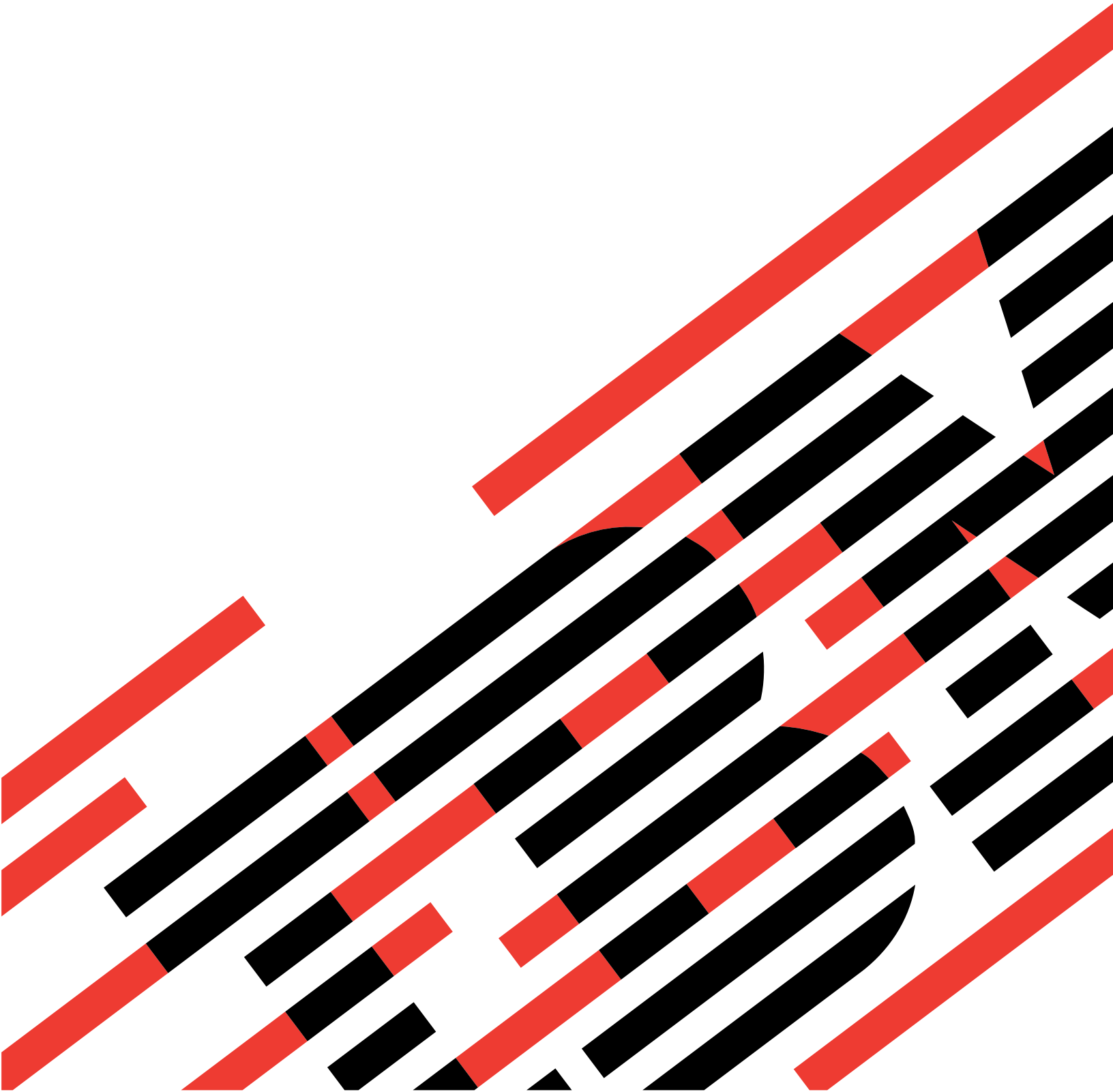
IBM Systems - iSeries

# IBM Directory Server (LDAP)

*Версия 5, выпуск 4*



IBM Systems - iSeries

# IBM Directory Server (LDAP)

*Версия 5, выпуск 4*

**Примечание**

Перед началом работы с этой информацией и описанным в ней продуктом, изучите раздел “Примечания”, на стр. 299 и руководство *Техника безопасности при работе с IBM eServer,*.

**Восьмое издание (февраль 2006 года)**

Это издание относится к версии 5, выпуску 4, модификации 0 IBM i5/OS (код продукта 5722–SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

# Содержание

# Глава 1. IBM Directory Server for iSeries (LDAP)

IBM Directory Server for iSeries (далее - сервер каталогов) представляет собой функцию i5/OS, реализующую сервер упрощенного протокола доступа к каталогам (LDAP) для системы iSeries. Протокол LDAP применяется в сетях TCP/IP как служба каталогов для Internet-приложений и других программных продуктов.

Ниже перечислены разделы, связанные с началом работы с сервером каталогов в системе iSeries:

# Глава 2. Что нового в версии V5R4

В версии V5R4 сервера каталогов появились следующие расширения и дополнения:

**Копирование**

- **Шлюзовое копирование:** Копирование обычно осуществляется в сетях через шлюзовые серверы. Шлюзовые серверы эффективнее собирают и распределяют информацию, за счет чего уменьшается сетевой трафик. См. раздел ″Шлюзовое копирование″ в книге “Обзор функции копирования” на стр. 40.
- **cn=IBMpolicies:** Это новый контейнер для записей, общий для серверов копирования. В отличие от cn=localhost, записи в котором не копируются, контейнер cn=IBMpolicies содержит информацию (параметры), которую может потребоваться копировать. См. раздел “Суффикс (контекст имен)” на стр. 17.

