5. Установите встроенный WebSphere Application Server, предоставленный с IBM Security Directory Server версии 6.3.1.
6. Не разворачивайте Web Administration Tool, предоставленный с версией 6.3.1, во встроенном WebSphere Application Server.

Поддерживается миграция Web Administration Tool следующих версий IBM Security Directory Server, развернутых в следующих версиях встроенного WebSphere Application Server:

- IBM Security Directory Server версии 6.1 и встроенный WebSphere Application Server версии 6.1.0.7 или выше
- IBM Security Directory Server версии 6.2 и встроенный WebSphere Application Server версии 6.1.0.13 или выше (в UNIX) или встроенный WebSphere Application Server версии 6.1.0.17 (в Windows) или выше
- IBM Security Directory Server версии 6.3 и встроенный WebSphere Application Server версии 7.0.0.7 или выше

При выполнении команды `idswmigr` для миграции параметров конфигурации предыдущей версии Web Administration Tool выполняются следующие операции:

1. Сохраняются файлы конфигурации для предыдущей версии Web Administration Tool.
2. Удаляется развертывание предыдущей версии Web Administration Tool из предыдущей версии встроенного WebSphere Application Server.

3. Создается резервная копия конфигурации предыдущей версии встроенного WebSphere Application Server во временном расположении, указанном вами.
4. Восстанавливается конфигурация предыдущей версии встроенного WebSphere Application Server в этом расположении.
5. Разворачивается Web Administration Tool текущей версии во встроенном WebSphere Application Server, предоставленном с IBM Security Directory Server версии 6.3.1.
6. Выполняется миграция файлов конфигурации предыдущей версии Web Administration Tool, и эти файлы восстанавливаются в более поздней версии встроенного WebSphere Application Server.

Примечание: Миграцию Web Administration Tool можно выполнить с помощью IBM Installation Manager только в том случае, если исходная основная версия встроенного WebSphere Application Server меньше основной версии нового встроенного WebSphere Application Server.

idswmigr

Команда **idswmigr** позволяет выполнить миграцию существующей конфигурации Web Administration Tool предыдущей версии в более позднюю версию Web Administration Tool.

Описание

Для миграции существующей конфигурации Web Administration Tool предыдущей версии с помощью команды **idswmigr** должны быть выполнены следующие условия:

1. В системе должна быть установлена предыдущая версия Web Administration Tool.
2. В системе должна быть установлена предыдущая версия встроенного WebSphere Application Server.
3. В предыдущей версии WebSphere Application Server должна быть развернута предыдущая версия Web Administration Tool.
4. Установите более позднюю версию Web Administration Tool.
5. Установите более позднюю версию встроенного WebSphere Application Server.
6. Не разворачивайте Web Administration Tool более поздней версии, входящий в состав встроенного сервера WebSphere Application Server.

Формат

```
idswmigr -l temp_path [-s source_path -t target_path  
-r профайл -a приложение -v -o каталог-портов ]
```

Опции

Команда **idswmigr** принимает следующие параметры:

-a *приложение*

Указывается имя приложения. Если значение не указано, то применяется значение по умолчанию `IDSWebApp.war`.

-l *временный_каталог*

Задаёт расположение для временных файлов.

-o *каталог-портов*

Задаёт полный путь к файлу определения портов. Если значение не указано, то применяется следующий путь по умолчанию:

Windows

C:\Program Files\IBM\ldap\V6.3.1\idstools\TDSWEBPortDef.props

AIX и Solaris

/opt/IBM/ldap/V6.3.1/idstools/TDSWEBPortDef.props

Linux /opt/ibm/ldap/V6.3.1/idstools/TDSWEBPortDef.props

-r *профайл*

Задает имя профайла для приложения. Если значение не указано, то применяется значение по умолчанию TDSWebAdminProfile.

-s *исходный_каталог*

Задает исходный каталог для предыдущей версии встроенного WebSphere Application Server.

-t *целевой_каталог*

Задает установочное расположение более поздней версии встроенного WebSphere Application Server.

-v Показывает информацию о версии.

Примеры

Пример 1

Для миграции существующей конфигурации Web Administration Tool версии 6.2 до версии 6.3.1 выполните следующую команду:

```
idswmigr -l /tmp/web_migr -s /opt/ibm/ldap/V6.2/appsrv \
-t /opt/ibm/ldap/V6.3.1/appsrv -r TDSWebAdminProfile \
-a IDSWebApp.war
```

Миграция Web Administration Tool вручную

Миграцию Web Administration Tool можно выполнить вручную.

Прежде чем начать

Для миграции Web Administration Tool вручную сначала необходимо установить Web Administration Tool. Выполните инструкции по миграции Web Administration Tool вручную. В показанном примере Web Administration Tool из IBM Security Directory Server V6.3 переносится в IBM Security Directory Server V6.3.1.

В системе AIX команды миграции аналогичны командам в Linux, однако вместо пути /opt/ibm/ldap следует указать /opt/IBM/ldap.

Процедура

1. Для Windows добавьте службу WebSphere Application Server с помощью следующей команды:

```
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe" -add  
TDSWebAdmin-V6.3.1 -serverName server1 -profilePath  
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile"  
-startType automatic
```
2. Создайте резервную копию файлов Web Administration Tool из предыдущего выпуска.
 - В системе Windows эти файлы расположены в следующем каталоге:

```
C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\  
WEB-INF\classes\
```

или

```
C:\Program Files\IBM\LDAP\V6.3\appsrv\installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes
```

- В системе Linux эти файлы расположены в следующем каталоге:
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/installedApps/DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes

или

```
/opt/ibm/ldap/V6.3/appsrv/installedApps/DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
```

Из этих каталогов следует скопировать только следующие файлы:

```
security\console_passwd  
IDSSessionConfig\IDSSessionMgmt.xml  
IDSServersConfig\IDSServersInfo.xml  
IDSAppReg\IDSAppReg.xml  
IDSSearchSettings\IDSSearchMgmt.xml
```

Пример:

```
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\security\console_passwd" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\IDSSessionConfig\IDSSessionMgmt.xml" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\IDSServersConfig\IDSServersInfo.xml" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\IDSAppReg\IDSAppReg.xml" c:\BackUp  
copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\IDSSearchSettings\IDSSearchMgmt.xml" c:\BackUp
```

3. Удалите файл war из предыдущего выпуска.

- В системе Windows команда расположена в следующем каталоге:
C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat

или

```
C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\wsadmin.bat
```

- В системе Linux команда расположена в следующем каталоге:
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh

или

```
/opt/ibm/ldap/V6.3/appsrv/bin/wsadmin.sh  
wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
```

Пример:

```
"C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat" -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
```

4. Если запущен встроенный сервер WebSphere Application Server предыдущей версии, остановите его.

- В системе Windows команда расположена в следующем каталоге:
C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\stopServer.bat

или

C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\stopServer.bat

- В системе Linux команда расположена в следующем каталоге:
/opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/stopServer.sh

или

/opt/ibm/ldap/V6.3/appsrv/bin/stopServer.sh

Пример:

"C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\stopServer.bat" server1

5. Проверьте существование профайла на новом встроенном сервере WebSphere Application Server. Если профайл не существует, создайте новый профайл.

- В системе Windows создайте профайл с помощью следующей команды:

```
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\bin\manageprofiles.bat" -create  
-profileName TDSWebAdminProfile -profilePath "C:\Program Files\IBM\  
LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile" -templatePath  
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profileTemplates\default"  
-nodeName DefaultNode -hostName localhost -cellName  
DefaultNode -isDefault -portsFile "C:\Program Files\IBM\LDAP\V6.3.1\idstools\  
\TDSWEBPortDef.props"
```

- В системе Linux создайте профайл с помощью следующей команды:

```
/opt/ibm/ldap/V6.3.1/appsrv/bin/manageprofiles.sh -create -profileName  
TDSWebAdminProfile -profilePath "/opt/ibm/ldap/V6.3.1/appsrv/profiles/  
TDSWebAdminProfile" -templatePath "/opt/ibm/ldap/V6.3.1/appsrv/  
profileTemplates/default" -nodeName DefaultNode -hostName localhost  
-cellName DefaultNode -isDefault -portsFile "/opt/ibm/ldap/V6.3.1/idstools  
/TDSWEBPortDef.props"
```

6. Скопируйте новый файл war в каталог нового WebSphere Application Server.

- В системе Windows выполните следующую команду:

```
copy "C:\Program Files\IBM\LDAP\V6.3.1\idstools\IDSWebApp.war"  
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installableApps"
```

- В системе Linux выполните следующую команду:

```
cp "/opt/ibm/ldap/V6.3.1/idstools/IDSWebApp.war"  
"/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installableApps"
```

7. Установите новый файл WAR на новом сервере WebSphere Application Server.

- В системе Windows выполните следующую команду:

```
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin\  
\wsadmin.bat" -conntype NONE -c "$AdminApp install {C:\Program Files\  
IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\installableApps\  
IDSWebApp.war} {-configroot \"C:\Program Files\IBM\LDAP\V6.3.1\  
appsrv\config\" -node DefaultNode -usedefaultbindings -nodeployejb  
-appname IDSWebApp.war -contextroot \"IDSWebApp\"}"
```

- В системе Linux выполните следующую команду:

```
"/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh"  
-conntype NONE -c "\"$AdminApp install {/opt/ibm/ldap/V6.3.1/appsrv/  
profiles/TDSWebAdminProfile/installableApps/IDSWebApp.war}  
{-configroot \" /opt/ibm/ldap/V6.3.1/appsrv/config\"  
-node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war  
-contextroot \"IDSWebApp\"}"
```

8. Восстановите ранее сохраненные файлы конфигурации Web Administration Tool.

- В системе Windows замените следующие файлы на файлы из резервной копии:

```
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\  
classes\security\console_passwd  
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\  
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\  
classes\security\console_passwd
```

Глава 16. Развертывание Web Administration Tool вручную

Для управления и администрирования экземпляров сервера каталогов с помощью Web Administration Tool необходимо развернуть Web Administration Tool на поддерживаемом сервере веб-приложений.

Для развертывания Web Administration Tool компьютер должен содержать поддерживаемую версию сервера веб-приложений. Носитель установки IBM Security Directory Server предоставляет встроенный WebSphere Application Server версии 7.0.0.25. Можно использовать IBM Installation Manager для установки Web Administration Tool и развернуть его во встроенном WebSphere Application Server.

Если операционная система не поддерживает установку IBM Security Directory Server с помощью IBM Installation Manager, выполните установку встроенного WebSphere Application Server вручную. После установки встроенного WebSphere Application Server необходимо развернуть Web Administration Tool во встроенном WebSphere Application Server.

Если компьютер содержит поддерживаемую версию WebSphere Application Server, можно развернуть в нем Web Administration Tool.

WebSphere Application Server является средой выполнения IBM для приложений на основе Java. Дополнительная информация приведена в документации по WebSphere Application Server: <http://www-01.ibm.com/support/knowledgecenter/SSEQTP/welcome>.

Установка встроенного WebSphere Application Server вручную

Для развертывания Веб-инструмента администрирования необходимо установить на компьютере встроенный WebSphere Application Server.

Прежде чем начать

Для установки встроенного WebSphere Application Server выполните следующие действия:

1. Откройте установочный носитель IBM Security Directory Server, содержащий устанавливаемый встроенный WebSphere Application Server. Обратитесь к разделу “Подготовка носителя установки” на стр. 6.

Об этой задаче

Для развертывания Веб-инструмента администрирования с помощью команды `deploy_IDSWebApp` без параметров необходимо задать следующие значения:

1. В качестве установочного каталога встроенного WebSphere Application Server укажите подкаталог `appsrv` установочного каталога IBM Security Directory Server. Дополнительная информация об установочном каталоге IBM Security Directory Server по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.

Однако для встроенного WebSphere Application Server может быть задан любой другой установочный каталог. В этом случае для развертывания Веб-инструмента администрирования в команде `deploy_IDSWebApp` следует задать параметры `-w`, `-p`, `-r` и `-o` с соответствующими значениями.

Процедура

1. Войдите в систему с правами доступа администратора.
2. Откройте окно ввода команд.
3. Перейдите в каталог, в котором содержится устанавливаемый встроенный WebSphere Application Server.
4. Для того чтобы установить встроенный WebSphere Application Server в установочном каталоге IBM Security Directory Server по умолчанию, введите следующую команду:

Операционные системы	Выполняемая команда:
Microsoft Windows	<code>install.bat -installRoot c:\Program Files\IBM\ldap\V6.3.1\appsrv</code>
AIX и Solaris	<code>install.sh -installRoot /opt/IBM/ldap/V6.3.1\appsrv</code>
Linux	<code>install.sh -installRoot /opt/ibm/ldap/V6.3.1\appsrv</code>

Дальнейшие действия

Если на компьютере не установлен Веб-инструмент администрирования, установите его. Обратитесь к разделу Глава 12, “Установка с помощью утилит командной строки операционной системы”, на стр. 69.

Если Веб-инструмент администрирования установлен на компьютере, выполните его развертывание. Обратитесь к разделу “Развертывание Веб-инструмента администрирования во встроенном WebSphere Application Server” на стр. 111.

Порты по умолчанию для веб-инструмента администрирования

Во избежание конфликтов портов между веб-инструментом администрирования и другими приложениями следует знать порты по умолчанию, применяемые веб-инструментом администрирования.

Embedded WebSphere Application Server использует следующие значения портов по умолчанию для веб-инструмента администрирования:

- Порт HTTP 1: 12100
- Транспортный протокол HTTPS (порт 2): 12101
- Порт консоли администрирования (для администрирования WebSphere Application Server): 12104
- Порт защиты консоли администрирования (для администрирования WebSphere Application Server): 12105

Embedded WebSphere Application Server использует следующие значения портов по умолчанию для других приложений:

- Порт Bootstrap/rmi: 12102
- Порт SOAP: 12103

Другие номера портов, которые могут использоваться встроенным WebSphere Application Server: 9405, 9406, 9407, 9375, 9105, 7276, 7286, 5558, 5577, 5075, 5076.

Если возникает конфликт портов с другим приложением, которое может использовать один или несколько портов по умолчанию, выполните одно из следующих действий в зависимости от вашей среды:

- Изменить порты по умолчанию на неиспользуемые порты и запустите приложение с незанятым портом.
- Если приложением, использующее порты по умолчанию, не является важной службой или сервером, измените его номер порта и освободите порт по умолчанию.

Для того чтобы изменить номера портов по умолчанию, используемые WebSphere Application Server для приложения, необходимо задать подходящий номер порта в файле `portdef.props`. Файл `portdef.props` находится в каталоге `\appsrv\profiles\TDSWebAdminProfile\properties\` в установочном расположении IBM Security Directory Server. Дополнительная информация об установочном расположении IBM Security Directory Server по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.

Порт HTTP 1

Для того чтобы изменить порт для транспортного протокола HTTP порт 1, измените запись с номером порта 12100 на свободный номер порта.

Транспортный протокол HTTPS порт 2

Для того чтобы изменить порт для транспортного протокола HTTPS порт 2, измените запись с номером порта 12101 на свободный номер порта.

Порт Bootstrap/rmi

Для того чтобы изменить порт для порта Bootstrap/rmi, измените запись с номером порта 12102 на свободный номер порта.

Порт SOAP

Для того чтобы изменить порт для порта соединения Soap, измените запись с номером порта 12103 на свободный номер порта.

Порт консоли администрирования

Для того чтобы изменить порт для порта административной консоли, измените запись с номером порта 12104 на свободный номер порта.

Порт защиты консоли администрирования

Для того чтобы изменить порт для порта защищенной административной консоли, измените запись с номером порта 12105 на свободный номер порта.

Развертывание Веб-инструмента администрирования во встроенном WebSphere Application Server

Для работы с Веб-инструментом администрирования его необходимо развернуть на сервере веб-приложений.

Прежде чем начать

Перед тем как развертывать Веб-инструмент администрирования, необходимо выполнить следующие действия:

1. Установите пакет Веб-инструмент администрирования для своей операционной системы.
2. Установите поддерживаемую версию сервера веб-приложений.
3. Если планируется переход от существующей конфигурации Веб-инструмента администрирования предыдущей версии к более новой версии, не следует развертывать новую версию Веб-инструмента администрирования.

Об этой задаче

При развертывании Веб-инструмента администрирования команда выполняет следующие действия:

1. Удаляет более раннюю версию Веб-инструмента администрирования (если она существует).
2. Развертывает Веб-инструмент администрирования на сервере веб-приложений.
3. Запускает сервер веб-приложений.

Процедура

1. Войдите в систему с правами доступа администратора.
2. Перейдите в каталог *установочный_каталог_DS/idstools*. Каталог *установочный_каталог_DS* - это установочный каталог IBM Security Directory Server. По умолчанию в различных операционных системах применяются следующие каталоги:

Операционные системы	Стандартное расположение установки:
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX и Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Введите следующую команду:

Примечание: Если встроенный WebSphere Application Server установлен в установочном каталоге IBM Security Directory Server по умолчанию, не указывайте в команде `deploy_IDSWebApp` никаких параметров. Для просмотра информации о формате команды `deploy_IDSWebApp` введите `deploy_IDSWebApp -h`.

Операционные системы	Выполняемая команда:
Microsoft Windows	<code>deploy_IDSWebApp.bat -w путь-к-файлу-war -p установочный-каталог-was -r профайл -o файл-портов</code>
AIX, Linux и Solaris	<code>deploy_IDSWebApp -w путь-к-файлу-war -p установочный-каталог-was -r профайл -o файл-портов</code>

Результаты

Эта команда развертывает Веб-инструмент администрирования на сервере веб-приложений, который задается параметром *установочный-каталог-was*.

Дальнейшие действия

Для доступа к Веб-инструменту администрирования откройте браузер и введите адрес `http://имя-хоста:12100/IDSWebApp`. *имя-хоста* - это имя хоста или IP-адрес компьютера, на котором установлен Веб-инструмент администрирования.

Развертывание Веб-инструмента администрирования в WebSphere Application Server

Для управления приложениями на компьютере с WebSphere Application Server можно развернуть Веб-инструмент администрирования в WebSphere Application Server.

Прежде чем начать

Для развертывания Веб-инструмента администрирования в WebSphere Application Server необходимо выполнить следующие требования:

1. Установите пакет Веб-инструмент администрирования для своей операционной системы. См. раздел “Установка с помощью IBM Installation Manager” на стр. 30.
2. На компьютере должна быть установлена поддерживаемая версия WebSphere Application Server.

Об этой задаче

Установочный носитель IBM Security Directory Server содержит Веб-инструмент администрирования и встроенную версию WebSphere Application Server. Если на компьютере уже существует WebSphere Application Server, то Веб-инструмент администрирования можно развернуть в WebSphere Application Server. Для развертывания Веб-инструмента администрирования необходимо развернуть файл IDWebApp.war в подкаталоге idstools установочного каталога IBM Security Directory Server.

Процедура

1. Для входа в Административную консоль WebSphere используйте URL `http://имя-хоста-сервера-WAS:9060/ibm/console`. Вместо переменной *имя-хоста-сервера-WAS* укажите имя хоста или IP-адрес своего компьютера, на котором установлен WebSphere Application Server. Если для доступа к Административной консоли WebSphere применяется пользовательский порт, то укажите его номер вместо порта по умолчанию 9060.
2. Введите ИД и пароль пользователя. Пользователю должны быть предоставлены права доступа, необходимые для выполнения операций в WebSphere Application Server.
3. На левой панели навигации выберите **Приложение > Создать приложение**.
4. На странице **Создать приложение** выберите **Создать приложение J2EE**.
5. На странице **Путь к новому приложению** выберите одну из следующих опций в зависимости от способа доступа к Административной консоли WebSphere:
 - При доступе к Административной консоли WebSphere с локального компьютера выберите **Локальная файловая система** и в поле **Полный путь** введите путь к файлу IDWebApp.war. Путь также можно выбрать с помощью кнопки **Обзор**.
 - При доступе к Административной консоли WebSphere с удаленного компьютера выберите **Удаленная файловая система** и в поле **Полный путь** введите путь к файлу IDWebApp.war. Путь также можно выбрать с помощью кнопки **Обзор**.
6. На странице **Способ установки приложения** выберите опцию **Команда быстрого доступа** и нажмите кнопку **Далее**.
7. На странице **Выбрать опции установки** выбраны опции по умолчанию.
8. Нажмите кнопку **Далее**.
9. На странице **Связать модули с сервером** можно связать модули с серверами, указанными в поле **Кластеры и серверы**.
 - a. Включите переключатель для требуемого модуля и нажмите кнопку **Применить**.
 - b. После завершения связывания нажмите кнопку **Далее**.
10. На странице **Связать виртуальные хосты с веб-модулями** можно связать веб-приложение с конкретными виртуальными серверами. При наличии

нескольких виртуальных хостов серверу для выбора правильного модуля требуется информация о среде WebSphere. В этом примере для выбора доступен вариант default_host.

11. Нажмите кнопку **Далее**.
12. На странице **Связать корневые контексты с веб-модулями** укажите в соответствующем поле корневой контекст /IDSWebApp.
13. Будет показана сводка, содержащая выбранные опции.
14. Нажмите кнопку **Готово**. Начнется установка приложения. Будет показан обзор установки.
15. Для сохранения изменений в главной конфигурации нажмите кнопку **Сохранить**.
16. На левой панели навигации выберите **Приложения > Типы приложений > Приложения WebSphere**.
17. На странице **Приложения J2EE** включите переключатель рядом с IDSWebApp_war и нажмите кнопку **Запустить**.
18. Запустите Веб-инструмент администрирования.
19. Для доступа к Веб-инструменту администрирования откройте браузер и введите следующий адрес:
 - Для незащищенного доступа (HTTP): `http://имя-хоста-сервера-WAS:9080/IDSWebApp`.
 - Для защищенного доступа (HTTPS): `https://имя-хоста-сервера-WAS:9443/IDSWebApp`

Порт 9080 - это порт HTTP по умолчанию для WebSphere Application Server, а порт 9443 - порт HTTPS по умолчанию. Если для WebSphere Application Server не настроены эти порты, задайте номер соответствующего порта. Если для WebSphere Application Server настроена глобальная или административная защита, то должны быть выполнены следующие требования:

- a. Разверните Веб-инструмент администрирования в WebSphere Application Server как новый профайл.
- b. Настройте SSL для Веб-инструмента администрирования.
- c. Если Веб-инструмент администрирования невозможно развернуть в профайле, добавьте в хранилище доверенных сертификатов профайла сертификат сервера каталогов. Для идентификации клиента и сервера добавьте сертификат профайла WebSphere Application Server в хранилище доверенных сертификатов сервера каталогов.

Запуск встроенного WebSphere Application Server для использования Веб-инструмента администрирования

Запустите сервер веб-приложений, связанный с Веб-инструментом администрирования, для добавления, управления и администрирования экземпляров сервера каталогов.

Прежде чем начать

Перед запуском сервера веб-приложений, связанного с Веб-инструментом администрирования, вы должны выполнить следующие задачи:

1. Установите Веб-инструмент администрирования.
2. Разверните Веб-инструмент администрирования на поддерживаемом сервере веб-приложений.

Примечание: Если вы используете IBM Installation Manager для установки и развертывания Веб-инструмента администрирования во встроенном WebSphere Application Server, то сервер приложений будет запущен после того, как вы закончите развертывание Веб-инструмента администрирования.

Процедура

1. Для того чтобы запустить сервер приложений, связанный с Веб-инструментом администрирования, выполните одну из следующих команд, в зависимости от операционной системы:

Windows

Если сервер приложений не запущен, выполните следующую команду:
установочный_путь\idstools\bin\startWebadminApp.bat

Установочный путь по умолчанию - C:\Program Files\IBM\ldap\V6.3.1.

AIX и Solaris

/opt/IBM/ldap/V6.3.1/idstools/bin/startWebadminApp

Linux

/opt/ibm/ldap/V6.3.1/idstools/bin/startWebadminApp

2. Откройте веб-браузер.
3. Введите следующий URL в адресной строке веб-браузера:

Примечание: Если вы установили и развернули Веб-инструмент администрирования в удаленной системе, то вместо localhost укажите имя хоста или IP-адрес этой системы.

`http://localhost:12100/IDSWebApp`

Дальнейшие действия

Для управления и администрирования экземпляров сервера каталогов добавьте серверы на консоль Веб-инструмента администрирования. См. раздел “Получение доступа к Web Administration Tool”.

Получение доступа к Web Administration Tool

Для удаленного управления экземплярами сервера каталогов откройте Web Administration Tool и настройте экземпляр сервера каталогов для удаленного управления.

Прежде чем начать

Перед запуском Web Administration Tool необходимо выполнить следующие задачи:

1. Установите Веб-инструмент администрирования.
2. Разверните Веб-инструмент администрирования на поддерживаемом сервере веб-приложений.
3. Запустите сервер веб-приложений, связанный с Веб-инструментом администрирования.

Процедура

1. Для того чтобы открыть Web Administration Tool, воспользуйтесь одним из приведенных ниже вариантов:
 - Откройте веб-браузер и введите следующий адрес:
 - Для незащищенного доступа введите `http://имя-хоста:12100/IDSWebApp`.

- Для защищенного доступа введите `https://имя-хоста:12101/IDSWebApp`.
- Откройте в веб-браузере следующий файл:

Windows

Для незащищенного доступа введите *каталог-ds\idstools\bin\idswebadmin.html*. Кроме того, можно выбрать **Пуск > Все программы > IBM Security Directory Server 6.3.1 > Web Administration Tool**.

Для защищенного доступа введите *каталог-ds\idstools\bin\idswebadminssl.html*. Кроме того, можно выбрать **Пуск > Все программы > IBM Security Directory Server 6.3.1 > Web Administration Tool (защищенный)**.

AIX, Linux и Solaris

Для незащищенного доступа введите *каталог-ds/idstools/bin/idswebadmin.html*.

Для защищенного доступа введите *каталог-ds/idstools/bin/idswebadminssl.html*.

Переменная *установочный-каталог-ds* содержит установочный каталог IBM Security Directory Server. Более подробная информация о расположении по умолчанию находится в разделе “Установочные расположения по умолчанию” на стр. 27.

2. Войдите в консоль Web Administration Tool от имени администратора консоли.
 - a. В поле **ИД пользователя** введите `superadmin`.
 - b. В поле **Пароль** введите `secret`.

Примечание: После первого входа в систему необходимо изменить пароль администратора консоли.

 - c. Нажмите кнопку **Вход в систему**.
3. Для добавления сервера каталогов в консоль, выполните следующие действия:
 - a. На странице **Введение** выберите **Управление серверами консоли**.
 - b. На странице **Управление серверами консоли** нажмите кнопку **Добавить**.
 - c. В поле **Имя сервера** введите уникальный идентификатор сервера. Если значение не указано, то приложение присваивает значение `хост:порт` или `IP-адрес:порт`.
 - d. В поле **Имя хоста** введите IP-адрес или имя хоста сервера каталогов.
 - e. В поле **Порт** введите номер порта сервера.
 - f. Для того чтобы разрешить защищенное взаимодействие консоли с сервером, включите переключатель **Включить шифрование SSL**.
 - g. Для включения управляющего элемента Порт администрирования выберите **Поддержка сервера администрирования**.
 - h. В поле **Порт администрирования** введите номер порта сервера администрирования.
 - i. Для применения изменений нажмите кнопку **ОК**.
4. Для выхода из консоли Web Administration Tool нажмите кнопку **Выход**.

Завершение работы сервера веб-приложений

Прежде чем удалять Веб-инструмент администрирования, вы должны завершить работу с ним и остановить связанный с ним сервер веб-приложений.

Прежде чем начать

Перед завершением работы сервера веб-приложений, связанного с Веб-инструментом администрирования, вы должны выполнить следующие задачи:

1. Разверните Веб-инструмент администрирования на поддерживаемом сервере веб-приложений.
2. Запустите сервер веб-приложений, связанный с Веб-инструментом администрирования.

Процедура

1. Войдите в систему как пользователь root в системах UNIX и как администратор - в Windows.
2. Откройте окно ввода команд.
3. Перейдите в подкаталог bin в профайле Веб-инструмента администрирования. Следующее расположение - это установочный путь по умолчанию встроенного WebSphere Application Server, на котором развернут Веб-инструмент администрирования. Если вы указали пользовательский установочный путь для встроенного WebSphere Application Server, то должны внести соответствующие изменения.

Операционная система	Путь
Windows	C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin
AIX и Solaris	/opt/IBM/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin
Linux	/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin

4. Для того чтобы остановить сервер веб-приложений, связанный с Веб-инструментом администрирования, выполните одну из следующих команд, в зависимости от операционной системы:

Операционная система	Выполняемая команда:
Windows	stopServer.bat server1
AIX, Linux и Solaris	./stopServer server1

Примечание: В Windows завершить работу службы, связанной с сервером веб-приложений, можно также из окна **Службы**.

HTTPS со встроенным WebSphere Application Server

Для того чтобы защитить доступ через Интернет к своему приложению, можно настроить и запустить приложение в режиме HTTPS.

После развертывания Web Administration Tool во встроенном WebSphere Application Server можно запустить приложение. Можно подключиться к Web Administration Tool защищено, указав веб-адрес HTTPS и защищенный порт.

Для использования HTTPS укажите следующий веб-адрес для доступа к Web Administration Tool:

`https://имя_хоста:12101/IDSWebApp`

Для использования простого соединения укажите следующий веб-адрес для доступа к Web Administration Tool:

`http://имя_хоста:12100/IDSWebApp`

Можно также изменить файлы JKS по умолчанию с помощью сертификатов, предоставленных с сервером веб-приложений для защищенной связи SSL/TLS. Можно создать новые файлы баз данных ключей и хранилища надежных сертификатов для использования с приложением, которое развернуто во встроенном WebSphere Application Server. Файлы баз данных ключей и хранилища надежных сертификатов по умолчанию разделены и находятся в каталоге *каталог_was/profiles/TDSWebAdminProfile/etc/*. Переменная *каталог_was* — это расположение установки встроенного WebSphere Application Server. Файлом базы данных ключей является *DummyServerKeyFile.jks*, а файлом базы данных хранилища надежных сертификатов является *DummyServerTrustFile.jks*.

Если созданы файлы JKS, можно изменить файлы баз данных ключей и хранилища надежных сертификатов. Для того чтобы настроить файлы JKS, пароли и форматы файлов, добавьте или измените следующие записи (выделенные **жирным шрифтом**) в файле *WAS_HOME/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml*:

```
<keyStores xmi:id="KeyStore_DefaultNode_10"
  name="DummyServerKeyFile"
  password="{xor}CDo9Hgw="
  provider="IBMJCE"
  location="{WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerKeyFile.jks"
  type="JKS"
  fileBased="true"
  hostList=""
  managementScope="ManagementScope_DefaultNode_1"/>
<keyStores xmi:id="KeyStore_DefaultNode_11"
  name="DummyServerTrustFile"
  password="{xor}CDo9Hgw="
  provider="IBMJCE"
  location="{WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerTrustFile.jks"
  type="JKS"
  fileBased="true"
  hostList=""
  managementScope="ManagementScope_DefaultNode_1"/>
```

Свертывание Веб-инструмента администрирования во встроенном WebSphere Application Server

Для того чтобы заменить существующую версию Веб-инструмента администрирования (файл *IDSWebApp.war*) на более позднюю версию, вы должны свернуть существующий Веб-инструмент администрирования.

Процедура

1. Запустите сервер веб-приложений, связанный с Веб-инструментом администрирования, если он остановлен. См. раздел “Запуск встроенного WebSphere Application Server для использования Веб-инструмента администрирования” на стр. 114.
2. Перейдите в каталог *установочный_каталог_DS/idstools*. Каталог *установочный_каталог_DS* - это установочный каталог IBM Security Directory Server. По умолчанию в различных операционных системах применяются следующие каталоги:

Операционные системы	Стандартное расположение установки:
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX и Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Введите следующую команду:

Примечание: Если вы установили встроенный WebSphere Application Server в пользовательском каталоге, то вы должны также указать параметры **-a**, **-w**, **-p** и **-r** в команде `deploy_IDSWebApp`. Для просмотра информации о формате команды `deploy_IDSWebApp` введите `deploy_IDSWebApp -h`.

Операционные системы	Выполняемая команда:
Microsoft Windows	<code>deploy_IDSWebApp.bat -u</code>
AIX, Linux и Solaris	<code>deploy_IDSWebApp -u</code>

Глава 17. Планирование конфигурации экземпляра

Необходимо выбрать параметры конфигурации для своего компьютера, перед тем как создавать и настраивать среду LDAP.

Для того чтобы создать экземпляр сервера каталогов или экземпляр прокси-сервера, необходимо сначала создать ИД пользователя системы, который владеет экземпляром. Для хранения сервер каталогов каталога в экземпляре сервера каталогов необходимо выбрать кодовую страницу для использования.

Установка IBM Security Directory Server и сопутствующего программного обеспечения, а также создание экземпляра сервера каталогов требует создания в системе пользователя и группы. Установка продуктов сопутствующего программного обеспечения IBM Security Directory Server, таких как IBM DB2, требует создания ИД пользователя системы для администратора DB2.

Пользователи и группы, связанные с экземпляром сервера каталогов

Для того чтобы создать экземпляр сервера каталогов или экземпляр прокси-сервера, необходимо создать пользователя и группу с требуемыми правами доступа.

Если вы хотите создать экземпляр на своем компьютере, необходимо связать экземпляр с ИД пользователя системы. Этот ИД пользователя является владельцем экземпляра сервера каталогов. Если ИД пользователя системы не существует для экземпляра, его необходимо создать. Для того чтобы создать ИД пользователя для владельца экземпляра сервера каталогов, владельца экземпляра базы данных и владельца базы данных, необходимо придерживаться правил именования. Более подробная информация о правилах именования находится в разделе “Правила присваивания имен” на стр. 122.

Для полного сервера необходимо также связать идентификаторы пользователей системы как владельцев экземпляра базы данных и самой базы данных. Для всех трех ролей можно использовать один и тот же ИД пользователя. Если используется одинаковый ИД пользователя, экземпляру сервера каталогов, экземпляру базы данных и владельцу базы данных будет присвоено одинаковое имя.

Инструмент администрирования экземпляра позволяет создать также ИД владельца экземпляра сервера каталогов при создании экземпляра сервера каталогов. Создать ИД владельца экземпляра сервера каталогов можно также с помощью команды **idsadduser**. Эта команда создает ИД пользователя, который удовлетворяет всем требованиям.

ИД пользователя, связанный с владельцем экземпляра сервера каталогов, владельцем экземпляра базы данных и владельцем базы данных, содержит следующие роли:

Владелец экземпляра сервера каталогов

На компьютере существовать ИД пользователя системы, который служит владельцем экземпляра сервера каталогов. Этот ИД будет также использоваться в качестве имени экземпляра сервера каталогов. Указанному пользователю предоставляются права на управление данным экземпляром сервера каталогов.

В системах Windows права на управление экземпляром сервера каталогов предоставляются также любому пользователю, входящему в группу Администраторы. В системах AIX, Linux и Solaris права на управление экземпляром сервера каталогов предоставляются также основной группе владельца экземпляра сервера каталогов.

Примечание: В системах AIX, Linux и Solaris в этих именах учитывается регистр символов. Для экземпляра сервера каталогов и его владельца необходимо указывать имена, в точности совпадающее с заданным ИД пользователя. Следующий пример показывает два различных имени владельца, JoeSmith и joesmith.

Владелец базы данных

ИД пользователя, который служит владельцем экземпляра базы данных, принадлежит экземпляру базы данных, настроенный для экземпляра сервера каталогов. Имя экземпляра базы данных и имя владельца экземпляра базы данных совпадают. Этот пользователь управляет экземпляром базы данных. Права на управление экземпляром базы данных предоставляются также владельцу экземпляра сервера каталогов. По умолчанию, этот ИД пользователя совпадает с ИД владельца экземпляра сервера каталогов.

Владелец базы данных

Пользователю с этим ИД принадлежит база данных, применяемая экземпляром сервера каталогов для хранения данных каталога. База данных находится в экземпляре базы данных, принадлежащем владельцу экземпляра базы данных. Экземпляр сервера каталогов применяет этот ИД пользователя и его пароль для подключения к базе данных.

Правила присваивания имен

ИД пользователя и основная группа для экземпляра сервера каталогов должны удовлетворять правилам именования.

Требования правил именования применяются к следующим ИД пользователей:

- К именам экземпляров сервера каталогов (идентификаторам пользователей, которым принадлежат экземпляры сервера каталогов).
- К именам экземпляров базы данных (идентификаторам пользователей, которым принадлежат экземпляры базы данных). Обычно этот ИД пользователя совпадает с именем экземпляра сервера каталогов.
- В системах AIX, Linux и Solaris - к основным группам ИД пользователя владельца экземпляра сервера каталогов и ИД пользователя владельца экземпляра базы данных.

Примечание: При создании ИД пользователя и группы необходимо назначить подходящие права доступа. Обратитесь к разделу “Требования к созданию пользователей и групп” на стр. 123.

ИД пользователей и групп должны удовлетворять следующим требованиям:

- Должны быть не больше 8 символов
- Не должны совпадать со следующими именами:
 - USERS
 - ADMINS
 - GUESTS
 - PUBLIC
 - LOCAL

- idslldap
- Не должны начинаться со следующих префиксов:
 - IBM
 - SQL
 - SYS
- Не должны содержать диакритические знаки
- Могут содержать следующие символы:
 - A - Z
 - a - z
 - 0 - 9
 - _ (подчеркивание)
- Должны начинаться с одной из следующих букв:
 - A - Z
 - a - z

Требования к созданию пользователей и групп

При создании пользователей и групп для своего экземпляра необходимо присвоить пользователям и группам подходящие права доступа и добавить каждого пользователя в качестве участника соответствующей группы.

После создания требуемых пользователей и групп для своего экземпляра необходимо присвоить подходящие права доступа и добавить пользователей в соответствующие группы. Необходимо соблюдать следующие требования к идентификаторам пользователей и групп:

Windows

- Добавьте владельца экземпляра сервера каталогов и владельца экземпляра базы данных в группу Администраторы.
- Задайте для допустимой локали владельца экземпляра базы данных тот язык, на котором сервер должен создавать сообщения. При необходимости войдите в систему от имени этого пользователя и измените локаль, указав нужное значение.

AIX, Linux и Solaris

- Добавьте ИД пользователя root как участника основной группы владельца экземпляра сервера каталогов и владельца экземпляра базы данных.
- Добавьте ИД пользователя root как участника группы idslldap.
- Добавьте владельца экземпляра сервера каталогов и владельца экземпляра базы данных в группу idslldap.
- Создайте домашние каталоги для владельца экземпляра сервера каталогов и для владельца экземпляра базы данных.
- Присвойте соответствующие права доступа к домашнему каталогу владельца экземпляра сервера каталогов.
 - Владелец экземпляра является владельцем экземпляра сервера каталогов.
 - Принадлежность группы для экземпляра определяется по основной группе владельца экземпляра сервера каталогов.
 - Необходимо присвоить права доступа к домашнему каталогу для чтения, записи и выполнения владельцу экземпляра сервера каталогов и его основной группе.

- Присвойте права доступа к расположению, в котором создана база данных, для чтения, записи и выполнения владельцу экземпляра сервера каталогов и его основной группе.
- Владелец экземпляра сервера каталогов и владелец экземпляра базы данных сервера каталогов могут быть разными пользователями. В таком случае владелец экземпляра сервера каталогов должен принадлежать основной группе владельца экземпляра базы данных.
- Если владелец экземпляра сервера каталогов, владелец экземпляра DB2 и владелец базы данных не являются одним и тем же лицом, все они должны быть участниками одной и той же группы.
- Сделайте сценарий оболочки Korn (/usr/bin/ksh) оболочкой входа в систему для владельца экземпляра сервера каталогов, владельца экземпляра базы данных и владельца базы данных.

Необходимо задать правильный, готовый к использованию пароль для владельца экземпляра сервера каталогов, владельца экземпляра базы данных и владельца базы данных. Пароль не должен быть просроченным или ожидающим какой-либо начальной проверки. Для проверки правильности заданного пароля можно обратиться к telnet компьютера и войти в систему с ИД пользователя и паролем.

При настройке базы данных в качестве расположения базы данных можно выбрать домашний каталог владельца экземпляра базы данных. Если будет выбрано другое расположение, в домашнем каталоге владельца экземпляра базы данных должно быть 3-4 МБ свободного пространства. DB2 создает связи и добавляет файлы в домашнем каталоге владельца экземпляра базы данных даже в том случае, если сама база данных хранится в другом месте. Если в домашнем каталоге владельца экземпляра базы данных недостаточно свободного пространства, можно добавить дополнительное пространство или изменить домашний каталог.

Примеры

Для создания владельца экземпляра, отвечающего требованиям к владельцу экземпляра сервера каталогов, можно запустить команду **idsadduser**. Команда **idsadduser** находится в каталоге sbin внутри установочного расположения IBM Security Directory Server.

Пример 1:

Для того чтобы создать учетную запись пользователя в AIX, Linux или Solaris со следующими значениями, введите команду **idsadduser**:

- Имя пользователя: JoeSmith
 - Основная группа: employees
 - Домашний каталог: /home/joe (в Solaris - /export/home/joe)
 - Пароль: joespw
- ```
idsadduser -u JoeSmith -g employees -l /home/joe -w joespw
```

### Пример 2:

Для того чтобы создать учетную запись пользователя как участника группы Администраторы в Windows со следующими значениями, введите команду **idsadduser**:

- Имя пользователя: JoeSmith
  - Пароль: joespw
- ```
idsadduser -u JoeSmith -w joespw
```

Планирование настройки

Для среды сервера каталогов необходимо определить, какой тип данных планируется сохранять, какую структуру данных и защиту данных требуется настроить.