**Безопасность**

- **Идентификация DIGEST-MD5:** DIGEST-MD5 - это способ идентификации SASL. Если клиент применяет механизм Digest-MD5, то пароль передается не в виде обычного текста, препятствуя атакам воспроизведения. См. раздел “Идентификация” на стр. 76.
- **TLS:** Для защиты обычного соединения с помощью TLS добавлена расширенная функция StartTLS. Кроме этого, сервер поддерживает комплект 256-разрядных шрифтов AES TLS. См. раздел “Поддержка протоколов SSL и TLS на сервере каталогов” на стр. 51.

**Поиск**

- **Поиск в поддеревьях с пустой базой:** Для поиска всех суффиксов, определенных в файле конфигурации, достаточно всего одного запроса поиска. При таком подходе отпадает необходимость применения для поиска по всему каталогу нескольких запросов поиска (с разными суффиксами в качестве базы поиска). См. раздел “Поиск записей каталога” на стр. 183.
- **Группы ограниченного поиска:** С помощью этой функции администратор может помимо общих ограничений, действующих для всех пользователей, настраивать группы с разными ограничениями для поиска. За счет этого администратор может легко определить, у кого какие ограничения поиска на конкретном сервере. См. раздел “Параметры поиска” на стр. 47.
- **Расширение обработки учета псевдонимов:** Если в каталоге нет псевдонимов, то применение функций учета псевдонимов значительно повышает быстродействие поиска. Кроме того, в новой версии добавлен параметр конфигурации, служащий для переопределения опций учета псевдонимов, указанных в клиентских запросах на поиск. См. раздел “Параметры поиска” на стр. 47.
- **Кэш атрибутов:** Кэш атрибутов позволяет повысить быстродействие, поскольку обработка фильтров поиска осуществляется в памяти. Это лучше, чем выполнение начальной обработки в базе данных с последующим сохранением в кэше фильтра. В отличие от кэша фильтра, кэш атрибутов не вычищается после каждой операции LDAP - добавления, изменения или удаления. Сервер можно настроить так, чтобы он автоматически запускал кэширование атрибутов в заданное время и кэшировал основные атрибуты в пределах максимального объема памяти, настроенного для этой цели. См. раздел “Кэш атрибутов” на стр. 88.

**Атрибуты**

- **Уникальные атрибуты:** Функция уникальных атрибутов гарантирует, что значения заданных атрибутов в пределах каталога всегда будут уникальными. Например, администратору могут потребоваться атрибуты, содержащие номера социального обеспечения (SSN). Эти атрибуты обязательно должны быть уникальными, поскольку двух людей с одинаковыми социальными номерами не бывает. См. раздел “Уникальные атрибуты” на стр. 86.

- **Сохранение операционных атрибутов:** В новой версии операционные атрибуты creatorsName, createTimestamp, modifiersName и modifyTimestamp копируются на серверы-потребители, а также импортируются и экспортируются в виде файлов LDIF. См. раздел “Операционные атрибуты” на стр. 87.
- **Языковые теги:** Языковые теги представляют собой средства, позволяющие присваивать значения кодам языков. Эти значения хранятся в каталоге и позволяют клиентам запрашивать каталог с учетом особых требований некоторых языков. См. раздел “Языковые теги” на стр. 48.

**Группы**

- **Группа администраторов:** Иногда требуется, чтобы у нескольких пользователей с разными отличительными именами (DN) были почти все те же администраторские права доступа, что и у администратора сервера LDAP. Эта функция позволяет нескольким пользователям выполнять задачи администрирования, не используя при этом общий ИД пользователя и пароль. См. раздел “Права доступа администратора” на стр. 59.
- **Группа Proxy-идентификации:** Proxy-идентификация позволяет клиенту LDAP подключаться под именем одного пользователя, а к целевому каталогу обращаться от имени другого. При таком подходе достигается большая гибкость клиентских приложений, поскольку тогда можно выполнять операции от имени нескольких пользователей, не подключая каждого по отдельности. См. раздел “Proxy-идентификация” на стр. 60.

**Прочая информация**

- **Расширения средств мониторинга:** В данной версии просмотр информации о сервере и соединении выполняется с помощью Web-инструмента администрирования. Для поддержки мониторинга добавлены следующие компоненты:
  - Удобство обслуживания и предотвращение отказа в обслуживании
    - Добавлена новая отслеживаемая информация, в том числе: количество выполненных операций по типам (BIND, MODIFY, COMPARE, SEARCH и тп глубина рабочей очереди, количество доступных нитей обработчика, количество сообщений, внесенных в протокол сервера, протокол контроля, ошибки CLI, число соединений SSL и TLS, сведения о простаивающих соединениях и статистику аварийных нитей.
    - Для поиска информации о нитях обработчика предусмотрена новая база поиска: ″cn=workers,cn=monitor″.
  - Кэш атрибутов
    - В кэше атрибутов хранится информация об атрибутах (настроенный размер, общий размер, количество успешных обращений) и о самом кэше.
    - Для получения информации из кэша атрибутов и занесения ее в протокол изменений добавлена новая база поиска ″cn=changelog,cn=monitor″.
- **Поддержка идентификации клиентских приложений в качестве текущего пользователя:** В данной версии расширены утилиты командной строки и клиента LDAP, предназначенные для поддержки идентификации на локальном сервере каталогов в качестве текущего пользователя. Это особенно важно при выполнения задач администрирования, если войти в систему как пользователь i5/OS с административными правами доступа к каталогу.
- **Управление доступом к системе и ограниченные атрибуты:** В этой версии можно управлять доступом к системе с помощью ограниченных атрибутов, связанных с правами доступа, а также с помощью других серверных атрибутов записей LDAP.
- **Копирование пользователей в контрольные списки каталога LDAP:** Сервер каталогов можно заполнить объектами каталогов на основе пользователей, определенных в контрольном списке HTTP. Кроме этого, сервер каталогов может идентифицировать пользователей на основе разрешений, скопированных из контрольных списков HTTP. Для этого предусмотрены новые программные интерфейсы приложений (API). См. раздел “Копирование пользователей из контрольного списка сервера HTTP на сервер каталогов” на стр. 101.
- **Предотвращение отказа в обслуживании и отключения DN:** С помощью новых пакетов расширений сервер получил возможность выявлять множество видов DoS-атак, восстанавливаться после них и успешно им