Перед настройкой и заполнением базы данных необходимо принять соответствующие решения и выполнить следующее:

Определить тип данных, применяемый для хранения на сервере каталогов

Необходимо выбрать схему для использования на сервере каталогов и тип данных, применяемый для хранения на сервере каталогов. С сервером каталогов поставляется стандартный набор определений типов атрибутов и определений классов объектов. Для настройки данных, возможно, потребуется добавить пользовательские определения типов атрибутов и классов объектов перед добавлением записей на сервер каталогов.

В схему можно вносить добавления и изменения после заполнения каталога данными. В некоторых случаях для изменения схемы может потребоваться выгрузка и повторная загрузка данных.

Выбрать кодовую страницу для использования

Необходимо выбрать способ создания базы данных: с помощью локальной кодовой страницы или с помощью универсального набора символов (UTF-8). Выбор локальной кодовой страницы позволяет приложениям и пользователям IBM Security Directory Server получать результаты поиска так, как это предусмотрено для упорядоченной последовательности языка. Однако при использовании локальной кодовой страницы в каталоге сохраняются данные, представленные с помощью этой конкретной кодовой страницы. При выборе UTF-8 в каталоге могут храниться любые данные в формате UTF-8. За дополнительной информацией об UTF-8 обратитесь к разделу “Поддержка UTF-8” на стр. 126.

Примечание: Если требуется применять теги языка, то для базы данных необходимо использовать UTF-8.

Определить структуру иерархии для хранения данных каталога

IBM Security Directory Server хранит данные каталога в иерархической структуре. Имена записей каталога зависят от относительного положения записей в этой структуре. Важно правильно организовать логическую структуру каталога для конкретной среды LDAP. Логическая организация упрощает для клиента выбор нужной ветви для поиска информации.

Определить требования к защите данных

Для предотвращения доступа к данным каталога через незащищенные порты можно настроить для сервера каталогов защищенную связь. Дополнительная информация о защите данных приведена в разделе Администрирование документации по IBM Security Directory Server.

Определить необходимые права доступа к данным каталогов

Информация об использовании прав доступа приведена в списках управления доступом приведена в разделе Администрирование документации по IBM Security Directory Server.

Определить, требуется ли прокси-сервер

Если данные каталогов большие и в среде выполняется много операций записи, следует рассмотреть вариант использования прокси-сервера. В больших средах каталогов с большим числом операций чтения можно достичь необходимого уровня масштабирования путем настройки репликации. Перед тем как принять решение об использовании

прокси-сервера следует ознакомиться со списком поддерживаемых функций прокси-сервера в разделе Администрирование документации по IBM Security Directory Server.

Поддержка UTF-8

Сервер каталогов можно настроить для хранения документов с любым набором символов, который можно представить в UTF-8.

Благодаря формату UTF-8, продукт IBM Security Directory Server поддерживает большое число национальных языков. В протоколе LDAP версии 3, все символьные данные, которыми обмениваются клиент и сервер LDAP, передаются в формате UTF-8.

Сервер определяет типы символов, которые могут быть сохранены и по которым может быть выполнен поиск, на основании кодовой страницы, используемой для настройки базы данных. Можно указать набор символов базы данных UTF-8 или использовать локальный набор символов системы, на которой расположен сервер. Локальный набор символов выбирается с учетом локали, языка и кодовой страницы системы.

Если вы выберете формат UTF-8, то в каталоге смогут храниться любые данные в формате UTF-8. Клиенты LDAP в системе, которые поддерживают какой-либо из языков, поддерживаемых UTF-8, могут правильно получать доступ к каталогу и выполнять в нем поиск. Если клиент LDAP находится в системе с локальным набором символов, он не может правильно показать результаты, полученные с сервера в определенном наборе символов.

Если используется база данных UTF-8, ее производительность повышается, так как не требуется выполнять преобразования данных при их сохранении и извлечении из базы данных.

Примечание: Для применения тегов языка база данных должна быть создана в формате UTF-8.

Использование UTF-8 на сервере каталогов

Для того чтобы выбрать кодовую страницу для использования, необходимо понимать, как сервер каталогов использует кодовую страницу для хранения данных каталога и доступа к ним.

В базах данных UTF-8 фиксирована последовательность упорядочения, и она является двоичным порядком символов UTF-8. В базе данных UTF-8 нельзя изменить порядок символов для определенного языка.

Для того чтобы приложения или пользователи LDAP получили следующие результаты, UTF-8 может оказаться неподходящим набором символов для базы данных:

- Поиск с помощью фильтра упорядочения, такого как "name >= SMITH", и в случае, если вы ожидаете порядок, подобный вашей локали.
- Поиск с помощью управляющего элемента для сортировки результатов, и в случае, если вы ожидаете порядок, подобный вашей локали.

В таких случаях в системах сервера LDAP и его клиентов наборы символов и локали должны совпадать.

Например, база данных сервера LDAP, который настроен на испанскую локаль, возвращает результаты поиска на основании порядка символов, ожидаемого испано-язычными клиентами. Такая конфигурация ограничивает пользователей каталога только одним набором символов в этой локали и последовательностью упорядочения.

Создание файла LDIF со значениями UTF-8 с помощью утилит сервера

Можно использовать расширение `charset` для создания файла формата LDIF со значениями UTF-8.

Файл LDIF, содержащий значения UTF-8, весьма сложно создать вручную. В заголовке файла LDIF можно указать расширение, которое поддерживает имя набора символов IANA (Комитет по предоставлению адресов Internet), наряду с номером версии. Дополнительная информация о поддерживаемых наборах символов IANA приведена в разделе “Поддерживаемые наборы символов IANA” на стр. 128.

Примеры

Пример 1:

Для того чтобы утилиты сервера автоматически преобразовывали указанный набор символов в UTF-8, можно использовать `tag charset`.

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, ou=University of New Mexico, o=sample
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIH1vd
title: Associate Dean
title: [заголовок на испанском языке]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

В следующем примере все значения, указанные после имени атрибута и одного двоеточия, преобразуются из набора символов ISO-8859-1 в UTF-8. Значения после имени атрибута и двоеточия, такие как `description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIH1vd`, должны быть заданы в кодировке base 64 и иметь двоичный вид содержаться в символьных строках UTF-8. Если значения, такие как атрибут `jpegPhoto`, заданный в веб-адресе, прочитаны из файла, они должны иметь тот же формат. Для таких значений атрибутов не выполняется преобразование из указанного `charset` в UTF-8.

Пример 2:

В следующем примере файла LDIF, не содержащего тега `charset`, предполагается, что файл содержит данные в UTF-8:

```
# Файл LDIF IBM Directorysample
#
#Перед загрузкой данных нужно определить "o=sample".
# суффикс "o=IBM, c=US".

version: 1

dn: o=sample
objectclass: top
objectclass: organization
o: sample

dn: ou=Austin, o=sample
```

```
ou: Austin
objectclass: organizationalUnit
seealso: cn=Mary Smith, ou=Austin, o=sample
```

В IBM Security Directory Server файл LDIF со следующим содержимым может быть использован без информации заголовка `version: 1`:

```
# Файл LDIF IBM Directorysample
#
#Перед загрузкой данных нужно определить "o=sample".
# суффикс "o=IBM, c=US".
```

```
dn: o=sample
objectclass: top
objectclass: organization
o: sample
```

```
dn: ou=Austin, o=sample
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=sample
```

Поддерживаемые наборы символов IANA

Имена наборов символов IANA (Комитет по предоставлению адресов Internet) можно использовать в файле LDIF или с помощью интерфейса клиента C для определения набора символов данных каталога.

В приведенной ниже таблице перечислены наборы символов IANA по операционной системе, поддерживаемые продуктом IBM Security Directory Server.

Более подробная информация о наборах символов, зарегистрированных в IANA, находится на веб-сайте Наборы символов по адресу www.iana.org/assignments/character-sets.

Таблица 38. Кодировки IANA

Символ	Локаль					Кодовая страница DB2	
	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
ISO-8859-1	X	X	X	X	X	819	1252
ISO-8859-2	X	X	X	X	X	912	1250
ISO-8859-5	X	X	X	X	X	915	1251
ISO-8859-6	X	X	X	X	X	1089	1256
ISO-8859-7	X	X	X	X	X	813	1253
ISO-8859-8	X	X	X	X	X	916	1255
ISO-8859-9	X	X	X	X	X	920	1254
ISO-8859-15	X	н/д	X	X	X		
IBM437	н/д	н/д	X	н/д	н/д	437	437
IBM850	н/д	н/д	X	X	н/д	850	850
IBM852	н/д	н/д	X	н/д	н/д	852	852
IBM857	н/д	н/д	X	н/д	н/д	857	857
IBM862	н/д	н/д	X	н/д	н/д	862	862
IBM864	н/д	н/д	X	н/д	н/д	864	864
IBM866	н/д	н/д	X	н/д	н/д	866	866

Таблица 38. Кодировки IANA (продолжение)

Символ	Локаль					Кодовая страница DB2	
	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
IBM869	н/д	н/д	Х	н/д	н/д	869	869
IBM1250	н/д	н/д	Х	н/д	н/д		
IBM1251	н/д	н/д	Х	н/д	н/д		
IBM1253	н/д	н/д	Х	н/д	н/д		
IBM1254	н/д	н/д	Х	н/д	н/д		
IBM1255	н/д	н/д	Х	н/д	н/д		
IBM1256	н/д	н/д	Х	н/д	н/д		
TIS-620	н/д	н/д	Х	Х	н/д	874	874
EUC-JP	Х	Х	н/д	Х	Х	954	н/д
EUC-KR	н/д	н/д	н/д	Х	Х	970	н/д
EUC-CN	н/д	н/д	н/д	Х	Х	1383	н/д
EUC-TW	Х	н/д	н/д	Х	Х	964	н/д
Shift-JIS	н/д	Х	Х	Х	Х	932	943
KSC	н/д	н/д	Х	н/д	н/д	н/д	949
GBK	н/д	н/д	Х	Х	н/д	1386	1386
Big5	Х	н/д	Х	Х	Х	950	950
GB18030	н/д	Х	Х	Х	Х		
HP15CN	Х (с не- GB18030)						

Примечание:

- Китайский стандартный набор символов GB18030 поддерживается соответствующими исправлениями, доступными на www.oracle.com и www.microsoft.com
- В операционных системах Windows необходимо установить для переменной среды *zhCNGB18030* значение TRUE.

Символы ASCII с кодом от 33 до 126

С помощью таблицы символов ASCII определите символы, которые можно использовать в качестве начального и дополнительного ключей шифрования для экземпляра сервера каталогов.

В начальном и дополнительном ключах шифрования допустимы символы ASCII с кодом от 33 до 126.

Таблица 39. Символы ASCII с кодом от 33 до 126

Код ASCII	Символ	Код ASCII	Символ	Код ASCII	Символ
33	! восклицательный знак	34	" двойная кавычка	35	# знак номера
36	\$ знак доллара	37	% знак процентов	38	& амперсанд
39	' апостроф	40	(левая круглая скобка	41) правая круглая скобка
42	* звездочка	43	+ плюс	44	, запятая

Таблица 39. Символы ASCII с кодом от 33 до 126 (продолжение)

Код ASCII	Символ	Код ASCII	Символ	Код ASCII	Символ
45	- дефис	46	. точка	47	/ косая черта
48	0	49	1	50	2
51	3	52	4	53	5
54	6	55	7	56	8
57	9	58	: двоеточие	59	; точка с запятой
60	< знак "меньше"	61	= знак "равно"	62	> знак "больше"
63	? вопросительный знак	64	@ знак "коммерческое а"	65	A прописная буква a
66	B прописная буква b	67	C прописная буква c	68	D прописная буква d
69	E прописная буква e	70	F прописная буква f	71	G прописная буква g
72	H прописная буква h	73	I прописная буква i	74	J прописная буква j
75	K прописная буква k	76	L прописная буква l	77	M прописная буква m
78	N прописная буква n	79	O прописная буква o	80	P прописная буква p
81	Q прописная буква q	82	R прописная буква r	83	S прописная буква s
84	T прописная буква t	85	U прописная буква u	86	V прописная буква v
87	W прописная буква w	88	X прописная буква x	89	Y прописная буква y
90	Z прописная буква z	91	[левая квадратная скобка	92	\ обратная косая черта
93] правая квадратная скобка	94	^ знак вставки (диакритический знак циркумфлекс)	95	_ символ подчеркивания
96	` гравис (диакритический знак)	97	a строчная буква a	98	b строчная буква b
99	c строчная буква c	100	d строчная буква d	101	e строчная буква e
102	f строчная буква f	103	g строчная буква g	104	h строчная буква h
105	i строчная буква i	106	j строчная буква j	107	k строчная буква k
108	l строчная буква l	109	m строчная буква m	110	n строчная буква n
111	o строчная буква o	112	p строчная буква p	113	q строчная буква q
114	r строчная буква r	115	s строчная буква s	116	t строчная буква t
117	u строчная буква u	118	v строчная буква v	119	w строчная буква w
120	x строчная буква x	121	y строчная буква y	122	z строчная буква z
123	{ левая фигурная скобка	124	вертикальная черта	125	} правая фигурная скобка
126	~ тильда				

Глава 18. Создание и администрирование экземпляра

Для работы с сервером каталогов в инфраструктуре идентификации необходимо создать экземпляр сервера каталогов в соответствии со своими требованиями.

По завершении установки IBM Security Directory Server необходимо создать экземпляр сервера каталогов и задать для него отличительное имя и пароль администратора. Можно создать полноценный сервер каталогов или прокси-сервер. Для того чтобы создать экземпляр сервера каталогов или экземпляр прокси-сервера, необходимо создать на компьютере ИД пользователя системы. ИД пользователя системы представляет владельца экземпляра сервера каталогов или экземпляра прокси-сервера.

Для того чтобы сервер каталогов был полноценным, необходимо создать базу данных DB2 и настроить ее для работы с экземпляром сервера каталогов. Для создания базы данных DB2 необходимо установить на компьютере поддерживаемую версию DB2. Необходимо проверить, обновлена ли в файле `ldapdb.properties` информация о пути установки DB2 и ее версии. Дополнительная информация приведена в разделе Приложение С, “Обновление файла `ldapdb.properties` вручную”, на стр. 251.

Примечание: Если применяется IBM Security Directory Server Инструмент администрирования экземпляра (**idsxinst**) для создания полноценного экземпляра сервера каталогов, то одновременно происходит создание файла `ldapdb.properties` в домашнем каталоге экземпляра. В Windows файл `ldapdb.properties` находится в каталоге *каталог-экземпляра\idsslapd-имя-экземпляра\etc*. В AIX, Linux и Solaris этот файл находится в каталоге *каталог-экземпляра/idsslapd-имя-экземпляра/etc*.

Если создается прокси-сервер, не следует создавать и настраивать базу данных DB2 для работы с экземпляром прокси-сервера.

Инструмент администрирования экземпляра - это графический пользовательский интерфейс, с помощью которого можно создавать экземпляры сервера каталогов и управлять ими. Для того чтобы использовать Инструмент администрирования экземпляра, необходим IBM Java Development Kit. При работе с инструментом администрирования экземпляра открывается мастер, помогающий выполнить задачу.

С помощью инструмента администрирования экземпляра можно создавать, просматривать, копировать, удалять экземпляры, а также изменять о них информацию. С помощью этого инструмента можно также создавать и изменять пользователей, владеющих экземплярами сервера каталогов, и обновлять экземпляры предыдущих версий IBM Security Directory Server. С помощью инструмента администрирования экземпляра можно запускать и останавливать сервер или сервер администрирования для своих экземпляров. Кроме того, можно открыть Инструмент настройки из инструмента администрирования экземпляра.

Для создания экземпляров сервера каталогов и управления ими можно также использовать утилиты командной строки.

Запуск Инструмента администрирования экземпляра

Запустите Инструмент администрирования экземпляра, чтобы создать и управлять экземпляром сервера каталогов или экземпляром сервера проху.

Прежде чем начать

Для использования Инструмента администрирования экземпляра вы должны установить IBM Security Directory Server с Server, Proxy Server или и тем, и другим. Для запуска Инструмента администрирования экземпляра войдите в систему со следующими разрешениями:

AIX, Linux и Solaris

Войдите в систему как пользователь root.

Windows

Войдите как участник группы администраторов.

В установочном пути IBM Security Directory Server должен существовать IBM Java Development Kit. Установочный путь по умолчанию IBM Security Directory Server приведен в разделе “Установочные расположения по умолчанию” на стр. 27.

Процедура

Запустите Инструмент администрирования экземпляра одним из следующих способов:

Способы открыть Инструмент администрирования экземпляра	Выполняемая команда:
Установка компонента Server IBM Security Directory Server	На странице Итоговый отчет выберите Инструмент администрирования экземпляра (idsxinst) . Дополнительная информация приведена в разделе “Установка с помощью IBM Installation Manager” на стр. 30.
Команда <code>idsxinst</code>	<p>Windows</p> <ol style="list-style-type: none">1. Из текущего каталога перейдите в каталог <code>sbin</code> в установочном каталоге IBM Security Directory Server.2. Выполните команду <code>idsxinst</code>. <p>Примечание: Вы также можете выбрать Пуск > Все программы > IBM Security Directory Server 6.3.1 > Инструмент администрирования экземпляра.</p> <p>AIX, Linux и Solaris</p> <ol style="list-style-type: none">1. Из текущего каталога перейдите в каталог <code>sbin</code> в установочном каталоге IBM Security Directory Server.2. Выполните команду <code>idsxinst</code>. <p>Дополнительная информация об установочном пути IBM Security Directory Server приведена в разделе “Установочные расположения по умолчанию” на стр. 27.</p>

Запуск Инструмента администрирования экземпляра для обновления экземпляра

Запустите Инструмент администрирования экземпляра с параметрами, чтобы открыть Инструмент администрирования экземпляра и обновить удаленный экземпляр, содержащий резервную копию данных.

Прежде чем начать

Для обновления удаленного экземпляра необходимо, чтобы были соблюдены следующие требования:

- На компьютере должна находиться резервная копия данных экземпляра, созданного с помощью команды **migbkup**. Вы должны использовать команду **migbkup** той версии, до уровня которой вы хотите обновить удаленный экземпляр.
- Войдите в систему как пользователь root в системах AIX, Linux и Solaris. В Windows войдите в систему как администратор.

Процедура

1. Откройте окно ввода команд.
2. Из текущего рабочего каталога перейдите в каталог `sbin` в установочном каталоге IBM Security Directory Server. Дополнительная информация об установочном расположении по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.
3. Выполните команду **idsxinst** в следующем формате:

```
idsxinst -migrate каталог_резервного_копирования
```

Вместо переменной *каталог_резервного_копирования* укажите каталог, в котором хранится резервная копия данных экземпляра, созданного с помощью команды **migbkup**.

Создание экземпляра сервера каталогов

Для работы с экземпляром сервера каталогов в среде LDAP создайте экземпляр, который будет криптографически синхронизирован с существующим экземпляром, чтобы достичь оптимальной производительности

Если созданный экземпляр сервера каталогов является копией существующего экземпляра сервера каталогов, то эти экземпляры будут синхронизированы криптографически. Синхронизировать их не требуется.

Если созданный экземпляр не является копией существующего экземпляра, криптографически синхронизируйте экземпляр с существующим экземпляром. Необходимо криптографически синхронизировать экземпляр сервера для получения наилучшей производительности в следующих случаях:

- При репликации
- В среде распределенного каталога
- При импорте и экспорте данных LDIF между экземплярами сервера

Необходимо синхронизировать экземпляры сервера перед выполнением следующих операций:

- Запуск нового экземпляра сервера.

- Ввод команды **idsbulkload** для экземпляра сервера.
- Ввод команды **idsldif2db** для экземпляра сервера.

Дополнительная информация о синхронизации серверов каталогов приведена в разделе *Администрирование* документации по IBM Security Directory Server.

После создания экземпляра сервера каталогов и настройки для него базы данных DB2 создайте резервную копию экземпляра сервера каталогов. Резервное копирование необходимо выполнить для файлов конфигурации, схемы, базы данных DB2 и бумажника каталогов. Для того чтобы создать резервную копию экземпляра сервера каталогов, можно использовать команду **idsdbback**. Если впоследствии потребуется восстановить файлы бумажника, то это можно сделать с помощью команды **idsdbrestore**. Дополнительная информация о командах резервного копирования и восстановления приведена в разделе *Справочник по командам*.

Создание экземпляра с помощью инструмента администрирования экземпляра

Необходимо изучить требования вашей среды и создать экземпляр сервера каталогов на том этапе, который подходит для вашей среды.

С помощью инструмента администрирования экземпляра можно создать экземпляр несколькими способами:

- Создать экземпляр по умолчанию с стандартными параметрами. Обратитесь к разделу “Создание экземпляра сервера каталогов по умолчанию”.
- Создать экземпляр с пользовательскими параметрами. Обратитесь к разделу “Создание экземпляра сервера каталогов с пользовательскими параметрами” на стр. 136.
- Обновить экземпляр предыдущей версии IBM Security Directory Server. Обратитесь к разделу “Обновление экземпляра предыдущей версии с помощью команды **idsimigr**” на стр. 92 или “Обновление экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра” на стр. 148.
- Создать экземпляр как копию экземпляра на этом или другом компьютере. Обратитесь к разделу “Создание копии существующего экземпляра с помощью Инструмента администрирования экземпляра” на стр. 154.

Создание экземпляра сервера каталогов по умолчанию

Опция создания экземпляра по умолчанию позволяет создать экземпляр сервера каталогов с предопределенным именем экземпляра и параметрами по умолчанию.

Прежде чем начать

Для создания экземпляра по умолчанию необходимо выполнить следующие задачи:

1. Установить IBM Security Directory Server с компонентом Сервер. См. раздел “Установка с помощью IBM Installation Manager” на стр. 30.
2. Установить IBM DB2. Обратитесь к разделу “Установка с помощью IBM Installation Manager” на стр. 30.
3. Проверить, содержит ли файл `ldapdb.properties` информацию об установочном каталоге и версии DB2. Обратитесь к разделу Приложение C, “Обновление файла `ldapdb.properties` вручную”, на стр. 251.

Об этой задаче

Если на компьютере уже существует экземпляр сервера каталогов с именем экземпляра по умолчанию, то создать экземпляр сервера каталогов по умолчанию не удастся.

Экземпляр сервера каталогов по умолчанию содержит следующие параметры, которые невозможно изменить:

Таблица 40. Параметры экземпляра сервера каталогов по умолчанию

Параметры	Microsoft Windows	AIX и Linux	Solaris
Имя	dsrdbm01	dsrdbm01	dsrdbm01
Расположение экземпляра	c:\idsslapd-dsrdbm01	/home/dsrdbm01	/export/home/dsrdbm01
Имя группы	Administrators	grrdbm01	grrdbm01
DN администратора	cn=root	cn=root	cn=root
Имя базы данных	dsrdbm01	dsrdbm01	dsrdbm01

Для хранения табличных пространств DB2 экземпляра сервера каталогов по умолчанию применяется технология DMS (хранение, управляемое базой данных).

Инструмент администрирования экземпляра создает для экземпляра сервера каталогов по умолчанию суффикс `o=sample`. Другие суффиксы можно добавить позже с помощью Инструмента настройки или команды `idscfgsuf`. Дополнительная информация приведена в разделе “Настройка суффикса” на стр. 204.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. Нажмите кнопку **Создать экземпляр**.
3. В окне **Создать экземпляр сервера каталогов** выполните следующие действия:
 - a. Нажмите кнопку **Создать экземпляр по умолчанию**.
 - b. Нажмите кнопку **Далее**.
 - c. В поле **Пароль пользователя** введите пароль пользователя, которому принадлежит экземпляр сервера каталогов.
 - d. В поле **Подтверждение пароля** повторно введите пароль пользователя, которому принадлежит экземпляр сервера каталогов.
 - e. В поле **Начальный ключ шифрования** введите начальный ключ шифрования для экземпляра сервера каталогов.

Напоминание: Начальный ключ шифрования экземпляра сервера каталогов необходимо запомнить, так как он может потребоваться для других задач настройки.

Начальный ключ шифрования должен содержать только печатаемые символы ASCII ISO-8859-1 с кодами из диапазона от 33 до 126. Его длина должна быть от 12 до 1016 символов. Информация о символах, которые можно использовать, приведена в разделе “Символы ASCII с кодом от 33 до 126” на стр. 129. Начальный ключ шифрования используется сервером каталогов для создания набора личных ключей AES. Значения ключей, которые хранятся в файле ключей экземпляра сервера каталогов, применяются для шифрования и расшифровки пароля и атрибутов.

- f. В поле **Подтверждение начального ключа** введите начальный ключ шифрования для экземпляра сервера каталогов.
 - g. В поле **Пароль отличительного имени администратора** введите пароль администратора экземпляра сервера каталогов.
 - h. В поле **Подтверждение пароля** введите пароль администратора экземпляра сервера каталогов.
 - i. Нажмите кнопку **Далее**.
 - j. Проверьте информацию об экземпляре сервера каталогов по умолчанию и
 - k. Нажмите кнопку **Готово** для запуска процедуры создания экземпляра сервера каталогов по умолчанию. Откроется окно результатов, содержащее информацию протокола.
4. Проверьте информацию протокола, показанную в окне **Результаты**.
 5. Для закрытия окна **Результаты** нажмите кнопку **Закрыть**.
 6. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Результаты

Инструмент администрирования экземпляра создаст на компьютере экземпляр сервера каталогов по умолчанию с именем dsrdbm01.

Дальнейшие действия

Необходимо запустить процесс `ibmslapd` и сервер администрирования, связанный с экземпляром сервера каталогов. Обратитесь к разделу “Запуск и остановка сервера каталогов и сервера администрирования” на стр. 157.

Создание экземпляра сервера каталогов с пользовательскими параметрами

Сервер администрирования экземпляра позволяет создать экземпляр сервера каталогов с пользовательскими значениями в соответствии с конкретными требованиями.

Прежде чем начать

Для создания экземпляра сервера каталогов необходимо выполнить следующие задачи:

1. Установить IBM Security Directory Server с компонентом Сервер. См. раздел “Установка с помощью IBM Installation Manager” на стр. 30.
2. Для создания полного сервера каталогов с базовой системой управления реляционными базами данных ()- установить IBM DB2. Обратитесь к разделу “Установка с помощью IBM Installation Manager” на стр. 30.
3. Проверить, содержит ли файл `ldapdb.properties` информацию об установочном каталоге и версии DB2. Обратитесь к разделу Приложение C, “Обновление файла `ldapdb.properties` вручную”, на стр. 251.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. Нажмите кнопку **Создать экземпляр**.
3. В окне **Создать экземпляр сервера каталогов** на панели **Создать или перейти к новой версии** выберите опцию **Создать экземпляр сервера каталогов**.

4. Нажмите кнопку **Далее**.
5. В окне **Создать экземпляр сервера каталогов** на панели **Сведения об экземпляре** укажите следующие значения:
 - a. В списке **Имя пользователя** выберите имя пользователя, которому будет принадлежать экземпляр сервера каталогов. Экземпляру сервера каталогов будет назначено имя, совпадающее с именем пользователя.
 - b. Если требуется создать учетную запись пользователя для экземпляра, нажмите кнопку **Создать пользователя**. В окне **Создать пользователя для экземпляра сервера каталогов** выполните следующие действия:
 - 1) В поле **Имя пользователя** введите имя пользователя.
 - 2) В поле **Пароль** введите пароль учетной записи пользователя.
 - 3) В поле **Подтверждение пароля** введите пароль учетной записи пользователя.
 - 4) В поле **Домашний каталог** введите домашний каталог, который требуется назначить для учетной записи пользователя. Для выбора домашнего каталога нажмите кнопку **Обзор**.
 - 5) В поле **Основная группа** введите имя основной группы пользователя.
 - 6) Для создания учетной записи пользователя нажмите кнопку **Создать**.
 - c. Для изменения существующей учетной записи выберите имя пользователя в списке **Имя пользователя** и нажмите кнопку **Изменить пользователя**. В окне **Изменить пользователя для экземпляра сервера каталогов** выполните следующие действия:
 - 1) Поле **Имя пользователя** содержит имя пользователя.
 - 2) В поле **Пароль** введите пароль учетной записи пользователя.
 - 3) В поле **Подтверждение пароля** введите пароль учетной записи пользователя.
 - 4) В поле **Домашний каталог** введите домашний каталог, который требуется назначить для учетной записи пользователя. Для выбора домашнего каталога нажмите кнопку **Обзор**.
 - 5) В поле **Основная группа** введите имя основной группы пользователя.
 - 6) Для изменения учетной записи пользователя нажмите кнопку **Изменить**.
6. В поле **Расположение экземпляра** введите расположение экземпляра сервера каталогов. Для выбора домашнего каталога экземпляра нажмите кнопку **Обзор**. В указанном расположении должно быть свободно не менее 30 МБ памяти. В системе Windows расположением является дисковый привод, например C:. Файлы экземпляра каталога хранятся в каталоге `\idslapd-экземпляр` на указанном приводе. Переменная *экземпляр* - это имя экземпляра сервера каталогов. В системах AIX, Linux и Solaris расположением по умолчанию для файлов экземпляра будет домашний каталог владельца экземпляра сервера каталогов, однако, можно указать и другой каталог.
7. В поле **Начальный ключ шифрования** введите начальный ключ шифрования для экземпляра сервера каталогов.

Напоминание: Начальный ключ шифрования экземпляра сервера каталогов необходимо запомнить, так как он может потребоваться для других задач настройки.

Начальный ключ шифрования должен содержать только печатаемые символы ASCII ISO-8859-1 с кодами из диапазона от 33 до 126. Его длина должна быть от 12 до 1016 символов. Информация о символах, которые можно использовать, приведена в разделе “Символы ASCII с кодом от 33 до 126” на стр. 129. Начальный ключ шифрования используется сервером каталогов для создания

набора личных ключей AES. Значения ключей, которые хранятся в файле ключей экземпляра сервера каталогов, применяются для шифрования и расшифровки пароля и атрибутов.

8. В поле **Подтверждение начального ключа** введите начальный ключ шифрования для экземпляра сервера каталогов.
9. Если требуется задать добавление для ключа шифрования, то включите переключатель **Использовать добавление для ключа шифрования**.
 - a. В поле **Добавление для ключа шифрования** введите строку добавления для экземпляра сервера каталогов. Добавление для ключа шифрования должно содержать только печатаемые символы ASCII ISO-8859-1 с кодами из диапазона от 33 до 126. Его длина должна быть равна 12 символам. Информация о символах, которые можно использовать, приведена в разделе “Символы ASCII с кодом от 33 до 126” на стр. 129. Для криптографической синхронизации сервера каталогов с другим экземпляром сервера каталогов необходимо использовать одни и те же значения начального ключа шифрования и добавления для ключа.
 - b. В поле **Подтверждение добавления для ключа шифрования** введите строку добавления для экземпляра сервера каталогов.
10. Необязательно: В поле **Описание экземпляра** введите описание экземпляра сервера каталогов. Описание помогает идентифицировать экземпляр.
11. Нажмите кнопку **Далее**.
12. В поле **Имя экземпляра DB2** на панели **Сведения об экземпляре DB2** укажите имя экземпляра DB2 для экземпляра сервера каталогов.

Примечание: Экземпляр DB2 для экземпляра сервера каталогов не должен быть настроен для использования другими программами или продуктами.

По умолчанию имя экземпляра DB2 совпадает с именем экземпляра сервера каталогов. Однако для экземпляра DB2 можно указать и другое имя. В качестве такого имени должен быть указан ИД пользователя системы, который уже существует на компьютере. Это имя учетной записи пользователя не должно быть связано с другим экземпляром сервера каталогов.

13. Нажмите кнопку **Далее**.
14. В панели **Параметры TCP/IP для хостов с несколькими домашними каталогами** выберите одну из следующих опций:
 - Если требуется чтобы экземпляр сервера каталогов принимал все IP-адреса, выберите **Использовать все настроенные IP-адреса**.
 - Если экземпляр должен применять только часть IP-адресов, настроенных на компьютере, выполните следующие действия:
 - a. Выключите переключатель **Использовать все настроенные IP-адреса**.
 - b. В списке **Выбрать конкретные IP-адреса для использования** выберите IP-адреса, которые должны использоваться экземпляром.
15. Нажмите кнопку **Далее**.
16. В панели **Параметры порта TCP/IP** укажите следующие значения:

Примечание: Необходимо назначить уникальные номера для портов сервера каталогов, которые не должны конфликтовать с портами, которые уже используются на компьютере. В системах AIX, Linux и Solaris порты с номерами в диапазоне 1-1000 могут использоваться только пользователем root.

- a. В поле **Порт сервера** введите номер порта, который должен использоваться сервером как незащищенный порт. Номер должен принадлежать диапазону 1-65535.

- b. В поле **Защищенный порт сервера** введите номер порта, который должен использоваться сервером как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - c. В поле **Порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как незащищенный порт. Номер должен принадлежать диапазону 1-65535.
 - d. В поле **Защищенный порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - e. Нажмите кнопку **Далее**.
17. На панели **Дополнительные действия** выполните следующие действия:
- a. Для настройки отличительного имени (DN) и пароля администратора экземпляра сервера каталогов выберите **Настроить DN администратора и пароль**. Для сервера прокси и для полного сервера каталогов необходимо задать отличительное имя администратора и пароль.
 - b. Для настройки базы данных экземпляра сервера каталогов выберите **Настроить базу данных**.
 - c. Нажмите кнопку **Далее**.
18. На панели **Настроить DN администратора и пароль** выполните следующие действия:
- a. В поле **DN администратора** введите допустимое отличительное имя или оставьте значение по умолчанию `cn=root`. Регистр символов в отличительном имени администратора не учитывается. Пользователю с указанным именем предоставляется полный доступ ко всем данным экземпляра сервера каталогов.
 - b. В поле **Пароль администратора** введите пароль администратора с указанным отличительным именем. Пароль вводится с учетом регистра символов. Двухбайтовые символы (DBCS) в паролях не поддерживаются.
 - c. В поле **Подтверждение пароля** введите пароль администратора с указанным DN. Необходимо запомнить пароль для использования в будущем.
 - d. Нажмите кнопку **Далее**.
19. На панели **Настроить базу данных** выполните следующие задачи для настройки базы данных для экземпляра сервера каталогов: Инструмент администрирования экземпляра добавляет информацию о базе данных в файл конфигурации `ibmslapd.conf` экземпляра сервера каталогов. Если база данных не существует, Инструмент администрирования экземпляра создаст ее.
- a. В поле **Имя пользователя базы данных** введите допустимый ИД администратора DB2. Указанный ИД администратора DB2 должен существовать на компьютере до начала настройки базы данных и обладать необходимыми правами доступа.

Примечание: До запуска сервера для этого ИД администратора DB2 должна быть настроена локаль, соответствующая языку, на котором будут выводиться сообщения сервера.

- b. В поле **Пароль** введите пароль администратора DB2. Пароль вводится с учетом регистра символов.

Примечание: Системный пароль администратора DB2 нельзя изменить с помощью Инструмента администрирования экземпляра. Это можно сделать с помощью Инструмента настройки или команды `idscfgdb` с параметром `-w`. Дополнительная информация приведена в разделе “Управление паролем администратора базы данных DB2” на стр. 182.

- c. В поле **Имя базы данных** введите имя базы данных DB2. Длина имени должна составлять от 1 до 8 символов.
- d. Необязательно: Если требуется задать любые из следующих параметров конфигурации DB2, выберите **Показать дополнительные опции табличного пространства**.

Примечание: DB2 может создавать табличные пространства в хранилищах, управляемых системой (SMS) или управляемых базой данных (DMS). В IBM Security Directory Server применяется технология DMS. В версиях IBM Security Directory Server до 6.2 включительно для всех баз данных используется SMS. Если переключатель **Показать дополнительные опции табличных пространств** выключен, то создаются табличные пространства USERSPACE1 и LDAPSPACE с применением DMS с размерами и расположением по умолчанию. В системах AIX, Linux и Solaris для табличного пространства USERSPACE1 по умолчанию используется следующий каталог и имя файла: *расположение-базы-данных/экземпляр/NODE0000/SQL00001/USPACE*. В системах Windows имя файла и каталог по умолчанию для табличного пространства USERSPACE1 - *расположение-базы-данных\экземпляр\NODE0000\SQL00001\USPACE*. В системах AIX, Linux и Solaris каталог и имя файла по умолчанию для табличного пространства LDAPSPACE - *расположение-базы-данных/ldap32kcont_экземпляр/ldapspace*. В Windows каталог и имя файла по умолчанию для табличного пространства LDAPSPACE - *расположение-базы-данных\ldap32kcont_экземпляр\ldapspace*.

- Требуется, чтобы для хранения табличных пространств базы данных DB2 применялась технология управляемого системой хранения (SMS). При использовании SMS табличное пространство для хранения таблиц DB2 выделяется и управляется администратором файловой системы операционной системы.
 - Требуется, чтобы для хранения табличных пространств базы данных DB2 применялась технология хранения, управляемого базой данных (DMS). Кроме того, требуется настроить табличные пространства USERSPACE1 и LDAPSPACE, их размер и расположение. При использовании DMS табличные пространства управляются администратором базы данных. Администратор базы данных отвечает за выбор устройств и файлов, а DB2 управляет памятью этих устройств и файлов.
- e. Нажмите кнопку **Далее**.
20. На панели **Опции базы данных** выполните следующие действия:
- a. В поле **Установочный каталог базы данных** введите расположение базы данных. Для выбора каталога нажмите кнопку **Обзор**. В Windows необходимо указать имя диска, например C:. В AIX, Linux и Solaris расположение должно быть именем каталога, например: /home/ldapdb.

Примечание: Минимальный объем памяти на диске для базы данных DMS составляет 1 ГБ. Для базы данных SMS требуется минимум 150 МБ дисковой памяти. Указанные требования относятся к пустой базе данных. Для хранения данных потребуется дополнительная память.

- b. Для того чтобы настроить сервер каталогов с базой данных для оперативного резервного копирования, выполните следующие действия:
 - 1) Выберите **Настроить для оперативного резервного копирования**.
 - 2) В поле **Расположение резервной копии базы данных** введите расположение для хранения образа резервной копии. Расположение можно выбрать с помощью кнопки **Обзор**.

Примечание: Не выходите из Инструмента администрирования экземпляра при запуске операции резервного копирования.

Если база данных настраивалась для оперативного резервного копирования, то после завершения ее настройки выполняется первоначальное автономное резервное копирование. После его завершения перезапускается сервер администрирования. Оперативное резервное копирование для экземпляра сервера каталогов также можно настроить с помощью команды **idscfgdb**. Однако отменить настройку оперативного резервного копирования с помощью команды **idscfgdb** и параметра **-c** нельзя. Если оперативное резервное копирование для экземпляра было настроено с помощью Инструмента администрирования экземпляра или Инструмента настройки, то его настройку можно отменить с помощью Инструмента настройки или команды **idscfgdb**.

- c. В области **Опция кодировки** выберите одну из следующих опций для создания типа базы данных:

Примечание: Если данные планируется хранить на сервере каталогов на нескольких языках, создайте универсальную базу данных DB2. Универсальная база данных DB2 также является наиболее эффективной, так как требуется меньше операций перевода данных. Для применения тегов языка база данных должна быть создана в формате UTF-8. За дополнительной информацией об UTF-8 обратитесь к разделу “Поддержка UTF-8” на стр. 126.

- Для создания базы данных UTF-8, в которой клиенты LDAP смогут хранить символьные данные UTF-8, выберите **Создать универсальную базу данных DB2**.
- Для создания базы данных с локальной кодовой страницей выберите **Создать базу данных DB2 с локальной кодовой страницей**.

- d. Нажмите кнопку **Далее**.

21. Если на панели **Настроить базу данных** был включен переключатель **Показать дополнительные опции табличных пространств**, то на панели **Настроить табличные пространства базы данных** необходимо задать следующие значения:

- a. В списке **Выбрать тип табличного пространства базы данных** выберите тип базы данных. Тип табличного пространства базы данных по умолчанию - DMS. При выборе типа табличного пространства SMS все остальные поля будут недоступны. Поддержка табличного пространства DMS используется только для табличных пространств USERSPACE1 и LDAPSPACE. Все остальные табличные пространства, например табличное пространство каталога или временное табличное пространство, имеют тип SMS.
- a. В области **Сведения о табличном пространстве USERSPACE1** укажите следующую информацию:

- 1) В списке **Контейнер табличного пространства** выберите тип контейнера. Если табличное пространство USERSPACE1 должно находиться в файловой системе, выберите **Файл**. Если контейнер табличного пространства базы данных расположен в файловой системе, то создается табличное пространство DMS cooked. Можно указать начальный размер табличного пространства и приращение для автоматического увеличения размера табличного пространства, если это потребуется. Если табличное пространство USERSPACE1 требуется создать на устройстве с линейным доступом, выберите **Устройство с линейным доступом**. Устройство с линейным доступом - это устройство, на котором отсутствует файловая система, например, жесткий диск без файловой системы. Если контейнер табличного пространства базы данных расположен на устройстве с линейным доступом, то создается табличное пространство DMS raw. В

этом случае размер контейнера табличного пространства базы данных фиксирован и не может быть увеличен. При выборе типа **Устройство с линейным доступом** вместо значений по умолчанию укажите размер и расположение контейнера.

- 2) Если в списке **Контейнер табличного пространства** выбран тип **Файл**, то укажите следующую информацию:
 - a) В поле **Путь к каталогу** укажите путь к каталогу, в котором требуется создать табличное пространство USERSPACE1. Для выбора каталога нажмите кнопку **Обзор**.
 - b) В поле **Имя файла** введите имя файла создаваемого табличного пространства или примите значение по умолчанию (USPACE).
 - c) В поле **Начальный размер** введите начальный размер табличного пространства USERSPACE1 в страницах или примите значение по умолчанию. Контейнер табличного пространства USERSPACE1 типа **Файл** является автоматически расширяемым. Можно задать начальный размер в поле **Начальный размер** и приращение в поле **Размер расширения**. Значение начального размера по умолчанию - 16000 страниц, приращение по умолчанию - 8000 страниц. Размер страницы контейнера табличного пространства USERSPACE1 равен 4 КБ.
- 3) Если в списке **Контейнер табличного пространства** выбран тип **Устройство с линейным доступом**, то укажите следующую информацию:
 - a) В поле **Путь к устройству** укажите расположение устройства с линейным доступом. В Windows путь должен начинаться с \\.\. Пример: \\.\имя-устройства. В AIX, Linux и Solaris необходимо указать допустимый путь к устройству.
 - b) В поле **Начальный размер** введите начальный размер табличного пространства USERSPACE1 или примите значение по умолчанию. Размер контейнера табличного пространства USERSPACE1 типа **Устройство с линейным доступом** является фиксированным. По умолчанию он составляет 16000 страниц. Для лучших результатов рекомендуется указать значение с учетом текущих требований.
- b. В области **Сведения о табличном пространстве LDAPSPACE** укажите следующую информацию:
 - 1) В списке **Контейнер табличного пространства** выберите тип контейнера. Если табличное пространство LDAPSPACE должно находиться в файловой системе, выберите **Файл**. Если табличное пространство LDAPSPACE требуется создать на устройстве с линейным доступом, выберите **Устройство с линейным доступом**. Устройство с линейным доступом - это устройство, на котором отсутствует файловая система, например, жесткий диск без файловой системы.
 - 2) Если в списке **Контейнер табличного пространства** выбран тип **Файл**, то укажите следующую информацию:
 - a) В поле **Путь к каталогу** укажите путь к каталогу, в котором требуется создать табличное пространство LDAPSPACE. Для выбора каталога нажмите кнопку **Обзор**.
 - b) В поле **Имя файла** введите имя файла создаваемого табличного пространства или примите значение по умолчанию (ldapspace).
 - c) В поле **Начальный размер** введите начальный размер табличного пространства LDAPSPACE в страницах или примите значение по умолчанию. Контейнер табличного пространства LDAPSPACE типа **Файл** является автоматически расширяемым. Можно задать начальный размер в поле **Начальный размер** и приращение в поле

Размер расширения. Значение начального размера по умолчанию - 16000 страниц, приращение по умолчанию - 8000 страниц. Размер страницы контейнера табличного пространства LDAPSPACE равен 32 КБ.

- 3) Если в списке **Контейнер табличного пространства** выбран тип **Устройство с линейным доступом**, то укажите следующую информацию:
 - a) В поле **Путь к устройству** укажите расположение устройства с линейным доступом. В Windows путь должен начинаться с \\.\. Пример: \\.\имя-устройства. В AIX, Linux и Solaris необходимо указать допустимый путь к устройству.
 - b) В поле **Начальный размер** введите начальный размер табличного пространства LDAPSPACE или примите значение по умолчанию. Размер контейнера табличного пространства LDAPSPACE типа **Устройство с линейным доступом** является фиксированным. По умолчанию он составляет 16000 страниц. Для лучших результатов рекомендуется указать значение с учетом текущих требований.
 - c. Если в одном или в обоих полях **Контейнер табличного пространства** выбрано значение **Файл**, то в поле **Размер расширения** укажите число страниц для расширения контейнеров.
 - d. Нажмите кнопку **Далее**.
22. В панели **Проверить параметры** проверьте обзорные сведения.
 23. Нажмите кнопку **Готово** для запуска процедуры создания экземпляра сервера каталогов.
 24. В окне **Результаты** проверьте сообщения из протокола, которые записаны для операций создания экземпляра.
 25. Для закрытия окна **Результаты** нажмите кнопку **Закрыть**.
 26. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Результаты

Инструмент администрирования экземпляра создаст экземпляр сервера каталогов на компьютере.

Дальнейшие действия

Необходимо запустить процесс `ibmslapd` и сервер администрирования, связанный с экземпляром сервера каталогов. Обратитесь к разделу “Запуск и остановка сервера каталогов и сервера администрирования” на стр. 157.

Создание экземпляра сервера прокси с пользовательскими параметрами

Сервер администрирования экземпляра позволяет создать экземпляр сервера прокси с пользовательскими значениями в соответствии с конкретными требованиями.

Прежде чем начать

Для создания экземпляра сервера прокси необходимо выполнить следующие задачи:

1. Установить IBM Security Directory Server с компонентом Сервер прокси. См. раздел “Установка с помощью IBM Installation Manager” на стр. 30.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. Нажмите кнопку **Создать экземпляр**.
3. В окне **Создать экземпляр сервера каталогов** на панели **Создать или перейти к новой версии** выполните следующие действия для создания экземпляра сервера прокси:
 - a. Выберите **Создать экземпляр сервера каталогов**.
 - b. Выберите **Настроить как прокси**.
4. Нажмите кнопку **Далее**.
5. В окне **Создать экземпляр сервера каталогов** на панели **Сведения об экземпляре** укажите следующие значения:
 - a. В списке **Имя пользователя** выберите имя пользователя, которому будет принадлежать экземпляр. Имя, присваиваемое экземпляру, совпадает с именем этого пользователя.
 - b. Если требуется создать учетную запись пользователя для экземпляра, нажмите кнопку **Создать пользователя**. В окне **Создать пользователя для экземпляра сервера каталогов** выполните следующие действия:
 - 1) В поле **Имя пользователя** введите имя пользователя.
 - 2) В поле **Пароль** введите пароль учетной записи пользователя.
 - 3) В поле **Подтверждение пароля** введите пароль учетной записи пользователя.
 - 4) В поле **Домашний каталог** введите домашний каталог, который требуется назначить для учетной записи пользователя. Для выбора домашнего каталога нажмите кнопку **Обзор**.
 - 5) В поле **Основная группа** введите имя основной группы пользователя.
 - 6) Для создания учетной записи пользователя нажмите кнопку **Создать**.
 - c. Для изменения существующей учетной записи выберите имя пользователя в списке **Имя пользователя** и нажмите кнопку **Изменить пользователя**. В окне **Изменить пользователя для экземпляра сервера каталогов** выполните следующие действия:
 - 1) Поле **Имя пользователя** содержит имя пользователя.
 - 2) В поле **Пароль** введите пароль учетной записи пользователя.
 - 3) В поле **Подтверждение пароля** введите пароль учетной записи пользователя.
 - 4) В поле **Домашний каталог** введите домашний каталог, который требуется назначить для учетной записи пользователя. Для выбора домашнего каталога нажмите кнопку **Обзор**.
 - 5) В поле **Основная группа** введите имя основной группы пользователя.
 - 6) Для изменения учетной записи пользователя нажмите кнопку **Изменить**.
 - 7) В окне подтверждения **Изменить пользователя для экземпляра сервера каталогов** нажмите кнопку **Да**.
6. В поле **Расположение экземпляра** введите расположение экземпляра сервера прокси. Для выбора домашнего каталога экземпляра нажмите кнопку **Обзор**. В указанном расположении должно быть свободно не менее 30 МБ памяти. В системе Windows расположением является дисковый привод, например С:.
Файлы экземпляра каталога хранятся в каталоге `\idsldap-экземпляр` на указанном приводе, где *экземпляр* - это имя экземпляра сервера прокси. В

системах AIX, Linux и Solaris расположением по умолчанию для файлов экземпляра будет домашний каталог владельца экземпляра сервера прокси, однако можно указать и другой каталог.

7. В поле **Начальный ключ шифрования** введите начальный ключ шифрования для экземпляра.

Напоминание: Начальный ключ шифрования экземпляра необходимо запомнить, так как он может потребоваться для других задач настройки. Начальный ключ шифрования должен содержать только печатаемые символы ASCII ISO-8859-1 с кодами из диапазона от 33 до 126. Его длина должна быть от 12 до 1016 символов. Информация о символах, которые можно использовать, приведена в разделе “Символы ASCII с кодом от 33 до 126” на стр. 129. Начальный ключ шифрования используется сервером каталогов для создания набора личных ключей AES. Значения ключей, которые хранятся в файле ключей экземпляра сервера каталогов, применяются для шифрования и расшифровки пароля и атрибутов.

8. В поле **Подтверждение начального ключа** введите начальный ключ шифрования для экземпляра.
9. Если требуется задать добавление для ключа шифрования, то включите переключатель **Использовать добавление для ключа шифрования**.
 - a. В поле **Добавление для ключа шифрования** введите строку добавления для экземпляра. Добавление для ключа шифрования должно содержать только печатаемые символы ASCII ISO-8859-1 с кодами из диапазона от 33 до 126. Его длина должна быть равна 12 символам. Информация о символах, которые можно использовать, приведена в разделе “Символы ASCII с кодом от 33 до 126” на стр. 129.
 - b. В поле **Подтверждение добавления для ключа шифрования** введите строку добавления для экземпляра.
10. Необязательно: В поле **Описание экземпляра** введите описание экземпляра. Описание помогает идентифицировать экземпляр.
11. Нажмите кнопку **Далее**.
12. В панели **Параметры TSP/IP для хостов с несколькими домашними каталогами** выберите одну из следующих опций:
 - Если экземпляр должен использовать все IP-адреса, выберите **Использовать все настроенные IP-адреса**.
 - Если экземпляр должен применять только часть IP-адресов, настроенных на компьютере, выполните следующие действия:
 - a. Выключите переключатель **Использовать все настроенные IP-адреса**.
 - b. В списке **Выбрать конкретные IP-адреса для использования** выберите IP-адреса, которые должны использоваться экземпляром.
13. Нажмите кнопку **Далее**.
14. В панели **Параметры порта TSP/IP** укажите следующие значения:

Примечание: Необходимо назначить уникальные номера для портов сервера каталогов, которые не должны конфликтовать с портами, которые уже используются на компьютере. В системах AIX, Linux и Solaris порты с номерами в диапазоне 1-1000 могут использоваться только пользователем root.

- a. В поле **Порт сервера** введите номер порта, который должен использоваться сервером как незащищенный порт. Номер должен принадлежать диапазону 1-65535.

- b. В поле **Защищенный порт сервера** введите номер порта, который должен использоваться сервером как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - c. В поле **Порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как незащищенный порт. Номер должен принадлежать диапазону 1-65535.
 - d. В поле **Защищенный порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - e. Нажмите кнопку **Далее**.
15. На панели **Дополнительные действия** выполните следующие действия:
- a. Для настройки отличительного имени (DN) и пароля администратора для экземпляра выберите **Настроить DN администратора и пароль**. Для экземпляра сервера прокси необходимо задать отличительное имя администратора и пароль.
 - b. Нажмите кнопку **Далее**.
16. На панели **Настроить DN администратора и пароль** выполните следующие действия:
- a. В поле **DN администратора** введите допустимое отличительное имя или оставьте значение по умолчанию `cn=root`. Регистр символов в отличительном имени администратора не учитывается. Пользователю с указанным именем предоставляется полный доступ ко всем данным экземпляра.
 - b. В поле **Пароль администратора** введите пароль администратора с указанным отличительным именем. Пароль вводится с учетом регистра символов. Двухбайтовые символы (DBCS) в паролях не поддерживаются.
 - c. В поле **Подтверждение пароля** введите пароль администратора с указанным DN. Необходимо запомнить пароль для использования в будущем.
 - d. Нажмите кнопку **Далее**.
17. В панели **Проверить параметры** проверьте обзорные сведения.
18. Нажмите кнопку **Готово** для запуска процедуры создания экземпляра сервера прокси.
19. В окне **Результаты** проверьте сообщения из протокола, которые записаны для операций создания экземпляра.
20. Для закрытия окна **Результаты** нажмите кнопку **Закрыть**.
21. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Результаты

Инструмент администрирования экземпляра создаст экземпляр сервера прокси на компьютере.

Дальнейшие действия

Необходимо запустить сервер администрирования и процесс `ibmslapd` в режиме настройки и настроить базовые серверы. См. раздел *Администрирование* в документации по IBM Security Directory Server.

Создание экземпляра с помощью утилиты командной строки

Создайте экземпляр с помощью утилиты командной строки `idsicrt`.

Прежде чем начать

Для того чтобы создать экземпляр с помощью утилиты командной строки, необходимо выполнить следующие условия:

1. Должен быть установлен IBM Security Directory Server с компонентом Сервер, или Сервер прокси, или с обоими этими компонентами. См. раздел “Установка с помощью IBM Installation Manager” на стр. 30.
2. Должен существовать ИД пользователя системы - владельца экземпляра. Дополнительная информация о создании ИД пользователя системы приведена в разделе “Пользователи и группы, связанные с экземпляром сервера каталогов” на стр. 121.

Об этой задаче

При выполнении команды **idsicrt** создается экземпляр и экземпляр базы данных DB2 для экземпляра полного сервера каталогов.

Процедура

1. Войдите в систему AIX, Linux или Solaris как пользователь root, а в систему Windows - как участник группы администраторов.
2. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
3. Для создания экземпляра введите следующую команду: Вместо переменной *экземпляр* укажите допустимый ИД пользователя системы.

Выполняемая задача	Выполняемая команда:
Создать экземпляр сервера каталогов	<code>idsicrt -I <i>экземпляр</i> -e mysecretkey! -l instance_home</code>
Создать экземпляр сервера прокси	<code>idsicrt -I <i>экземпляр</i> -e mysecretkey! -l instance_home -x</code>

Дополнительная информация о команде **idsicrt** приведена в *Справочнике по командам*.

Примеры

Пример 1:

Для создания экземпляра сервера каталогов со следующими значениями в системе AIX, Linux или Solaris выполните следующую команду:

- Имя экземпляра: `myinst`
- Незащищенный порт: 389
- Защищенный порт: 636
- Начальный ключ шифрования: `mysecretkey!`
- Добавление для ключа шифрования: `mysecretsalt`
- Домашний каталог экземпляра: `/home/myinst` (в AIX и Linux) и `/export/home/myinst` (в Solaris)

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myinst
```

Для создания экземпляра сервера каталогов со следующими значениями в системе Windows выполните следующую команду:

- Имя экземпляра: `myinst`
- Незащищенный порт: 389

- Защищенный порт: 636
- Начальный ключ шифрования: mysecretkey!
- Добавление для ключа шифрования: mysecretsalt
- Домашний каталог экземпляра: C:

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C:
```

Пример 2:

Для создания экземпляра сервера прокси со следующими значениями в системе AIX, Linux или Solaris выполните следующую команду:

- Имя экземпляра: myпроху
- Незащищенный порт: 389
- Защищенный порт: 636
- Начальный ключ шифрования: mysecretkey!
- Добавление для ключа шифрования: mysecretsalt
- Домашний каталог экземпляра: /home/myпроху (в AIX и Linux) и /export/home/myпроху (в Solaris)

```
idsicrt -I myпроху -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l /home/myпроху -x
```

Для создания экземпляра сервера прокси со следующими значениями в системе Windows выполните следующую команду:

- Имя экземпляра: myпроху
- Незащищенный порт: 389
- Защищенный порт: 636
- Начальный ключ шифрования: mysecretkey!
- Добавление для ключа шифрования: mysecretsalt
- Домашний каталог экземпляра: C:

```
idsicrt -I myпроху -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C: -x
```

Дальнейшие действия

Для создания действующего экземпляра выполните следующую настройку:

1. Настройте экземпляр базы данных DB2 для экземпляра полного сервера каталогов.
2. Настройте отличительное имя и пароль администратора для экземпляра.
3. Настройте суффиксы для экземпляра.

Обновление экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра

Используйте Инструмент администрирования экземпляра для обновления экземпляра сервера каталогов или экземпляра сервера Проху с предыдущей версии до версии 6.3.1.

Прежде чем начать

Перед обновлением экземпляра с помощью Инструмента администрирования экземпляра требуется выполнить следующие задачи:

- Установите IBM Security Directory Server версии 6.3.1. См. “Запуск установки” на стр. 28.

- Настройте среду перед обновлением экземпляра. См. “Настройка среды перед обновлением экземпляра” на стр. 90.
- Войдите в систему от лица пользователя root при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Об этой задаче

После обновления экземпляра предыдущей версии он преобразуется в полнофункциональный экземпляр IBM Security Directory Server версии 6.3.1.

Процедура

1. Откройте окно ввода команд.
2. Измените текущий рабочий каталог на sbin. В различных операционных системах используются следующие расположения по умолчанию:

Microsoft Windows

C:\Program Files\IBM\ldap\V6.3.1\sbin

AIX и Solaris

/opt/IBM/ldap/V6.3.1/sbin

Linux /opt/ibm/ldap/V6.3.1/sbin

3. Для запуска Инструмента администрирования экземпляра запустите следующую команду:

Примечание: В системе Windows можно начать с меню **Пуск**. Откройте **Пуск > Программы > IBM Security Directory Server 6.3.1 > Инструмент администрирования экземпляра**.

idsxinst

4. Выберите предыдущую версию экземпляра, который требуется обновить.
5. Выберите **Перенести**.
6. В окне **Перенести экземпляр сервера каталогов** выберите **Перенести**.
7. В ответ на запрос Инструмента администрирования экземпляра после завершения обновления нажмите кнопку **ОК**.
8. Проверьте обзорную информацию.
9. Для закрытия окна **Перенести экземпляр сервера каталогов** нажмите кнопку **Заккрыть**.
10. Создайте резервную копию экземпляра без подключения. Дополнительная информация приведена в разделе “Резервное копирование сервера каталогов” на стр. 190.
11. Для закрытия Инструмента администрирования экземпляра нажмите **Заккрыть**.

Результаты

Инструмент администрирования экземпляра обновит прежнюю версию экземпляра сервера каталогов до версии 6.3.1.

Дальнейшие действия

Необходимо запустить процесс `ibmslapd` и сервер администрирования, связанный с экземпляром сервера каталогов. Обратитесь к разделу “Запуск и остановка сервера каталогов и сервера администрирования” на стр. 157.

Обновление удаленного экземпляра предыдущей версии с помощью Инструмента администрирования экземпляра

Используйте Инструмент администрирования экземпляра для обновления удаленного экземпляра сервера каталогов или экземпляра сервера Proxu предыдущей версии до версии 6.3.1.

Прежде чем начать

Перед обновлением экземпляра с помощью Инструмента администрирования экземпляра требуется выполнить следующие задачи:

- Настройте среду перед обновлением экземпляра. См. “Настройка среды перед обновлением экземпляра” на стр. 90.
- Войдите в систему от лица пользователя root при использовании операционной системы AIX, Linux или Solaris или как участник группы администраторов при использовании операционной системы Windows.

Об этой задаче

После завершения процесса обновления Инструмент администрирования экземпляра создаст экземпляр 6.3.1 на компьютере с информацией об удаленном экземпляре.

Процедура

1. Создайте резервную копию экземпляра сервера каталогов, расположенного на удаленном сервере, с помощью команды **idsdb2ldif**.

Важное замечание: Если выполняется обновление экземпляра сервера Proxu, не создавайте резервную копию базы данных. Сервер Proxu не содержит базу данных, которая с ним связана.

```
idsdb2ldif -I экземпляр -o inst_out.ldif
```

Дополнительная информация о команде **idsdb2ldif** приведена в *Справочнике по командам*.

2. Выполните установку IBM Security Directory Server версии 6.3.1 на компьютере, на котором требуется обновить удаленный экземпляр. См. “Запуск установки” на стр. 28.
3. Для резервного копирования файлов схемы и конфигурации удаленного экземпляра запустите команду **migbkup** версии 6.3.1, до которой требуется провести обновление:

Операционная система	Выполняемая команда:
Microsoft Windows	migbkup.bat диск\idsldapd-экземпляр резервный-каталог
AIX, Linux и Solaris	migbkup домашний-каталог-пользователя/idsldapd-экземпляр резервный-каталог

Команда **migbkup** расположена в подкаталоге `tools` установочного носителя IBM Security Directory Server.

4. Скопируйте резервный каталог резервный-каталог, созданный с помощью **migbkup**, с удаленного компьютера на компьютер с IBM Security Directory Server версии 6.3.1.
5. Необязательно: Скопируйте файл резервной копии базы данных `inst_out.ldif` с удаленного компьютера на компьютер с IBM Security Directory Server версии 6.3.1.

6. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
7. Нажмите кнопку **Создать экземпляр**.
8. В панели **Создать или перенести** выполните следующие действия:
 - a. Нажмите кнопку **Перенести из предыдущей версии сервера каталогов**.
 - b. В поле **Ввести путь к резервной копии файлов** введите путь к резервной копии файлов конфигурации и схемы удаленного экземпляра. Для того чтобы указать расположение резервной копии, можно воспользоваться кнопкой **Обзор**.
 - c. Нажмите кнопку **Далее**.
9. В панели **Сведения об экземпляре** окна **Создать экземпляр сервера каталогов** укажите следующие значения:

Примечание: Если производится обновление экземпляра, то отредактировать имеющуюся информацию о пользователе невозможно.

- a. В списке **Имя пользователя** выберите имя пользователя, которого требуется назначить владельцем экземпляра сервера каталогов. Экземпляру сервера каталогов будет назначено имя, совпадающее с именем пользователя.
 - b. Если требуется создать учетную запись пользователя для экземпляра, нажмите кнопку **Создать пользователя**. В окне **Создать пользователя для экземпляра сервера каталогов** выполните следующие действия:
 - 1) В поле **Имя пользователя** введите имя пользователя.
 - 2) В поле **Пароль** введите пароль учетной записи пользователя.
 - 3) В поле **Подтверждение пароля** введите пароль учетной записи пользователя.
 - 4) В поле **Домашний каталог** введите домашний каталог, который требуется назначить для учетной записи пользователя. Для выбора домашнего каталога нажмите кнопку **Обзор**.
 - 5) В поле **Основная группа** введите имя основной группы пользователя.
 - 6) Для создания учетной записи пользователя нажмите кнопку **Создать**.
10. В поле **Расположение экземпляра** введите расположение экземпляра сервера каталогов. Для выбора домашнего каталога экземпляра нажмите кнопку **Обзор**. В указанном расположении должно быть свободно не менее 30 МБ памяти. В системе Windows расположением является дисковый привод, например C:. Файлы экземпляра каталога хранятся в каталоге `\idslapd-экземпляр` на указанном приводе. Переменная *экземпляр* - это имя экземпляра сервера каталогов. В системах AIX, Linux и Solaris стандартным путем является домашний каталог владельца экземпляра сервера каталогов, но можно указать и другой путь.
 11. Необязательно: В поле **Описание экземпляра** введите описание экземпляра сервера каталогов. Описание помогает идентифицировать экземпляр.
 12. Нажмите кнопку **Далее**.
 13. Если обновление удаленного экземпляра сервера каталогов выполняется с указанием сведений о базе данных DB2, нажмите кнопку **Далее** в панели **Сведения об экземпляре DB2**. Если файлы резервной копии принадлежат удаленному экземпляру сервера Проху, то панель **Сведения об экземпляре DB2** может не выводиться.
 14. В панели **Параметры ТСР/ІР для хостов с несколькими домашними каталогами** выберите одну из следующих опций:
 - Если требуется чтобы экземпляр сервера каталогов принимал все ІР-адреса, выберите **Использовать все настроенные ІР-адреса**.

- Если экземпляр сервера каталогов должен применять только часть IP-адресов, настроенных на компьютере, отмените выбор **Использовать все настроенные IP-адреса**. Выберите из списка IP-адрес или адреса, которые должны применяться.
15. Нажмите кнопку **Далее**.
 16. В панели **Параметры порта TSP/IP** укажите следующие значения:

Примечание: Необходимо назначить уникальные номера для портов сервера каталогов, которые не должны конфликтовать с портами, которые уже используются на компьютере. В системах AIX, Linux и Solaris порты с номерами в диапазоне 1-1000 могут использоваться только пользователем root.

 - a. В поле **Порт сервера** введите номер порта, который должен использоваться сервером как незащищенный порт. Номер должен принадлежать диапазону 1-65535.
 - b. В поле **Защищенный порт сервера** введите номер порта, который должен использоваться сервером как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - c. В поле **Порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как незащищенный порт. Номер должен принадлежать диапазону 1-65535.
 - d. В поле **Защищенный порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - e. Нажмите кнопку **Далее**.
 17. В панели **Проверить параметры** проверьте обзорные сведения.
 18. Для запуска процесса создания экземпляра сервера каталогов с использованием резервных копий файлов конфигурации и схемы нажмите кнопку **Готово**.
 19. В окне **Результаты** проверьте сообщения из протокола, которые записаны для операций создания экземпляра.
 20. Для закрытия окна **Результаты** нажмите кнопку **Закрыть**.
 21. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Результаты

Инструмент администрирования экземпляра создаст экземпляр сервера каталогов на компьютере.

Дальнейшие действия

Необходимо запустить процесс `ibmslapd` и сервер администрирования, связанный с экземпляром сервера каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера” на стр. 158.

Создайте резервную копию экземпляра. Дополнительная информация по резервному копированию экземпляра сервера каталогов приведена в разделе “Резервное копирование сервера каталогов” на стр. 190.

Создание экземпляра на основе существующего экземпляра

С помощью инструмента администрирования экземпляра можно создать экземпляр сервера каталогов на основе существующего экземпляра, имеющегося на локальном компьютере или в удаленной системе. Исходный сервер каталогов служит шаблоном для целевого экземпляра сервера каталогов.

IBM Security Directory Server Инструмент администрирования экземпляра поддерживает копирование исходного экземпляра сервера каталогов только в случае совпадения версий инструмента и экземпляра. Целевой сервер каталогов создается на компьютере, где выполняется Инструмент администрирования экземпляра. Если исходный сервер каталогов находится на другом компьютере, операционные системы двух компьютеров могут отличаться. Например, в системе Windows можно создать копию экземпляра сервера каталогов, работающего в системе Linux.

Если этот инструмент применяется для копирования исходного экземпляра, то можно выполнить следующие операции на основе входных данных:

- Можно создать целевой сервер каталогов с теми же параметрами конфигурации и файлами схемы, которые настроены в исходном экземпляре сервера каталогов. При этом также синхронизируются файлы бумажника ключей целевого и исходного серверов.
- Если исходный экземпляр сервера каталогов представляет собой полный сервер каталогов, то создаваемый целевой экземпляр сервера каталогов также будет полным сервером каталогов. Можно выбрать копирование данных из существующего экземпляра сервера каталогов. Если для исходного сервера каталогов настроено резервное копирование онлайн, можно создать работающий целевой сервер каталогов с записями его базы данных.
- Если исходный экземпляр сервера каталогов представляет собой прокси-сервер, то создаваемый целевой экземпляр сервера каталогов также будет прокси-сервером.
- Если исходный сервер каталогов находится в среде репликации, можно настроить целевой экземпляр как сервер-реплика или как равноправный сервер для исходного сервера.
- Если исходный сервер каталогов находится в распределенной среде, можно настроить целевой экземпляр сервера каталогов как прокси-сервер.
- Если исходный экземпляр сервера каталогов настроен для защищенной связи, Инструмент администрирования экземпляра копирует файлы базы ключей на целевой сервер каталогов.

Перед созданием сервера каталогов на основе исходного сервера каталогов необходимо убедиться, что исходный сервер каталогов отвечает следующим условиям:

- Исходный сервер каталогов должен быть IBM Security Directory Server версии 6.3.1 или выше. Исходный сервер каталогов не должен быть экземпляром предыдущей версии.
- Исходный сервер каталогов должен выполняться в обычном режиме. Не поддерживается копирование экземпляра, работающего в режиме настройки.
- Исходный сервер каталогов должен быть доступен с компьютера, на котором работает Инструмент администрирования экземпляра.
- Для того чтобы создать целевой сервер каталогов как реплику или равноправный сервер, в исходном экземпляре сервера каталогов должен существовать контекст репликации. С помощью инструмента администрирования экземпляра невозможно настроить первую реплику или равноправный сервер в топологии репликации. В исходном экземпляре сервера каталогов должен содержаться хотя бы один уже контекст репликации, группа репликации, а также определена вложенная запись репликации. Если требуется настроить экземпляр как реплику, то в исходном экземпляре необходимо определить начальную топологию репликации, в том числе соглашение хотя бы с одним другим сервером. Если требуется настроить экземпляр как равноправный сервер, исходный сервер необходимо настроить как главный сервер для одной или нескольких вложенных записей в конфигурации репликации.

- Если требуется создать экземпляр как равноправный сервер или реплику, то будет создана новая вложенная запись репликации в разделе DN `ibm-repl:iscGroup=default`, *контекст-репликации*. Если DN не указано, копирование экземпляра будет невозможно.

Если требуется скопировать данные из исходного экземпляра сервера каталогов в целевой экземпляр сервера каталогов, то должны быть соблюдены следующие требования:

- Версия DB2 в одном экземпляре сервера каталогов может отличаться от версии в другом. Функции резервного копирования и восстановления поддерживаются в пределах одного типа операционной системы. Например, можно восстановить базу данных, созданную с помощью DB2 UDB версии 9 в системах Windows, в системе с DB2 версии 10. В системах AIX, Linux и Solaris можно восстанавливать данные из резервных копий, созданных с помощью DB2 UDB версии 9, в DB2 версии 10, если совпадает порядок байтов (в начале младший байт или в начале старший байт) операционных систем, обеспечивающих создание и восстановление резервной копии.
- Необходимо настроить исходный экземпляр сервера каталогов для резервного копирования онлайн. Резервное копирование онлайн можно настроить при начальной настройке базы данных. Для настройки резервного копирования онлайн можно использовать Инструмент администрирования экземпляра или Инструмент настройки.
- Перед тем как использовать Инструмент администрирования экземпляра для копирования экземпляра сервера каталогов, необходимо создать начальную резервную копию исходного экземпляра сервера каталогов в автономном режиме. В указанном для резервного копирования каталоге должен содержаться только один образ резервной копии.
- Каталог с образом резервной копии должен быть доступен как для исходного, так и для целевого экземпляров сервера каталогов.

Создание копии существующего экземпляра с помощью Инструмента администрирования экземпляра

Создайте копию существующего экземпляра с помощью Инструмента администрирования экземпляра.

Прежде чем начать

Для создания копии существующего экземпляра необходимо выполнить следующие требования:

- Запустите процесс `ibms1apd` и сервер администрирования экземпляра в обычном режиме.
- Убедитесь, что исходный сервер каталогов доступен из Инструмента администрирования экземпляра.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. Выберите одну из следующих опций для создания копии существующего экземпляра:
 - Для создания копии существующего экземпляра на локальном компьютере выберите **Скопировать локальный экземпляр**.
 - Для создания копии существующего экземпляра на локальном компьютере выберите **Скопировать удаленный экземпляр**.

3. На панели **Создать копию экземпляра сервера каталогов** задайте следующие значения:
- a. В поле **Хост** введите IP-адрес или имя хоста, если исходный сервер каталогов находится на удаленном компьютере. Если исходный сервер каталогов находится на локальном компьютере, это поле содержит значение `localhost` и недоступно для изменения.
 - b. В поле **Порт** введите номер порта сервера каталогов, если номер порта, указанный в этом поле, недопустим. Если требуется использовать защищенное соединение, необходимо указать защищенный порт исходного экземпляра сервера каталогов.
 - c. Если экземпляр находится на удаленном компьютере, то в поле **DN администратора** введите DN администратора исходного сервера каталогов. Если исходный сервер каталогов находится на локальном компьютере, то это поле будет содержать DN администратора, которое нельзя изменить.
 - d. В поле **Пароль** введите пароль администратора с указанным DN.
 - e. В поле **Начальный ключ шифрования** введите начальный ключ шифрования для исходного экземпляра сервера каталогов.
 - f. Если для исходного сервера каталогов настроены защищенные соединения, и для целевого сервера каталогов также требуется настроить защищенные соединения, выберите **Использовать защищенное соединение (SSL)**.
 - 1) В поле **Файл ключей** введите полное имя (включая путь) файла базы данных ключей. Для выбора расположения файла нажмите кнопку **Обзор**.
 - 2) В поле **Имя ключа** введите имя используемого личного ключа из файла ключей исходного сервера каталогов.
 - 3) В поле **Пароль для ключей** введите пароль базы данных ключей файла ключей.
 - g. Нажмите кнопку **Далее**.
4. На панели **Настройка экземпляра - шаг 1** выполните следующие действия:
- a. Проверьте информацию об исходном сервере каталогов в полях **Исходный URL** и **Тип исходного экземпляра**. В качестве значения поля **Тип исходного экземпляра** можно указать полный сервер каталогов или экземпляр сервера прокси.
 - b. Для того чтобы настроить целевой сервер каталогов как равноправный узел или как реплику в существующей топологии репликации, включите переключатель **Настроить как равноправный сервер или как сервер-реплику** и выберите одну из следующих опций:
 - Для настройки целевого сервера каталогов как сервера-реплики выберите **Реплика**.
 - Для настройки целевого сервера каталогов как равноправного сервера выберите **Равноправный сервер**.
 - c. В поле **Имя пользователя** введите ИД пользователя системы, которому должен принадлежать целевой экземпляр сервера каталогов. Длина имени не должна превышать 8 символов. Это же имя используется также в качестве имени экземпляра сервера каталогов, ИД администратора DB2, имени экземпляра базы данных и имени базы данных. Этот ИД пользователя должен существовать в системе, и он не должен быть связан ни с каким-либо другим экземпляром сервера каталогов на этом компьютере. Подробная информация об ИД пользователя приведена в разделе “Пользователи и группы, связанные с экземпляром сервера каталогов” на стр. 121.
 - d. В поле **Пароль** введите пароль пользователя с указанным ИД.

- e. В поле **Расположение экземпляра** введите расположение экземпляра сервера каталогов. Для выбора домашнего каталога экземпляра нажмите кнопку **Обзор**. В указанном расположении должно быть свободно не менее 30 МБ памяти. В системе Windows расположением является дисковый привод, например C:. Файлы экземпляра каталога хранятся в каталоге `\idsldap-экземпляр` на указанном приводе. Переменная *экземпляр* - это имя экземпляра сервера каталогов. В системах AIX, Linux и Solaris стандартным путем является домашний каталог владельца экземпляра сервера каталогов, но можно указать и другой путь.
 - f. Нажмите кнопку **Далее**.
5. На панели **Настройка экземпляра - шаг 2** выполните следующие действия:
- a. В поле **DN администратора** введите допустимое отличительное имя (DN) для целевого экземпляра сервера каталогов. Регистр символов в отличительном имени администратора не учитывается. Пользователю с указанным именем предоставляется полный доступ ко всем данным экземпляра сервера каталогов.
 - b. В поле **Пароль** введите пароль администратора с указанным отличительным именем. Пароль вводится с учетом регистра символов. Двухбайтовые символы (DBCS) в паролях не поддерживаются.
 - c. В поле **Подтверждение пароля** введите пароль администратора с указанным DN. Необходимо запомнить пароль для использования в будущем.
 - d. Для копирования данных с исходного сервера на целевой сервер выберите опцию **Скопировать данные из исходного экземпляра в новый экземпляр** и выполните следующие действия:
 - Примечание:** Если был выбран вариант создания целевого сервера каталогов как равноправного сервера или реплики, то этот переключатель включен, и выключить его нельзя.
 - 1) В поле **Каталог образов резервной копии** введите имя каталога образа резервной копии исходного сервера. Для выбора каталога нажмите кнопку **Обзор**. Если исходный экземпляр находится на удаленном компьютере, то каталог резервной копии может быть общим и должен быть достижим как с исходного, так и с целевого компьютера. Примером общего каталога может служить файловая система NFS, доступная для чтения и записи.
 - e. Нажмите кнопку **Далее**.
6. В панели **Проверить параметры** проверьте обзорные сведения.
7. Для запуска процесса копирования исходных серверов каталогов нажмите кнопку **Готово**.
8. В окне **Результаты** проверьте сообщения из протокола, которые записаны для операций создания экземпляра.
9. Для закрытия окна **Результаты** нажмите кнопку **Закрыть**.
10. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Результаты

Инструмент администрирования экземпляра создаст копию исходного экземпляра сервера каталогов на компьютере.

Дальнейшие действия

Необходимо запустить процесс `ibmslapd` и сервер администрирования, связанный с экземпляром сервера каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера” на стр. 158.

Создайте резервную копию экземпляра. Дополнительная информация по резервному копированию экземпляра сервера каталогов приведена в разделе “Резервное копирование сервера каталогов” на стр. 190.

Создание копии существующего экземпляра с помощью утилиты командной строки

Создайте копию экземпляра с помощью утилиты командной строки `idsideploy`.

Прежде чем начать

Для создания копии существующего экземпляра необходимо выполнить следующие требования:

- Запустите процесс `ibmslapd` и сервер администрирования исходного экземпляра в обычном режиме. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.
- Убедитесь, что исходный сервер каталогов доступен с компьютера, на котором требуется создать копию экземпляра.

Процедура

1. Войдите в систему AIX, Linux или Solaris как пользователь `root`, а в систему Windows - как участник группы администраторов.
2. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
3. Для того чтобы создать копию экземпляра без данных на основе существующего экземпляра сервера каталогов, введите следующую команду:

```
idsideploy -sU ldap://хост:порт -sD DN-админ-src -sw пароль-админ-src  
-e начальный-ключ-шифрования -I экземпляр -a пароль-экземпляра -D DN-администратора  
-w пароль-администратора -l расположение-экземпляра
```

Дополнительная информация о команде `idsideploy` приведена в *Справочнике по командам*.

Запуск и остановка сервера каталогов и сервера администрирования

Для использования экземпляра сервера каталогов необходимо запустить процесс `ibmslapd` и сервер администрирования, связанный с экземпляром.

При изменении конфигурации сервера каталогов может потребоваться остановить и запустить сервер каталогов и сервер администрирования для применения изменений. Сервер каталогов и сервер администрирования можно остановить, только если они выполняются в обычном режиме или режиме настройки.

Для запуска и остановки серверов можно использовать Инструмент настройки или утилиты сервера, такие как `ibmslapd` или `ibmdiradm`. Процесс `ibmslapd` связан с сервером каталогов. Экземпляр сервера каталогов можно запустить с помощью

Инструмента администрирования экземпляра только в обычном режиме. В режиме настройки сервер каталогов можно запустить с помощью командной строки.

Сервер каталогов может находиться в одном из следующих состояний:

- Запущен
- Остановлен
- Запущен (только для настройки)

Сервер администрирования может находиться в одном из следующих состояний:

- Запущен
- Остановлен

Запуск и завершение работы сервера каталогов и административного сервера

С помощью Инструмента администрирования экземпляра можно запустить или остановить сервер каталогов, административный сервер или оба этих сервера, связанные с экземпляром.

Прежде чем начать

Для того чтобы можно было запустить или остановить сервер каталогов и административный сервер экземпляра, должны быть выполнены следующие условия:

1. Должен существовать экземпляр с той же версией Инструмента администрирования экземпляра.
2. Если экземпляр не существует, создайте его. См. раздел “Создание экземпляра сервера каталогов по умолчанию” на стр. 134 или “Создание экземпляра сервера каталогов с пользовательскими параметрами” на стр. 136.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. В списке **Список экземпляров каталогов сервера, установленных в системе** выберите экземпляр с той же версией Инструмента администрирования экземпляра.
3. Для того чтобы запустить или остановить сервер каталогов, административный сервер или оба этих сервера, нажмите **Запустить/Остановить**.
4. В окне **Управлять состоянием сервера** выполните следующие действия:
 - Для того чтобы запустить сервер каталогов, административный сервер или оба этих сервера, выполните следующие действия:
 - Для того чтобы запустить сервер каталогов, нажмите **Запустить сервер**.
 - Для того чтобы запустить административный сервер, нажмите **Запустить административный сервер**.
 - Нажмите **ОК**.
 - Для того чтобы остановить сервер каталогов, административный сервер или оба этих сервера, выполните следующие действия:
 - Для того чтобы остановить сервер каталогов, нажмите **Остановить сервер**.
 - Для того чтобы остановить административный сервер, нажмите **Остановить административный сервер**.
 - Нажмите **ОК**.
5. Для закрытия окна **Управлять состоянием сервера** нажмите **Закрыть**.

6. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки

С помощью утилит командной строки можно запустить или остановить сервер каталогов, административный сервер или оба этих сервера, связанные с экземпляром.

Прежде чем начать

Для того чтобы можно было запустить или остановить сервер каталогов и административный сервер экземпляра, должны быть выполнены следующие условия:

- Должен существовать экземпляр с той же версией утилит командной строки. Если экземпляр не существует, создайте его. См. раздел “Создание экземпляра сервера каталогов по умолчанию” на стр. 134 или “Создание экземпляра сервера каталогов с пользовательскими параметрами” на стр. 136.