противостоять. Теперь администратору предоставляется больше возможностей для управления сервером и автоматической настройки. См. раздел “Предотвращение отказа в обслуживании” на стр. 80.

- **Больше функций для Web-администрирования:** С помощью Web-инструмента администрирования теперь можно выполнить гораздо больше задач. Большинство новых функций можно найти в новой категории **Администрирование сервера**.

# Глава 3. Документ в формате PDF

Для просмотра или загрузки этого документа в формате PDF выберите ссылку Сервер каталогов (LDAP) (около 2700 Кб).

**Прочая информация**

Для просмотра и печати других файлов PDF, а также руководств Redbook обратитесь к разделу Глава 10, “Связанная информация”, на стр. 297.

**Сохранение файлов PDF**

Для того чтобы сохранить файл PDF на рабочей станции для печати и просмотра, выполните следующие действия:

1. В окне браузера щелкните правой кнопкой мыши на приведенной выше ссылке на файл PDF.
2. Щелкните на опции локального сохранения PDF.
3. Выберите каталог, в котором следует сохранить файл PDF.
4. Нажмите кнопку **Сохранить**.

**Загрузка программы Adobe Reader**

Для просмотра и печати файлов PDF необходима программа Adobe Reader. Вы можете бесплатно загрузить ее с Web-сайта фирмы Adobe (www.adobe.com/products/acrobat/readstep.html)  .

# Глава 4. Общие понятия о сервере каталогов

Сервер каталогов реализует спецификацию LDAP V3, разработанную рабочей группой Internet Engineering Task Force (IETF). В нем также применяется ряд технических и функциональных расширений и усовершенствований, разработанных IBM. В этой версии в качестве базового хранилища информации, обеспечивающего целостность операций LDAP, высокую производительность, а также возможность резервного копирования и восстановления, применяется универсальная база данных IBM DB2. При этом обеспечивается взаимодействие с клиентами, отвечающими спецификации IETF LDAP V3. Отдельные вопросы построения и особенности работы сервера каталогов описаны в следующих разделах:



## Каталоги

Сервер каталогов обеспечивает доступ к базе данных, информация в которой хранится в иерархической структуре, аналогичной интегрированной файловой системе i5/OS.

Если известно имя объекта, то можно получить его характеристики. Если имя отдельного объекта неизвестно, то можно выполнить в каталоге поиск и получить список объектов, отвечающих заданным требованиям. Поиск в каталогах обычно выполняется по определенным условиям, а не по предопределенному набору категорий.

Каталог представляет собой специализированную базу данных, особые характеристики которой позиционируют ее несколько в стороне от реляционных баз данных общего назначения. Одной их характеристик каталога является тот факт, что обращение к нему для чтения или поиска выполняется гораздо чаще, чем для обновления или записи. Поскольку каталоги должны поддерживать большое количество запросов на чтение, то они обычно оптимизируются для обработки именно таких запросов. Так как каталоги не должны поддерживать столь же широкий набор функций, как базы данных общего назначения, то их можно оптимизировать для экономичного и быстрого предоставления множеству приложений доступа к требуемым данным в больших распределенных средах.

Каталог может быть централизованным или распределенным. В случае централизованного каталога существует один сервер каталога (или кластер серверов), обеспечивающий доступ к каталогу. В случае распределенного каталога существует несколько серверов, обеспечивающих доступ к каталогу, обычно разнесенных территориально.

В распределенном каталоге информация может разбиваться на разделы или копироваться (тиражироваться). При разбиении информации на разделы на каждом сервере каталога хранится уникальный, не пересекающийся с другими серверами, блок информации. Таким образом, каждая запись каталога хранится на одном и только на одном сервере. Для разбиения каталога на разделы применяется технология перенаправления LDAP. Ссылки перенаправления LDAP позволяют пользователям направлять запросы LDAP к тому же или к другому пространству имен, размещенному на другом (или на том же) сервере. При копировании информации одна и та же запись каталога хранится сразу на нескольких серверах. В распределенном каталоге часть информации может быть разбита на разделы, а часть может копироваться.

Модель сервера каталогов LDAP основана на записях (называемых также объектами). Каждая запись состоит из одного или нескольких атрибутов, таких как имя, адрес и тип. Обычно типы представлены мнемоническими сочетаниями символов, например, cn - common name (имя) или mail - адрес электронной почты.

Пример каталога в разделе рис. 1 на стр. 11 содержит запись Tim Jones с атрибутами mail и telephoneNumber. Дополнительно можно указать такие атрибуты, как fax, title, sn (фамилия) и jpegPhoto.