Процедура

1. Войдите в систему с необходимыми правами доступа. Обратитесь к разделу Глава 20, “Настройка экземпляра”, на стр. 169.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для того чтобы запустить сервер и административный сервер экземпляра, *имя_экземпляра*, выполните следующие команды: Вместо значения *имя_экземпляра* укажите имя экземпляра.

```
ibmslapd -I имя_экземпляра
ibmdiradm -I имя_экземпляра
```
5. Для того чтобы остановить сервер и административный сервер экземпляра, выполните следующие команды: Вместо значения *имя_экземпляра* укажите имя экземпляра.

```
ibmslapd -I экземпляр -k
ibmdiradm -I экземпляр -k
```

Управление конфигурацией экземпляра сервера каталогов

Для проверки состояния, управления и изменения конфигурации экземпляра сервера каталогов или экземпляра прокси-сервера можно использовать Инструмент настройки.

Для управления и изменения конфигурации экземпляра сервера каталогов или экземпляра прокси-сервера можно использовать Инструмент настройки той же версии. Невозможно использовать Инструмент настройки, предоставленный с IBM Security Directory Server для управления экземпляром сервера каталогов или экземпляром прокси-сервера предыдущей или более поздней версии.

Можно открыть Инструмент настройки для экземпляра одним из следующих способов:

- Используйте Инструмент администрирования экземпляра.
- Выполните команду **idsxcfg** с именем экземпляра в качестве значения параметра.

Более подробная информация об Инструменте настройки находится в разделе Глава 20, “Настройка экземпляра”, на стр. 169.

Открытие Инструмента настройки из Инструмента администрирования экземпляра

Откройте Инструмент настройки IBM Security Directory Server, чтобы управлять или изменить конфигурацию экземпляра сервера каталогов или экземпляра сервера проху.

Прежде чем начать

Для управления экземпляром с помощью Инструмента настройки должны быть выполнены следующие условия:

- Должен существовать экземпляр с той же версией Инструмента настройки. Если экземпляр не существует, создайте его. См. раздел “Создание экземпляра сервера каталогов по умолчанию” на стр. 134 или “Создание экземпляра сервера каталогов с пользовательскими параметрами” на стр. 136.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. В списке **Список экземпляров каталогов сервера, установленных в системе** выберите экземпляр с той же версией Инструмента администрирования экземпляра.
3. Для управления экземпляром с помощью Инструмента настройки нажмите **Управлять**. Откроется окно Инструмент настройки IBM Security Directory Server для экземпляра.
4. Для того чтобы закрыть Инструмент настройки, выберите **Файл > Выход**.
5. В окне подтверждения Инструмент настройки нажмите **Да**.

Изменение параметров TCP/IP экземпляра

С помощью Инструмента администрирования экземпляра или утилит командной строке можно изменить параметры TCP/IP экземпляра сервера каталогов или экземпляра прокси-сервера.

Для изменения параметров TCP/IP экземпляра должны совпадать версии экземпляра и Инструмента администрирования экземпляра.

Изменение параметров TCP/IP экземпляра с помощью Инструмента администрирования экземпляра

Параметры TCP/IP существующего экземпляра можно изменить с помощью Инструмента администрирования экземпляра.

Прежде чем начать

Для изменения параметров TCP/IP экземпляра с помощью Инструмента администрирования экземпляра необходимо выполнение следующих условий:

1. Должен существовать экземпляр с той же версией Инструмента администрирования экземпляра.
2. Необходимо остановить сервер каталогов и сервер администрирования экземпляра. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера” на стр. 158.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. В списке **Список экземпляров каталогов сервера, установленных в системе** выберите экземпляр с той же версией Инструмента администрирования экземпляра.
3. Для изменения параметров TSP/IP экземпляра выберите **Изменить параметры TSP/IP**. Откроется окно **Изменить параметры TSP/IP** для экземпляра.
4. В окне **Изменить параметры TSP/IP** выберите одну из следующих опций:
 - Если экземпляр должен использовать все настроенные на компьютере IP-адреса, выберите **Использовать все настроенные IP-адреса**.
 - Если экземпляр должен применять только часть IP-адресов, настроенных на компьютере, выполните следующие действия:
 - a. Выключите переключатель **Использовать все настроенные IP-адреса**.
 - b. В списке **Выбрать конкретные IP-адреса для использования** выберите IP-адреса, которые должны использоваться экземпляром.
5. Нажмите кнопку **Далее**.
6. На панели **Сведения о портах** укажите следующие значения:

Примечание: Портам сервера каталогов необходимо присвоить уникальные номера, которые не должны конфликтовать с существующими портами, которые используются на компьютере. В системах AIX, Linux и Solaris порты с номерами в диапазоне 1-1000 могут использоваться только пользователем root.

- a. В поле **Порт сервера** введите номер порта, который должен использоваться сервером как незащищенный порт. Номер должен принадлежать диапазону 1-65535.
 - b. В поле **Защищенный порт сервера** введите номер порта, который должен использоваться сервером как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - c. В поле **Порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как незащищенный порт. Номер должен принадлежать диапазону 1-65535.
 - d. В поле **Защищенный порт сервера администрирования** введите номер порта, который должен использоваться сервером администрирования как защищенный порт. Номер должен принадлежать диапазону 1-65535.
 - e. Нажмите кнопку **Готово**.
7. В окне **Изменить TSP/IP - Результаты** проверьте сообщения протокола для операции изменения параметров TSP/IP.
 8. Для закрытия окна **Изменить TSP/IP - Результаты** нажмите кнопку **Закрыть**.
 9. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Изменение параметров TSP/IP экземпляра с помощью утилит командной строки

Параметры TSP/IP и портов существующего экземпляра можно изменить с помощью команд **idssethost** и **idssetport**.

Прежде чем начать

Для изменения параметров TSP/IP экземпляра с помощью утилит командной строки необходимо выполнение следующих условий:

1. Должен существовать экземпляр с той же версией утилит командной строки.
2. Необходимо остановить сервер каталогов и сервер администрирования экземпляра. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему AIX, Linux или Solaris как пользователь root, а в систему Windows - как участник группы администраторов.
2. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
3. Для изменения IP-адреса сервера каталогов *экземпляр* выберите одну из следующих опций: Вместо переменной *экземпляр* укажите имя своего экземпляра.

IP-адрес для связывания	Выполняемая команда:
Конкретный IP-адрес <code>xx.xx.xx.xx</code> на компьютере	<code>idssethost -I <i>экземпляр</i> -i xx.xx.xx.xx</code>
Все IP-адреса, настроенные на компьютере	<code>idssethost -I <i>экземпляр</i> -i all</code>

4. Для изменения номеров портов сервера каталогов *экземпляр* введите следующую команду: Вместо переменной *экземпляр* укажите имя своего экземпляра.

Примечание: Портам сервера каталогов необходимо присвоить уникальные номера, которые не должны конфликтовать с существующими портами, которые используются на компьютере. В системах AIX, Linux и Solaris порты с номерами в диапазоне 1-1000 могут использоваться только пользователем root.

Настраиваемые порты	Выполняемая команда:
Порт сервера	<code>idssetport -I <i>экземпляр</i> -p порт</code>
Защищенный порт сервера	<code>idssetport -I <i>экземпляр</i> -s порт</code>
Порт сервера администрирования	<code>idssetport -I <i>экземпляр</i> -a адм-порт</code>
Защищенный порт сервера администрирования	<code>idssetport -I <i>экземпляр</i> -с адм-защищ-порт</code>

Дополнительная информация о командах **idssethost** и **idssetport** приведена в *Справочнике по командам*.

5. Запустите сервер каталогов и сервер администрирования. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Просмотр информации об экземпляре

С помощью Инструмента администрирования экземпляра или утилиты командной строки можно просмотреть сведения об экземпляре, такие как домашний каталог, IP-адреса и порты экземпляра.

Можно просмотреть информацию о всех существующих экземплярах на компьютере. Состоянием экземпляра может быть остановлен или запущен.

Команда **idsilist** также предоставляет подобную информацию для данного экземпляра или всех экземпляров, доступных на компьютере. Более подробная информация о команде **idsilist** находится в *Справочнике по командам*.

Просмотр сведений об экземпляре с помощью Инструмента администрирования экземпляра

Используйте Инструмент администрирования экземпляра для просмотра сведений об имеющемся экземпляре.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. В **Списке экземпляров сервера каталогов, установленных в системе** выберите экземпляр, сведения о котором требуется просмотреть.
3. Нажмите кнопку **Просмотреть**. Откроется окно **Просмотреть сведения об экземпляре** с общими сведениями и данными о ТСП/IP выбранного экземпляра.
4. Для закрытия окна **Просмотреть сведения об экземпляре** нажмите кнопку **Закрыть**.
5. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Просмотр сведений об экземпляре с помощью утилиты командной строки

Используйте команду **idsilist** для просмотра сведений об имеющемся экземпляре.

Процедура

1. Войдите в систему AIX, Linux или Solaris как пользователь root, а в систему Windows - как участник группы администраторов.
2. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
3. Для просмотра информации об экземплярах на компьютере запустите соответствующую команду **idsilist**:

Выполняемая задача	Выполняемая команда:
Перечислить все экземпляры	<code>idsilist</code>
Перечислить все экземпляры с полной информацией и описанием	<code>idsilist -a</code>
Перечислить все экземпляры с полной информацией в необработанном формате	<code>idsilist -r</code>
Показать определенный экземпляр	<code>idsilist -I <i>экземпляр</i></code>
Показать определенный экземпляр с полной информацией и описанием	<code>idsilist -I <i>экземпляр</i> -a</code>
Показать определенный экземпляр с полной информацией в необработанном формате	<code>idsilist -I <i>экземпляр</i> -r</code>

Дополнительные сведения о команде **idsilist** приведены в *Справочнике по командам*.

Удаление экземпляра сервера каталогов

С помощью инструмента администрирования экземпляра или утилиты командной строки можно удалить экземпляр сервера каталогов или экземпляр прокси-сервера.

Может потребоваться удалить экземпляр с компьютера, если экземпляр был перенесен на другой компьютер или больше не нужен.

Если требуется удалить сервер каталогов с базой данных DB2, рекомендуется перед удалением экземпляра создать его резервную копию. Если требуется удалить экземпляр прокси-сервера, рекомендуется создать резервную копию экземпляра.

Примечание: В случае экземпляра прокси-сервера единственной допустимой опцией является удаление экземпляра.

В случае использования инструмента администрирования экземпляра можно выбрать один из следующих вариантов:

- Удалить экземпляр сервера каталогов, но не удалять экземпляр базы данных
- Удалить экземпляр сервера каталогов, а также удалять связанный экземпляр базы данных DB2

В случае использования команды **idsidrop** можно выбрать один из следующих вариантов:

- Удалить экземпляр сервера каталогов, но не удалять экземпляр базы данных
- Удалить экземпляр сервера каталогов, а также удалять связанный экземпляр базы данных DB2
- Удалить конфигурацию, связывающую экземпляр сервера каталогов с экземпляром базы данных DB2, но не удалять экземпляр сервера каталогов

Дополнительная информация о команде **idsidrop** приведена в разделе *Справочник по командам*.

Удаление экземпляра с помощью Инструмента администрирования экземпляра

Экземпляр сервера каталогов или сервера прокси можно удалить с помощью Инструмента администрирования экземпляра.

Прежде чем начать

Для изменения параметров TCP/IP экземпляра с помощью Инструмента администрирования экземпляра необходимо выполнение следующих условий:

1. Должен существовать экземпляр с той же версией Инструмента администрирования экземпляра.
2. Необходимо остановить сервер каталогов и сервер администрирования экземпляра. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера” на стр. 158.

Процедура

1. Запустите Инструмент администрирования экземпляра. См. раздел “Запуск Инструмента администрирования экземпляра” на стр. 132.
2. В списке **Список экземпляров каталогов сервера, установленных в системе** выберите экземпляр с той же версией Инструмента администрирования экземпляра.
3. Для запуска процедуры удаления нажмите кнопку **Удалить**.
4. В окне **Удалить экземпляр сервера каталогов** выполните следующие действия:
 - a. Выберите один из следующих методов удаления:
 - Для удаления экземпляра сервера каталогов без удаления связанного экземпляра базы данных DB2 выберите опцию **Удалить только экземпляр сервера каталогов**.

Примечание: В случае экземпляра сервера прокси опция **Удалить только экземпляр сервера каталогов** будет единственной доступной опцией.

- Для удаления экземпляра сервера каталогов вместе со связанным экземпляром базы данных DB2 выберите опцию **Удалить экземпляр сервера каталогов и уничтожить связанный экземпляр базы данных**.
- b. Нажмите кнопку **Удалить**.
- c. В окне **Предупреждение** нажмите кнопку **Да**, чтобы подтвердить удаление экземпляра.
- d. В окне **Информация** нажмите кнопку **ОК**.
- e. Для закрытия окна **Удалить экземпляр сервера каталогов** нажмите кнопку **Закрыть**.
- f. Для закрытия Инструмента администрирования экземпляра нажмите **Закрыть**.

Удаление экземпляра с помощью утилиты командной строки

Существующий экземпляр можно удалить с помощью команды **idsidrop**.

Прежде чем начать

Для удаления экземпляра с помощью утилиты командной строки необходимо выполнить следующие условия:

1. Должен существовать экземпляр с той же версией утилиты командной строки.
2. Необходимо остановить сервер каталогов и сервер администрирования экземпляра. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему AIX, Linux или Solaris как пользователь root, а в систему Windows - как участник группы администраторов.
2. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
3. Для удаления экземпляра *экземпляр* выберите одну из следующих опций: Вместо переменной *экземпляр* укажите имя своего экземпляра.

Выполняемая задача	Выполняемая команда:
Удалить экземпляр сервера каталогов и сохранить связанный экземпляр базы данных	<code>idsidrop -I <i>экземпляр</i></code>
Удалить экземпляр сервера каталогов вместе со связанным экземпляром базы данных	<code>idsidrop -I <i>экземпляр</i> -r</code>
Удалить конфигурацию связанного экземпляра базы данных без удаления экземпляра сервера каталогов	<code>idsidrop -I <i>экземпляр</i> -R</code>

Дополнительная информация о команде **idsidrop** приведена в *Справочнике по командам*.

Глава 19. Проверка структуры каталогов

После установки IBM Security Directory Server необходимо проверить структуру каталогов.

32-разрядные и 64-разрядные системы Windows

Завершив установку IBM Security Directory Server в операционной системе Windows, можно убедиться в наличии следующих каталогов и файлов в установочном расположении, например в расположении C:\Program Files\IBM\LDAP\V6.3.1 (установочное расположение можно изменить):

- appsrv
- etc
- java
- lib
- messages
- bin
- examples
- javaliб
- lib64
- nls
- var
- codeset
- idstools
- jre
- license
- properties
- config
- include
- ldapcfg.ico
- протоколы
- sbin

64-разрядные системы Linux

Завершив установку IBM Security Directory Server в операционной системе Linux, можно убедиться в наличии следующих каталогов и файлов в установочном расположении, например в расположении /opt/ibm/ldap/V6.3.1 (установочное расположение изменить нельзя):

- bin
- codeset
- config
- etc
- examples
- idstools
- include
- javaliб
- LAPID
- lib
- lib64
- nls

properties
sbin
tmp
web

Глава 20. Настройка экземпляра

С помощью инструмента настройки или утилит командной строки можно настроить экземпляр сервера каталогов или экземпляр прокси-сервера в соответствии с вашими требованиями.

IBM Security Directory Server Инструмент администрирования экземпляра (**idsxcfg**) - это графический пользовательский интерфейс (GUI), с помощью которого можно настроить экземпляр. Для того чтобы использовать Инструмент настройки, необходим IBM Java Development Kit.

Для запуска инструмента настройки необходимо войти в систему со следующими идентификационными данными:

AIX, Linux или Solaris

- Пользователь Root
- Владелец экземпляра сервера каталогов
- ИД пользователя из главной группы владельца экземпляра сервера каталогов

Windows

- ИД пользователя из группы администраторов по умолчанию

С помощью инструмента настройки можно также изменить конфигурацию сервера каталогов.

С помощью инструмента настройки в полноценном экземпляре сервера каталогов можно выполнять следующие задачи:

- Запускать и останавливать сервер
- Управлять DN и паролем главного администратора
- Настраивать и выключать базу данных DB2 для экземпляра сервера каталогов
- Оптимизировать базу данных, связанную с экземпляром
- Обслуживать базу данных DB2 с помощью организации индексов DB2 или сжатия строк DB2
- Выполнять резервное копирование и восстановление базы данных
- Настраивать производительность экземпляра сервера каталогов
- Включать и выключать протокол изменений
- Добавлять и удалять суффиксы
- Добавлять и удалять файлы схемы
- Импортировать и экспортировать данные LDIF
- Настроить синхронизацию Active Directory

С помощью инструмента настройки в экземпляре прокси-сервера можно выполнять следующие задачи:

- Запускать и останавливать сервер
- Управлять DN и паролем главного администратора
- Добавлять и удалять суффиксы
- Добавлять и удалять файлы схемы
- Выполнять резервное копирование и восстановление экземпляра

Запуск Инструмента настройки

Запустите Инструмент настройки IBM Security Directory Server для экземпляра, чтобы настроить экземпляр в соответствии с требованиями среды каталогов.

Прежде чем начать

Для управления экземпляром с помощью Инструмента настройки должны быть выполнены следующие условия:

- Должен существовать экземпляр с той же версией Инструмента настройки. Если экземпляр не существует, создайте его. См. раздел “Создание экземпляра сервера каталогов с пользовательскими параметрами” на стр. 136 или “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.
- В установочном пути IBM Security Directory Server должен существовать IBM Java Development Kit. Установочный путь по умолчанию IBM Security Directory Server приведен в разделе “Установочные расположения по умолчанию” на стр. 27.

Процедура

1. Войдите в систему с необходимыми правами доступа. Обратитесь к разделу Глава 20, “Настройка экземпляра”, на стр. 169.
2. Откройте командную строку.
3. Из текущего рабочего каталога перейдите в подкаталог `sbin` в установочном каталоге IBM Security Directory Server.
4. Выполните команду `idsxcfg` в следующем формате: Вместо переменной *имя_экземпляра* укажите имя экземпляра.

```
idsxcfg -I имя_экземпляра
```

Откроется окно Инструмент настройки IBM Security Directory Server для указанного экземпляра.

5. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
6. В окне подтверждения Инструмент настройки нажмите **Да**.

Запуск и остановка сервера каталогов и сервера администрирования с помощью Инструмента настройки

Инструмент настройки можно использовать для запуска процесса `ibmslapd` и сервера администрирования, связанного с экземпляром.

При изменении конфигурации сервера каталогов может потребоваться остановить и запустить сервер каталогов и сервер администрирования для применения изменений. Сервер каталогов и сервер администрирования можно остановить, только если они выполняются в обычном режиме или режиме настройки.

Для запуска и остановки сервера каталогов и сервера администрирования можно использовать Инструмент настройки или утилиты сервера, такие как `ibmslapd` или `ibmdiradm`. Процесс `ibmslapd` связан с сервером каталогов. Экземпляр сервера каталогов можно запустить с помощью Инструмента настройки только в обычном режиме. В режиме настройки сервер каталогов можно запустить с помощью командной строки.

Сервер каталогов может находиться в одном из следующих состояний:

- Запущен
- Остановлен

- Запущен (только для настройки)

Сервер администрирования может находиться в одном из следующих состояний:

- Запущен
- Остановлен

Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки

С помощью Инструмента настройки можно запустить или остановить сервер каталогов, административный сервер или оба этих сервера, связанные с экземпляром.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Управлять состоянием сервера**.
3. На странице **Текущее состояние** проверьте текущее состояние сервера и административного сервера.
4. На странице **Текущее состояние** выполните следующие действия:
 - Для того чтобы запустить сервер каталогов, административный сервер или оба этих сервера, выполните следующие действия:
 - Для того чтобы запустить сервер каталогов, нажмите **Запустить сервер**.
 - Для того чтобы запустить административный сервер, нажмите **Запустить административный сервер**.
 - В окне **Информация** нажмите **ОК**.
 - Для того чтобы остановить сервер каталогов, административный сервер или оба этих сервера, выполните следующие действия:
 - Для того чтобы остановить сервер каталогов, нажмите **Остановить сервер**.
 - Для того чтобы остановить административный сервер, нажмите **Остановить административный сервер**.
 - В окне **Информация** нажмите **ОК**.
5. Для закрытия страницы **Текущее состояние** нажмите **Закрыть**.
6. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
7. В окне подтверждения Инструмент настройки нажмите **Да**.

Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки

С помощью утилит командной строки можно запустить или остановить сервер каталогов, административный сервер или оба этих сервера, связанные с экземпляром.

Прежде чем начать

Для того чтобы можно было запустить или остановить сервер каталогов и административный сервер экземпляра, должны быть выполнены следующие условия:

- Должен существовать экземпляр с той же версией утилит командной строки. Если экземпляр не существует, создайте его. См. раздел “Создание экземпляра сервера каталогов по умолчанию” на стр. 134 или “Создание экземпляра сервера каталогов с пользовательскими параметрами” на стр. 136.

Процедура

1. Войдите в систему с необходимыми правами доступа. Обратитесь к разделу Глава 20, “Настройка экземпляра”, на стр. 169.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для того чтобы запустить сервер и административный сервер экземпляра, *имя_экземпляра*, выполните следующие команды: Вместо значения *имя_экземпляра* укажите имя экземпляра.

```
ibmslapd -I имя_экземпляра  
ibmdiradm -I имя_экземпляра
```
5. Для того чтобы остановить сервер и административный сервер экземпляра, выполните следующие команды: Вместо значения *имя_экземпляра* укажите имя экземпляра.

```
ibmslapd -I экземпляр -k  
ibmdiradm -I экземпляр -k
```

Управление DN главного администратора для экземпляра

Для доступа к конфигурации и всем данным каталога экземпляра необходимо создать и настроить DN главного администратора для экземпляра.

DN администратора - это DN, применяемое главным администратором экземпляра. Можно создать только одного главного администратора для экземпляра.

DN по умолчанию равен `cn=root`. Значение DN не учитывает регистр символов.

DN содержит пары атрибут:значение, разделенные запятыми. Ниже показан пример значения DN.

```
cn=Ben Gray,ou=dept_audit,o=sample
```

Для того чтобы установить или изменить DN главного администратора, можно использовать Инструмент настройки или утилиту командной строки **idsdnpw**. Для того чтобы задать или изменить DN главного администратора, необходимо остановить процесс `ibmslapd`, связанный с экземпляром.

Настройка отличительного имени (DN) главного администратора с помощью Инструмента настройки

DN главного администратора для экземпляра можно настроить с помощью Инструмента настройки.

Прежде чем начать

Для настройки DN главного администратора для экземпляра необходимо выполнение следующих требований:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на левой панели навигации выберите **Работа с DN администратора**.

3. В поле **DN администратора** введите отличительное имя главного администратора или оставьте значение по умолчанию `cn=root`.
4. Нажмите **ОК**.
5. Для подтверждения этого действия нажмите кнопку **ОК**.
6. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
7. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Настройка отличительного имени (DN) главного администратора с помощью утилиты командной строки

DN главного администратора для экземпляра можно настроить с помощью утилиты командной строки **idsdnpw**.

Прежде чем начать

Для настройки DN главного администратора для экземпляра необходимо выполнение следующих требований:

- Необходимо остановить сервер каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Об этой задаче

Если отличительное имя администратора не указано, то в файле `ibmslapd.conf` для экземпляра сервера каталогов задается DN администратора по умолчанию `cn=root`. Требуется задать пароль главного администратора для экземпляра.

Если пароль не указан, команда **idsdnpw** выдает запрос на ввод пароля. При вводе пароля он не будет отображаться в командной строке.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sb1n` в расположении установки IBM Security Directory Server.
4. Для задания DN администратора для экземпляра введите следующую команду:
Вместо переменных экземпляр, DN-администратора и пароль-администратора укажите значения в соответствии с конкретными требованиями.
`idsdnpw -I экземпляр -u DN-администратора -p пароль-администратора`

Дополнительная информация о команде **idsdnpw** приведена в *Справочнике по командам*.

Дальнейшие действия

Запустите сервер каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Управление паролем главного администратора для экземпляра

Для выполнения аутентификации в экземпляре и доступа к конфигурации и всем данным каталога необходимо создать и настроить пароль главного администратора для экземпляра.

Пароль администратора учитывает регистр символов. В пароле нельзя использовать набор двухбайтовых символов (DBCS), так как он не поддерживается. Необходимо сохранить пароль администратора.

Для настройки пароля главного администратора можно использовать Инструмент настройки или утилиту командной строки **idsdnpw**. Для настройки пароля администратора необходимо остановить процесс `ibmslapd`, связанный с экземпляром.

Если включена стратегия управления паролем администратора, то пароль главного администратора должен отвечать требованиям этой стратегии. Информация о стратегии паролей приведена в разделе *Администрирование* документации по IBM Security Directory Server.

Настройка пароля главного администратора с помощью Инструмента настройки

Пароль главного администратора для экземпляра можно настроить с помощью Инструмента настройки.

Прежде чем начать

Для настройки пароля главного администратора экземпляра необходимо выполнение следующих требований:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на левой панели навигации выберите **Управление паролем администратора**.
3. В поле **Пароль администратора** введите пароля главного администратора.
4. В поле **Подтверждение пароля** введите пароль главного администратора.
5. Нажмите **ОК**.
6. Для подтверждения этого действия нажмите кнопку **ОК**.
7. Для закрытия страницы **Управление паролем администратора** нажмите кнопку **ОК**.
8. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
9. Для подтверждения этого действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Настройка пароля главного администратора с помощью утилиты командной строки

Для настройки пароля главного администратора для экземпляра можно использовать утилиту командной строки **idsdnpw**.

Прежде чем начать

Для настройки пароля главного администратора для экземпляра необходимо выполнение следующих требований:

- Необходимо остановить сервер каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для задания пароля администратора для экземпляра введите следующую команду: Вместо переменных экземпляр, DN-администратора и пароль-администратора укажите значения в соответствии с конкретными требованиями.

```
idsdnpw -I экземпляр -u DN-администратора -p пароль-администратора
```

Дополнительная информация о команде **idsdnpw** приведена в *Справочнике по командам*.

Дальнейшие действия

Запустите сервер каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Настройка базы данных для экземпляра сервера каталогов

Для того чтобы использовать экземпляр как сервер каталогов и хранить данные каталогов, необходимо настроить для экземпляра базу данных DB2.

Инструмент администрирования экземпляра, Инструмент настройки или команда **idscfgdb** позволяют создать и настроить базу данных DB2. Перед настройкой или отключением базы данных необходимо остановить сервер каталогов. Дополнительная информация о команде **idscfgdb** приведена в разделе *Справочник по командам*.

Если выбран вариант создания экземпляра по умолчанию с помощью инструмента администрирования экземпляра, то для экземпляра будет также создан и настроен экземпляр базы данных DB2. Если создается прокси-сервер, то настраивать базу данных DB2 не требуется.

Если для экземпляра настраивается база данных DB2, то в файле конфигурации экземпляра появляется информация о базе данных DB2. Инструмент также создает параметры базы данных и локальной обратной связи.

Если параметры базы данных и локальной обратной связи не существовали, то они будут созданы. Можно указать, какая кодировка должна применяться для создаваемой базы данных - локальная кодовая страница или UTF-8. По умолчанию для создания базы данных DB2 применяется кодовая страница UTF-8.

Настройка базы данных экземпляра с помощью Инструмента настройки

Настройте базу данных DB2 экземпляра сервера каталогов с помощью Инструмента настройки.

Прежде чем начать

Для того чтобы настроить базу данных DB2 для экземпляра сервера каталогов, необходимо выполнить следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.
- Должен существовать ИД пользователя системы - владельца экземпляра базы данных DB2. Дополнительная информация о требованиях к ИД пользователя системы приведена в разделе “Пользователи и группы, связанные с экземпляром сервера каталогов” на стр. 121.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на левой панели навигации выберите **Задачи базы данных > Настроить базу данных**.
3. На странице **Настроить базу данных** выберите одну из следующих опций:
 - Для настройки базы данных для экземпляра выполните следующие действия:
 - a. В поле **Имя пользователя базы данных** введите ИД пользователя системы, которому принадлежит база данных. Этот ИД будет применяться сервером каталогов для подключения к базе данных.
 - b. В поле **Пароль** введите пароль администратора базы данных.
 - c. В поле **Имя базы данных** введите имя базы данных.
 - d. Если требуется задать любые из следующих параметров конфигурации DB2, выберите **Показать дополнительные опции табличного пространства**.
 - Требуется, чтобы для хранения табличных пространств базы данных DB2 применялась технология управляемого системой хранения (SMS). При использовании SMS табличное пространство для хранения таблиц DB2 выделяется и управляется администратором файловой системы операционной системы.
 - Требуется, чтобы для хранения табличных пространств базы данных DB2 применялась технология хранения, управляемого базой данных (DMS). Кроме того, требуется настроить табличные пространства USERSPACE1 и LDAPSPACE, их размер и расположение. При использовании DMS табличные пространства управляются администратором базы данных. Администратор базы данных отвечает за выбор устройств и файлов, а DB2 управляет памятью этих устройств и файлов.

Если переключатель **Показать дополнительные опции табличных пространств** не включен, то создается база данных DB2 с табличными пространствами USERSPACE1 и LDAPSPACE с использованием DMS с размерами и расположением по умолчанию. Если настраивается экземпляр

с существующей базой данных, то при вводе имени существующей базы данных в поле **Имя базы данных** переключатель **Показать дополнительные опции табличных пространств** выключается.

- e. Нажмите кнопку **Далее**.
- Для повторной настройки пароля администратора базы данных выполните следующие действия:
 - a. Нажмите кнопку **Сбросить пароль**.
 - b. В поле **Пароль** введите пароль администратора базы данных.
 - c. В поле **Подтверждение пароля** введите пароль администратора базы данных.
 - d. Нажмите кнопку **Далее**.
- 4. Если создается и настраивается база данных DB2, выполните следующие действия:
 - a. В поле **Установочный каталог базы данных** введите расположение базы данных. Для выбора каталога нажмите кнопку **Обзор**. В Windows необходимо указать имя диска, например C: . В AIX, Linux и Solaris расположение должно быть именем каталога, например: /home/ldapdb.

Примечание: Минимальный объем памяти на диске для базы данных DMS составляет 1 ГБ. Для базы данных SMS требуется минимум 150 МБ дисковой памяти. Указанные требования относятся к пустой базе данных. Для хранения данных потребуются дополнительная память.

- b. Для того чтобы настроить сервер каталогов с базой данных для оперативного резервного копирования, выполните следующие действия:
 - 1) Выберите **Настроить для оперативного резервного копирования**.
 - 2) В поле **Расположение резервной копии базы данных** введите расположение для хранения образа резервной копии. Расположение можно выбрать с помощью кнопки **Обзор**.

Примечание: Не выходите из Инструмента настройки и не отменяйте операцию при запуске операции резервного копирования. Если база данных настраивалась для оперативного резервного копирования, то после завершения ее настройки выполняется первоначальное автономное резервное копирование. После его завершения перезапускается сервер администрирования. Оперативное резервное копирование для экземпляра сервера каталогов также можно настроить с помощью команды **idscfgdb**. Однако отменить настройку оперативного резервного копирования с помощью команды **idscfgdb** и параметра **-c** нельзя. Если оперативное резервное копирование для экземпляра было настроено с помощью Инструмента администрирования экземпляра или Инструмента настройки, то его настройку можно отменить с помощью Инструмента настройки или команды **idscfgdb**.

- c. В области **Опция кодировки** выберите одну из следующих опций для создания типа базы данных:

Примечание: Если данные планируется хранить на сервере каталогов на нескольких языках, создайте универсальную базу данных DB2. Универсальная база данных DB2 также является наиболее эффективной, так как требуется меньше операций перевода данных. Для применения тегов языка база данных должна быть создана в формате UTF-8. За дополнительной информацией об UTF-8 обратитесь к разделу “Поддержка UTF-8” на стр. 126.

- Для создания базы данных UTF-8, в которой клиенты LDAP смогут хранить символьные данные UTF-8, выберите **Создать универсальную базу данных DB2**.
 - Для создания базы данных с локальной кодовой страницей выберите **Создать базу данных DB2 с локальной кодовой страницей**.
- d. Нажмите кнопку **Далее**.
5. Если включен переключатель **Показать дополнительные опции табличных пространств**, то необходимо выполнить следующие действия:
- a. В списке **Выбрать тип табличного пространства базы данных** выберите тип базы данных. Тип табличного пространства базы данных по умолчанию - DMS. При выборе типа табличного пространства SMS все остальные поля будут недоступны. Поддержка табличного пространства DMS используется только для табличных пространств USERSPACE1 и LDAPSPACE. Все остальные табличные пространства, например табличное пространство каталога или временное табличное пространство, имеют тип SMS.
 - a. В области **Сведения о табличном пространстве USERSPACE1** укажите следующую информацию:
 - 1) В списке **Контейнер табличного пространства** выберите тип контейнера. Если табличное пространство USERSPACE1 должно находиться в файловой системе, выберите **Файл**. Если контейнер табличного пространства базы данных расположен в файловой системе, то создается табличное пространство DMS cooked. Можно указать начальный размер табличного пространства и приращение для автоматического увеличения размера табличного пространства, если это потребуется. Если табличное пространство USERSPACE1 требуется создать на устройстве с линейным доступом, выберите **Устройство с линейным доступом**. Устройство с линейным доступом - это устройство, на котором отсутствует файловая система, например, жесткий диск без файловой системы. Если контейнер табличного пространства базы данных расположен на устройстве с линейным доступом, то создается табличное пространство DMS raw. В этом случае размер контейнера табличного пространства базы данных фиксирован и не может быть увеличен. При выборе типа **Устройство с линейным доступом** вместо значений по умолчанию укажите размер и расположение контейнера.
 - 2) Если в списке **Контейнер табличного пространства** выбран тип **Файл**, то укажите следующую информацию:
 - a) В поле **Путь к каталогу** укажите путь к каталогу, в котором требуется создать табличное пространство USERSPACE1. Для выбора каталога нажмите кнопку **Обзор**.
 - b) В поле **Имя файла** введите имя файла создаваемого табличного пространства или примите значение по умолчанию (USPACE).
 - c) В поле **Начальный размер** введите начальный размер табличного пространства USERSPACE1 в страницах или примите значение по умолчанию. Контейнер табличного пространства USERSPACE1 типа **Файл** является автоматически расширяемым. Можно задать начальный размер в поле **Начальный размер** и приращение в поле **Размер расширения**. Значение начального размера по умолчанию - 16000 страниц, приращение по умолчанию - 8000 страниц. Размер страницы контейнера табличного пространства USERSPACE1 равен 4 КБ.
 - 3) Если в списке **Контейнер табличного пространства** выбран тип **Устройство с линейным доступом**, то укажите следующую информацию:

- a) В поле **Путь к устройству** укажите расположение устройства с линейным доступом. В Windows путь должен начинаться с \\.\. Пример: \\.\имя-устройства. В AIX, Linux и Solaris необходимо указать допустимый путь к устройству.
 - b) В поле **Начальный размер** введите начальный размер табличного пространства USERSPACE1 или примите значение по умолчанию. Размер контейнера табличного пространства USERSPACE1 типа **Устройство с линейным доступом** является фиксированным. По умолчанию он составляет 16000 страниц. Для лучших результатов рекомендуется указать значение с учетом текущих требований.
- b. В области **Сведения о табличном пространстве LDAPSPACE** укажите следующую информацию:
- 1) В списке **Контейнер табличного пространства** выберите тип контейнера. Если табличное пространство LDAPSPACE должно находиться в файловой системе, выберите **Файл**. Если табличное пространство LDAPSPACE требуется создать на устройстве с линейным доступом, выберите **Устройство с линейным доступом**. Устройство с линейным доступом - это устройство, на котором отсутствует файловая система, например, жесткий диск без файловой системы.
 - 2) Если в списке **Контейнер табличного пространства** выбран тип **Файл**, то укажите следующую информацию:
 - a) В поле **Путь к каталогу** укажите путь к каталогу, в котором требуется создать табличное пространство LDAPSPACE. Для выбора каталога нажмите кнопку **Обзор**.
 - b) В поле **Имя файла** введите имя файла создаваемого табличного пространства или примите значение по умолчанию (ldapspace).
 - c) В поле **Начальный размер** введите начальный размер табличного пространства LDAPSPACE в страницах или примите значение по умолчанию. Контейнер табличного пространства LDAPSPACE типа **Файл** является автоматически расширяемым. Можно задать начальный размер в поле **Начальный размер** и приращение в поле **Размер расширения**. Значение начального размера по умолчанию - 16000 страниц, приращение по умолчанию - 8000 страниц. Размер страницы контейнера табличного пространства LDAPSPACE равен 32 КБ.
 - 3) Если в списке **Контейнер табличного пространства** выбран тип **Устройство с линейным доступом**, то укажите следующую информацию:
 - a) В поле **Путь к устройству** укажите расположение устройства с линейным доступом. В Windows путь должен начинаться с \\.\. Пример: \\.\имя-устройства. В AIX, Linux и Solaris необходимо указать допустимый путь к устройству.
 - b) В поле **Начальный размер** введите начальный размер табличного пространства LDAPSPACE или примите значение по умолчанию. Размер контейнера табличного пространства LDAPSPACE типа **Устройство с линейным доступом** является фиксированным. По умолчанию он составляет 16000 страниц. Для лучших результатов рекомендуется указать значение с учетом текущих требований.
 - c. Если в одном или в обоих полях **Контейнер табличного пространства** выбрано значение **Файл**, то в поле **Размер расширения** укажите число страниц для расширения контейнеров.
6. Нажмите кнопку **Готово**.
 7. Для подтверждения выполнения задачи нажмите кнопку **ОК**.

8. Проверьте протоколы, созданные в ходе настройки базы данных.
9. Для закрытия страницы **Настроить базу данных** нажмите кнопку **Заккрыть**.
10. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
11. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

После настройки базы данных необходимо выполнить следующие действия для настройки экземпляра:

- Настроить DN и пароль главного администратора. (См. раздел “Настройка отличительного имени (DN) главного администратора с помощью Инструмента настройки” на стр. 172 и “Настройка пароля главного администратора с помощью Инструмента настройки” на стр. 174.)
- Настроить требуемые суффиксы. Обратитесь к разделу “Настройка суффикса” на стр. 204.

Настройка базы данных экземпляра с помощью утилиты командной строки

Настройте базу данных DB2 экземпляра сервера каталогов с помощью утилиты командной строки **idscfgdb**.

Прежде чем начать

Для того чтобы настроить базу данных DB2 для экземпляра сервера каталогов, необходимо выполнить следующие действия:

- Не задавайте переменную среды *DB2COMM* при настройке базы данных.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.
- Должен существовать ИД пользователя системы - владельца экземпляра базы данных DB2. Дополнительная информация о требованиях к ИД пользователя системы приведена в разделе “Пользователи и группы, связанные с экземпляром сервера каталогов” на стр. 121.

Об этой задаче

Команда **idscfgdb** позволяет выполнить следующие операции:

- Создать и настроить базу данных для экземпляра сервера каталогов. Создать локальные параметры обратной связи, если они не существуют.
- Добавить информацию о базе данных в файл *ibmslapd.conf* экземпляра сервера каталогов

Можно указать, какая кодировка должна применяться для создаваемой базы данных - локальная кодовая страница или UTF-8, применяемая по умолчанию.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог *sbin* в расположении установки IBM Security Directory Server.
4. Для того чтобы настроить базу данных DB2 для экземпляра сервера каталогов с указанными значениями, выполните следующую команду:

- Имя экземпляра: ldapdb
- Имя базы данных: ldapdb
- ИД администратора базы данных DB2: ldapdb
- Пароль администратора базы данных DB2: ldapdb123
- Расположение базы данных: /home/ldapdb

```
idscfgdb -I ldapdb -a ldapdb
-w ldapdb123 -t ldapdb
-l /home/ldapdb
```

В Windows укажите для расположения базы данных имя диска. В Solaris укажите соответствующее расположение базы данных. Дополнительная информация о команде **idscfgdb** приведена в *Справочнике по командам*. Эта команда настроит базу данных с табличными пространствами DMS стандартных размеров.

Примеры

Пример 1:

Для настройки базы данных с табличным пространством DMS конкретного размера, расположенным в файловой системе, введите команду **idscfgdb** со следующими значениями:

- Имя экземпляра: ldapdb
- Имя базы данных: ldapdb
- ИД администратора базы данных DB2: dbadmin
- Пароль администратора базы данных DB2: ldapdb123
- Расположение базы данных: c:\dblocation
- Расположение табличного пространства USERSPACE1: c:\dblocation\ldapinst\tablespaceloc\USPACE
- Размер контейнера табличных пространств USERSPACE1: 10000 страниц
- Размер расширения: 16 страниц

```
idscfgdb -I ldapdb -a dbadmin
-t ldapdb
-w ldapdb123 -n -l c:\dblocation
-u c:\dblocation\ldapinst\tablespaceloc\USPACE -U 10000 -z 16
```

Пример 2:

Для настройки такой же базы данных с табличными пространствами SMS введите команду **idscfgdb** со следующими значениями:

- Имя экземпляра: ldapdb
- Имя базы данных: ldapdb
- ИД администратора базы данных DB2: dbadmin
- Пароль администратора базы данных DB2: ldapdb123
- Расположение базы данных: c:\dblocation

```
idscfgdb -I ldapdb -a dbadmin
-t ldapdb
-w ldapdb123 -n -l c:\dblocation
-m SMS
```

Дальнейшие действия

После настройки базы данных необходимо выполнить следующие действия для настройки экземпляра:

- Настроить DN и пароль главного администратора. (См. раздел “Настройка отличительного имени (DN) главного администратора с помощью утилиты

командной строки” на стр. 173 и “Настройка пароля главного администратора с помощью утилиты командной строки” на стр. 175.)