У каждого каталога есть схема, которая представляет собой набор правил, определяющих структуру и содержимое каталога. Схему можно просмотреть с помощью Web-инструмента администрирования. Дополнительная информация о схеме приведена в разделе “Схема” на стр. 18.

Каждая запись каталога содержит специальный атрибут objectClass. Этот атрибут определят список обязательных и допустимых атрибутов в записи. Другими словами, значение атрибута objectClass задает правила схемы, которым должна отвечать запись.

Помимо атрибутов, определенных в схеме, с записью может также быть связан набор атрибутов, поддерживаемых сервером. Такие атрибуты, называемые операционными, содержат например, такие сведения, как время создания и время последнего обращения к записи. Дополнительная информация об операционных атрибутах приведена в разделе “Операционные атрибуты” на стр. 87.

Как правило, записи каталога LDAP расположены в соответствии с иерархической структурой политического, географического или юридического образования (см. рис. 1 на стр. 11). Записи, соответствующие странам и регионам, находятся на верхнем уровне структуры. Записи, соответствующие штатам и государственным организациям, находятся на втором уровне. Записи на последующих уровнях представляют людей, организации, принтеры, документы и другие объекты.

Для идентификации записей в LDAP применяются отличительные имена (DN). Они состоят из имени самой записи и имен объектов, расположенных над записью в структуре каталога. Эти имена перечисляются в направлении от нижнего уровня к верхнему. Например, полное DN записи, расположенной в нижнем левом углу в примере рис. 1 на стр. 11, равно cn=Tim Jones, o=IBM, c=US. Каждая запись содержит по крайней мере один атрибут, применяемый как имя записи. Этот атрибут называется относительным отличительными именем (RDN) записи. Запись, расположенная выше заданного RDN, называется родительским отличительным именем. В приведенном выше примере cn=Tim Jones задает имя записи, то есть ее RDN. Значение o=IBM, c=US представляет родительское DN записи cn=Tim Jones. За дополнительной информацией о DN обратитесь к разделу “Отличительные имена (DN)” на стр. 13.

Для того чтобы у сервера LDAP была возможность работать с частью каталога LDAP, родительские отличительные имена верхнего уровня указываются в конфигурации сервера. Эти отличительные имена называются суффиксами. Сервер может обращаться ко всем объектам, расположенным в структуре каталога ниже указанного суффикса. Например, если сервер LDAP содержит каталог, приведенный в примере рис. 1 на стр. 11

стр. 11, то в его конфигурации должен быть задан суффикс o=ibm, c=us. В противном случае сервер не сможет отвечать на запросы клиентов, относящиеся к записи Tim Jones.

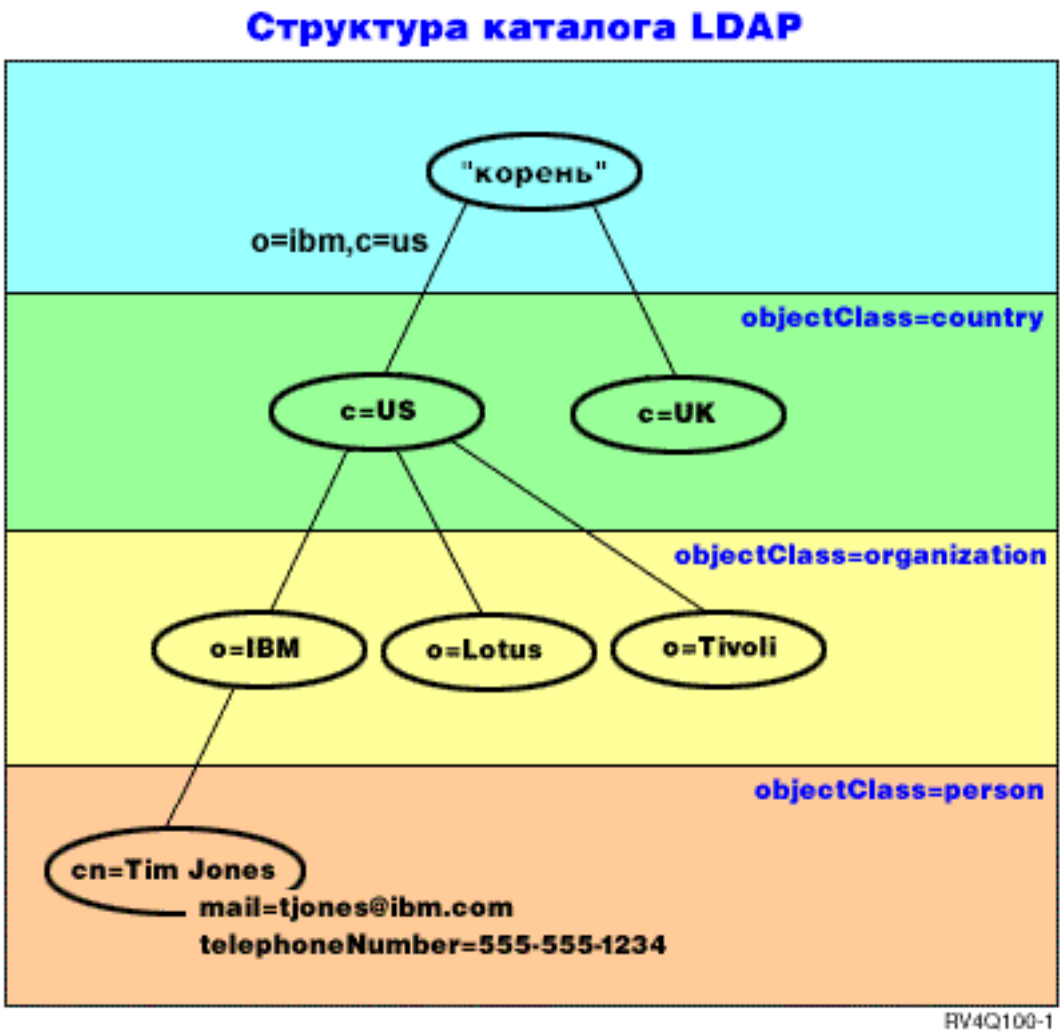



*Рисунок 1. Структура каталога LDAP*

Структура каталога может отличаться от традиционной. Например, все чаще встречается структура на основе компонентов доменов. В этой структуре записи состоят из компонентов имен доменов TCP/IP. Например, запись dc=ibm,dc=com может указывать на o=ibm,c=us.

Допустим, что вы хотите создать каталог, соответствующей структуре доменов, и содержащий сведения о сотрудниках, например, имена, номера телефонов и адреса электронной почты. Контекст суффиксов или имен определяется доменом TCP/IP. Такой каталог можно схематично представить следующим образом:

```
/
|
+- ibm.com
   |
   +- employees
      |
      +- Tim Jones
      |  555-555-1234
      |  tjones@ibm.com
```

```
      |
      +- John Smith
         555-555-1235
         jsmith@ibm.com
```

После ввода этих сведений в базу данных сервера каталогов они будут выглядеть примерно следующим образом:

```
# suffix ibm.com
dn: dc=ibm,dc=com
 objectclass: top
objectclass: domain
dc: ibm

# employees directory
dn: cn=employees,dc=ibm,dc=com
 objectclass: top
objectclass: container
cn: employees

# employee Tim Jones
dn: cn=Tim Jones,cn=employees,dc=ibm,dc=com
 objectclass: top
      objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: Tim Jones
cn: "Jones, Tim"
sn: Jones
givenname: Tim
telephonenumber: 555-555-1234
mail: tjones@ibm.com

# employee John Smith
dn: cn=John Smith,cn=employees,dc=ibm,dc=com
 objectclass: top
      objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: John Smith
cn: "Smith, John"
sn: Smith
givenname: John
telephonenumber: 555-555-1235
mail: jsmith@ibm.com
```

Вы заметите, что каждая запись содержит значения атрибутов с именем objectclass. Значения objectclass определяют, какие атрибуты допустимы для данной записи, например, telephonenumber или givenname. Допустимые классы объектов определяются схемой. Схема - это набор правил, определяющих тип записей, которые можно создать в базе данных.

**Клиенты и серверы каталога**

Обращение к каталогам обычно осуществляется с применением модели клиент-сервер. Процессы клиента и сервера могут работать как в одной системе, так и в разных. Сервер может обслуживать множество клиентов. Приложение, которое хочет прочитать или записать информацию каталога, не обращается к каталогу непосредственно. Вместо этого оно вызывает функцию или интерфейс прикладной программы (API), которые в свою очередь отправляют сообщение другому процессу. Этот второй процесс обращается к информации каталога от имени запрашивающего приложения. Результаты операции чтения или записи возвращаются запрашивающему приложению.

API определяет программный интерфейс, применяемый для обращения к службе с помощью определенного языка программирования. Формат и содержимое сообщений, передаваемых между сервером и клиентом, должны соответствовать заранее согласованному протоколу. LDAP определяет протокол сообщений, которыми обмениваются серверы и клиенты каталогов. Кроме того, существуют API LDAP для языка C и способы обращения к каталогам из приложений на Java с помощью интерфейса Java Naming and Directory Interface (JNDI).

**Защита каталога**

Каталог должен поддерживать основные функции, необходимые для реализации стратегии защиты. Каталог может не обеспечивать непосредственно все требуемые возможности защиты, но должна обеспечиваться возможность его интеграции со службой защиты сети, предоставляющей основные функции защиты. Во-первых, требуется способ идентификации пользователей. При идентификации проверяется достоверность предоставленных пользователями сведений о себе. В качестве основного способа идентификации применяется проверка имени и пароля пользователя. После идентификации пользователя необходимо проверить, есть ли у него права доступа, необходимые для выполнения запрошенной операции над указанным объектом.

Проверка прав доступа часто выполняется с помощью списков управления доступом (ACL). ACL - это список прав доступа, который можно связывать с объектами или атрибутами каталога. В ACL перечислены типы прав доступа, разрешенные или запрещенные для каждого пользователя или группы пользователей. Для того чтобы сократить размер ACL и упростить управление ими, пользователей с одинаковыми правами доступа часто объединяют в группы.

## Отличительные имена (DN)

Каждая запись каталога имеет отличительное имя (DN). DN - это имя, уникальным образом идентифицирующее каждую запись каталога. DN состоит из пар вида атрибут=значение, разделенных запятыми, например:

```
cn=Ben Gray,ou=editing,o=New York Times,c=US
cn=Lucille White,ou=editing,o=New York Times,c=US
cn=Tom Brown,ou=reporting,o=New York Times,c=US
```

В DN могут применяться любые атрибуты, определенные в схеме каталога. При этом учитывается порядок следования пар атрибут=значение. DN содержит по одному компоненту для каждого уровня иерархии, начиная от корневого уровня, до уровня размещения рассматриваемой записи. DN LDAP начинаются с наиболее конкретного атрибута (обычно это какой-либо вид имени), за которым последовательно указываются все более широкие атрибуты, а последним чаще всего указывается атрибут страны. Первый компонент DN называется относительным отличительным именем (RDN). Он позволяет отличить данную запись от всех остальных записей, имеющих ту же родительскую запись, что и рассматриваемая. В приведенном выше примере RDN ″cn=Ben Gray″ позволяет отличить первую запись от второй (с RDN ″cn=Lucille White″). Во всем остальном эти два DN эквивалентны. Пара атрибут=значение, составляющая RDN записи, также обязательно должна присутствовать в записи. (Для других компонентов DN это требование не является обязательным.)