- Настроить требуемые суффиксы. Обратитесь к разделу “Настройка суффикса” на стр. 204.

Управление паролем администратора базы данных DB2

Если пароль системы для владельца экземпляра DB2 изменен, необходимо обновить пароль в файле конфигурации сервера каталогов.

При изменении пароля системы для владельца экземпляра DB2 базы данных, который настроен в экземпляре, пароль не обновляется в файле конфигурации экземпляра. Если пароль администратора базы данных в файле конфигурации экземпляра не соответствует паролю системы владельца экземпляра DB2, связанного с базой данных, экземпляр может не запускаться в обычном режиме. Необходимо обновить файл конфигурации экземпляра с помощью последнего пароля владельца экземпляра DB2.

Для обновления пароля администратора базы данных DB2 можно использовать Инструмент настройки, команду `idscfgdb` или команду `idsldapmodify`.

При использовании Инструмента настройки или команды `idscfgdb` для изменения пароля администратора базы данных необходимо остановить сервер каталогов перед изменением пароля. Для того чтобы изменить пароль администратора базы данных с помощью команды `idsldapmodify`, необходимо запустить сервер каталогов в режиме настройки. Введите команду `idsldapmodify`, указав в ней идентификационные данные главного администратора сервера каталогов или участника локальной группы администраторов с ролью `dirdata`.

Более подробная информация о командах `idscfgdb` и `idsldapmodify` находится в *Справочнике по командам*.

Изменение пароля администратора базы данных DB2 с помощью Инструмента настройки

Для обновления пароля администратора базы данных DB2 в файле конфигурации экземпляра сервера каталогов можно использовать Инструмент настройки.

Прежде чем начать

Для обновления пароля администратора базы данных DB2 в файле конфигурации экземпляра необходимо выполнить следующие задачи:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Об этой задаче

Инструмент настройки обновляет пароль администратора базы данных DB2 в файле конфигурации экземпляра сервера каталогов. Если для экземпляра настроен протокол изменений, то инструмент также обновляет пароль владельца базы данных протокола изменений в файле конфигурации.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на левой панели навигации выберите **Задачи базы данных > Настроить базу данных**.
3. На странице **Настроить базу данных** выполните следующие действия:
 - a. Выберите **Сбросить пароль**.
 - b. В поле **Пароль** введите пароль администратора базы данных.
 - c. В поле **Подтверждение пароля** введите пароль администратора базы данных.
 - d. Нажмите кнопку **Далее**.
4. Нажмите кнопку **Готово**.
5. Для подтверждения выполнения задачи нажмите кнопку **ОК**.
6. Проверьте протоколы, созданные в ходе настройки пароля базы данных.
7. Для закрытия страницы **Настроить базу данных** нажмите кнопку **Закрыть**.
8. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
9. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Изменение пароля администратора базы данных DB2 с помощью утилиты командной строки

Для обновления пароля администратора базы данных DB2 в файле конфигурации экземпляра сервера каталогов можно использовать утилиту командной строки **idscfgdb** или **idsldapmodify**.

Прежде чем начать

Для обновления пароля администратора базы данных DB2 в файле конфигурации экземпляра необходимо выполнить следующие задачи:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью утилиты командной строки” на стр. 180.

Об этой задаче

Команда **idscfgdb** позволяет изменить пароль администратора базы данных DB2 в файле конфигурации экземпляра. Перед тем как выполнять команду **idscfgdb**, необходимо остановить сервер каталогов.

Команда **idsldapmodify** позволяет изменить пароль, когда экземпляр сервера каталогов работает. Введите команду **idsldapmodify**, указав в ней идентификационные данные главного администратора сервера каталогов или участника локальной группы администраторов с ролью `dirdata`.

Дополнительная информация о командах **idscfgdb** и **idsldapmodify** приведена в *Справочнике по командам*.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Выберите один из следующих способов пароля администратора базы данных DB2:
 - Для изменения пароля администратора базы данных DB2 с помощью команды **idscfgdb** выполните следующие действия:
 - a. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
 - b. Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.
 - c. Введите команду **idscfgdb** следующего формата:

```
idscfgdb -I экземпляр -w пароль-администратора-db2
```
 - d. Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.
 - Для изменения пароля администратора базы данных DB2 с помощью команды **idsldapmodify** выполните следующие действия:
 - a. Перейдите в подкаталог `bin` установочного каталога IBM Security Directory Server.
 - b. Введите команду **idsldapmodify** следующего формата:

```
idscfgdb -h  
IP-адрес -p порт -D DN-администратора -w  
пароль-администратора -i file1.ldif
```

`file1.ldif` содержит следующие записи:

```
dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration  
changetype: modify  
replace: ibm-slapdDbUserPW  
ibm-slapdDbUserPW: пароль-администратора-db2
```
 - c. Перезапустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Удаление конфигурации базы данных из экземпляра сервера каталогов

Для того чтобы использовать существующий экземпляр сервера каталогов с другой базой данных DB2, необходимо удалить конфигурацию существующей базы данных DB2 из экземпляра.

Для экземпляра сервера каталогов можно удалить конфигурацию базы данных, только если настроена база данных DB2 для экземпляра.

С помощью Инструмента настройки или команды **idsucfgdb** можно выполнить следующие операции:

- Удалить информацию о базе данных DB2 из файла конфигурации экземпляра сервера каталогов. В этой операции утилита удаляет конфигурацию базы данных DB2 из экземпляра, но не удаляет саму базу данных DB2.

- Удалить информацию о базе данных DB2 из файла конфигурации экземпляра сервера каталогов и удалить базу данных DB2. В этой операции удаляется база данных DB2, и все данные теряются.

После удаления базы данных DB2 из экземпляра сервера каталогов она становится недоступной для экземпляра.

Для экземпляра прокси-сервера операция удаления конфигурации базы данных не поддерживается.

Более подробная информация о команде `idsucfgdb` находится в *Справочнике по командам*.

Отключение базы данных DB2 от экземпляра с помощью Инструмента настройки

С помощью Инструмента настройки можно отключить базу данных DB2 от экземпляра сервера каталогов.

Прежде чем начать

Для отключения базы данных DB2 от экземпляра необходимо, чтобы экземпляр отвечал следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Задачи базы данных > Отключить базу данных**.
3. На странице **Отключить базу данных** выполните следующие действия:
 - a. В области Опции выберите одну из следующих опций:
 - Для отключения базы данных DB2 от экземпляра, не удаляя ее, нажмите **Отключить базу данных**.
 - Для отключения базы данных DB2 от экземпляра и ее удаления нажмите **Отключить и удалить базу данных**.
 - b. Для удаления резервной копии базы данных для экземпляра в случае, если база данных настроена для интерактивного резервного копирования, выберите **Удалить резервную копию базы данных**.
 - c. Для того чтобы начать отключение, нажмите **Отключить**.
 - d. В окне подтверждения нажмите **Да**.
4. Для того чтобы принять выполнение задачи, нажмите **ОК**.
5. Проверьте протоколы, созданные для операции отключения базы данных.
6. Для закрытия страницы **Отключить базу данных** нажмите **Отмена**.
7. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
8. Для подтверждения своего действия нажмите кнопку **Да**.

Отключение базы данных DB2 от экземпляра с помощью утилиты командной строки

С помощью утилиты командной строки, **idsucfgdb**, вы можете отключить базу данных DB2 от экземпляра сервера каталогов.

Прежде чем начать

Для отключения базы данных DB2 от экземпляра необходимо, чтобы экземпляр отвечал следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью утилиты командной строки” на стр. 180.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sb1n` в расположении установки IBM Security Directory Server.
4. Для отключения базы данных DB2 от экземпляра выберите одну из следующих опций:
 - Для того чтобы отключить базу данных от экземпляра сервера каталогов, выполните команду **idsucfgdb** в следующем формате:
`idsucfgdb -I имя_экземпляра`
 - Для того чтобы отключить базу данных от экземпляра сервера каталогов и удалить ее, выполните команду **idsucfgdb** в следующем формате:
`idsucfgdb -I имя_экземпляра -r`

Оптимизация базы данных

Для повышения производительности поиска в базе данных DB2 можно оптимизировать базу данных и обновить статистические данные DB2 для таблиц базы данных.

Для оптимизации базы данных DB2 можно использовать Инструмент настройки или команду, такую как **idsrunstats**. Необходимо выполнять операцию оптимизации DB2 периодически или после обновлений базы данных, например после импорта данных.

При выполнении оптимизации базы данных инструмент собирает статистические данные обо всех индексах, которые определены в таблицах, и обновляет их. Оптимизатор запросов DB2 использует эти статистические данные для определения оптимального пути доступа к данным.

Невозможно выполнить оптимизацию DB2, если экземпляр является прокси-сервером или не настроен с помощью базы данных DB2.

Более подробная информация о команде **idsrunstats** находится в *Справочнике по командам*.

Оптимизация базы данных с помощью Инструмента настройки

С помощью Инструмента настройки оптимизируйте базу данных DB2, связанную с экземпляром.

Прежде чем начать

Для оптимизации базы данных DB2 экземпляра необходимо, чтобы экземпляр отвечал следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Задачи базы данных > Оптимизировать базу данных**.
3. На странице **Оптимизировать базу данных** выполните следующие действия:
 - a. Для того чтобы начать оптимизацию базы данных, нажмите **Оптимизировать**.
 - b. Для подтверждения выполнения задачи нажмите кнопку **ОК**.
 - c. Проверьте протоколы, созданные для операции оптимизации базы данных.
 - d. Для очистки протоколов нажмите **Очистить результаты**.
4. Для закрытия страницы **Оптимизировать базу данных** нажмите **Закрыть**.
5. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
6. Для подтверждения своего действия нажмите кнопку **Да**.

Оптимизация базы данных с помощью утилиты командной строки

С помощью утилиты командной строки, **idsrunstats**, оптимизируйте базу данных DB2, связанную с экземпляром.

Прежде чем начать

Для оптимизации базы данных DB2 экземпляра необходимо, чтобы экземпляр отвечал следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью утилиты командной строки” на стр. 180.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для оптимизации базы данных DB2 выполните команду **idsrunstats** в следующем формате:

```
idsrunstats -I имя_экземпляра
```

Дополнительная информация о команде **idsrunstats** приведена в *Справочнике по командам*.

Обслуживание базы данных

Для повышения производительности поиска и операций обновления в экземпляре можно выполнить реорганизацию индекса DB2 или компрессию строк DB2.

Для выполнения реорганизации индекса DB2 или компрессии строк DB2 можно использовать Инструмент настройки или команду, такую как **idsdbmaint**.

После большого числа операций добавления и удаления информации в таблицах DB2 снижается скорость поиска и обновления базы данных. При выполнении реорганизации индекса DB2 производительность поиска и операций обновления повышается.

При выполнении компрессии строк DB2 инструмент находит повторяющиеся шаблоны и заменяет их на более короткие символьные строки. Инструмент анализирует, а затем выполняет компрессию строк, только если она приведет к улучшению более чем на 30 процентов.

Кроме того, с помощью команды **idsdbmaint** можно изменить табличное пространство SMS на DMS и наоборот. Преобразование табличного пространства не поддерживается Инструментом настройки. Более подробная информация о команде **idsdbmaint** находится в *Справочнике по командам*.

Обслуживание базы данных с помощью Инструмента настройки

С помощью Инструмента настройки вы можете обслуживать базу данных DB2, связанную с экземпляром.

Прежде чем начать

Для обслуживания базы данных DB2 экземпляра необходимо, чтобы экземпляр отвечал следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Задачи базы данных > Обслуживание**.
3. На странице **Обслуживание** выполните следующие действия:
 - a. Выберите операцию обслуживания базы данных DB2, которую вы хотите выполнить:
 - Для реорганизации индекса DB2 нажмите **Выполнить реорганизацию индекса**.

- Для сжатия строк DB2 нажмите **Проверить таблицы и выполнить сжатие строк**.
 - b. Нажмите **ОК**.
 - c. В окне выполнения задачи нажмите **ОК**.
 - d. Проверьте протоколы, созданные для операции обслуживания базы данных.
 - e. Для очистки протоколов нажмите **Очистить результаты**.
4. Для закрытия страницы **Обслуживание** нажмите **Закрыть**.
 5. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
 6. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Обслуживание базы данных с помощью утилиты командной строки

С помощью утилиты командной строки, **idsdbmaint**, вы можете обслуживать базу данных DB2, связанную с экземпляром.

Прежде чем начать

Для выполнения операции обслуживания базы данных DB2 необходимо, чтобы экземпляр отвечал следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью утилиты командной строки” на стр. 180.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для реорганизации индекса DB2 выполните команду **idsdbmaint** в следующем формате:
`idsdbmaint -I имя_экземпляра -i`

Дополнительная информация о команде **idsdbmaint** приведена в *Справочнике по командам*.

5. Для выполнения сжатия строк DB2 выполните команду **idsdbmaint** в следующем формате:
`idsdbmaint -I имя_экземпляра -r`

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Резервное копирование сервера каталогов

Для возможности восстановления экземпляра сервера каталогов после сбоя необходимо регулярно создавать резервную копию экземпляра сервера каталогов.

Для резервного копирования экземпляра можно использовать Инструмент настройки или команду **idsdbback**. Невозможно использовать команду **idsdbback** для резервного копирования экземпляра прокси-сервера, так как с прокси-сервером не связана база данных.

Можно настроить базу данных, связанную с экземпляром, для резервного копирования онлайн с помощью команды **idscfgdb**. Однако невозможно удалить конфигурацию резервного копирования онлайн с помощью команды **idscfgdb** с параметром **-c**). Если для настройки онлайн применяется Инструмент администрирования экземпляра или Инструмент настройки, то можно удалить конфигурацию с помощью Инструмент настройки или команды **idscfgdb**. Для получения наиболее надежных результатов резервного копирования онлайн для экземпляра с базой данных используйте для настройки резервного копирования онлайн Инструмент администрирования экземпляра или Инструмент настройки.

Также можно использовать команду **idsdb2ldif** для экспорта записей сервера каталогов в файл LDIF. Можно использовать команду **migbkup** для резервного копирования файлов схемы и конфигурации для экземпляра сервера каталогов и экземпляра прокси-сервера. Дополнительная информация о командах **idsdbback**, **idsdb2ldif** и **migbkup** приведена в разделе *Справочник по командам*. Дополнительная информация о подходящей команде для конкретной среды приведена в разделе *Настройка производительности и планирование ресурсов* в документации по IBM Security Directory Server.

С помощью инструмента настройки можно выполнить следующие действия:

- Резервное копирование параметров конфигурации для экземпляра сервера каталогов или экземпляра прокси-сервера.
- Резервное копирование экземпляра сервера каталогов вместе с базой данных.
- Резервное копирование экземпляра сервера каталогов и базы данных протокола изменений, если она была настроена для экземпляра.

Дополнительная информация об операциях резервного копирования и восстановления приведена в разделе *Администрирование* в документации по IBM Security Directory Server.

Резервное копирование базы данных сервера каталогов с помощью Configuration Tool

С помощью Configuration Tool можно выполнить резервное копирование экземпляра сервера каталогов вместе с базой данных с целью восстановления в случае сбоя.

Прежде чем начать

Для резервного копирования экземпляра сервера каталогов вместе с базой данных должны быть выполнены следующие требования:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
 2. В списке задач на панели навигации слева выберите **Резервное копирование и восстановление > Резервное копирование базы данных**.
 3. На странице **Резервное копирование базы данных** выполните следующие действия:
 - a. В поле **Каталог резервного копирования** введите имя каталога для сохранения всех данных и параметров конфигурации. Кроме того, каталог можно выбрать с помощью кнопки **Обзор**.
 - b. Для оперативного резервного копирования выберите один из следующих вариантов:
 - Для настройки оперативного резервного копирования сервера каталогов и базы данных включите переключатель **Обновить конфигурацию базы данных для поддержки интерактивного резервного копирования**.
 - Для запуска оперативного резервного копирования экземпляра сервера каталогов выберите **Выполнить интерактивное резервное копирование**.
 - c. Для резервного копирования базы данных протокола изменений для экземпляра выберите **Включить данные протокола изменений в процесс резервного копирования**.
 - d. Для того чтобы исключить файлы баз данных из процедуры резервного копирования, выберите **Не сохранять файлы баз данных**. Если включен переключатель **Не сохранять файлы базы данных**, то файлы базы данных и протокола изменений экземпляра сервера каталогов не сохраняются. Инструмент создает резервную копию файлов экземпляра сервера каталогов, таких как файл бумажника, схема и файлы конфигурации.
 - e. Для продолжения или отмены резервного копирования, если каталог резервного копирования уже существует, выберите один из следующих вариантов:
 - Для создания каталога резервного копирования, если он не существует, выберите **При необходимости создавать каталог резервной копии**.
 - Если каталог резервной копии не существует и вы не хотите его создавать, то выберите **Отменить, если каталог резервной копии не найден**. Если каталог резервной копии не существует, то при выборе этой опции база данных не будет сохранена.
- Прим.:** В ходе выполнения операции резервного копирования не следует закрывать Configuration Tool.
- f. Для запуска операции резервного копирования выберите **Резервное копирование**.
 - g. Если для резервного копирования требуется остановить сервер каталогов, нажмите кнопку **Да**.
 - h. Для подтверждения выполнения задачи нажмите **ОК**.
 - i. Проверьте протоколы, созданные для операции резервного копирования.

- j. Для очистки протоколов нажмите **Очистить результаты**.
- k. Для того чтобы закрыть страницу **Резервное копирование базы данных**, нажмите кнопку **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
5. Для подтверждения своего действия нажмите кнопку **Да**.

Резервное копирование экземпляра прокси-сервера с помощью Configuration Tool

С помощью Configuration Tool можно выполнить резервное копирование экземпляра прокси-сервера с целью восстановления в случае сбоя.

Прежде чем начать

Для резервного копирования экземпляра прокси-сервера этот экземпляр должен существовать. См. раздел “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на панели навигации слева выберите **Резервное копирование и восстановление > Создать резервную копию экземпляра**.
3. На странице **Создать резервную копию экземпляра** выполните следующие действия:
 - a. В поле **Каталог резервного копирования** введите имя каталога для сохранения схемы и файлов конфигурации. Кроме того, каталог можно выбрать с помощью кнопки **Обзор**.
 - b. Для экземпляра прокси-сервера включен переключатель **Не сохранять файлы базы данных**.
 - c. Для продолжения или отмены резервного копирования, если каталог резервного копирования уже существует, выберите один из следующих вариантов:
 - Для создания каталога резервного копирования, если он не существует, выберите **При необходимости создавать каталог резервной копии**.
 - Если каталог резервной копии не существует и вы не хотите его создавать, то выберите **Отменить, если каталог резервной копии не найден**. Если каталог резервной копии не существует, то при выборе этой опции экземпляр прокси-сервера не будет сохранен.
4. Для запуска операции резервного копирования выберите **Резервное копирование**.
 - d. Для запуска операции резервного копирования выберите **Резервное копирование**.
 - e. Если для выполнения операции требуется остановить экземпляр, нажмите кнопку **Да**.
 - f. Для подтверждения выполнения задачи нажмите **ОК**.
 - g. Проверьте протоколы, созданные для операции резервного копирования.
 - h. Для очистки протоколов нажмите **Очистить результаты**.
 - i. Для того чтобы закрыть страницу **Создать резервную копию экземпляра**, нажмите кнопку **Закрыть**.

Прим.: В ходе выполнения операции резервного копирования не следует закрывать Configuration Tool.

5. Для подтверждения своего действия нажмите кнопку **Да**.

Восстановление сервера каталогов

При возникновении ошибки в экземпляре сервера каталогов можно восстановить экземпляр с помощью последнего образа резервного копирования.

Можно использовать Инструмент настройки или команду **idsdbestore** для восстановления данных каталога и, по выбору, параметров конфигурации, которые были сохранены ранее. Перед восстановлением базы данных и/или параметров конфигурации необходимо остановить сервер каталогов.

Для прокси-сервера можно восстановить параметры конфигурации. Для прокси-сервера необходимо выполнить команду **idsdbrestore** с параметром **-x**.

Для экземпляра с базой данных DB2 можно восстановить базу данных с тем же именем, которое использовалось для резервной копии базы данных. Можно выполнить восстановление сервера каталогов с базой данных DB2, только если база данных настроена для экземпляра сервера каталогов. Команда **idsdbestore** восстанавливает резервную копию базы данных в настроенной базе данных. Команда не будет выполнена, если имя сохраненной базы данных или ее экземпляра не совпадает с именем настроенной базы данных или ее экземпляра. Для того чтобы восстановить базу данных, расположения сохраненной базы данных и базы данных, которая восстанавливается командой, должны совпадать.

Более подробная информация о команде **idsdbrestore** находится в *Справочнике по командам*.

Восстановление базы данных сервера каталогов с помощью Инструмента настройки

С помощью Инструмента настройки восстановите экземпляр сервера каталогов и его базу данных из резервного образа.

Прежде чем начать

Для восстановления экземпляра сервера каталогов и его базы данных необходимо, чтобы экземпляр отвечал следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Должен существовать резервный образ экземпляра сервера каталогов. См. раздел “Резервное копирование базы данных сервера каталогов с помощью Configuration Tool” на стр. 190.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Сохранить резервную копию/Восстановить > Восстановить базу данных**.
3. На странице **Восстановить базу данных** выполните следующие действия:

- a. В поле **Восстановить каталог** введите путь к каталогу, содержащему резервный образ экземпляра. Можно также нажать **Обзор** и указать путь к каталогу.
 - b. Для того чтобы восстановить только данные каталога, без параметров конфигурации, отметьте переключатель **Сохранить текущие параметры конфигурации**. Для того чтобы восстановить и данные каталога, и параметры конфигурации, сотрите отметку с переключателя **Сохранить текущие параметры конфигурации**.
 - c. Если для экземпляра настроен протокол изменений и вы хотите восстановить данные протокола, отметьте переключатель **Восстановить данные протокола изменений**.
 - d. Для того чтобы начать восстановление, нажмите **Восстановить**.
 - e. Если операция потребует остановить сервер каталогов, нажмите **Да**.
 - f. Для подтверждения выполнения задачи нажмите **ОК**.
 - g. Проверьте протоколы, созданные для операции восстановления.
 - h. Для очистки протоколов нажмите **Очистить результаты**.
 - i. Для закрытия страницы **Восстановить базу данных** нажмите **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
 5. Для подтверждения своего действия нажмите кнопку **Да**.

Восстановление экземпляра сервера проху с помощью Инструмента настройки

С помощью Инструмента настройки вы можете восстановить экземпляр сервера проху при любом сбое.

Прежде чем начать

Для восстановления экземпляра сервера проху необходимо, чтобы он отвечал следующим требованиям:

- Экземпляр сервера проху должен существовать. См. раздел “Создание экземпляра сервера прокси с пользовательскими параметрами” на стр. 143.
- Должен существовать резервный образ экземпляра сервера проху. См. раздел “Резервное копирование экземпляра прокси-сервера с помощью Configuration Tool” на стр. 192.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Сохранить резервную копию/Восстановить > Восстановить экземпляр**.
3. На странице **Восстановить экземпляр** выполните следующие действия:
 - a. В поле **Восстановить каталог** введите путь к каталогу, содержащему резервный образ экземпляра. Можно также нажать **Обзор** и указать путь к каталогу.
 - b. Для того чтобы восстановить параметры конфигурации из резервного образа, отметьте переключатель **Сохранить текущие параметры конфигурации**.
 - c. Для того чтобы начать восстановление, нажмите **Восстановить**.
 - d. Если операция потребует остановить сервер каталогов, нажмите **Да**.
 - e. Для подтверждения выполнения задачи нажмите **ОК**.

- f. Проверьте протоколы, созданные для операции восстановления.
 - g. Для очистки протоколов нажмите **Очистить результаты**.
 - h. Для закрытия страницы **Восстановить экземпляр** нажмите **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
 5. Для подтверждения своего действия нажмите кнопку **Да**.

Настройка сервера каталогов для повышения производительности

Необходимо настроить экземпляр сервера каталогов для повышения производительности поиска и обновления.

Можно выполнить Инструмент настройки или команду **idsperf tune** для настройки экземпляра сервера каталогов. Инструмент генерирует значения параметров настройки производительности для кэшей сервера каталогов и буферных пулов DB2. Инструмент генерирует параметры настройки на основании предоставленных вами сведений о экземпляре сервера каталогов. Инструмент может также изменить параметры настройки для экземпляра. Инструмент сохраняет копию файла `ibmslapd.conf` в файле `logs/ibmslapd.conf.save` в домашнем каталоге экземпляра сервера каталогов.

Инструмент сохраняет указанную вами информацию в файле `logs/perftune_input.conf` в домашнем каталоге экземпляра сервера каталогов.

Инструмент настройки или команда **idsperf tune** использует предоставленные вами значения для вычисления следующих параметров настройки для экземпляра:

- Размер кэша записей
- Размер кэша фильтров
- Размер кэша участников групп
- Предел пропуска кэша участников групп
- Размер буферного пула DB2 LDAPDB
- Размер буферного пула DB2 IBMDEFAULTDB

Если запущен экземпляр сервера каталогов, инструмент отслеживает его производительность и предоставляет информацию о работоспособности базы данных. Информация о работоспособности базы данных включает в себя следующие параметры DB2:

- DB2_NUM_IOSERVERS
- DB2_NUM_IOCLEANERS
- CATALOGCACHE_SZ
- PCKCACHESZ
- LOGFILSIZ
- LOCKLIST

При выполнении расширенной настройки экземпляра инструмент собирает и анализирует данные о экземпляре сервера каталогов. Необходимо выполнять экземпляр некоторое время для сбора данных настройки DB2 в процессе анализа работоспособности базы данных. Инструмент генерирует значения настройки для следующих параметров DB2 и сохраняет их в файле `logs/perftune_stat.log` для экземпляра.

- SORTHEAP
- MAXFILOP

- DBHEAP
- CHNGPGS_THRESH
- NUM_IOSERVERS
- NUM_IOCLEANERS

Для параметров DB2 может быть рекомендовано одно из следующих значений:

- ОК
- Увеличение
- Уменьшение
- Нет данных

Для параметров DB2, которые не проанализированы, назначается значение Не собран. Вы можете использовать предложенные значения для настройки параметров DB2 в целях повышения производительности.

Для улучшения производительности необходимо выполнить инструмент в экземпляре сразу после загрузки начальных данных каталога. После начальной настройки выполняйте инструмент периодически, особенно после добавления большого количества записей или изменения содержимого записей. Более подробная информация о настройке экземпляра сервера каталогов приведена в разделе *Настройка производительности и планирование ресурсов* в документации по IBM Security Directory Server.

Невозможно использовать Инструмент настройки или команду **idsperf tune** для настройки экземпляра прокси-сервера или экземпляра, для которого не настроена база данных.

Настройка сервера каталогов для тонкой настройки производительности с помощью Configuration Tool

С помощью Configuration Tool можно настроить сервер каталогов для повышения производительности операций поиска и обновления.

Прежде чем начать

Для тонкой настройки экземпляра сервера каталогов должны быть выполнены следующие требования:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на панели навигации слева выберите **Задачи базы данных > Настройка производительности**.
3. На странице **Тонкая настройка производительности** выполните следующие действия:
 - a. В поле **Доля свободной памяти, которая будет выделена этому экземпляру каталогов** введите процент памяти, выделяемой этому экземпляру. Доступная память системы распределяется между несколькими экземплярами сервера каталогов или между экземплярами и другими серверами, которые

планируется запустить в системе. С учетом указанного значения инструмент вычисляет размеры кэшей записей и фильтров.

- b. В поле **Запланированное количество групп** введите число групп, которые планируется добавить в экземпляр. С учетом указанного значения инструмент вычисляет размеры кэшей сервера каталогов.
- c. В поле **Максимальное число часто используемых элементов в группе** введите среднее число участников для группы, на которые часто создаются ссылки.
- d. В разделе **Число записей и средний размер записи** выберите один из следующих вариантов:
 - Для оценки числа записей в каталоге и среднего размера записи выполните следующие действия:
 - 1) В поле **Запланированное количество записей** введите общее число записей, запланированных для экземпляра. Инструмент попытается определить это число. Если ему это не удастся, то используется значение по умолчанию - 10000 записей. Эта информация используется для расчета размера кэшей сервера каталогов.
 - 2) В поле **Средний размер записи** введите средний размер записи экземпляра в байтах. Инструмент попытается определить этот размер. Если ему это не удастся, то используется значение по умолчанию - 2560 байт. Эта информация используется для расчета размера кэшей сервера каталогов.
 - Для просмотра определения общего числа записей и среднего размера записи с помощью инструмента выберите **Загрузить из базы данных экземпляра сервера**. Инструмент заполняет поля **Запланированное количество записей** и **Средний размер записи**.
- e. В области **Частота обновления** выберите следующие значения:
 - Если ожидается частое обновление экземпляра, выберите **Частые обновления**. Одно обновление на 500 запросов поиска считается частым обновлением.
 - Если планируются редкие обновления или они будут сгруппированы в пакет и выполняться в определенное время суток, выберите **Пакетные обновления**.

Эта информация применяется для настройки размера кэша фильтров. Кэш фильтров полезен только при нечастом обновлении экземпляра, если одни и те же запросы выполняются несколько раз. Если ожидаются частые обновления, то размер кэша фильтров будет равен 0. Если ожидаются нечастые или пакетные обновления, то в кэше фильтров будет создано 1024 записи.

- f. Переключатель **Включить сбор дополнительных данных о системе для расширенной настройки** позволяет собрать данные для анализа производительности.
 - Вместе с этим переключателем включаются параметры BUFFERPOOL и SORTHEAP монитора DB2. Включение сбора данных с помощью монитора DB2 может привести к снижению производительности экземпляра сервера каталогов.
 - Для получения более точных данных об оптимальной настройке экземпляра сервера каталогов включите этот переключатель в то время, когда система работает в типичных условиях для вашей среды. Если проверка состояния базы данных была выполнена в период с низкой нагрузкой на сервер, то данные по оптимизации производительности могут быть неточными.

- g. Нажмите кнопку **Далее**. Откроется страница **Настройка производительности: Проверка**.
4. На странице **Тонкая настройка производительности: проверка** выполните следующие действия:
- a. В списке **Состояние базы данных** проверьте параметры тонкой настройки производительности, созданные инструментом. Если для экземпляра не выполняются операции базы данных, то список **Состояние базы данных** может не быть заполнен. Список заполняется, если инструмент собирает информацию по крайней мере об одном параметре DB2. Кроме того, параметры тонкой настройки сохраняются в файле `perf_tune_stat.log`.
 - b. Для изменения значений параметров базы данных выберите **Настроить параметры базы данных**. Откроется окно **Параметры базы данных**.
 - c. В окне **Параметры базы данных** укажите значения следующих параметров базы данных:
 - 1) В поле **Куча базы данных** введите максимальный размер кучи базы данных в страницах. Куча базы данных содержит информацию об управляющих блоках для таблиц, индексов, табличных пространств и пулов буферов. Кроме того, она содержит память для буфера протокола и временную память, используемую утилитами.
 - 2) В поле **Размер кэша пакета** укажите размер кэша фрагментов статических и динамических операторов SQL и XQuery (в страницах).
 - 3) В поле **Размер буфера протокола** введите размер буфера записей протоколов в страницах. Укажите размер кучи базы данных, которая будет использоваться в качестве буфера записей протокола.
 - 4) В поле **Максимальное число открытых файлов базы данных на приложение** введите максимальное число ссылок на файл, которые можно открыть для каждого агента базы данных.
 - 5) В поле **Пороговое значение измененных страниц** введите процент измененных страниц.
 - 6) В поле **Размер кучи сортировки** введите максимальный размер кучи сортировки в страницах. Кучу сортировки можно использовать в качестве частных или общих страниц памяти для частных или общих операций сортировки.
 - 7) В поле **Размер файла протокола** введите размер файлов протоколов в килобайтах. Этот параметр определяет размер каждого основного или вспомогательного файла протокола.
 - 8) В поле **Путь к протоколу базы данных** выберите расположение для сохранения файлов протоколов. Расположение можно выбрать с помощью кнопки **Обзор**.
 - 9) Для сохранения указанных значений и обновления параметров базы данных нажмите кнопку **ОК**. Если параметры не указаны, то применяются значения по умолчанию.
5. Для подтверждения применения параметров тонкой настройки каталога и базы данных выберите один из следующих вариантов:
- Для обновления параметров тонкой настройки экземпляра сервера каталогов выберите **Да, использовать рекомендуемые значения для обновления параметров конфигурации каталога и базы данных**.
 - Для отказа от использования параметров тонкой настройки нажмите кнопку **Нет, сохранить текущие параметры. Параметры конфигурации не обновляются**.
6. Для применения изменений нажмите кнопку **Готово**.
7. Для подтверждения завершения задачи нажмите кнопку **ОК**.

8. Проверьте протоколы, созданные в ходе обновления параметров тонкой настройки.
9. Для очистки протоколов нажмите **Очистить результаты**.
10. Для того чтобы закрыть страницу **Тонкая настройка производительности**, нажмите кнопку **Закрыть**.
11. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
12. Для подтверждения своего действия нажмите кнопку **Да**.

Настройка сервера каталогов для тонкой настройки производительности с помощью командной строки

С помощью команды **idsperftune** настройте сервер каталогов для повышения производительности операций поиска и обновления.

Прежде чем начать

Для тонкой настройки экземпляра сервера каталогов должны быть выполнены следующие требования:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью утилиты командной строки” на стр. 180.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для тонкой настройки сервера каталогов и его базы данных выполните команду **idsperftune**.

- Для базовой настройки сервера каталогов выполните команду **idsperftune** в следующем формате:

```
idsperftune -I имя-экземпляра
-i файл-свойств -B -u
```

Если указан параметр **-u**, то параметры кэша LDAP и пула буферов DB2 обновляются на сервере и в базе данных. Если не указан параметр **-u**, то параметры тонкой настройки сохраняются только в файле `perftune_stat.log`.

- Для просмотра числа записей и среднего размера записи в экземпляре и базе данных выполните команду **idsperftune** в следующем формате:

```
idsperftune -I имя-экземпляра -s
```

- Для дополнительной настройки сервера каталогов выполните команду **idsperftune** в следующем формате:

```
idsperftune -I имя-экземпляра
-i файл-свойств -A -m
```

Параметр **-m** позволяет включить параметры `BUFFERPOOL` и `SORT`. Для получения более точных данных об оптимальной настройке экземпляра выполните команду в то время, когда система работает в типичных условиях для вашей среды.

Дополнительная информация о команде **idsperftune** приведена в разделе *Справочник по командам*.

Управление протоколом изменений для экземпляра сервера каталогов

Можно настроить базу данных протокола изменений для записей изменений, вносимых в схему и записи каталога экземпляра.

В протокол изменений заносится информация обо всех операциях обновления, выполняемых над экземпляром сервера каталогов: `add`, `delete`, `modify` и `modrpn`. С помощью утилит клиента можно получать данные протокола изменений, записанные при внесении изменений в базу данных сервера каталогов.

С помощью инструмента настройки или утилит командной строки можно включить или выключить базу данных протокола изменений. Перед настройкой или отключением базы данных протокола изменений необходимо остановить сервер каталогов.

Для того чтобы настроить протокол изменений для сервера каталогов, воспользуйтесь командой `idscfgchg1g`. Для того чтобы отключить протокол изменений для сервера каталогов, воспользуйтесь командой `idsucfgchg1g`. Невозможно настроить базу данных протокола изменений для экземпляра прокси-сервера.

Для того чтобы настроить протокол изменений для экземпляра сервера каталогов, необходимо соблюдать следующие критерии:

1. Необходимо наличие экземпляра DB2 с тем же именем, которое присвоено экземпляру сервера каталогов.
2. Необходимо настроить базу данных для экземпляра сервера каталогов.
3. В AIX, Linux и Solaris в файле `/etc/services` должна быть зарегистрирована локальная служба обратной связи.

Настраиваемая база данных протокола изменений создается в том же экземпляре базы данных, что и база данных экземпляра сервера каталогов. Для базы данных протокола изменений дополнительно требуется 30 МБ памяти на жестком диске. При настройке протокола изменений запись протокола изменений добавляется в файл конфигурации экземпляра сервера каталогов.

Настройка протокола изменений с помощью Инструмента настройки

Настройте базу данных протокола изменений для экземпляра сервера каталогов с помощью Инструмента настройки.

Прежде чем начать

Для того чтобы настроить протокол изменений для экземпляра, необходимо выполнить следующие требования для этого экземпляра:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Управлять протоколом изменений**.
3. На странице **Управлять протоколом изменений** выполните следующие действия:
 - a. Для настройки протокола изменений выберите **Включить базу данных протокола изменений**.
 - b. В области **Максимальное число записей протокола** укажите максимальное число записей, которые должны заноситься в базу данных протокола изменений.
 - Для сохранения неограниченного числа записей в протоколе изменений выберите **Не ограничено**.
 - Для сохранения определенного числа записей выберите **Число записей** и введите число записей. Число записей по умолчанию - 1000000.
 - c. В области **Максимальный срок хранения** укажите срок, в течение которого необходимо хранить записи в базе данных протокола изменений.
 - Если записи должны храниться в протоколе изменений неограниченное время, выберите **Не ограничен**.
 - Если записи должны храниться только в течение определенного времени, выберите **Срок хранения** и введите число дней и часов.
 - d. Для применения изменений нажмите **Обновить**.
 - e. Для подтверждения выполнения задачи нажмите **ОК**.
 - f. Проверьте протоколы, созданные при настройке базы данных протокола изменений.
 - g. Для очистки протоколов нажмите **Очистить результаты**.
 - h. Для закрытия страницы **Управлять протоколом изменений** нажмите **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
5. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Настройка протокола изменений с помощью утилиты командной строки

Настройте базу данных протокола изменений для экземпляра сервера каталогов с помощью утилиты командной строки **idscfgchg1g**.

Прежде чем начать

Для того чтобы настроить протокол изменений для экземпляра, необходимо выполнить следующие требования для этого экземпляра:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью утилиты командной строки” на стр. 180.

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для настройки протокола изменений экземпляра сервера каталогов выполните команду **idscfgchg1g**.
 - Для того чтобы настроить для экземпляра сервера каталогов протокол изменений без ограничения срока хранения или размера, выполните следующую команду **idscfgchg1g**:
`idscfgchg1g -I экземпляр -m 0`
 - Для того чтобы настроить для экземпляра сервера каталогов протокол изменений с максимальным размером 1000000 и сроком хранения 25 часов, введите следующую команду **idscfgchg1g**:
`idscfgchg1g -I экземпляр -m 1000000 -y 1 -h 1`

Дополнительная информация о команде **idscfgchg1g** приведена в *Справочнике по командам*.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Отключение протокола изменений с помощью Инструмента настройки

С помощью Инструмента настройки можно отключить базу данных протокола изменений от экземпляра сервера каталогов.

Прежде чем начать

Для отключения протокола изменений от экземпляра необходимо, чтобы экземпляр отвечал следующим требованиям:

- Протокол изменений для экземпляра должен быть настроен. См. раздел “Настройка протокола изменений с помощью Инструмента настройки” на стр. 200.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Управлять протоколом изменений**.
3. На странице **Управлять протоколом изменений** выполните следующие действия:
 - a. Для отключения протокола изменений сотрите отметку с переключателя **Включить базу данных протокола изменений**.

- b. Для применения изменений нажмите **Обновить**.
 - c. В окне **Управлять протоколом изменений** нажмите **Да**, чтобы подтвердить действие.
 - d. Проверьте протоколы, созданные во время удаления базы данных протокола изменений.
 - e. Для очистки протоколов нажмите **Очистить результаты**.
 - f. Для закрытия страницы **Управлять протоколом изменений** нажмите **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
 5. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Отключение протокола изменений с помощью утилиты командной строки

С помощью утилиты командной строки, **idsucfgchg1g**, вы можете отключить базу данных протокола изменений от экземпляра сервера каталогов.

Прежде чем начать

Для отключения протокола изменений от экземпляра необходимо, чтобы экземпляр отвечал следующим требованиям:

- Протокол изменений для экземпляра должен быть настроен. См. раздел “Настройка протокола изменений с помощью утилиты командной строки” на стр. 201.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sb1n` в расположении установки IBM Security Directory Server.
4. Для того чтобы отключить протокол изменений для экземпляра сервера каталогов, выполните команду **idsucfgchg1g** в следующем формате:
`idsucfgchg1g -I имя_экземпляра`

Дополнительная информация о команде **idsucfgchg1g** приведена в *Справочнике по командам*.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Настройка суффикса

Для создания структуры каталогов необходимо настроить требуемый суффикс экземпляра сервера каталогов.

Суффикс представляет собой контекст именованя. Это отличительное имя (DN), определяющее верхнюю запись в структуре каталогов. В LDAP применяется схема относительного именованя. Поэтому DN также является суффиксом для всех записей в структуре каталогов. На сервере каталогов можно добавлять несколько суффиксов, каждый из которых определяет структуру каталогов. Когда добавляется суффикс, запись добавляется в файл конфигурации экземпляра сервера каталогов. В следующем примере показана запись суффикса `o=sample`.

Можно использовать Инструмент настройки для добавления или удаления суффиксов. Также можно использовать команду **idscfgsuf** для добавления суффиксов и команду **idsucfgsuf** для удаления суффиксов. Перед добавлением или удалением суффикса необходимо остановить сервер каталогов. Дополнительная информация о команде **idscfgsuf** или **idsucfgsuf** приведена в разделе *Справочник по командам*.

Невозможно удалить из экземпляра сервера каталогов суффиксы, определенные системой. Эти суффиксы недоступны в экземплярах прокси-сервера. Системой определяются следующие суффиксы:

- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`
- `cn=Deleted Objects`

При добавлении записей на сервер каталогов необходимо учесть следующие моменты:

- Необходимо добавить запись суффикса на сервер каталогов для DN суффикса.
- DN записи, добавляемый на сервер каталогов, должен содержать суффикс, совпадающий со значением DN суффикса. В следующем примере показана запись с DN суффикса: `ou=Marketing,o=sample`.
- Нельзя добавлять запись в экземпляр прокси-сервера или на сервер каталогов, на котором не настроена база данных DB2.

Если запрос содержит суффикс, который не совпадает ни с одним суффиксом локальной базы данных, то запрос переадресуется серверу LDAP, ссылка на который задана по умолчанию. Если ссылка на сервер LDAP по умолчанию не задана, то будет создано сообщение *Объект не существует*.

Добавление суффикса с помощью Configuration Tool

С помощью Configuration Tool добавьте суффикс для экземпляра.

Прежде чем начать

Для того чтобы добавить суффикс для экземпляра, необходимо выполнить следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Об этой задаче

Добавление суффикса в экземпляр предусматривает добавление записи в файл конфигурации экземпляра.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Управлять суффиксами**.
3. На странице **Управлять суффиксами** выполните следующие действия:
 - a. В поле Суффикс DN введите суффикс для добавления к экземпляру.
 - b. Нажмите кнопку **Добавить**.
 - c. Для применения изменений нажмите кнопку **ОК**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
5. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Добавление суффикса с помощью командной строки

С помощью команды **idscfgsuf** добавьте суффикс для экземпляра.

Прежде чем начать

Для того чтобы добавить суффикс для экземпляра, необходимо выполнить следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Об этой задаче

Добавление суффикса в экземпляр предусматривает добавление записи в файл конфигурации экземпляра.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для добавления суффикса `o=sample` в экземпляр, выполните команду **idscfgsuf** в следующем формате:

```
idscfgsuf -I имя-экземпляра -s "o=sample"
```

Дополнительная информация о команде **idscfgsuf** приведена в разделе *Справочник по командам*.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Удаление суффикса с помощью Инструмента настройки

С помощью Инструмента настройки можно удалить суффикс из экземпляра сервера каталогов.

Прежде чем начать

Для удаления суффикса из экземпляра сервера каталогов выполните следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Об этой задаче

Когда вы удаляете суффикс для экземпляра, запись суффикса удаляется из файла конфигурации экземпляра.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Управлять суффиксами**.
3. На странице **Управлять суффиксами** выполните следующие действия:
 - a. В списке **Текущие DN суффиксов** выберите суффикс, который вы хотите удалить. В случае полного сервера каталогов нельзя удалить следующие системные суффиксы:
 - cn=localhost
 - cn=configuration
 - cn=ibmpolicies
 - cn=Deleted Objects
 - b. Нажмите **Удалить**.
 - c. В окне подтверждения **Управлять суффиксами** нажмите **Да**.
 - d. Для применения изменений нажмите кнопку **ОК**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
5. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Удаление суффикса с помощью командной строки

С помощью утилиты командной строки, **idsucfgsuf**, удалите суффикс из экземпляра.

Прежде чем начать

Для удаления суффикса из экземпляра выполните следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Об этой задаче

Когда вы удаляете суффикс для экземпляра, запись суффикса удаляется из файла конфигурации экземпляра. В случае полного сервера каталогов нельзя удалить следующие системные суффиксы:

- cn=localhost
- cn=configuration
- cn=ibmpolicies
- cn=Deleted Objects

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для удаления суффикса `o=sample` для экземпляра выполните команду **idsucfgsuf**:
`idsucfgsuf -I имя_экземпляра -s "o=sample"`

Дополнительная информация о команде **idsucfgsuf** приведена в *Справочнике по командам*.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Управление схемой

Если вы хотите, чтобы экземпляр поддерживал пользовательские атрибуты и классы объектов, необходимо добавить файл схемы, который определяет их.

Для управления файлами схем можно использовать Инструмент настройки или утилиты командной строки, такие как **idscfgsch** или **idsucfgsch**. Указанный файл схемы должен существовать на компьютере. Более подробная информация о командах **idscfgsch** и **idsucfgsch** находится в *Справочнике по командам*.

Перед добавлением или удалением файлов схем необходимо остановить сервер каталогов.

При добавлении или удалении файлов схем обновляется файл конфигурации экземпляра. Можно выполнить следующие операции по управлению схемой:

- Добавить файл схем в список файлов схем, загружаемого во время запуска сервера.
- Удалить файл схем из списка файлов схем, обновляемого во время запуска сервера.
- Изменить тип проверки правильности данных, выполняемой для файлов схем.

Невозможно удалить следующие файлы схем, определенные системой:

- V3.config.at
- V3.config.oc
- V3.ibm.at
- V3.ibm.oc
- V3.system.at
- V3.system.oc
- V3.user.at
- V3.user.oc
- V3.ldapsyntaxes
- V3.matchingrules
- V3.modifiedschema

Можно также использовать Инструмент настройки, чтобы указать правило проверки схемы. Правилom проверки схемы по умолчанию является Версия 3 (нестрогая проверка). Следующие правила проверки схем поддерживаются сервером каталогов:

Версия 3 (строгая проверка)

Сервер выполняет для записей строгую проверку LDAP версии 3. В этом случае при добавлении записей должны присутствовать все родительские классы объектов.

Версия 3 (нестрогая проверка)

Сервер выполняет для записей нестрогую проверку LDAP версии 3. В этом случае при добавлении записей не требуется, чтобы присутствовали все родительские классы объектов. Нестрогая проверка LDAP версии 3 является правилom проверки схемы по умолчанию.

Версия 2

Сервер выполняет для записей проверку LDAP версии 2.

Нет Сервер не выполняет проверки.

Управление файлом схемы с помощью Configuration Tool

С помощью Configuration Tool можно управлять файлами схемы экземпляра.

Прежде чем начать

Для управления файлами схемы экземпляра необходимо выполнить следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Об этой задаче

Добавление или удаление файла схемы предусматривает обновление файла конфигурации экземпляра.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на левой панели навигации выберите **Управление файлами схемы**.
3. На странице **Управление файлами схем** выберите операцию.

- Для того чтобы добавить файл схемы в файл конфигурации экземпляра, выполните следующие действия:
 - a. В поле **Каталог и имя файла** введите полное имя файла схемы. Файл схемы можно выбрать с помощью кнопки **Обзор**.
 - b. Нажмите кнопку **Добавить**.
- Для того чтобы удалить файл схемы из файла конфигурации экземпляра, выполните следующие действия:
 - a. В списке **Текущие файлы схемы** выберите имя файла схемы для удаления.
 - b. Нажмите **Удалить**.
 - c. В окне **Управление файлами схем** нажмите кнопку **ОК**.
- 4. Для применения изменений нажмите кнопку **ОК**.
- 5. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
- 6. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Управление файлом схемы с помощью командной строки

С помощью утилит командной строки можно управлять файлами схемы для экземпляра сервера каталогов.

Прежде чем начать

Для управления файлами схемы экземпляра необходимо выполнить следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Об этой задаче

Добавление или удаление файла схемы предусматривает обновление файла конфигурации экземпляра.

Процедура

1. Войдите в систему под именем владельца экземпляра сервера каталогов.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для управления файлом схемы экземпляра выберите требуемую операцию.
 - Для добавления файла схемы для экземпляра выполните команду **idscfgsch** в следующем формате:


```
idscfgsch -I имя-экземпляра -s schema_file.oc
```
 - Для удаления файла схемы из экземпляра выполните команду **idsucfgsch** в следующем формате:


```
idsucfgsch -I имя-экземпляра -s schema_file.oc
```

Дополнительная информация о команде **idscfgsch** или **idsucfgsch** приведена в разделе *Справочник по командам*.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Настройка проверки правильности схемы с помощью Инструмента настройки

Настройте проверку правильности схемы для экземпляра с помощью Инструмента настройки.

Прежде чем начать

Для того чтобы настроить правило проверки схемы для экземпляра, необходимо выполнить следующие действия:

- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Об этой задаче

При настройке проверки правильности схемы файл конфигурации экземпляра обновляется с учетом нового значения.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на левой панели навигации выберите **Управление файлами схемы**.
3. В области **Правила проверки схемы** на странице **Управление файлами схемы** выберите для настройки одно из следующих правил проверки схемы:
 - Для настройки строгой проверки LDAP версии 3 выберите **Версия 3 (строгая проверка)**.
 - Для настройки нестрогой проверки LDAP версии 3 выберите **Версия 3 (нестрогая проверка)**.
 - Для настройки проверки LDAP версии 2 выберите **Версия 2**.
 - Для настройки проверки LDAP версии 2 выберите **Нет**.
4. Для применения изменений нажмите кнопку **ОК**.
5. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
6. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Управление данными LDIF

Для использования данных каталога необходимо добавить данные в экземпляр сервера каталогов из существующего экземпляра или из файла Формата обмена данными LDAP (LDIF).

С помощью Инструмента настройки можно импортировать данные из файла LDIF в базу данных или экспортировать данные из базы данных в файл LDIF. Формат LDIF предназначен для текстового представления записей LDAP. Импортируемые данные можно добавить в пустую базу данных каталога или базу данных, которая уже содержит записи. Кроме того, с помощью Инструмента настройки можно проверить данные в файле LDIF, не добавляя их в каталог.

Можно добавить данные в экземпляр, настроенный с помощью базы данных DB2. Не следует добавлять данные каталога в экземпляр прокси-сервера, так как он не поддерживается.

При импорте данных LDIF из другого экземпляра сервера необходимо выполнить синхронизацию средств шифрования и экземпляра сервера. Необходимо синхронизировать двустороннее шифрование между экземплярами сервера каталогов для сокращения времени, требуемого для шифрования и расшифровки данных в процессе обмена данными с сервером. При импорте данных LDIF, для которых не синхронизировано шифрование, записи файла, зашифрованные с помощью AES, не импортируются. Более подробная информация о синхронизации двустороннего шифрования находится в *Справочнике по командам*.

Если шифрование не синхронизировано между экземплярами сервера, укажите затравку и соль шифрования целевого сервера при экспорте файла LDIF с исходного сервера. Данные, зашифрованные с помощью AES, расшифровываются с помощью ключей AES исходного сервера, а затем зашифровываются с помощью значений затравки и соли шифрования целевого сервера. Зашифрованные таким образом данные хранятся в файле LDIF.

Для импорта данных необходимо удовлетворить следующие требования перед началом процесса:

- Импорт и экспорт данных LDIF не поддерживается для экземпляра прокси-сервера или экземпляра, которые не настроен с помощью базы данных DB2.
- Добавьте требуемые суффиксы к целевому серверу, на который вы хотите импортировать данные. Обратитесь к разделу “Настройка суффикса” на стр. 204.
- Необходимо остановить целевой сервер, на который вы хотите импортировать данные.

После загрузки большого количества данных, например после заполнения базы данных с помощью утилиты **idsbulkload**, необходимо оптимизировать базу данных. Эта операция может повысить производительность базы данных.

Импортировать, экспортировать или проверить данные LDIF можно также в командной строке:

- Для импорта данных из файла LDIF можно воспользоваться или утилитой **idsldif2db**, или утилитой **idsbulkload**.
- Для экспорта данных в файл LDIF можно использовать утилиту **idsdb2ldif**.
- Для проверки файла LDIF используйте утилиту **idsbulkload**.

Более подробная информация об утилитах командной строки находится в *Справочнике по командам*.

Примеры

Для того чтобы извлечь значение соли шифрования для сервера, выполните команду **idsldapsearch** следующего формата:

```
idsldapsearch -h имя_хоста  
-p порт -D DN_администратора  
-w пароль_администратора \  
-b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt  
  
ibm-slapdCryptoSalt=:SxaQ+.qdKor
```

Строка после знака равенства (=) в атрибуте `ibm-slapdCryptoSalt` является солью шифрования. В этом примере `:SxaQ+.qdKor` является солью шифрования.

Импорт данных LDIF с помощью Инструмента настройки

Инструмент настройки позволяет импортировать данные из файла LDIF в экземпляр сервера каталогов.

Прежде чем начать

Для того чтобы импортировать данные из файла LDIF в экземпляр, для этого экземпляра должны быть выполнены следующие требования:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Следует настроить требуемые записи суффиксов. Обратитесь к разделу “Добавление суффикса с помощью Configuration Tool” на стр. 204.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Задачи LDIF > Импортировать данные LDIF**.
3. На странице **Импортировать данные LDIF** выполните следующие действия:
 - a. В поле **Путь и имя файла LDIF** введите путь и имя файла LDIF, из которого требуется импортировать данные. Также можно нажать кнопку **Обзор** и указать имя файла LDIF с путем.
 - b. Для удаления из данных конечных пробелов включите переключатель **Удалять конечные пробелы при стандартном импорте или загрузке**.
 - c. В зависимости от количества импортируемых записей выберите соответствующую опцию:
 - Для импорта данных с помощью утилиты **idsldif2db** выберите **Стандартный импорт**. Используйте эту опцию, если файл LDIF содержит небольшое число записей.
 - Для импорта данных с помощью утилиты **idsbulkload** выберите **Загрузка**. При импорте данных из файлов LDIF с большим количеством записей утилита **idsbulkload** работает быстрее, чем утилита **idsldif2db**.
 - d. Если для импорта данных выбрана опция **Загрузка**, укажите, какие типы проверки должны выполняться для данных LDIF:
 - 1) Для проверки данных LDIF на соответствие схеме выберите **Включить проверку схемы**.
 - 2) Для проверки наличия в данных LDIF соответствующих ACL выберите **Включить проверку ACL**.
 - e. Для запуска процедуры импорта нажмите кнопку **Импортировать**.

- f. Для подтверждения завершения задачи нажмите кнопку **ОК**.
 - g. Проверьте протоколы, созданные в ходе импорта файла LDIF.
 - h. Для очистки протоколов нажмите **Очистить результаты**.
 - i. Для закрытия страницы **Импортировать данные LDIF** нажмите кнопку **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
 5. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171. После загрузки большого количества данных, например после заполнения базы данных с помощью утилиты **idsbulkload**, необходимо оптимизировать базу данных. Дополнительная информация об оптимизации базы данных приведена в разделе “Оптимизация базы данных с помощью Инструмента настройки” на стр. 187.

Проверка данных LDIF с помощью Инструмента настройки

Используйте Инструмент настройки для проверки файла LDIF на соответствие схемы сервера каталогов без добавления данных в базу данных.

Прежде чем начать

Для того чтобы проверить данные из файла LDIF на соответствие схеме сервера каталогов, экземпляр должен соответствовать следующим требованиям:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач в левой панели навигации выберите **Задачи LDIF > Импортировать данные LDIF**.
3. На странице **Импортировать данные LDIF** выполните следующие действия:
 - a. В поле **Путь и имя файла LDIF** введите путь и имя файла LDIF, из которого требуется импортировать данные. Также можно нажать кнопку **Обзор** и указать имя файла LDIF с путем.
 - b. Выберите опцию **Только проверка данных**.
 - c. Для начала операции проверки данных нажмите кнопку **Импортировать**.
 - d. Для подтверждения завершения задачи нажмите кнопку **ОК**.
 - e. Проверьте протоколы, созданные для операции проверки данных.
 - f. Для очистки протоколов нажмите **Очистить результаты**.
 - g. Для закрытия страницы **Импортировать данные LDIF** нажмите кнопку **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
5. Для подтверждения своего действия нажмите кнопку **Да**.

Дальнейшие действия

Запустите сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Экспорт данных LDIF с помощью Инструмента настройки

Инструмент конфигурации позволяет экспортировать данные каталога из экземпляра в файл LDIF.

Прежде чем начать

Для того чтобы экспортировать данные из экземпляра в файл LDIF, для этого экземпляра должны быть выполнены следующие требования:

- Должен существовать экземпляр сервера каталогов с базой данных DB2. См. раздел “Настройка базы данных экземпляра с помощью Инструмента настройки” на стр. 176.
- Экземпляр должен содержать записи каталога.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на левой панели навигации выберите **Задачи LDIF > Экспортировать данные LDIF**.
3. На странице **Экспортировать данные LDIF** выполните следующие действия:
 - a. В поле **Полное имя файла LDIF** введите полное имя файла LDIF, в который требуется экспортировать данные. Также можно нажать кнопку **Обзор** и указать имя файла LDIF с путем.
 - b. Если файл существует и должен быть заменен, включите переключатель **Заменить существующий файл**.
 - c. Для экспорта операционных атрибутов, таких как `creatorsName`, `createTimestamp`, `modifiersName` и `modifyTimestamp`, выберите **Экспортировать операционные атрибуты**. Операционные атрибуты создаются и изменяются сервером при создании или изменении записи каталога. Эти атрибуты содержат сведения о пользователе, создавшем или изменившем запись, а также о времени ее создания или изменения. Они хранятся в файле LDIF в виде записей формата Base64.
 - d. Если данные требуется импортировать на целевой сервер, для которого поддерживается расширенный стандарт шифрования (AES), но средства шифрования на исходном и целевом сервере не синхронизированы, выберите **Экспортировать данные для сервера с поддержкой AES**.
 - e. Для экспорта записей, которые были удалены, но продолжают храниться в корзине, выберите **Экспортировать удаленные записи**. Дополнительная информация приведена в разделе Администрирование документации по IBM Security Directory Server.
 - f. При выборе опции **Экспортировать данные для сервера с поддержкой AES** укажите следующие значения:
 - В поле **Начальный ключ шифрования** введите начальный ключ шифрования целевого сервера.

- В поле **Добавление для ключа шифрования** введите добавление для ключа шифрования целевого сервера. Дополнительная информация о способах получения добавления приведена в разделе “Управление данными LDIF” на стр. 210.
 - g. Для того чтобы задать фильтр для записей, экспортируемых в файл LDIF, в поле **DN записи фильтра** укажите отличительное имя фильтра репликации. В результате применения фильтра в файл LDIF будут экспортированы отдельные, соответствующие критериям, записи базы данных. Дополнительная информация о фильтрах репликации приведена в разделе Администрирование документации по IBM Security Directory Server.
 - h. Если в файл LDIF требуется добавить комментарии, введите их в поле **Комментарии**.
 - i. Для экспорта записей из конкретного поддерева введите отличительное имя этого поддерева в поле **DN поддерева**. DN поддерева задает запись верхнего уровня того поддерева, которое необходимо записать в файл LDIF. В файл будет помещена эта запись и все записи, расположенные ниже нее в иерархии каталогов этого поддерева. Если DN поддерева не указано, то в выходной файл заносятся все записи каталогов, которые хранятся в базе данных. Для идентификации записей используются суффиксы, указанные в файле конфигурации экземпляра сервера каталогов.
 - j. Для запуска процедуры экспорта нажмите кнопку **Экспортировать**.
 - k. Для подтверждения завершения задачи нажмите кнопку **ОК**.
 - l. Проверьте протоколы, созданные в ходе экспорта данных LDIF.
 - m. Для очистки протоколов нажмите **Очистить результаты**.
 - n. Для закрытия страницы **Экспортировать данные LDIF** нажмите кнопку **Закрыть**.
4. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
 5. Для подтверждения своего действия нажмите кнопку **Да**.

Синхронизация Active Directory

Можно синхронизировать записи в контейнере пользователей и групп, находящихся в Microsoft Active Directory, с экземпляром IBM Security Directory Server. Синхронизация данных выполняется в одном направлении - из Active Directory в экземпляр сервера каталогов.

Примечание: Начиная с IBM Security Directory Server версии 6.3.1, решение синхронизации Active Directory устарело. В качестве замены следует использовать решение LDAPSync.

Для настройки и запуска синхронизации Active Directory можно использовать Инструмент настройки или утилиты командной строки, такие как **idsadscfg** и **idsadsrun**.

Примечание: Синхронизация пользователей и групп из Active Directory в экземпляр IBM Security Directory Server через IBM Security Directory Proxy Server не поддерживается.

Синхронизация Active Directory задействует IBM Security Directory Integrator для синхронизации контейнеров пользователей и групп. Для того чтобы можно было использовать синхронизацию Active Directory, сначала необходимо установить IBM Security Directory Integrator.

IBM Security Directory Integrator необходим для следующих действий:

- Запуск конфигурации
- Запуск, остановка, перезапуск и отслеживание операций

При настройке синхронизации Active Directory необходимо учесть следующие моменты:

- Приложение синхронизации Active Directory и IBM Security Directory Integrator должны находиться на том же компьютере, где установлен экземпляр сервера каталогов.
- Синхронизация Active Directory выполняется только для контейнера пользователей и групп. Это средство не синхронизирует другие объекты или контейнеры с экземпляром сервера каталогов.
- Кроме того, решение проверяет членство записи пользователя в группах, после чего запись пользователя добавляется в те группы экземпляра, которые синхронизированы с Active Directory. Когда запись пользователя удаляется из контейнера пользователя, пользователь удаляется из экземпляра. Запись пользователя также удаляется из всех групп в экземпляре.
- Синхронизация Active Directory не работает с вложенными подразделениями (ou).
- Невозможно связать несколько атрибутов Active Directory с одним атрибутом в экземпляре сервера каталогов.
- Невозможно связать атрибутов userpassword из Active Directory с экземпляром сервера каталогов. Данное решение не синхронизирует пароль пользователя.
- Синхронизация Active Directory позволяет синхронизировать пользователей и группы из одного или нескольких контейнеров пользователей Active Directory с одним подразделением (ou) сервера каталогов. Однако данное средство не позволяет синхронизировать несколько контейнеров пользователей и групп Active Directory с несколькими подразделениями (ou) сервера каталогов.
- Можно указать несколько контейнеров пользователей для синхронизации с одним подразделением (ou) в сервере каталогов, используя точку с запятой (;) в качестве разделителя. Использование других символов в качестве разделителя не поддерживается. При использовании точки с запятой (;) в качестве разделителя аргумент следует заключать в кавычки ("). В следующем примере показано применение точки с запятой (;) в качестве разделителя:
`"ou=SWUGroups,dc=adsync,dc=com;ou=STGGGroups,dc=adsync,dc=com"`.
- Атрибут SAMAccountName из Active Directory используется для составления атрибута \$dn в IBM Security Directory Server. Атрибут SAMAccountName является уникальным в домене, не возникает конфликтов при синхронизации нескольких контейнеров пользователей Active Directory с одним подразделением сервера каталогов.
- Данное решение поддерживает защищенное соединение с Active Directory, но не поддерживает защищенное соединение с экземпляром сервера каталогов.
- Если изменить DN и/или пароль администратора для экземпляра сервера каталогов после настройки синхронизации Active Directory, то синхронизацию Active Directory необходимо будет настроить заново.
- Если во время выполнения синхронизации Active Directory происходит изменение контейнеров пользователей или групп Active Directory, необходимо настроить синхронизацию Active Directory заново, указав измененные имена. В противном случае программа синхронизации Active Directory может не запуститься.
- Если для изменения пользователей или групп IBM Security Directory Server использовать другое средство, отличное от синхронизации Active Directory, то синхронизация Active Directory может выполняться неправильно.

Настройка и запуск синхронизации Active Directory

Для синхронизации контейнеров пользователей и групп Active Directory с экземпляром IBM Security Directory Server настройте и запустите синхронизацию Active Directory.

Прежде чем начать

Для настройки и выполнения синхронизации Active Directory необходимо установить следующее программное обеспечение:

- IBM Security Directory Server
- IBM Security Directory Integrator

Процедура

1. Если IBM Security Directory Integrator установлен в пользовательском каталоге, задайте переменную среды *IDS_LDAP_TDI_HOME*, указав в ней этот каталог.

Примечание: В системе Windows указанное в этой переменной среды имя каталога не должно содержать пробелов и кавычек. При задании каталога используйте краткое имя.

По умолчанию IBM Security Directory Integrator устанавливается в следующем каталоге:

AIX и Solaris

`/opt/IBM/TDI/V7.1`

Linux `/opt/ibm/TDI/V7.1`

Windows

`C:\Program Files\IBM\TDI\V7.1`

2. Необязательно: Загрузите примеры файлов `users.ldif` и `groups.ldif` в Active Directory.
3. Для настройки синхронизации Active Directory выполните команду **idsadscfg**. Кроме того, для настройки синхронизации Active Directory можно запустить Инструмент настройки. Эта команда создает файлы `adsync_private.prop` и `adsync_public.prop`.
4. Измените файл `adsync_public.prop`, указав в нем параметры SSL и дополнительные атрибуты. Дополнительная информация о файлах и безопасном обмене данными приведена в разделе *Администрирование* в документации по IBM Security Directory Server.
5. Введите команду **idsadsrun** для запуска синхронизации Active Directory. Команда предложит выбрать один из вариантов: запуск полной синхронизации с последующей синхронизацией в реальном времени, или запуск синхронизации в реальном времени. Инструмент синхронизации Active Directory выявляет изменения в записях Active Directory и синхронизирует их с записями в IBM Security Directory Server.
6. Необязательно: Для администрирования и отслеживания синхронизации запустите Консоль администрирования и мониторинга IBM Security Directory Integrator.

Настройка синхронизации Active Directory с помощью Configuration Tool

С помощью Configuration Tool можно настроить синхронизацию Active Directory с экземпляром сервера каталогов.

Прежде чем начать

Для настройки синхронизации Active Directory должны быть выполнены следующие требования:

- Установите IBM Security Directory Integrator.
- Необходимо остановить сервер каталогов. См. раздел “Запуск и завершение работы сервера каталогов и административного сервера с помощью Инструмента настройки” на стр. 171.

Процедура

1. Запустите Инструмент настройки для экземпляра. См. раздел “Запуск Инструмента настройки” на стр. 170.
2. В списке задач на панели навигации слева выберите **Синхронизация Active Directory**.
3. На странице **Синхронизация Active Directory: сведения об экземпляре** укажите сведения о конфигурации экземпляра IBM Security Directory Server. Предоставленная информация сохраняется в файлах `adsync_private.properties` и `adsync_public.properties`. Файлы расположены в подкаталоге `etc/tdisoldir` домашнего каталога экземпляра.
4. В поле **Суффикс каталога** укажите суффикс сервера каталогов, который требуется использовать для синхронизации Active Directory. В поле **LDAP URL** показан URL экземпляра сервера каталогов. Данное поле недоступно для изменения.
5. В поле **DN записи контейнера групп** введите DN контейнера, в который необходимо скопировать группы из Active Directory. Синхронизация будет выполнена для групп и участников групп между Active Directory и IBM Security Directory Server. Добавление или удаление пользователя из группы Active Directory предусматривает добавление или удаление записи из соответствующей группы экземпляра IBM Security Directory Server.
6. В поле **DN записи контейнера пользователей** введите DN контейнера, в который необходимо скопировать пользователей из Active Directory.
7. Если для подключения к Active Directory должно применяться соединение SSL, то включите переключатель **Использовать соединение SSL с Active Directory**. Соединения SSL с IBM Security Directory Server не поддерживаются. Инструкции по настройке соединения SSL с Active Directory приведены в разделе *Администрирование* документации по IBM Security Directory Server.
8. Нажмите кнопку **Далее**. Откроется страница **Синхронизация Active Directory: Сведения Active Directory**.
9. В поле **Адрес хоста** введите имя хоста или IP-адрес контроллера домена Active Directory.
10. В поле **Порт хоста** укажите порт, применяемый Active Directory.
11. В поле **Имя пользователя** введите имя пользователя, которое должно применяться IBM Security Directory Integrator для преобразования к Active Directory. Этому пользователю должны быть предоставлены права на чтение записей Active Directory, которые планируется копировать в экземпляр сервера каталогов.
12. В поле **Пароль для входа в систему** введите пароль, применяемый IBM Security Directory Integrator для преобразования к Active Directory.
13. В поле **База поиска** укажите поддерево Active Directory, из которого копируются изменения в экземпляр. Изменения записей пользователей из поддерева

передаются в экземпляр сервера каталогов. Для передачи всех пользователей из групп Active Directory в экземпляр в качестве базы поиска укажите верхний уровень иерархии Active Directory.

14. В поле **DN записи контейнера групп** введите DN контейнера Active Directory для синхронизации групп с экземпляром.
15. В поле **DN записи контейнера пользователей** введите DN контейнера Active Directory для синхронизации записей пользователей с экземпляром.
16. Нажмите кнопку **Готово**. Откроется окно **Синхронизация Active Directory: Результаты**.
17. Проверьте сообщения протокола, создаваемые для конфигурации синхронизации Active Directory.
18. Для очистки протоколов нажмите **Очистить результаты**.
19. Для того чтобы закрыть страницу **Синхронизация Active Directory**, нажмите кнопку **Закрыть**.
20. Для закрытия окна Инструмент настройки воспользуйтесь меню **Файл > Выход**.
21. Для подтверждения своего действия нажмите кнопку **Да**.

Настройка синхронизации Active Directory с помощью командной строки

С помощью команды **idsadscfg** настройте синхронизацию Active Directory с экземпляром сервера каталогов.

Прежде чем начать

Для настройки синхронизации Active Directory должны быть выполнены следующие требования:

- Установите IBM Security Directory Integrator.
- Необходимо остановить сервер каталогов. Обратитесь к разделу “Запуск и завершение работы сервера каталогов и административного сервера с помощью утилит командной строки” на стр. 159.

Процедура

1. Войдите в систему AIX, Linux, Solaris или Windows от имени пользователя root или администратора.
2. Откройте окно ввода команд.
3. Измените текущий рабочий каталог на подкаталог `sbin` в расположении установки IBM Security Directory Server.
4. Для настройки синхронизации Active Directory с экземпляром выполните команду **idsadscfg** в следующем формате:

```
idsadscfg -I имя-экземпляра
-adH ldap://LDAP_server1:389 -adb dc=adsyncctest,dc=com
-adD cn=administrator,cn=users,dc=adsyncctest,dc=com -adw secret -adg ou=testgroup1,
dc=adsyncctest,dc=com -adu ou=testuser1,dc=adsyncctest,dc=com -ids o=sample -idsg
ou=Testgroup1,ou=groups,o=sample -idsu ou=Testuser1,ou=users,o=sample
```

Дополнительная информация о команде **idsadscfg** приведена в разделе *Справочник по командам*.

Дальнейшие действия

Выполните команду **idsadsrun** для запуска синхронизации Active Directory.
Дополнительная информация о команде **idsadsrun** приведена в *Справочнике по командам*.

Глава 21. Автоматический запуск экземпляров сервера каталогов при запуске операционной системы

Можно настроить автоматический запуск экземпляров сервера каталогов при запуске компьютера, который может быть выключен для обслуживания или модернизации.

При создании экземпляра сервера каталогов сервер администрирования запускается, если экземпляр был создан успешно. Для того чтобы запустить сервер каталогов с базой данных DB2, для экземпляра необходимо запустить процесс `ibmslapd` или `idslapd`.

При перезапуске компьютера необходимо одновременно запустить связанные с экземпляром сервер администрирования и процесс `ibmslapd`. Однако в операционной системе можно настроить автоматический запуск служб и процессов, связанных с экземпляром.

Для того чтобы запускать экземпляр сервера каталогов при запуске операционной системы AIX, Linux или Solaris, необходимо обновить информацию о сервере в файле `/etc/inittab`. Файл `inittab` определяет, какие процессы должны запускаться при запуске операционной системы и во время обычной работы. Запись для сервера каталогов добавляется в файл `inittab` в следующем формате:

ид:уровни-запуска:действие:процесс

Атрибуты в файле `inittab` должны содержать следующие значения:

id Уникальный ИД в файле, занимающий от 1 до 4 разрядов.

runlevels

Атрибут `runlevels` показывает режим `runlevel` операционной системы, в которой процесс запускается автоматически. Он относится к режиму работы операционной системы AIX, Linux или Solaris. В различных операционных системах атрибут `runlevels` настраивается по-разному. Сведения о настройке `runlevel` приведены в руководстве по конкретной операционной системе.

action Атрибут `action` задает тип действия.

process

Атрибут `process` задает процесс, которые требуется запускать.

Настройка автоматического запуска экземпляра сервера каталогов в системе Windows

Окно **Службы** позволяет настроить автоматический запуск экземпляра сервера каталогов в системе Windows.

Прежде чем начать

Для настройки автоматического запуска экземпляра сервера каталогов в ходе запуска операционной системы компьютер должен соответствовать следующим требованиям:

- Компьютер должен содержать экземпляр сервера каталогов, который может работать в обычном режиме.

Об этой задаче

В системе Windows сервер каталогов (процесс `idsldapd`) можно запустить с помощью окна **Службы** или команды `idsldapd`. Для экземпляра сервера каталогов с базой данных DB2, необходимо указать службу, связанную с сервером каталогов, который зависит от службы экземпляра DB2. Для экземпляра сервера каталогов с базой данных DB2, перед запуском процесса `idsldapd` необходимо запустить DB2. Если зависимость на задана и в поле **Тип запуска** для службы, связанной с сервером, указано значение **Автоматически**, то после перезапуска компьютера может возникнуть ошибка. Для экземпляра прокси-сервера не требуется настраивать зависимость от службы, связанной с экземпляром DB2.

Для экземпляра прокси-сервера выполните шаги 1, 2, 4, 5 и 6.

Процедура

1. Войдите в систему от имени администратора.
2. Для того чтобы открыть окно **Службы**, выполните следующие действия:
 - a. Выберите **Пуск > Выполнить**.
 - b. В поле **Открыть** введите `services.msc`.
 - c. Нажмите **ОК**.
3. Найдите службу DB2, связанную с экземпляром сервера каталогов, который должен запускаться автоматически. Имя службы начинается с символов DB2 - SDSV631DB2 -. Для экземпляра DB2 с именем DSRDBM01 следует указать запись DB2 - SDSV631DB2 - DSRDBM01. Дважды щелкните на службе и запишите значение после строки DB2 - SDSV631DB2 - в поле **Отображаемое имя**. В этом примере применяется значение DSRDBM01.
4. Найдите службу, связанную с экземпляром сервера каталогов, которую требуется настроить для автоматического запуска. Имя службы начинается со строки IBM Security Directory Server Instance 6.3.1. Для экземпляра с именем dsrdbm01 следует указать запись IBM Security Directory Server Instance 6.3.1 - dsrdbm01. Дважды щелкните на службе и запишите значение после строки IBM Security Directory Server Instance 6.3.1 - в поле **Отображаемое имя**. В этом примере для dsrdbm01 применяется значение `idsldapd-dsrdbm01`.
5. В окне свойств Экземпляр IBM Security Directory Server 6.3.1 - dsrdbm01 в списке **Тип запуска** выберите **Автоматически**.
6. Нажмите **ОК**.
7. Для того чтобы закрыть страницу **Службы**, выберите **Файл > Выход**.
8. Для того чтобы открыть реестр Windows, выполните следующие действия:
 - a. Выберите **Пуск > Выполнить**.
 - b. В поле **Открыть** введите `regedit`.
 - c. Нажмите **ОК**.
9. На панели навигации выберите **Мой компьютер > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services**.
10. Найдите службу, связанную с экземпляром сервера каталогов. В этом примере применяется значение `idsldapd-dsrdbm01`.
11. Щелкните на службе, связанной с экземпляром.
12. На правой панели дважды щелкните на атрибуте `DependOnService`.
13. В окне **Изменение многострочного параметра** добавьте имя службы DB2, связанной с экземпляром **LanmanServer**. В этом примере применяется значение DSRDBM01.

14. Нажмите **ОК**. Создается зависимость от службы DB2.
15. Для того чтобы закрыть реестр Windows, выберите **Файл > Выход**.

Результаты

После перезапуска системы экземпляр сервера каталогов будет запущен автоматически.

Настройка автоматического запуска экземпляра сервера каталогов в системе UNIX

Добавьте в файл `/etc/inittab` записи сервера каталогов для настройки автоматического запуска экземпляра сервера каталогов в системе AIX, Linux или Solaris.

Прежде чем начать

Для настройки автоматического запуска экземпляра сервера каталогов в ходе запуска операционной системы компьютер должен соответствовать следующим требованиям:

- Компьютер должен содержать экземпляр сервера каталогов, который может работать в обычном режиме.

Процедура

1. Войдите в систему от имени пользователя `root`.
2. Для настройки автоматического запуска экземпляра сервера каталогов или экземпляра прокси-сервера добавьте следующие записи в файл `/etc/inittab`:
 - a. Для добавления процесса `idsslapd` и сервера администрирования, связанного с экземпляром сервера каталогов, добавьте следующие записи:

```
AIX   srv1:2:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I  
        имя-экземпляра > /dev/null 2>&1 #Autostart IBM Directory  
        Server Instance
```

```
        adm1:2:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I  
        имя-экземпляра > /dev/null 2>&1 #Autostart IBM Directory  
        Administartion Server
```

```
Linux srv1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmslapd -I  
        имя-экземпляра > /dev/null 2>&1 #Autostart IBM Directory  
        Server Instance
```

```
        adm1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmdiradm -I  
        имя-экземпляра > /dev/null 2>&1 #Autostart IBM Directory  
        Administartion Server
```

```
Solaris srv1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmslapd -I  
        имя-экземпляра > /dev/null 2>&1 #Autostart IBM Directory  
        Server Instance
```

```
        adm1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I  
        имя-экземпляра > /dev/null 2>&1 #Autostart IBM Directory  
        Administartion Server
```

Вместо переменной *экземпляр* укажите имя своего экземпляра.

- b. Для добавления процесса `idsslapd` и сервера администрирования, связанного с экземпляром прокси-сервера, сначала необходимо запустить экземпляры

сервера каталогов. Перед запуском прокси-сервера необходимо запустить все серверы каталогов с базой данных DB2. Если на компьютере установлены полный сервер каталогов и прокси-сервер, то их запуск следует выполнять с задержкой. В следующем примере задержка добавляется с помощью записи в следующем формате: id:2345:wait (файл /etc/inittab).

```
AIX  srv1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
      имя-экземпляра-1 > /dev/null 2>&1 #Autostart IBM Directory
      Server Instance

      adm1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
      имя-экземпляра-1 > /dev/null 2>&1 #Autostart IBM Directory
      Administartion Server

      srv2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
      имя-экземпляра-2 > /dev/null 2>&1 #Autostart IBM Directory
      Server Instance

      adm2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
      имя-экземпляра-2 > /dev/null 2>&1 #Autostart IBM Directory
      Administartion Server

      srv3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
      экземпляр-прокси-сервера-1 -k > /dev/null 2>&1 #Autostart IBM
      Directory Proxy Server Instance

      adm3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
      экземпляр-прокси-сервера-1 -k > /dev/null 2>&1 #Autostart IBM
      Directory Administartion Server

      srv4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
      экземпляр-прокси-сервера-1 > /dev/null 2>&1 #Autostart IBM
      Directory Proxy Server Instance

      adm4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
      экземпляр-прокси-сервера-1 > /dev/null 2>&1 #Autostart IBM
      Directory Administartion Server
```

Вместо переменных *имя-экземпляра-1* и *имя-экземпляра-2* укажите имена экземпляров сервера каталогов. Вместо переменной *экземпляр-прокси-сервера-1* укажите имя экземпляра прокси-сервера.

Результаты

После добавления записей в файл /etc/inittab экземпляр сервера каталогов готов к автоматическому запуску вместе с системой.

Глава 22. Стратегия пакетов исправлений

Приведена информация пакетах исправлений и исправлениях для IBM Security Directory Server.

Для систем AIX, Linux, Solaris и HP-UX доступны исправления и пакеты исправлений, устанавливаемые с помощью сценариев.

Для Windows доступны исправления и пакеты исправлений на основе IBM Installation Manager.

Исправления и пакеты исправлений на основе IBM Installation Manager можно установить с помощью графического пользовательского интерфейса или в режиме без вывода сообщений.

Версию установленного исправления или пакета исправлений можно определить с помощью IBM Installation Manager.

- Выберите **Файл > Просмотреть установленные пакеты**
- Выполните команду **imcl** из каталога tools, расположенного в установочном каталоге IBM Installation Manager.

В системах UNIX для определения версии установленного исправления или пакета исправлений обратитесь к версии внутреннего пакета.

Примечание: После применения внутреннего пакета исправлений к базовой версии не следует выполнять действия по изменению и удалению с помощью IBM Installation Manager. После применения внутреннего пакета исправлений дальнейшие действия следует выполнять только в рамках внутреннего метода.

Установка пакетов исправлений с помощью IBM Installation Manager

С помощью IBM Installation Manager можно применить пакеты исправлений или установить усовершенствования потока служб в системах Microsoft Windows.