Ниже приведен пример создания записи для пользователя:

```
dn: cn=Tim Jones,o=ibm,c=us
 objectclass: top
      objectclass: person
cn: Tim Jones
sn: Jones
telephonenumber: 555-555-1234
```

**Правила указания специальных символов в DN**

Некоторые символы имеют в DN специальное значение. Например, символ = (равно) разделяют имя и значение атрибута, а символ , (запятая) разделяет пары атрибут=значение. К специальным относятся

следующие символы **,** (запятая), **=** (равно), **+** (плюс), **<** (меньше), **>** (больше), # (символ номера), **;** (точка с запятой), \ (обратная косая черта) и **"** (символ кавычек, код ASCII 34).

При указании специальных символов в значениях атрибутов применяются особые способы, позволяющие отключить специальное значение этих символов. Для указания этих и других символов в значениях атрибутов в строке DN применяются следующие способы:

1. Если необходимо указать один из специальных символов, то перед ним следует указать обратную косую черту (’\’ ASCII 92). Пример указания запятой в названии организации:

   ```
   CN=L. Eagle,O=Sue\, Grabbit and Runn,C=GB
   ```

   Это предпочитаемый способ.
2. В противном случае символ необходимо заменить на обратную косую черту и две шестнадцатеричные цифры, соответствующие коду этого символа. Код символа должен быть задан в кодировке **UTF-8**.

   ```
   CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB
   ```
3. Заключите все значение атрибута в символы **""** (кавычки, ASCII 34), не являющиеся частью значения.Между парой кавычек все символы, за исключением \ (обратная косая черта) обрабатываются ″как есть″. Для указания перечисленных ранее специальных символов, обратной косой черты (ASCII 92) или кавычек (ASCII 34), а также шестнадцатеричных значений, используемых в способе 2, может применяться символ \ (обратная косая черта). Например, для указания кавычек в значении `cn=xyz"qrs"abc` применяется обозначение `cn=xyz\"qrs\"abc`, а для указания символа \ - обозначение:

   ```
   "одиночную обратную косую черту можно указать так \\"
   ```

   Еще один пример: строка `"\Zoo"` является недопустимой, поскольку символ ’Z’ нельзя указывать в таком контексте.

**Псевдо DN**

Псевдо DN применяются при определении и вычислении прав доступа. Каталог LDAP поддерживает несколько псевдо DN (например, ″group:CN=THIS″ и ″access-id:CN=ANYBODY″), которые позволяют обозначить большое число DN, имеющих общие характеристики по отношению либо к выполняемой операции, либо к объекту, над которым выполняется эта операция. Дополнительная информация об управлении доступом приведена в разделе “Защита сервера каталогов” на стр. 51.

Сервер каталогов поддерживает следующие три псевдо DN:

- access-id: CN=THIS

  При указании в ACL это DN обозначает bindDN, соответствующий DN, используемому для выполнения операции. Например, если операция выполняется над объектом ″cn=personA, ou=IBM, c=US″ и используется bindDn ″cn=personA, ou=IBM, c=US″, то предоставленные права доступа будут определяться сочетанием прав доступа ″CN=THIS″ и прав доступа ″cn=personA, ou=IBM, c=US″.
- group: CN=ANYBODY

  При указании в ACL это DN обозначает всех пользователей, в том числе не идентифицированных. Пользователей нельзя удалить из этой группы, а эту группу нельзя удалить из базы данных.
- group: CN=AUTHENTICATED

  Это DN соответствует любому DN, идентифицированному каталогом. Способ идентификации при этом не учитывается.

  **Примечание:** ″CN=AUTHENTICATED″ относится к DN, которое было идентифицировано на сервере, без учета местоположения объекта, представленного этим DN. Это значение следует применять с осторожностью. Допустим, например, что в суффиксе ″cn=Secret″ существует узел с именем ″cn=Confidential Material″ и записью aclentry ″group:CN=AUTHENTICATED:normal:rsc″. В другом суффиксе, ″cn=Common″, существует узел ″cn=Public Material″. Если эти два узла

находятся на одном сервере, то подключение к ″cn=Public Material″ будет рассматриваться как успешная идентификация и приведет к предоставлению прав доступа класса normal к объекту ″cn=Confidential Material″.

Несколько примеров псевдо DN:

**Пример 1**

Рассмотрим следующий ACL объекта: cn=personA, c=US

```
AclEntry: access-id: CN=THIS:critical:rwsc
AclEntry: group: CN=ANYBODY: normal:rsc
AclEntry: group: CN=AUTHENTICATED: sensitive:rcs
```

| Имя пользователя при подключении | Предоставленные права доступа |
|---|---|
| cn=personA, c=US | normal:rsc:sensitive:rcs:critical:rwsc |
| cn=personB, c=US | normal:rsc:sensitive:rsc |
| Anonymous | normal:rsc |

В этом примере personA предоставляются права доступа, соответствующие ИД ″CN=THIS″, а также права доступа, соответствующие группам псевдо DN ″CN=ANYBODY″ и ″CN=AUTHENTICATED″.

**Пример 2**

Рассмотрим следующий ACL объекта: cn=personA, c=US AclEntry: access-id:cn=personA, c=US: object:ad

```
AclEntry: access-id: CN=THIS:critical:rwsc
AclEntry: group: CN=ANYBODY: normal:rsc
AclEntry: group: CN=AUTHENTICATED: sensitive:rcs
```

Для операции, выполняемой над cn=personA, c=US:

| Имя пользователя при подключении | Предоставленные права доступа |
|---|---|
| cn=personA, c=US | object:ad:critical:rwsc |
| cn=personB, c=US | normal:rsc:sensitive:rsc |
| Anonymous | normal:rsc |

В этом примере personA предоставляются права доступа, соответствующие ИД ″CN=THIS″, а также права доступа, соответствующие самому DN ″cn=personA, c=US″. Обратите внимание, что права доступа группы не предоставляются, поскольку для применяемого DN подключения (″cn=personA, c=US″) существует более конкретная запись aclentry (″access-id:cn=personA, c=US″).

**Расширенная обработка DN**

Составное RDN в DN может включать несколько компонентов, связанных операторами ‘+’. Сервер обеспечивает возможность поиска записей с такими DN. Составное RDN можно указывать в качестве основы операции поиска в любом порядке.

```
ldapsearch -b "cn=mike+ou=austin,o=ibm,c=us" "(objectclass=*)"
```

Сервер поддерживает расширенную операцию нормализации DN. Расширенная операция нормализации DN нормализует применяемые DN с помощью схемы сервера. Такая расширенная операция может быть полезна в приложениях, использующих DN. Дополнительные сведения о расширенных операциях приведена в разделе “Элементы управления и расширенные операции” на стр. 89.

**Синтаксис отличительных имен**

Формальный синтаксис отличительных имен (DN) основан на RFC 2253. Ниже приведены синтаксические диаграммы в формате Бэкуса-Наура (BNF):

```
<имя> ::= <компонент-имени> ( <символ-разделитель> )
          | <компонент-имени> <символ-разделитель> <имя>

   <символ-разделитель> ::= <необязательный-разделитель>
                            <разделитель>
                            <необязательный-разделитель>

   <разделитель> ::=  "," | ";"

   <необязательный-разделитель> ::= ( <CR> ) *( " " )

   <компонент-имени> ::= <атрибут>
           | <атрибут> <необязательный-разделитель> "+"
             <необязательный-разделитель> <компонент-имени>

   <атрибут> ::= <строка>
           | <ключ> <необязательный-разделитель> "=" <необязательный-разделитель> <строка>

   <ключ> ::= 1*( <ключевой-символ> ) | "OID." <oid> | "oid." <oid>
   <ключевой-символ> ::= буквы, цифры и пробел

   <oid> ::= <числовая-строка> | <числовая-строка> "." <oid>
   <числовая-строка> ::= 1*<цифра>
   <цифра> ::= цифры 0-9

   <строка> ::= *( <символ> | <пара> )
            | '"' *( <символ> | <специальный-символ> | <пара> ) '"'
            | "#" <шестн.>


   <специальный-символ> ::= "," | "=" | <CR> | "+" | "<" |  ">"
            | "#" | ";"

   <пара> ::= "\" ( <специальный-символ> | "\" | '"')
   <символ> ::= любой символ, кроме <специальных-символов>, "\" или '"'


   <шестн.> ::= 2*<шестн.-символ>
   <шестн.-символ> ::= 0-9, a-f, A-F
```

Для отделения RDN в отличительном имени может применяться точка с запятой (;), однако обычно применяется запятая (,).

Рядом с запятой или точкой с запятой может присутствовать пробел. Пробелы игнорируются и точка с запятой заменяется на запятую.

Кроме того, перед символами ’+’ и ’=’, а также после них могут присутствовать символы пробела (’ ’ ASCII 32). При анализе эти пробелы игнорируются.

Ниже приведен пример отличительного имени, записанного с применением формата, удобного для записи обычных имен. Это имя имеет три компонента. Первый компонент представляет собой составное RDN. Составное RDN включает несколько пар атрибут:значение и может применяться для однозначного обозначения записи в ситуациях, когда простое значение CN может оказаться недостаточным:

```
OU=Sales+CN=J. Smith,O=Widget Inc.,C=US
```

## Суффикс (контекст имен)

Суффикс (называемый также контекстом имен) - это отличительное имя (DN), представляющее запись верхнего уровня в локальной иерархии каталога. Поскольку в LDAP применяются относительные имена, то это DN представляет собой суффикс любой записи, входящей в данную иерархию каталога. У сервера каталогов может быть несколько суффиксов, каждый из которых связан с некоторой локальной иерархией каталога, например, o=ibm,c=us.

В каталог необходимо добавить запись, соответствующую суффиксу. Создаваемая запись должна использовать objectclass, содержащий применяемый атрибут имени. Для создания записей, соответствующих суффиксу, можно воспользоваться Web-инструментом администрирования или утилитой Qshell ldapadd. Дополнительная информация приведена в разделах “Управление записями каталога” на стр. 179 и “ldapmodify и ldapadd” на стр. 203.

Концептуально существует глобальное пространство имен LDAP. В глобальном пространстве LDAP DN могут быть представлены в следующем виде:

- cn=John Smith,ou=Rochester,o=IBM
- cn=Jane Doe,o=My Company,c=US
- cn=system administrator,dc=myco,dc=com

Суффикс ″o=IBM″ указывает серверу, что только первое DN находится в пространстве имен этого сервера. Попытки обращения к объектам, находящимся за его пределами, приведут к возникновению ошибки, связанной с отсутствием требуемого объекта или перенаправления.