Прежде чем начать

- Ознакомьтесь с информацией стратегии пакетов исправлений.
- Убедитесь, что в системе установлен IBM Installation Manager версии 1.7.0 или более поздней. Обратитесь к документации по IBM Installation Manager.
- Перед тем как приступить к установке пакета исправлений, остановите все активные процессы и службы IBM Security Directory Server. Это можно сделать вручную или с помощью кнопки **Завершить все блокирующие процессы** в Installation Manager.

Об этой задаче

Пакет исправлений обновляет только уже установленные компоненты. Обновите продукт перед установкой новых компонентов с помощью мастера **Изменить**.

Пакет исправлений не обновляет IBM DB2, IBM GSKit, встроенный IBM WebSphere Application Server и IBM Java Development Kit. Это программное обеспечение можно обновить с помощью мастера **Изменить**.

Процедура

1. Загрузите пакет исправлений с веб-страницы <http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631>.
 2. Укажите параметры хранилища в IBM Installation Manager.
 - a. Для запуска IBM Installation Manager в меню **Пуск** выберите **Все программы > IBM Installation Manager > IBM Installation Manager**.
 - b. На странице Запуск продукта IBM Installation Manager выберите **Файл > Параметры**.
 - c. На странице Хранилища выберите **Добавить хранилище**.
 - d. На странице Добавить хранилище укажите одно из следующих хранилищ:
 - Путь к локальному каталогу или удаленному общему диску, содержащему пакет продукта, загруженный с веб-сайта службы поддержки IBM.
 - URL хранилища на веб-сервере.
 - e. Нажмите **ОК**. Если вы указали HTTPS или расположение хранилища с ограниченным доступом, то вам будет предложено ввести ИД пользователя и пароль. Будет указано новое или изменившееся расположение хранилища.
 - f. Для проверки доступа к хранилищу выберите **Проверить соединения**.
 - g. Нажмите **ОК**, чтобы завершить работу со страницей Хранилища.
 3. Запустите установку.
 - Если IBM Security Directory Server версии 6.3.1 не установлен, выполните следующие действия:
 - a. На начальной странице IBM Installation Manager выберите **Установить**. Мастер **Установить** помогает выполнить этапы процесса установки.
 - b. Выполните действия по установке из раздела “Установка с помощью IBM Installation Manager” на стр. 30.
 - Если IBM Security Directory Server версии 6.3.1 установлен, то для применения пакета исправлений выполните следующие действия:
 - a. На начальной странице IBM Installation Manager выберите **Обновить**. Мастер **Обновить** выполняет поиск доступных обновлений для пакетов, установленных в системе.
 - b. Выберите **IBM Security Directory Server**. Отображается установочный каталог версии 6.3.1; его нельзя изменить. Нажмите кнопку **Далее**.
 - c. Выберите продукт для обновления (**IBM Security Directory Server**) и версию обновления (**Версия 6.3.1.5**). Нажмите кнопку **Далее**.
 - d. Примите лицензионное соглашение на пакет исправлений и нажмите кнопку **Далее**.
 - e. Обновляемые компоненты выбираются по умолчанию из числа установленных компонентов. Нажмите кнопку **Далее**.
- Примечание:** Если отменить выбор компонента, то он будет помечен для удаления.
- Ограничение:** На этой странице по умолчанию выбран компонент IBM DB2, однако он не обновляется. Предварительно необходимое программное обеспечение не обновляется с помощью мастера **Обновить**, входящего в состав IBM Installation Manager. Не отменяйте выбор компонента IBM DB2, поскольку вместе с ним будет отменен выбор компонента сервера.
- f. Проверьте информацию на странице обзора и нажмите кнопку **Далее**, чтобы начать установку.

4. Проверьте правильность установки. Инструкции по проверке с помощью для IBM Installation Manager и разных операционных систем приведены в разделе Глава 13, “Проверка компонентов IBM Security Directory Server”, на стр. 85.

Дальнейшие действия

Для удаления пакет исправлений запустите мастер **Откатить**, позволяющий восстановить предыдущую версию пакета.

Установка пакетов исправлений без вывода сообщений

IBM Installation Manager позволяет установить пакеты исправлений в режиме без вывода сообщений.

Примечание: В файле ответов для обновлений можно указать только компоненты, которые уже установлены. Если указать отсутствующий компонент, то возникнет сбой процесса обновления.

Создайте новый файл ответов для установки пакета исправлений

Если файл ответов, с помощью которого был установлен продукт, недоступен, то создайте новый файл ответов.

1. Запустите IBM Installation Manager в режиме имитации установки. Например:

```
C:\Program Files\IBM\Installation Manager\eclipse\IBMIM.exe  
-record c:\SDS_6310\install_resp.xml -skipInstall
```

расположение-агента-данных

где

расположение-данных-агента содержит данные, необходимые для установки продукта.

2. Укажите параметры хранилища для версии 6.3.1.0.
3. Выполните процесс имитации установки.
4. Закройте IBM Installation Manager. Файл ответов для процесса установки создается без установки продукта.
5. Выполните инструкции из следующего раздела.

Установка с помощью файла ответов, который использовался для установки продукта

1. Откройте файл ответов `install_resp.xml` и внесите в него следующие изменения:

- a. Укажите путь к хранилищу версии 6.3.1.5.

```
<repository location='C:\SDS_6315\ibm_sds' />
```

- b. Обновите версию предложения до 6.3.1.5.

```
<offering id='com.ibm.security.directoryserver.v631' version='6.3.1.5' profile=.....
```

2. Запустите установку в режиме без вывода сообщений, чтобы применить пакет исправлений. Например:

```
C:\Program Files\IBM\Installation Manager\eclipse\tools\imcl.exe  
input c:\SDS_6310\install_resp.xml -acceptLicense -showProgress
```

В этой команде можно указать параметр `-stopBlockingProcesses`, позволяющий предварительно остановить все процессы, блокирующие установку пакета исправлений.

Установка пакетов исправлений с помощью стандартных сценариев

Запустите сценарий из командной строки, чтобы применить пакеты исправлений или установить усовершенствования потока служб в системах AIX, Linux и Solaris.

Прежде чем начать

Ознакомьтесь с информацией о стратегии пакетов исправлений.

Процедура

1. Загрузите пакет исправлений с веб-страницы <http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631>.
2. Распакуйте архив исправлений в каталог, в котором достаточно свободного места. Сведения о содержимом пакета исправлений, включая имена каталогов и файлов, указаны в файле *README*, который поставляется вместе с пакетом исправлений.
3. Остановите все процессы клиента и сервера, связанные с IBM Security Directory Server. Набор процессов демона включает сервер каталогов, сервер администрирования, прокси-сервер (если применяется) и пользовательские приложения LDAP. Программы и библиотеки нельзя заменить, если они используются. Если включена трассировка, остановите ее с помощью команды **ldtrc off**. Дополнительная информация об остановке экземпляров сервера каталогов и процессов администрирования приведена в разделе Основные задачи администрирования сервера в документации по IBM Security Directory Server.
4. В командной строке перейдите в каталог, в который был распакован архив исправлений.
5. Запустите следующую команду от имени пользователя root:

```
idsinstall -u -f
```

Программа установки устанавливает обновления компонентов, которые уже установлены в системе.

6. Проверьте правильность установки.
 - a. Программа установки выдает сообщение с информацией о состоянии установки. Проверьте протокол установки: `/tmp/idsinstall_время`.
 - b. Если в ходе установки возникли ошибки или выдано сообщение о том, что установлены не все пакеты, исправьте ошибки, зарегистрированные в протоколе, например, освободите дисковую память. Затем снова запустите программу установки и убедитесь, что все пакеты установлены правильным образом.
 - c. Проверьте номер версии пакетов. Инструкции приведены в разделе Глава 6, “Запрос пакетов IBM Security Directory Server”, на стр. 47.

Глава 23. Удаление IBM Security Directory Server: обзор

Обзор удаления продукта IBM Security Directory Server и важные инструкции по подготовке к удалению.

Прежде чем начать

Для удаления IBM Security Directory Server войдите в систему от имени пользователя root (AIX, Linux, Solaris и HP-UX) или от имени администратора (Windows).

Об этой задаче

Вместе с IBM Security Directory Server не удаляются экземпляры и файлы конфигурации.

Процедура

1. Остановите все процессы клиента или сервера IBM Security Directory Server, включая демон администрирования и пользовательские приложения LDAP. Программы и библиотеки нельзя заменить, если они используются. Если включена трассировка, выключите ее с помощью команды **ldtrc off**.
2. Удалите IBM Security Directory Server с учетом операционной системы и режима установки IBM Security Directory Server. Доступны следующие способы установки пакетов IBM Security Directory Server:
 - a. Программа удаления с графическим пользовательским интерфейсом.
 - b. Утилиты операционной системы. Имена пакетов в системах Linux незначительно отличаются для обновлений по сравнению с версией GA. Пример имени пакета базового клиента в версии GA для xSeries Linux: `idsldap-cltbase63-6.3.0-0.i386.rpm`. Список всех пакетов можно просмотреть с помощью команды **rpm -qa**.
3. После удаления IBM Security Directory Server проверьте правильность удаления всех пакетов IBM Security Directory Server. Дополнительная информация приведена в разделе Глава 6, “Запрос пакетов IBM Security Directory Server”, на стр. 47.

Информация, связанная с данной:

 <http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome>

Дополнительная информация приведена в разделе *Удаление IBM Security Directory Server* в главе *Установка и настройка* в документации по IBM Security Directory Server.

Глава 24. Удаление из системы IBM Security Directory Server и сопутствующего программного обеспечения

Может потребоваться удалить IBM Security Directory Server и сопутствующее программное обеспечение, если вы планируете использовать компьютер для других целей или вывести его из строя.

Можно использовать IBM Installation Manager или утилиты операционной системы для удаления из системы IBM Security Directory Server. Для удаления из системы необходимо использовать то же средство, которое использовалось для установки. Как для установки, так и для удаления из системы, необходимо использовать или IBM Installation Manager, или утилиты операционной системы. Нельзя смешивать средства для установки и для удаления из системы.

Если вы хотите удалить IBM Security Directory Server из системы, учтите перед этим следующее:

1. Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server.
 - Сервер каталогов
 - Административный сервер
 - Трассировка LDAP
 - Web Administration Tool и связанный с ним сервер приложений
 - Пользовательские приложения LDAP
2. Если вы планируете снова выполнить установку IBM Security Directory Server на компьютере, не требуется удалять экземпляр сервера каталогов или удалять конфигурацию базы данных DB2 из этого экземпляра. Если IBM Security Directory Server удален из системы, экземпляры сервера каталогов остаются нетронутыми, если их не удалить вручную.
3. Группа и пользователь `idsldap`, созданные при установке IBM Security Directory Server, остаются в системе после удаления из системы. Необходимо учесть дополнительные условия перед удалением IBM Security Directory Server из системы AIX, Linux или Solaris.
 - Если вы не хотите оставлять определенных пользователя и группу `idsldap`, удалите их с помощью утилит операционной системы. Пользователь и группа `idsldap` требуются как для прокси-сервера, так и для полного сервера каталогов, поэтому они должны существовать на компьютере, если установлен IBM Security Directory Server.
 - Если пользователь `idsldap` удален, но не удален домашний каталог пользователя, могут возникнуть неполадки при создании пользователя `idsldap` в процессе установки IBM Security Directory Server. Поэтому, обязательно удалите домашний каталог пользователя `idsldap` при удалении пользователя `idsldap`. При удалении пользователя `idsldap` с помощью команды `userdel` следует указать опцию удаления домашнего каталога `-r` (`userdel -r idsldap`).
4. В системах Windows службы сервера администрирования и сервера каталогов удаляются в процессе удаления из системы IBM Security Directory Server. Службы не перемещаются в процессе установки IBM Security Directory Server. Команда `idsslapd` добавляет службу сервера каталогов, а команда `idsdiradm` добавляет службу сервера администрирования. Более подробная информация о командах `idsslapd` и `idsdiradm` находится в *IBM Security Directory Server Справочнике по командам*.

Удаление из системы с помощью IBM Installation Manager

Если IBM Security Directory Server установлен с помощью IBM Installation Manager, используйте IBM Installation Manager для удаления IBM Security Directory Server и его компонентов из системы.

При использовании IBM Installation Manager для удаления из системы IBM Security Directory Server, программа удаляет IBM Security Directory Server и все его сопутствующее программное обеспечение, которое было установлено. Невозможно выборочно удалить компоненты IBM Security Directory Server в процессе удаления из системы с помощью IBM Installation Manager.

Если установлена база данных IBM DB2, предоставленная с IBM Security Directory Server, необходимо удалить все экземпляры DB2, созданные с помощью копии DB2, для успешного удаления IBM DB2. Если экземпляр DB2, созданный с помощью копии DB2, остается на компьютере, то в процессе удаления из системы IBM Security Directory Server DB2 не удаляется. IBM Installation Manager вносит сообщения об ошибках в свой файл протокола.

Для установки, изменения или удаления из системы IBM Security Directory Server и его компонентов необходимо использовать IBM Installation Manager или утилиты операционной системы. Нельзя использовать и IBM Installation Manager, и утилиты операционной системы, для установки, изменения или удаления из системы IBM Security Directory Server и его компонентов.

Удаление с помощью IBM Installation Manager

С помощью IBM Installation Manager можно удалить IBM Security Directory Server, если вы устанавливали IBM Security Directory Server с помощью IBM Installation Manager.

Прежде чем начать

Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Пользовательские приложения LDAP

При наличии активных процессов удалить программы и библиотеки нельзя.

Процедура

1. Запустите IBM Installation Manager.
 - AIX и Linux:
 - a. Откройте окно командной строки и перейдите в каталог, содержащий IBM Installation Manager. Следующий каталог служит установочным каталогом по умолчанию IBM Installation Manager:
`opt/IBM/InstallationManager/eclipse`
 - b. Введите следующую команду:
`./IBMIM`
 - Microsoft Windows:
 - a. Выберите **Пуск > Все программы > IBM Installation Manager > IBM Installation Manager**.

2. Нажмите **Удалить**.
3. Выберите **IBM Security Directory Server** соответствующей версии и нажмите **Далее**.
4. В окне **Удалить пакеты** просмотрите перечень пакетов, выбранных для удаления.

Важное замечание: Если вы хотите продолжить работу с существующей версией DB2 или GSKit в процессе установки, IBM Installation Manager обновляет свой реестр с помощью записи компонента. При удалении компонента, который был установлен с помощью опции **Продолжить работу с существующей версией**, Installation Manager выполняет следующие действия:

- Удаляет запись компонента из реестра IBM Installation Manager.
- Не удаляет компонент из системы.

Если существуют экземпляры DB2, которые вы создали вместе с копией DB2, установленной с помощью IBM Installation Manager, то удалить IBM Security Directory Server нельзя. В этом случае вы должны вручную удалить экземпляры DB2 и затем повторить попытку. Перед удалением экземпляров DB2 рекомендуется создать резервную копию базы данных.

5. Нажмите **Удалить**. По окончании удаления IBM Installation Manager укажет, успешно ли прошло удаление.
6. Необязательно: Если во время удаления произойдет ошибка, нажмите **Просмотреть файл протокола**, чтобы ознакомиться со сведениями об ошибке. Дополнительная информация приведена в разделе Глава 5, “Протоколы IBM Installation Manager”, на стр. 45.
7. Нажмите кнопку **Готово**.
8. Выберите **Файл > Выход**.

Результаты

IBM Installation Manager удалит IBM Security Directory Server и его компоненты.

Удаление без вывода сообщений с помощью файла ответов

Выполните процедуру удаления компонентов IBM Security Directory Server без вывода сообщений, используя файл ответов.

Прежде чем начать

IBM Installation Manager версии 1.7.0 или выше необходим для установки пакетов IBM Security Directory Server без вывода сообщений.

Об этой задаче

Вы можете воспользоваться файлом ответов по умолчанию или записать свой файл ответов и использовать его в качестве входного файла для удаления без вывода сообщений.

Процедура

1. Войдите в систему как администратор.
2. Откройте команду **IBMIM** в установочном каталоге IBM Installation Manager.

Операционная система	Каталог по умолчанию команды IBMIM:
Microsoft Windows	C:\Program Files\IBM\ InstallationManager\ eclipse
AIX и Linux	/opt/IBM/InstallationManager/eclipse

3. Необязательно: Выполните команду **IBMIM** для записи файла ответов, предназначенного для процедуры удаления.
- a. Выполните одну из следующих команд, в зависимости от операционной системы:

Microsoft Windows

```
IBMIM.exe -record путь\uninstall_responseFile.xml -skipInstall
каталог_данных_агента
```

AIX и Linux

```
./IBMIM -record путь/uninstall_responseFile.xml -skipInstall
каталог_данных_агента
```

Команда откроет IBM Installation Manager.

- b. Закончите запись процедуры удаления IBM Security Directory Server. Дополнительная информация приведена в разделе 2 на стр. 233.
4. Выполните команду **IBMIM**, чтобы запустить удаление без вывода сообщений с использованием файла ответов в качестве входного.

Операционная система	Выполняемая команда:
Microsoft Windows	IBMIM.exe -silent -input путь\uninstall_responseFile.xml -noSplash
AIX и Linux	./IBMIM -silent -input путь/uninstall_responseFile.xml -noSplash

5. Просмотрите итоговый отчет об удалении и файлы протокола.

Операционная система	Путь к протоколу по умолчанию:
Microsoft Windows	C:\ProgramData\IBM\InstallationManager\ logs
AIX и Linux	/var/ibm/InstallationManager/logs/

6. Убедитесь, что пакеты IBM Security Directory Server удалены.

Операционная система	Проверка пакетов:
Microsoft Windows	См. раздел “Проверка компонентов IBM Security Directory Server в Windows” на стр. 85.
AIX и Linux	См. раздел “Проверка пакетов IBM Security Directory Server” на стр. 86.

Результаты

IBM Installation Manager удалит компоненты IBM Security Directory Server без вывода сообщений.

Удаление в режиме без вывода сообщений с помощью команды `imcl uninstall`

Выполните процедуру удаления компонентов IBM Security Directory Server без вывода сообщений с помощью команды `imcl uninstall`.

Прежде чем начать

IBM Installation Manager версии 1.7.0 или выше необходим для установки пакетов IBM Security Directory Server без вывода сообщений.

Об этой задаче

С помощью команды `imcl uninstall` можно удалить IBM Security Directory Server в режиме без вывода сообщений.

Процедура

1. Войдите в систему как администратор.
- 2.
3. Выполните команду `imcl listInstalledPackages` из каталога `<каталог-IBM-Installation-Manager>/eclipse/tools`.

Операционная система	Команда
Microsoft Windows	<code>imcl.exe listInstalledPackages</code>
AIX и Linux	<code>./imcl listInstalledPackages</code>

Позволяет просмотреть список всех пакетов, установленных с помощью IBM Installation Manager.

4. Выполните команду `imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0`. Воспользуйтесь записью Security Directory Server, которая выдается командой `imcl listInstalledPackages`.

Операционная система	Выполняемая команда:
Microsoft Windows	<code>imcl.exe uninstall com.ibm.security.directoryserver.v631_6.3.1.0</code>
AIX и Linux	<code>./imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0</code>

Результаты

IBM Installation Manager удалит компоненты IBM Security Directory Server без вывода сообщений.

Удаление из системы IBM Security Directory Server с помощью утилит операционной системы

Если для установки IBM Security Directory Server использовались утилиты операционной системы, то используйте их для удаления IBM Security Directory Server из системы.

Можно использовать утилиты операционной системы для удаления IBM Security Directory Server с компьютеров, выполняющих операционные системы AIX, Linux,

Solaris и HP-UX. В системах Windows необходимо использовать IBM Installation Manager как для установки, так и для удаления из системы IBM Security Directory Server. Обратитесь к разделу “Удаление с помощью IBM Installation Manager” на стр. 232.

При использовании утилит операционной системы для удаления IBM Security Directory Server программа удаляет IBM Security Directory Server. Можно выборочно удалить компоненты IBM Security Directory Server в процессе удаления из системы с помощью утилит операционной системы.

Перед удалением IBM Security Directory Server необходимо остановить все процессы сервера и клиента IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Web Administration Tool и связанный с ним сервер приложений
- Пользовательские приложения LDAP

Если создан и настроен экземпляр сервера каталогов с базой данных DB2, они не удаляются при использовании утилит операционной системы для удаления IBM Security Directory Server.

Удаление из системы с помощью утилит AIX

С помощью утилит командной строки AIX можно удалить IBM Security Directory Server из системы AIX.

Можно использовать одну из следующих утилит для удаления из системы IBM Security Directory Server:

SMIT Предпочтительным методом удаления из системы является использование утилиты. Дополнительная информация приведена в разделе “Удаление с помощью SMIT”.

installp

Дополнительная информация приведена в разделе “Удаление с помощью **installp**” на стр. 237.

Удаление с помощью SMIT

Команда **smi**t позволяет удалить IBM Security Directory Server из системы AIX.

Прежде чем начать

Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Web Administration Tool и связанный с ним сервер приложений
- Пользовательские приложения LDAP

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.

3. Выполните команду **smi t**. Откроется окно **Установка и обслуживание программного обеспечения**.
4. Выберите **Установка и обслуживание программного обеспечения > Обслуживание программного обеспечения и утилиты**.
5. Выберите **Удалить установленное программное обеспечение**.
6. В поле **Имя программного обеспечения** нажмите **F4**, чтобы просмотреть список установленного программного обеспечения. Вы можете указать значение `idsldap` в поле, чтобы просмотреть список всех пакетов IBM Security Directory Server.
7. Выберите пакеты для удаления и нажмите Enter.

Результаты

Утилита SMIT удаляет IBM Security Directory Server из системы AIX. Если вы выбрали удаление всех пакетов IBM Security Directory Server, то утилита также удалит установочный каталог IBM Security Directory Server, `/opt/IBM/ldap/V6.3.1`, из системы AIX.

Дальнейшие действия

Проверьте, успешно ли выполнено удаление IBM Security Directory Server. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Удаление с помощью installp

Команда **installp** позволяет удалить IBM Security Directory Server из системы AIX.

Прежде чем начать

Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Web Administration Tool и связанный с ним сервер приложений
- Пользовательские приложения LDAP

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты IBM Security Directory Server требуется удалить:

```
lslpp -l 'idsldap*'
```

4. Для удаления пакета IBM Security Directory Server выполните следующую команду:

```
installp -u пакет
```

Для полного удаления IBM Security Directory Server удалите все пакеты IBM Security Directory Server. Для удаления IBM Security Directory Server, необходимо указать пакеты в порядке, обратном тому, в котором они устанавливались. Дополнительная информация о последовательности приведена в разделе “Пакеты для установки в системе AIX” на стр. 69. Для удаления пакета `idsldap.ent631` выполните следующую команду:

```
installp -u idsldap.ent631
```

Дальнейшие действия

Проверьте, успешно ли выполнено удаление IBM Security Directory Server. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Удаление из системы с помощью утилит Linux

С помощью утилит командной строки Linux можно удалить IBM Security Directory Server из системы Linux.

Имена пакетов IBM Security Directory Server различаются для компьютеров с различными операционными системами и архитектурами. Необходимо проверить установленные пакеты IBM Security Directory Server перед удалением из системы.

Удаление с помощью утилит Linux

Используйте команду **rpm** для удаления IBM Security Directory Server из системы Linux.

Прежде чем начать

Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Web Administration Tool и связанный с ним сервер приложений
- Пользовательские приложения LDAP

Об этой задаче

В приведенном ниже примере демонстрируется удаление пакетов IBM Security Directory Server из системы AMD64 Opteron/EM64T Linux. Для Linux на System z, System i, System p или System x подставьте соответствующие имена пакетов.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты IBM Security Directory Server требуется удалить:

```
rpm -qa | grep -i idsldap
```

4. Для удаления пакета IBM Security Directory Server выполните следующую команду:

```
rpm -ev пакет
```

Для полного удаления IBM Security Directory Server удалите все пакеты IBM Security Directory Server. В процессе удаления IBM Security Directory Server необходимо указывать пакеты в порядке, обратном порядку установки. Дополнительные сведения о последовательности приведены в разделе “Пакеты для установки в системе Linux” на стр. 75. Для удаления пакета `idsldap-srv64bit631-6.3.1-0.x86_64.rpm` выполните следующую команду:

```
rpm -ev idsldap-srv64bit631-6.3.1-0.x86_64.rpm
```

Дальнейшие действия

Проверьте, успешно ли выполнено удаление IBM Security Directory Server. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Удаление из системы с помощью утилит Solaris

С помощью утилит командной строки Solaris можно удалить IBM Security Directory Server из системы Solaris.

Имена пакетов IBM Security Directory Server одинаковы для систем Solaris SPARC и Solaris X64.

Удаление с помощью утилит Solaris

Используйте команду `pkgrm` для удаления IBM Security Directory Server из системы Solaris.

Прежде чем начать

Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Web Administration Tool и связанный с ним сервер приложений
- Пользовательские приложения LDAP

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты IBM Security Directory Server требуется удалить:

```
pkginfo | grep -i IDS1
```
4. Для удаления пакета IBM Security Directory Server выполните следующую команду:

```
pkgrm пакет
```

Для полного удаления IBM Security Directory Server удалите все пакеты IBM Security Directory Server. В процессе удаления IBM Security Directory Server необходимо указывать пакеты в порядке, обратном порядку установки. Дополнительные сведения о последовательности приведены в разделе “Пакеты для установки в системе Solaris” на стр. 79. Для удаления пакета `IDS1ent631` выполните следующую команду:

```
pkgrm IDS1ent631
```

Дальнейшие действия

Проверьте, успешно ли выполнено удаление IBM Security Directory Server. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Удаление из системы с помощью утилит HP-UX

С помощью утилит командной строки HP-UX можно удалить IBM Security Directory Server из системы HP-UX.

На компьютерах HP-UX (Itanium) поддерживаются только пакеты клиента IBM Security Directory Server.

Удаление с помощью утилит HP-UX

Используйте команду **swremove** для удаления IBM Security Directory Server из системы HP-UX.

Прежде чем начать

Необходимо остановить все клиентские процессы IBM Security Directory Server.

- Трассировка LDAP
- Пользовательские приложения LDAP

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты IBM Security Directory Server требуется удалить:

```
swlist | grep -i idsldap
```

4. Для удаления пакета IBM Security Directory Server выполните следующую команду:

```
swremove пакет
```

Для полного удаления IBM Security Directory Server удалите все пакеты IBM Security Directory Server. В процессе удаления IBM Security Directory Server необходимо указывать пакеты в порядке, обратном порядку установки. Дополнительные сведения о последовательности приведены в разделе “Пакеты для установки в системе HP-UX Itanium” на стр. 82. Для удаления пакета `idsldap.cltjava631.depot` выполните следующую команду:

```
swremove idsldap.cltjava631.depot
```

Дальнейшие действия

Проверьте, успешно ли выполнено удаление IBM Security Directory Server. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Удаление из системы IBM DB2 с помощью команд DB2

Если копия IBM DB2, предоставленная с IBM Security Directory Server, установлена вручную, используйте команды DB2 для удаления IBM DB2 из системы.

Если копия IBM DB2 установлена с помощью IBM Installation Manager в процессе установки IBM Security Directory Server, она установлена в предопределенном расположении. Более подробная информация о расположении по умолчанию находится в разделе “Установочные расположения по умолчанию” на стр. 27. Если копия IBM DB2 установлена с помощью IBM Installation Manager, то для удаление ее из системы необходимо использовать Installation Manager.

Если компьютер содержит экземпляры DB2 для копии IBM DB2, необходимо вручную удалить экземпляры DB2 перед удалением из системы IBM DB2. Рекомендуется скопировать базы данных DB2 и данные перед удалением из системы.

Если IBM DB2 установлена вручную в пользовательском расположении с помощью команд DB2, то для ее удаления из системы используйте команды DB2. В системах AIX, Linux и Solaris выполните команду **db2_deinstall** в каталоге *установочный-каталог-DB2/install/* для удаления из системы IBM DB2. В системе Windows выполните команду **db2unins** в каталоге *установочный-каталог-DB2\bin* для удаления из системы IBM DB2. Более подробная информация об удалении IBM DB2 приведена в документации по продукту: <http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome>.

Удаление из системы IBM Global Security Kit с помощью утилит операционной системы

Если для установки IBM Global Security Kit (GSKit) использовались утилиты операционной системы, то используйте их для удаления GSKit из системы.

Можно использовать утилиты операционной системы для удаления GSKit с компьютеров, выполняющих операционные системы AIX, Linux, Solaris и HP-UX.

в системах Windows можно выполнить удаление из системы GSKit вручную, только если версия GSKit была установлена с помощью IBM Installation Manager. Если на компьютере установлен IBM Security Directory Server, то не следует удалять GSKit при его использовании. Если вы хотите перейти на последнюю версию GSKit, необходимо с помощью IBM Installation Manager изменить компонент GSKit для удаления его из реестра. Затем можно выполнить удаление из системы GSKit.

Удаление IBM Global Security Kit с помощью SMIT

Команда **smit** позволяет удалить IBM Global Security Kit (GSKit) из системы AIX.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните команду **smi t**. Откроется окно **Установка и обслуживание программного обеспечения**.
4. Выберите **Установка и обслуживание программного обеспечения > Обслуживание программного обеспечения и утилиты**.
5. Выберите **Удалить установленное программное обеспечение**.
6. В поле **Имя программного обеспечения** нажмите **F4**, чтобы просмотреть список установленного программного обеспечения. Вы можете указать значение **GSKi t** в поле, чтобы просмотреть список всех пакетов GSKit.
7. В поле **Удалить зависимое программное обеспечение** укажите **Да**, чтобы удалить программные продукты и обновления, зависимые от удаляемого продукта.
8. Выберите пакеты для удаления и нажмите Enter.
9. Убедитесь, что удаление GSKit успешно выполнено.

```
lslpp -l 'GSK*'
```

Удаление IBM Global Security Kit с помощью installp

Используйте команду **installp** для удаления IBM Global Security Kit (GSKit) из системы AIX.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты GSKit требуется удалить:

```
ls1pp -l 'GSK*'
```

4. Для удаления пакета GSKit выполните следующую команду:

```
installp -u пакет
```

Для полного удаления GSKit удалите все пакеты GSKit одной и той же версии. Для того чтобы удалить GSKit из системы сперва нужно удалить пакет GSKit SSL, а затем - пакет GSKit Crypt. Для удаления пакетов GSKit8.gskssl64.ppc.rte и GSKit8.gskcrypt64.ppc.rte выполните следующую команду:

```
installp -u GSKit8.gskssl64.ppc.rte  
installp -u GSKit8.gskcrypt64.ppc.rte
```

5. Убедитесь, что удаление GSKit успешно выполнено.

```
ls1pp -l 'GSK*'
```

Удаление IBM Global Security Kit с помощью утилит Linux

Используйте команду **rpm** для удаления IBM Global Security Kit (GSKit) из системы Linux.

Об этой задаче

В приведенном ниже примере демонстрируется удаление пакетов GSKit из системы AMD64 Opteron/EM64T Linux. Для Linux на System z, System i, System p или System x подставьте соответствующие имена пакетов.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты GSKit требуется удалить:

```
rpm -qa | grep -i gsk
```

4. Для удаления пакета GSKit выполните следующую команду:

```
rpm -ev пакет
```

Для полного удаления GSKit удалите все пакеты GSKit одной и той же версии. Для того чтобы удалить GSKit из системы сперва нужно удалить пакет GSKit SSL, а затем - пакет GSKit Crypt. Для удаления пакетов gskssl64-8.0-14.26.x86_64 и gskcrypt64-8.0-14.26.x86_64 выполните следующую команду:

```
rpm -ev gskssl64-8.0-14.26.x86_64  
rpm -ev gskcrypt64-8.0-14.26.x86_64
```

5. Убедитесь, что удаление GSKit успешно выполнено.

```
rpm -qa | grep -i gsk
```

Удаление IBM Global Security Kit с помощью утилит Solaris

Используйте команду **pkgrm** для удаления IBM Global Security Kit (GSKit) из системы Solaris.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты GSKit требуется удалить:
`pkginfo | grep -i gsk`
4. Для удаления пакета GSKit выполните следующую команду:
`pkgrm пакет`

Для полного удаления GSKit удалите все пакеты GSKit одной и той же версии. Для того чтобы удалить GSKit из системы сперва нужно удалить пакет GSKit SSL, а затем - пакет GSKit Crypt. Для удаления пакетов gsk8ssl64 и gsk8cry64 выполните следующую команду:

```
pkgrm gsk8ssl64
pkgrm gsk8cry64
```

5. Убедитесь, что удаление GSKit успешно выполнено.
`pkginfo | grep -i gsk`

Удаление IBM Global Security Kit с помощью утилит HP-UX

Используйте команду **swremove** для удаления IBM Global Security Kit (GSKit) из системы HP-UX.

Процедура

1. Войдите в систему как пользователь root.
2. Откройте окно ввода команд.
3. Выполните следующую команду для того чтобы определить, какие пакеты GSKit требуется удалить:
`swlist | grep -i gsk`
4. Для удаления пакета GSKit выполните следующую команду:
`swremove пакет`

Для полного удаления GSKit удалите все пакеты GSKit одной и той же версии. Для того чтобы удалить GSKit из системы сперва нужно удалить пакет GSKit SSL, а затем - пакет GSKit Crypt. Для удаления пакетов gskssl64 и gskcrypt64 выполните следующую команду:

```
swremove gskssl64
swremove gskcrypt64
```

5. Убедитесь, что удаление GSKit успешно выполнено.
`swlist | grep -i gsk`

Удаление IBM Global Security Kit в операционной системе Windows

Используйте команды IBM Global Security Kit (GSKit) для удаления GSKit из операционной системы Windows.

Об этой задаче

В примере демонстрируется удаление 64-разрядных пакетов GSKit SSL и GSKit Crypt из системы Windows на архитектуре AMD64/EM64T в режиме без вывода сообщений. Для операционной системы Windows на архитектуре IA32/x86 используются другие

имена пакетов GSKit. Информация об именах пакетов GSKit приведена в разделе Глава 10, “Установка IBM Global Security Kit”, на стр. 57.

Примечание: Кроме того, для удаления пакетов GSKit можно использовать меню **Пуск > Панель управления > Установка и удаление программ**.

Процедура

1. Войдите как участник группы администраторов.
2. Откройте окно ввода команд.
3. Измените текущий каталог на каталог `gskit`, в котором хранится программа установки IBM Global Security Kit.
4. Для удаления 64-разрядных пакетов GSKit в режиме без вывода сообщений выполните следующие команды: Для полного удаления GSKit удалите все пакеты GSKit одной и той же версии. Для того чтобы удалить GSKit из системы сперва нужно удалить пакет GSKit SSL, а затем - пакет GSKit Crypt.

```
gsk8ssl64.exe /s /x /v"/quiet"  
gsk8crypt64.exe /s /x /v"/quiet"
```

Удаление из системы языковых пакетов

Для того чтобы выполнить удаление из системы IBM Security Directory Server, необходимо удалить языковые пакеты, установленные в системе.

Если IBM Security Directory Server и языковые пакеты установлены с помощью IBM Installation Manager, то для удаление языковых пакетов из системы необходимо использовать Installation Manager.

Если для установки языковых пакетов использовались утилиты операционной системы, то для удаления языковых пакетов из системы примените их же.

Все языковые пакеты удаляются из системы, если для установки не выбран компонент Прокси-сервер или Сервер.

Удаление языковых пакетов с помощью утилит операционной системы

Используйте утилиты операционной системы для удаления языкового пакета, если он установлен с помощью утилит операционной системы.

Прежде чем начать

Необходимо остановить все клиентские и серверные процессы IBM Security Directory Server перед удалением языковых пакетов IBM Security Directory Server.

- Сервер каталогов
- Административный сервер
- Трассировка LDAP
- Пользовательские приложения LDAP

Процедура

1. Войдите в систему как пользователь `root`.
2. Откройте окно ввода команд.
3. Определите языковые пакеты на своем компьютере, которые требуется удалить:

Операционная система	Выполняемая команда:
AIX	lslpp -l 'idsldap.msg631*'
Linux	rpm -qa grep -i idsldap-msg631
Solaris	pkginfo grep IDS1

4. Для удаления языкового пакета определенного языка запустите команды удаления пакета. В приведенном ниже примере демонстрируется удаление языкового пакета для французского языка. Любой языковой пакет можно удалить, заменив соответствующие имена пакетов для операционной системы.

Операционная система	Выполняемая команда:
AIX	installp -u idsldap.msg631.fr_FR
Linux	rpm -ev idsldap-msg631-fr-6.3.1-0.noarch.rpm
Solaris	pkgrm IDS1fr631

5. Проверьте, успешно ли выполнено удаление языковых пакетов. Дополнительная информация приведена в разделе “Проверка пакетов IBM Security Directory Server” на стр. 86.

Приложение А. Язык описания служб каталогов

С помощью языка описания служб каталогов можно представлять в формате XML информацию структуры каталогов, запросы и обновления каталогов и результаты операций над каталогами.

После завершения установки IBM Security Directory Server Веб-инструмент администрирования, архив файлов языка описания служб каталогов (DSML), DSML.zip будут храниться на вашем компьютере. Файл DSML.zip хранится в каталоге idstools установочного расположения IBM Security Directory Server. Дополнительная информация об установочном расположении IBM Security Directory Server по умолчанию приведена в разделе “Установочные расположения по умолчанию” на стр. 27.

Файл DSML.zip содержит устанавливаемые файлы DSML и документацию, помогающую установить и настроить DSML и работать с ним. Файл DSML.zip содержит следующие файлы:

DSMLReadme.txt

В файлах DSMLReadme.txt приведены файлы пакета и инструкции по установке и настройке DSML.

dsm1.pdf

Файл dsm1.pdf имеет формат PDF и содержит описание порядка работы с DSML.

dsm1.htm

Файл dsm1.htm имеет формат HTML и содержит описание порядка работы с DSML.

Приложение В. Загрузка примера базы данных и запуск сервера

Загрузите пример базы данных и запустите сервер каталогов для добавления, обновления и поиска записей.

Прежде чем начать

Создайте экземпляр сервера каталогов. Обратитесь к разделу “Создание экземпляра сервера каталогов” на стр. 133.

Об этой задаче

С помощью Configuration Tool загрузите данные LDIF на сервер каталогов и запустите сервер.

Процедура

1. Для запуска Configuration Tool выполните следующую команду:
`idsxcfg -I экземпляр`
2. В области навигации выберите **Задачи LDIF > Импортировать данные LDIF**.
3. В поле **Каталог и имя файла LDIF** введите полное имя файла LDIF. Кроме того, файл данных LDIF можно выбрать с помощью кнопки Обзор. В следующей таблице перечислены расположения и имена файлов данных LDIF по умолчанию для различных операционных систем:

Windows

`установочный-каталог\examples\sample.ldif`

AIX и Solaris

`/opt/IBM/ldap/V6.3.1/examples/sample.ldif`

Linux `/opt/ibm/ldap/V6.3.1/examples/sample.ldif`

4. Выберите **Стандартный импорт**.
5. Нажмите кнопку **Импортировать**.
6. Для того чтобы запустить экземпляр сервера каталогов, выполните следующие действия:
 - a. В области навигации выберите **Управление состоянием сервера**.
 - b. Выберите **Запустить сервер**.

Приложение С. Обновление файла `ldapdb.properties` вручную

Если вы устанавливаете IBM Security Directory Server на компьютере, не содержащем поддерживаемую версию IBM DB2, то файл `ldapdb.properties` не заполняется во время установки. В этом случае вы должны установить поддерживаемую версию IBM DB2 и затем обновить файл `ldapdb.properties` вручную.

Прежде чем начать

Вы должны убедиться, что установлен полный пакет сервера каталогов.

Процедура

1. Установите поддерживаемую версию IBM DB2, если она еще не установлена.
2. Выполните команду `db21s`, чтобы просмотреть версии DB2, установленные на компьютере, и их установочный путь.
3. Обновите файл `ldapdb.properties`, добавив в него поддерживаемую версию DB2 и установочный путь. Расположение по умолчанию файла `ldapdb.properties` с примерами значений для различных операционных систем:

Microsoft Windows

```
C:\Program Files\IBM\ldap\V6.3.1\etc\ldapdb.properties
currentDB2InstallPath=C:\Program Files\IBM\SQLLIB
currentDB2Version=9.7.0.6
```

AIX и Solaris

```
/opt/IBM/ldap/V6.3.1/etc/ldapdb.properties
currentDB2InstallPath=/opt/IBM/db2/V9.7
currentDB2Version=9.7.0.6
```

Linux

```
/opt/ibm/ldap/V6.3.1/etc/ldapdb.properties
currentDB2InstallPath=/opt/ibm/db2/V9.7
currentDB2Version=9.7.0.6
```

4. Сохраните файлы `ldapdb.properties`.

Приложение D. Специальные возможности для Security Directory Server

Специальные возможности позволяют успешно работать с продуктами информационных технологий людям с такими физическими ограничениями, как ограниченная подвижность или ослабленное зрение.

Основные специальные возможности, предусмотренные в этом продукте, позволяют выполнять следующие действия:

- Использовать вспомогательные технологии, такие как программа считывания текста с экрана, воспроизводящая отображаемый на экране текст. Дополнительная информация по использованию вспомогательных технологий в продукте приведена в документации по продукту.
- Работать с различными функциями с помощью клавиатуры.
- Увеличивать изображение на экране.

Кроме того, в документацию было добавлено описание следующих специальных возможностей:

- Вся документация доступна в формате HTML, для предоставления возможности пользователям применять программные продукты считывания текста с экрана.
- Все рисунки в документации снабжены пояснительным альтернативным текстом, благодаря чему пользователи с ослабленным зрением могут ознакомиться с содержанием изображения.

Специальные возможности

Ниже перечислены основные функции специальных возможностей продукта IBM Security Directory Server.

- Поддерживает операции "только с клавиатурой"
- Поддерживает интерфейсы, обычно используемые программами чтения с экрана
- Клавиши различимы на ощупь и не активируются простым прикосновением.

В документации по IBM Security Directory Server реализованы специальные возможности. Специальные возможности документации описаны в одном из разделов.

Навигация с помощью клавиатуры

В продукте применяются стандартные клавиши быстрого доступа операционной системы. Дополнительная информация приведена в документации по операционной системе.

Данный продукт использует стандартные клавиши навигации Microsoft Windows.

Увеличение изображения, показанного на экране

Изображение на экране можно увеличить с помощью средств операционной системы. Например, в среде Microsoft Windows для этой цели можно уменьшить разрешение экрана. Дополнительная информация приведена в документации по операционной системе.

IBM и специальные возможности

Дополнительная информация о деятельности фирмы IBM по предоставлению специальных возможностей приведена на сайте IBM Human Ability and Accessibility Center: <http://www.ibm.com/able>

Индекс

A

- Active Directory
 - запустить синхронизацию 217
- AIX
 - установка с помощью SMIT 72
- AIX, GSKit
 - удаление с помощью SMIT 241
- AIX, автоматический запуск сервера каталогов
 - настройка 223
 - общая информация 221
- AIX, сервер каталогов
 - удаление с помощью SMIT 236
- AIX, требования к дисковой памяти сервер каталогов, компоненты 3
- AIX, удаление с помощью installp
 - GSKit 242
 - сервер каталогов 237
- AIX, установка с помощью installp
 - IBM Global Security Kit 58
 - сервер каталогов 73

C

- Configuration Tool, открытие
 - настройка 170
- Configuration Tool, резервное копирование базы данных
 - настройка 191
- Configuration Tool, резервное копирование прокси-сервера
 - настройка 192
- Configuration Tool, синхронизация Active Directory
 - настройка 218
- Configuration Tool, тонкая настройка производительности сервер каталогов 196, 199

D

- DB2, перенос данных
 - настройка 98
 - общая информация 97
- DB2, сервер каталогов
 - общая информация 53

G

- GSKit, проверка
 - Windows 88
- GSKit, проверка установки
 - UNIX 88

H

- HP-UX, требования к дисковой памяти сервер каталогов, компоненты 3

- HP-UX, удаление с помощью swremove
 - GSKit 243
 - сервер каталогов 240
- HP-UX, установка с помощью swinstall
 - IBM Global Security Kit 61
 - сервер каталогов 83
- HTTPS, встроенный WebSphere Application Server
 - общая информация 117

I

- IBM
 - Support Assistant
 - ix
 - поддержка программного обеспечения ix
 - IBM Installation Manager, запуск установки сервер каталогов 31
 - IBM Installation Manager, изменение сервера каталогов
 - общая информация 39
 - IBM Installation Manager, протоколы
 - общая информация 45
 - расположения 45
 - IBM Installation Manager, удаление из системы сервера каталогов
 - общая информация 232
 - IBM Installation Manager, установка сервера каталогов
 - поддерживаемые операционные системы, общая информация 21
 - IBM JDK, сервер каталогов
 - общая информация 55
 - IBM Security Directory Server
 - сценарии установки 26
 - IBM Security Directory Server, IBM Installation Manager
 - запустить установку, настройка 28
 - запустить установку, способы 28
 - IBM Security Directory Server, Passport Advantage
 - загрузка продукта 7
 - IBM Security Directory Server, изменение компоненты 39
 - IBM Security Directory Server, компоненты
 - общая информация 24
 - IBM Security Directory Server, носитель установки
 - общая информация 6
 - IBM Security Directory Server, пакеты установки
 - типы, общая информация 22
 - IBM Security Directory Server, проверка компоненты 85
 - связанный продукт, DB2 85
 - связанный продукт, Embedded WebSphere Application Server 85
 - связанный продукт, GSKit 85
 - IBM Security Directory Server, сценарии установки
 - общая информация 26

- IBM Security Directory Server, удаление компоненты 232
- IBM Security Directory Server, установка
 - общая информация 23
 - предварительно требуемые пакеты 15
- IBM Security Directory Server, установочные хранилища
 - общая информация 27

L

- Linux, автоматический запуск сервера каталогов
 - настройка 223
 - общая информация 221
- Linux, требования к дисковой памяти сервер каталогов, компоненты 3
- Linux, удаление с помощью rpm
 - GSKit 242
 - сервер каталогов 238
- Linux, установка с помощью rpm
 - IBM Global Security Kit 59
 - сервер каталогов 77

P

- Passport Advantage, IBM Security Directory Server
 - загрузка продукта 7
- Passport Advantage, загрузка IBM Security Directory Server 7
- pkgadd, установка
 - IBM Global Security Kit 60
 - сервер каталогов 81

R

- rpm, установка
 - IBM Global Security Kit 59
 - сервер каталогов 77

S

- Solaris, автоматический запуск сервера каталогов
 - настройка 223
 - общая информация 221
- Solaris, требования к дисковой памяти сервер каталогов, компоненты 3
- Solaris, удаление с помощью pkgm
 - GSKit 243
 - сервер каталогов 239
- Solaris, установка с помощью pkgadd
 - IBM Global Security Kit 60
- swinstall, установка сервер каталогов 83
- swinstall, установка
 - IBM Global Security Kit 61

U

UTF-8
национальный язык, символы 126

W

web administration tool
миграция конфигурации 102
миграция, команда idswmig 103
миграция, общая информация 102
WebSphere Application Server,
развертывание Веб-инструмента
администрирования
настройка 113
Windows, GSKit
проверка 88
Windows, автоматический запуск сервера
каталогов
настройка 221
общая информация 221
Windows, требования к дисковой памяти
сервер каталогов, компоненты 3
Windows, удаление
GSKit 243
Windows, установка
IBM Global Security Kit 61
Windows, установка без вывода сообщений
IBM Global Security Kit 62

A

автоматический запуск сервера каталогов,
AIX
настройка 223
автоматический запуск сервера каталогов,
Linux
настройка 223
автоматический запуск сервера каталогов,
Solaris
настройка 223
автоматический запуск сервера каталогов,
Windows
настройка 221
автоматический запуск, сервер каталогов
общая информация 221

Б

база данных DB2, Инструмент настройки
настройка 176
отключение 185
пароль, настройка 182
база данных DB2, настройка
Instance Administration Tool 136
база данных DB2, оперативное резервное
копирование
Instance Administration Tool 136
база данных DB2, утилиты сервера
настройка 180
база данных, планирование конфигурации
кодовая страница 125
общая информация 125
права доступа 125
структура иерархии 125

В

веб-адрес, HTTPS
общая информация 117
веб-инструмент администрирования,
порты по умолчанию
общая информация 110
Веб-инструмент администрирования,
развертывание
WebSphere Application Server 113
общая информация 109
Веб-инструмент администрирования,
свертывание
настройка 118
вручную, установка
встроенный WebSphere Application
Server 109
встроенный WebSphere Application Server
установка 109
встроенный WebSphere Application Server,
HTTPS
общая информация 117

Г

главный администратор, управление
общая информация 172

Д

доступ, Web Administration Tool
настройка 115

З

запуск, Web Administration Tool
настройка 115

И

изменение без вывода сообщений, файл
ответов
настройка 36
имена пакетов
языковой пакет 66
Инструмент администрирования
экземпляра
обновить экземпляр 148
инструмент администрирования
экземпляра, запуск и остановка
экземпляра
общая информация 157
Инструмент администрирования
экземпляра, запустить
настройка 132
Инструмент администрирования
экземпляра, запустить или остановить
административный сервер
настройка 158
Инструмент администрирования
экземпляра, запустить или остановить
сервер каталогов
настройка 158
Инструмент администрирования
экземпляра, изменить параметры TCP/IP
настройка 160

Инструмент администрирования
экземпляра, изменить параметры
TCP/IP (*продолжение*)
экземпляр 160
Инструмент администрирования
экземпляра, настройка
запустить или остановить
административный сервер 158
запустить или остановить сервер 158
создать копию экземпляра 154
Инструмент администрирования
экземпляра, обновление
удаленный экземпляр 150
Инструмент администрирования
экземпляра, открыть
Инструмент настройки 160
настройка 132
инструмент администрирования
экземпляра, просмотр сведений об
экземпляре
общая информация 162
Инструмент администрирования
экземпляра, просмотреть сведения об
экземпляре
настройка 163
Инструмент администрирования
экземпляра, создание сервера прокси
пользовательские параметры 143
Инструмент администрирования
экземпляра, создать копию экземпляра
настройка 154
инструмент администрирования
экземпляра, удаление экземпляра
общая информация 163
Инструмент администрирования
экземпляра, удаление экземпляра
настройка 164
Инструмент администрирования
экземпляра, удаленное обновление
экземпляр с резервной копией
данных 133
инструмент настройки
общая информация 169
Инструмент настройки
общая информация 159
Инструмент настройки, администратор
базы данных DB2
пароль, настройка 182
Инструмент настройки, база данных DB2
настройка 176
отключение 185
Инструмент настройки, восстановить базу
данных
настройка 193
Инструмент настройки, восстановить
сервер проху
настройка 194
Инструмент настройки, восстановление
общая информация 193
Инструмент настройки, запуск
настройка 170
Инструмент настройки, запуск и остановка
экземпляра
общая информация 170
Инструмент настройки, запустить или
остановить административный сервер
настройка 171

Инструмент настройки, запустить или остановить сервер каталогов
настройка 171

Инструмент настройки, импортировать данные LDIF
настройка 212

Инструмент настройки, конфигурация сервера
общая информация 159

Инструмент настройки, настроить DN администратора, настройка 172
пароль администратора, настройка 174

Инструмент настройки, настроить DN администратора
настройка 172

Инструмент настройки, настроить пароль администратора
настройка 174

Инструмент настройки, настройка запустить или остановить административный сервер 171
запустить или остановить сервер 171

инструмент настройки, настройка базы данных
общая информация 175

Инструмент настройки, обслуживание базы данных
общая информация 188

Инструмент настройки, оптимизация базы данных
общая информация 186

Инструмент настройки, отключить протокол изменений
настройка 202

Инструмент настройки, пароль администратора базы данных
общая информация 182

Инструмент настройки, проверить данные LDIF
настройка 213

Инструмент настройки, протокол изменений
настройка 200
общая информация 200

инструмент настройки, резервное копирование
общая информация 190

Инструмент настройки, сервер каталогов добавление суффикса, конфигурация 204
обслуживать базу данных, настройка 188
оптимизировать базу данных, настройка 187
проверка правильности схемы, настройка 210
удалить суффикс, настройка 206
управление схемой, конфигурация 208

инструмент настройки, суффикс
общая информация 204

Инструмент настройки, удаление конфигурации базы данных
общая информация 184

Инструмент настройки, управление данными LDIF
общая информация 211

Инструмент настройки, управление схемой
общая информация 207

Инструмент настройки, экспортировать данные LDIF
настройка 214

информация о каталогах, язык описания служб каталогов
общая информация 247

К

клиентские утилиты, администратор базы данных DB2
пароль, настройка 183

кодовая страница DB2
локаль, IANA 128

кодовая страница, DB2
набор символов, IANA 128

кодовая страница, различия UTF-8, локаль 126

команда, миграция
web administration tool, idswmigr 103

компоненты установки, IBM Security Directory Server
общая информация 24

компоненты, изменение
компоненты IBM Security Directory Server 39

компоненты, проверка
IBM Security Directory Server 85

компоненты, удаление
IBM Security Directory Server 232

конфигурация, планирование базы данных
общая информация 125

М

методы установки
общая информация 18

миграция данных и решений
общая информация 97

Н

набор символов, IANA
кодovая страница, DB2 128

настройка среды
обновление экземпляра 90

национальный язык, символы UTF-8 126

неинтерактивная модификация, файл ответов
общая информация 35

неинтерактивная установка, файл ответов
общая информация 35

неинтерактивное удаление из системы, файл ответов
общая информация 35

необходимый объем дисковой памяти сервер каталогов, компоненты 3

носитель установки, IBM Security Directory Server
общая информация 6

О

обзор установки, сервер каталогов
общая информация 3

обновить удаленный экземпляр, конфигурация
Instance Administration Tool 150

обновить экземпляр
Instance Administration Tool 148

удаленный, поддерживаемые операционные системы 94

обновить экземпляр, конфигурация команда idsimigr, -u 94
удаленно, idsimigr -u 94
удаленно, Инструмент администрирования экземпляра 150

обновить, экземпляр проху команда idsimigr 92

обновить, экземпляр каталога команда idsimigr 92

обновление экземпляра
настройка среды 90

обновление экземпляра, удаленно
общая информация 93

обновление, экземпляр
общая информация 89

образование ix

обучение ix

операционная система, языковой пакет имена пакетов 66

операционные системы, обновление предварительно требуемые пакеты 15

определение неполадок ix

остановить, сервер веб-приложений
настройка 117

открытие, Web Administration Tool
настройка 115

П

пакеты для установки, сервер каталогов
HP-UX 82

пакеты исправлений 225

пакеты сервера каталогов, HP-UX
общая информация 82

пакеты установки, типы
общая информация 22

панель запуска, установка сервер каталогов 28

пароль главного администратора, управление
общая информация 174

поддерживаемые операционные системы
обновить экземпляр, удаленный 94

пользователи и группы, владелец базы данных
общая информация 121

пользователи и группы, владелец экземпляра базы данных
общая информация 121

пользователи и группы, владелец экземпляра сервера каталогов
общая информация 121

пользователи и группы, сервер каталогов
общая информация 121

пользователь и группа, idsldap
общая информация 17

пользователь и группа, `idsldap`
(продолжение)
 требования 17

порты по умолчанию, веб-инструмент администрирования
 общая информация 110

правила именования, экземпляр сервера каталогов
 ИД пользователей, основная группа 122

предварительные требования для установки
 общая информация 15

проверка в AIX, сервер каталогов
 настройка 87

проверка в HP-UX, сервер каталогов
 настройка 87

проверка в Linux, сервер каталогов
 настройка 87

проверка в Solaris, сервер каталогов
 настройка 87

проверка в Windows, сервер каталогов
 настройка 85

проверка установки, GSKit
 UNIX 88

проверка, версия
 Web Administration Tool 87

проверка, сервер каталогов
 общая информация 85

прокси-сервер, главный администратор
 общая информация 172

прокси-сервер, добавить суффикс
 настройка 204, 205

прокси-сервер, изменение конфигурации
 общая информация 159

прокси-сервер, настройка экземпляра
 общая информация 169

прокси-сервер, пароль главного администратора
 общая информация 174

прокси-сервер, резервное копирование
 настройка 192
 общая информация 190

прокси-сервер, создание конфигурации системы 121

прокси-сервер, состояние
 общая информация 159

прокси-сервер, удаление экземпляра
 общая информация 163

прокси-сервер, управление конфигурацией
 общая информация 159

прокси-сервер, управление схемой
 настройка 208, 209

публикации
 список для этого продукта vii
 электронные vii

Р

развертывание
 Web Administration Tool 111

развертывание, Веб-инструмент администрирования
 WebSphere Application Server 113
 общая информация 109

расположения протоколов
 IBM Installation Manager 45

решение SNMP, перенос в новую версию
 настройка 100

Решение синхронизации Active Directory,
 перенос в новую версию
 настройка 101

решение управления протоколами, перенос
 в новую версию
 настройка 99

С

свертывание, Веб-инструмент администрирования
 настройка 118

сервер ргоху, восстановить
 настройка 194
 общая информация 193

сервер ргоху, открыть
 Инструмент настройки 160

сервер Ргоху, просмотреть сведения об
 экземпляре
 настройка 163
 общая информация 162

сервер ргоху, удалить суффикс
 настройка 206, 207

сервер Ргоху, утилиты сервера
 изменить параметры TCP/IP,
 настройка 161
 просмотреть сведения об экземпляре,
 конфигурация 163
 удаление экземпляра, настройка 165

сервер администрирования экземпляра,
 создание экземпляра
 пользовательские параметры 136
 экземпляр по умолчанию 134

сервер администрирования, запуск и
 остановка
 общая информация 157, 170

сервер веб-приложений, запустить
 настройка 114

сервер веб-приложений, остановить сервер
 приложений
 настройка 117

сервер каталогов
 загрузка данных 249
 запуск сервера 249
 запустить, сервер веб-приложений 114
 отключить базу данных DB2 185

пакеты для установки в системе
 Solaris 79

создание экземпляра 133

сервер каталогов, Active Directory
 синхронизация, общая
 информация 16, 215

сервер каталогов, Configuration Tool
 настройка производительности 196,
 199

сервер каталогов, DB2
 общая информация 53

сервер каталогов, IBM JDK
 общая информация 55

сервер каталогов, Solaris
 установка с помощью `pkgadd` 81

сервер каталогов, администратор базы
 данных DB2
 пароль, настройка 182, 183

сервер каталогов, администрирование
 экземпляра
 общая информация 131

сервер каталогов, база данных DB2
 обслуживание 188, 189
 оптимизация 187
 отключение 186

сервер каталогов, восстановить базу
 данных
 настройка 193

сервер каталогов, восстановление
 общая информация 193

сервер каталогов, главный администратор
 общая информация 172

сервер каталогов, добавить суффикс
 настройка 204, 205

сервер каталогов, добавление экземпляра
 настройка 154
 топология репликации 153

сервер каталогов, запуск и остановка
 общая информация 157, 170

сервер каталогов, изменение
 общая информация 39

сервер каталогов, изменение без вывода
 сообщений
 настройка 36

сервер каталогов, изменение конфигурации
 общая информация 159

сервер каталогов, изменить параметры
 TCP/IP
 настройка 160
 общая информация 160

сервер каталогов, импортировать данные
 LDIF
 настройка 212

сервер каталогов, инструмент
 администрирования экземпляра
 общая информация 131

сервер каталогов, компоненты
 необходимый объем дисковой
 памяти 3

сервер каталогов, копия
 общая информация 153

сервер каталогов, миграция решений
 общая информация 97

сервер каталогов, настроить DN
 администратора
 настройка 172, 173

сервер каталогов, настроить базу данных
 DB2
 настройка 176, 180

сервер каталогов, настроить пароль
 администратора
 настройка 174, 175

сервер каталогов, настройка
 общая информация 195
 производительность, общая
 информация 195

сервер каталогов, настройка базы данных
 общая информация 175

сервер каталогов, настройка экземпляра
 общая информация 169

сервер каталогов, неинтерактивная
 модификация
 общая информация 35

сервер каталогов, неинтерактивная установка
 общая информация 35

сервер каталогов, неинтерактивное удаление из системы
 общая информация 35

сервер каталогов, обзор установки
 общая информация 3

сервер каталогов, обновление экземпляра
 общая информация 89

сервер каталогов, обслуживание базы данных
 общая информация 188

сервер каталогов, оптимизация базы данных
 общая информация 186

сервер каталогов, отключить протокол изменений
 настройка 202, 203

сервер каталогов, открыть
 Инструмент настройки 160

сервер каталогов, пакеты для установки в AIX
 общая информация 70

сервер каталогов, пакеты для установки в Linux
 общая информация 75

сервер каталогов, пароль администратора базы данных
 общая информация 182

сервер каталогов, пароль главного администратора
 общая информация 174

сервер каталогов, перенос базы данных
 настройка 98

сервер каталогов, перенос решения SNMP в новую версию
 настройка 100

сервер каталогов, перенос решения синхронизации Active Directory в новую версию
 , настройка 101

сервер каталогов, перенос решения управления протоколами в новую версию
 настройка 99

сервер каталогов, пользователи и группы
 общая информация 121
 права доступа, общая информация 123
 создание, общая информация 123
 требования 121

сервер каталогов, правила именования ИД пользователей, основная группа 122
 общая информация 122

сервер каталогов, предварительные требования для установки
 общая информация 15

сервер каталогов, проверка
 Версия Веб-инструмента администрирования 87
 общая информация 85

сервер каталогов, проверка в AIX
 настройка 87

сервер каталогов, проверка в HP-UX
 настройка 87

сервер каталогов, проверка в Linux
 настройка 87

сервер каталогов, проверка в Solaris
 настройка 87

сервер каталогов, проверка в Windows
 настройка 85

сервер каталогов, проверка данных LDIF
 настройка 213

сервер каталогов, проверка правильности схемы
 настройка 210

сервер каталогов, производительность
 настройка, общая информация 195

сервер каталогов, просмотреть сведения об экземпляре
 настройка 163
 общая информация 162

сервер каталогов, протокол изменений
 настройка 200, 201
 общая информация 200

сервер каталогов, развертывание
 Web Administration Tool 111

сервер каталогов, резервное копирование
 общая информация 190

сервер каталогов, резервное копирование базы данных
 настройка 191

сервер каталогов, синхронизация
 общая информация 16, 215

сервер каталогов, синхронизация Active Directory
 настройка 218, 219

сервер каталогов, создание
 конфигурация системы 121
 общая информация 153

сервер каталогов, создание экземпляра Instance Administration Tool 134
 настройка 147, 157
 общая информация 131, 133
 пользовательские параметры 136
 экземпляр по умолчанию 134

сервер каталогов, состояние
 общая информация 159

сервер каталогов, суффикс
 общая информация 204

сервер каталогов, удаление без вывода сообщений
 настройка 36, 233, 235

сервер каталогов, удаление из системы
 общая информация 231, 232

сервер каталогов, удаление из системы с помощью утилит AIX
 общая информация 236

сервер каталогов, удаление конфигурации базы данных
 общая информация 184

сервер каталогов, удаление экземпляра
 настройка 164
 общая информация 163

сервер каталогов, удалить суффикс
 настройка 206, 207

сервер каталогов, управление данными LDIF
 общая информация 211

сервер каталогов, управление конфигурацией
 общая информация 159

сервер каталогов, управление схемой
 настройка 208, 209
 общая информация 207

сервер каталогов, установка
 IBM Installation Manager 31
 панель запуска, настройка 28
 предварительные требования для установки, общая информация 15
 требования, общая информация 1
 утилиты операционной системы 69
 хранилище 29

сервер каталогов, установка без вывода сообщений
 настройка 36

сервер каталогов, установка вручную
 Solaris 78

сервер каталогов, установка с помощью IBM Installation Manager
 поддерживаемые операционные системы, общая информация 21

сервер каталогов, установка с помощью утилит AIX
 общая информация 69

сервер каталогов, утилиты сервера
 изменить параметры TCP/IP,
 настройка 161
 просмотреть сведения об экземпляре,
 конфигурация 163
 удаление экземпляра, настройка 165

сервер каталогов, утилиты сервера и клиента
 ссылки, общая информация 96

сервер каталогов, файл свойств DB2
 настройка 251

сервер каталогов, экспортировать данные LDIF
 настройка 214

сервер прокси, изменить параметры TCP/IP
 настройка 160
 общая информация 160

сервер прокси, настроить DN администратора
 настройка 172, 173

сервер прокси, настроить пароль администратора
 настройка 174, 175

сервер прокси, проверка правильности схемы
 настройка 210

сервер прокси, создание экземпляра
 пользовательские параметры 143

сервер прокси, удаление экземпляра
 настройка 164

сервер, утилиты
 Instance Administration Tool 148
 команда idsimigr 92
 команда idsimigr, -u 94

символы ASCII
 поддерживаемый начальный ключ шифрования 129
 с кодом от 33 по 126 129

символы, национальный язык
 UTF-8 126

синхронизация
 из Active Directory в Security Directory Server 16, 215

- Синхронизация Active Directory
 - настройка 217
- создание экземпляра, конфигурация системы
 - общая информация 121
- создание экземпляра, методы
 - общая информация 131
- создание экземпляра, параметры Instance Administration Tool 134
- специальные возможности ix, 253
- структура каталогов
 - установка, расположение 167
- структура каталогов, загруженные файлы
 - AIX 7
 - Linux 7
 - Solaris 7
 - Windows 7
- сценарии установки, IBM Security Directory Server
 - общая информация 26

Т

- терминология vii
- требования к установке, IBM Security Directory Server
 - общая информация 23

У

- удаление SMIT
 - GSKit 241
 - сервер каталогов 236
- удаление без вывода сообщений, команда imcl
 - настройка 235
- удаление без вывода сообщений, файл ответов
 - настройка 36, 233
- удаление из системы DB2, команды DB2
 - общая информация 240
- удаление из системы GSKit, утилиты операционной системы
 - общая информация 241
- удаление из системы в режиме без вывода сообщений
 - GSKit 243
- удаление из системы вручную, утилиты AIX
 - общая информация 236
- удаление из системы вручную, утилиты HP-UX
 - общая информация 240
- удаление из системы вручную, утилиты Linux
 - общая информация 238
- удаление из системы вручную, утилиты Solaris
 - общая информация 239
- удаление из системы с помощью утилит операционной системы, GSKit
 - общая информация 241
- удаление из системы с помощью утилит операционной системы, сервер каталогов
 - общая информация 235

- удаление из системы сервера каталогов, утилиты операционной системы
 - общая информация 235
- удаление из системы, DB2
 - общая информация 240
- удаление из системы, сервер каталогов
 - общая информация 231
- удаление из системы, утилиты HP-UX
 - общая информация 240
- удаление из системы, утилиты Linux
 - общая информация 238
- удаление из системы, утилиты Solaris
 - общая информация 239
- удаление с помощью installp
 - GSKit 242
 - сервер каталогов 237
- удаление с помощью pkgrm
 - GSKit 243
 - сервер каталогов 239
- удаление с помощью rpm
 - GSKit 242
 - сервер каталогов 238
- удаление с помощью swremove
 - GSKit 243
 - сервер каталогов 240
- удаление, IBM Installation Manager
 - IBM Security Directory Server 232
- удаление, команда GSKit
 - GSKit 243
- удаление, команда installp
 - GSKit 242
 - сервер каталогов 237
- удаление, команда pkgrm
 - GSKit 243
 - сервер каталогов 239
- удаление, команда rpm
 - GSKit 242
 - сервер каталогов 238
- удаление, команда swremove
 - GSKit 243
 - сервер каталогов 240
- удаление, утилита SMIT
 - GSKit 241
 - сервер каталогов 236
- удаление, языковые пакеты
 - общая информация 244
 - утилиты AIX 244
 - утилиты Linux 244
 - утилиты Solaris 244
- удаленное обновление, Инструмент администрирования экземпляра
 - экземпляр с резервной копией данных 133
- удаленное управление, экземпляр Web Administration Tool,
 - конфигурация 115
- установка
 - вручную
 - HP-UX 82
 - команда pkgadd 81
 - пакеты сервера каталогов в Solaris 79
 - утилиты HP-UX 82
 - установка без вывода сообщений, IBM Global Security Kit
 - Windows 62
 - установка без вывода сообщений, Windows IBM Global Security Kit 62

- установка без вывода сообщений, файл ответов
 - настройка 36
- установка вручную, утилиты AIX
 - общая информация 69
- установка вручную, утилиты Linux
 - общая информация 74
- установка с помощью installp
 - IBM Global Security Kit 58
 - сервер каталогов 73
- установка с помощью SMIT
 - сервер каталогов 72
- установка, DB2
 - общая информация 53
- установка, GSKit
 - имена пакетов 57
 - общая информация 57
- установка, IBM Global Security Kit
 - Windows 61
- установка, IBM Installation Manager
 - обзор 21
 - общая информация 21
- установка, IBM JDK
 - общая информация 55
- установка, Windows
 - IBM Global Security Kit 61
- установка, вручную
 - встроенный WebSphere Application Server 109
- установка, инструмент
 - IBM Installation Manager 21
- установка, команда installp
 - IBM Global Security Kit 58
 - сервер каталогов 73
- установка, команда pkgadd
 - IBM Global Security Kit 60
- установка, команда rpm
 - IBM Global Security Kit 59
 - сервер каталогов 77
- установка, команда swinstall
 - IBM Global Security Kit 61
- установка, настройка хранилища
 - сервер каталогов 29
- установка, обзор
 - IBM Installation Manager 21
- установка, пакеты сервера каталогов в AIX
 - общая информация 70
- установка, пакеты сервера каталогов в Linux
 - общая информация 75
- установка, планирование
 - общая информация 1
- установка, расположение
 - структура каталогов 167
- установка, сервер каталогов
 - IBM Installation Manager 31
 - Команда swinstall 83
 - панель запуска, настройка 28
 - утилиты операционной системы 69
 - хранилище 29
- установка, требования среды
 - общая информация 1
- установка, утилита SMIT
 - сервер каталогов 72
- установка, утилиты AIX
 - общая информация 69

- установка, утилиты Linux
 - общая информация 74
- установка, утилиты Solaris
 - сервер каталогов 78
- установка, языковые пакеты
 - общая информация 65
 - утилиты AIX 67
 - утилиты Linux 67
 - утилиты Solaris 67
- установочные расположения
 - по умолчанию, общая информация 27
- установочные расположения по умолчанию
 - общая информация 27
- установочные хранилища
 - общая информация 27
- устранение неполадок ix
 - утилиты AIX, удаление языковых пакетов 244
- утилиты AIX, установка языковых пакетов 67
- утилиты Linux, удаление языковых пакетов 244
- утилиты Linux, установка языковых пакетов 67
- утилиты Solaris, удаление языковых пакетов 244
- утилиты Solaris, установка языковых пакетов 67
- утилиты клиента, ссылки
 - общая информация 96
- утилиты клиента, управление данными LDIF
 - общая информация 211
- утилиты операционной системы, удаление из системы GSKit
 - общая информация 241
- утилиты операционной системы, удаление из системы сервера каталогов
 - общая информация 235
- утилиты операционной системы, установка сервера каталогов
 - общая информация 69
- утилиты сервера, администратор базы данных DB2
 - пароль, настройка 183
- утилиты сервера, база данных DB2
 - настройка 180
- утилиты сервера, восстановление
 - общая информация 193
- утилиты сервера, главный администратор
 - общая информация 172
- утилиты сервера, запустить или остановить административный сервер
 - настройка 159, 171
- утилиты сервера, запустить или остановить сервер каталогов
 - настройка 159, 171
- утилиты сервера, изменить параметры TCP/IP
 - настройка 161
- утилиты сервера, командная строка
 - запустить или остановить сервер 157
- утилиты сервера, настроить DN администратора, настройка 173
- утилиты сервера, пароль администратора, настройка 175

- утилиты сервера, настроить DN администратора
 - настройка 173
- утилиты сервера, настроить пароль администратора
 - настройка 175
- утилиты сервера, настройка
 - запустить или остановить административный сервер 159, 171
 - запустить или остановить сервер 159, 171
 - создать копию экземпляра 157
- утилиты сервера, настройка базы данных
 - общая информация 175
- утилиты сервера, обслуживание базы данных
 - настройка 189
 - общая информация 188
- утилиты сервера, оптимизация базы данных
 - общая информация 186
- утилиты сервера, оптимизировать базу данных
 - настройка 187
- утилиты сервера, отключить протокол изменений
 - настройка 203
- утилиты сервера, пароль администратора базы данных
 - общая информация 182
- утилиты сервера, пароль главного администратора
 - общая информация 174
- утилиты сервера, просмотреть сведения об экземпляре
 - настройка 163
- утилиты сервера, протокол изменений
 - настройка 201
 - общая информация 200
- утилиты сервера, резервное копирование
 - общая информация 190
- утилиты сервера, сервер каталогов
 - добавление суффикса, конфигурация 205
 - отключить базу данных DB2 186
 - удалить суффикс, настройка 207
 - управление схемой, конфигурация 209
- утилиты сервера, синхронизация Active Directory
 - настройка 219
- утилиты сервера, создание
 - файл LDIF, значения UTF-8 127
- утилиты сервера, создание файла LDIF
 - idsbulkload 127
 - idsdb2ldif 127
 - idsldif2db 127
- утилиты сервера, создание экземпляра
 - настройка 147
- утилиты сервера, создать копию экземпляра
 - настройка 157
- утилиты сервера, ссылки
 - общая информация 96
- утилиты сервера, суффикс
 - общая информация 204

- утилиты сервера, удаление конфигурации базы данных
 - общая информация 184
- утилиты сервера, удаление экземпляра
 - настройка 165
- утилиты сервера, управление данными LDIF
 - общая информация 211
- утилиты сервера, управление схемой
 - общая информация 207

Ф

- файл LDIF, создание значения UTF-8 127
- файл свойств DB2, сервер каталогов
 - настройка 251

Э

- экземпляр groxy
 - обновить сервер 92
- экземпляр groxy, удаленное обновление конфигурация, idsimigr -u 94
- экземпляр каталога
 - обновить сервер 92
- экземпляр каталога, удаленное обновление конфигурация, idsimigr -u 94
- экземпляр по умолчанию, создание сервер администрирования
 - экземпляра 134
- экземпляр сервера каталогов, создание
 - настройка 147
 - сервер администрирования
 - экземпляра 136
- экземпляр сервера прокси, создание
 - сервер администрирования
 - экземпляра 143
- экземпляр, Web Administration Tool
 - удаленное управление, конфигурация 115
- экземпляр, пользователи и группы
 - права доступа, общая информация 123
 - создание, общая информация 123
- экземпляр, создание
 - общая информация 133
- электронные
 - публикации vii
 - терминология vii

Я

- Язык описания служб каталогов
 - общая информация 247
- языковые пакеты, операционная система
 - поддерживаемые языки 65
- языковые пакеты, удаление из системы
 - общая информация 244
- языковые пакеты, установка
 - общая информация 65
- языковый пакет, имена пакетов
 - операционная система 66

Примечания

Эта информация относится к продуктам и услугам, предоставляемым на территории США. IBM может не предлагать обсуждаемые в этом документе продукты и услуги в других странах. Информацию о продуктах и услугах, доступных в настоящий момент в вашем регионе, можно получить в местном представительстве IBM. Любая ссылка на продукт, программу или услугу IBM не означает, что может быть использован продукт, программа или услуга только IBM. Вместо этого может применяться любые эквивалентные по своим функциональным возможностям продукт, программа или услуга, не нарушающие прав интеллектуальной собственности IBM. Однако ответственность за проверку работы любых продуктов, программ и услуг других фирм несет пользователь.

gkf могут принадлежать патенты или заявки на патенты на технологии, обсуждаемые в этом документе. Обладание этим документом не дает вам лицензии на данные патенты. Запросы на получение лицензии следует отправлять в письменном виде по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

По вопросам получения лицензии на информацию DBCS обратитесь в Подразделение IBM по правам интеллектуальной собственности в вашей стране или отправьте запрос на получение лицензии в письменном виде по адресу:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству:

INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ ЭТУ ПУБЛИКАЦИЮ "КАК ЕСТЬ" БЕЗ КАКОЙ-ЛИБО ГАРАНТИИ, ЛИБО ВЫРАЖЕННОЙ, ЛИБО ПОДРАЗУМЕВАЕМОЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ НЕНАРУШЕНИЯ ПРАВ, ВЫГОДНОСТИ ИЛИ ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ.

В некоторых странах отказ от предоставления явных и подразумеваемых гарантий при заключении определенных договоров запрещен, поэтому данное заявление может не иметь силы в вашем случае.

Эта публикация может содержать технические неточности и типографские опечатки. В представленную информацию периодически вносятся изменения; эти изменения будут включены в новые издания этой публикации. IBM может вносить улучшения и изменения в продукты и программы, описанные в настоящей документации, в любое время без уведомления.

Любые ссылки на Web-сайты других фирм представлены исключительно для удобства и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах не являются частью данного продукта IBM. Вы можете использовать эти Web-сайты на свой риск.

IBM оставляет за собой право использовать и распространять любую информацию, полученную от вас, по собственному усмотрению без каких-либо обязательств перед вами.

Обладателям лицензий на эту программу, которым нужна информация о ней для (i) организации обмена данными между независимыми продуктами, в число которых может входить данная программа, и (ii) обеспечения правильной интерпретации таких данных, следует обращаться по следующему адресу:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Эта информация может быть предоставлена с соответствующими сроками и условиями, включая, в некоторых случаях, оплату пошлины.

Лицензионная программа, описанная в этой публикации, а также все прочие лицензионные материалы, предоставляются IBM на условиях, изложенных в пользовательском соглашении IBM Customer Agreement, IBM International Program License Agreement, либо на иных аналогичных условиях, оговоренных между нами.

Все данные о производительности, приведенные в настоящей документации, были получены в управляемой среде. В связи с этим возможны значительные расхождения с результатами, полученными в других условиях. Некоторые измерения были выполнены в системах, находящихся на стадии разработки, и их результаты могут не совпадать с показателями в общедоступных системах. Кроме того, некоторые показатели были получены методом экстраполяции. Фактические результаты могут отличаться от приведенных показателей. Пользователям настоящей документации следует проверить данные, относящиеся к их собственной рабочей среде.

Сведения о продуктах других фирм были получены от поставщиков этих продуктов, публичных анонсов и других общедоступных источников. IBM не тестировала эти продукты и не может подтвердить точность данных об их производительности, совместимости и других заявленных характеристиках. Все вопросы по возможностям продуктов других фирм следует адресовать поставщикам этих продуктов.

Все заявления в отношении будущих направлений и намерений компании IBM могут изменяться или отклоняться без предупреждения и представляют только цели и задачи.

Все цены на продукцию IBM, указанные в публикации, являются рекомендуемыми розничными ценами на текущий момент и могут быть изменены без предупреждения. Дилерские цены могут отличаться от них.

Эта информация отражает только планируемые цели. Представленная здесь информация подвергается изменениям до выпуска описываемых продуктов.

Эта информация содержит примеры данных и отчетов, используемых в повседневной деятельности предприятия. Для того чтобы как можно полнее иллюстрировать их, примеры включают имена сотрудников, названия компаний, марок товаров и

продуктов. Все они являются вымышленными, и любое совпадение с реально существующими именами и названиями случайно.

Лицензия, связанная с авторскими правами:

В данном документе содержатся примеры прикладных программ на исходном языке, показывающие приемы программирования на различных операционных платформах. Разрешается копировать, изменять и распространять эти примеры программ в любом виде, без оплаты в пользу IBM, в целях разработки, использования, маркетинга или распространения прикладных программ, отвечающих требованиям интерфейса прикладных программ той операционной платформы, для которой созданы эти примеры программ. Эти примеры не были тщательно протестированы во всех условиях. Поэтому IBM не гарантирует, явно или косвенно, надежность, удобство обслуживания или функциональность этих программ. Разрешается копировать, изменять и распространять эти примеры программ в любом виде, без оплаты в пользу IBM, в целях разработки, использования, маркетинга или распространения прикладных программ, отвечающих требованиям интерфейсов прикладных программ IBM.

Каждая копия или любая часть этих примеров программ, а также созданные на их основе объекты, должны содержать оповещение об авторском праве следующего вида:

© (название вашей компании) (год). Часть данного кода создана на основе примеров программ IBM Corp. © Copyright IBM Corp. _введите год или годы_. Все права защищены.

Если вы просматриваете электронную версию этой информации, то фотографии и цветные иллюстрации могут быть недоступны.

Товарные знаки

IBM, эмблема IBM и ibm.com - товарные знаки или зарегистрированные товарные знаки корпорации International Business Machines в США и/или других странах. Названия других продуктов и служб могут являться товарными знаками IBM или других компаний. Последний список товарных знаков IBM можно найти на веб-странице www.ibm.com/legal/copytrade.shtml (раздел "Сведения об авторских правах и товарных знаках").

Adobe, Acrobat, PostScript и все товарные знаки на основе Adobe являются зарегистрированными товарными знаками или товарными знаками Adobe Systems Incorporated в Соединенных Штатах и/или других странах.

IT Infrastructure Library является зарегистрированным товарным знаком Central Computer and Telecommunications Agency, которое входит в состав Office of Government Commerce.

Intel, эмблема Intel, Intel Inside, эмблема Intel Inside, Intel Centrino, эмблема Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium и Pentium являются товарными знаками или зарегистрированными товарными знаками Intel Corporation или ее дочерних компаний в Соединенных Штатах и других странах.

Linux - товарный знак, зарегистрированный Линусом Торвальдсом в США и/или других странах.

Microsoft, Windows, Windows NT и логотип Windows - товарные знаки Microsoft Corporation в Соединенных Штатах, других странах или одновременно.

TPIL является зарегистрированным товарным знаком и зарегистрированным товарным сообществом Office of Government Commerce; товарный знак зарегистрирован в U.S. Patent and Trademark Office.

UNIX - зарегистрированный товарный знак The Open Group в Соединенных Штатах, других странах или одновременно.



Java и все товарные знаки и логотипы, основанные на Java, являются товарными знаками или зарегистрированными товарными знаками Oracle или ее дочерних компаний.

Cell Broadband Engine является товарным знаком Sony Computer Entertainment, Inc. в Соединенных Штатах и/или других странах и используется на условиях полученной от нее лицензии.

Linear Tape-Open, LTO, эмблема LTO, Ultrium и эмблема Ultrium являются товарными знаками HP, IBM Corp. и Quantum в Соединенных Штатах и других странах.



Напечатано в Дании

SC27-2747-02