На сервере может быть определено несколько суффиксов. На сервере каталогов заранее определено несколько суффиксов, которые могут применяться для хранения данных:

- cn=schema содержит представление схемы LDAP
- cn=changelog содержит протокол изменений сервера (если включена соответствующая опция)
- cn=localhost содержит не копируемую информацию, управляющую некоторыми аспектами работы сервера, например, объекты конфигурации копирования
- cn=IBMpolicies содержит *скопированные* данные о работе сервера.
- cn=pwdpolicy содержит данные стратегии управления паролями сервера
- суффикс ″os400-sys=system-name.mydomain.com″ предоставляет доступ LDAP к объектам i5/OS. В настоящее время возможен доступ только к пользовательским профайлам и группам

Сервер каталогов поставляется с заранее настроенным суффиксом по умолчанию dc=system-name,dc=domain-name, упрощающим начало работы с сервером. Вы можете не использовать этот суффикс. Вы также можете добавлять собственные суффиксы или удалять заранее настроенные суффиксы.

Существует два типичных соглашения о присвоении имен суффиксам. Одно из них использует структуру домена TCP/IP вашей организации. Второе основано на названии и размещении организации.

Например, если используется домен TCP/IP mycompany.com, то вы можете выбрать суффикс `dc=mycompany,dc=com`, где атрибут `dc` обозначает компонент домена. В этом случае запись верхнего уровня в каталоге будет выглядеть следующим образом (в виде LDIF, текстового формата, применяемого для представления записей LDAP):

```
dn: dc=mycompany,dc=com
objectclass: domain
dc: mycompany
```

Класс объекта `domain` также имеет некоторые дополнительные атрибуты, которые вы можете применять. Просматривать схему, а также редактировать созданные записи и просматривать доступные дополнительные атрибуты можно с помощью Web-инструмента администрирования. Дополнительная информация приведена в разделе “Управление схемой” на стр. 168.

Если ваша организация расположена в США и называется `My Company`, то вы можете выбрать следующие суффиксы:

```
o=My Company
o=My Company,c=US
ou=Widget Division,o=My Company,c=US
```

здесь `ou` - название класса объекта organizationalUnit (отдел организации), `o` - название класса объекта organization (организация), а `c` - стандартное двухбуквенное обозначение страны. В этом случае запись верхнего уровня будет выглядеть следующим образом:

```
dn: o=My Company,c=US
 objectclass: organization
o: My Company
```

Применяемые вами приложения, возможно, потребуют создания каких-либо особых суффиксов или применения определенного соглашения о присвоении имен. Например, если каталог применяется для управления цифровыми сертификатами, то для части каталога может потребоваться создать структуру таким образом, чтобы имена записей соответствовали DN субъектов, которым принадлежат сертификаты.

Суффикс записей, добавляемых в каталог, должен совпадать с DN. Например, `ou=Marketing,o=ibm,c=us`. Если запрос содержит суффикс, который не совпадает ни с одним суффиксом локальной базы данных, то запрос перенаправляется серверу LDAP, ссылка на который задана по умолчанию. Если сервер LDAP по умолчанию не задан, то будет возвращено сообщение об ошибке Объект не существует.

Дополнительная информация о добавлении и удалении суффиксов приведена в разделе “Добавление и удаление суффиксов сервера каталогов” на стр. 127.

## Схема

Схема - это набор правил, определяющих тип данных, которые можно хранить в каталоге. Схема определяет допустимые типы записей, а также структуру и синтаксис их атрибутов.

Данные сохраняются в каталоге посредством записей каталога. Запись включает в себя обязательный класс объекта, а также атрибуты. Атрибуты могут быть как обязательными, так и необязательными. Класс объекта указывает, какой вид информации описывается данной записью, и определяет набор атрибутов этой записи. Каждый атрибут может иметь одно или несколько значений. Дополнительная информация об управлении записями приведена в разделе “Управление записями каталога” на стр. 179.

Дополнительные сведения о схеме можно найти в следующих разделах:

## Схема IBM Directory Server

Схема каталога Directory Server определена заранее, однако при наличии дополнительных требований вы можете вносить в нее изменения. Дополнительные сведения об изменении схемы приведены в разделе “Управление схемой” на стр. 168.

Сервер каталогов обеспечивает поддержку динамической схемы. Схема публикуется как часть информации каталога и к ней можно обращаться с помощью записи Subschema (DN=″cn=schema″). Обращаться к схеме можно с помощью API ldap_search(), а изменять - с помощью API ldap_modify(). Дополнительная информация об этих API приведена в разделе “API сервера каталогов”.

Схема содержит гораздо больше информации о конфигурации, чем определено в RFC LDAP версии 3 или в стандартных спецификациях. Например, можно указать, какие индексы следует поддерживать для определенного атрибута. Эта дополнительная информация о конфигурации хранится в записи подсхемы. Еще один дополнительный класс объекта определен для записи подсхемы IBMsubschema, у которой есть атрибуты ″MAY″, позволяющие сохранять расширенную информацию схемы.

Сервер каталогов определяет единую схему для всего сервера. Обращаться к этой схеме можно с помощью специальной записи каталога ″cn=schema″. Эта запись содержит все определенные для сервера схемы. Для получения информации о схеме можно выполнить операцию ldap_search:

```
DN: "cn=schema", search scope: base, filter: objectclass=subschema
или objectclass=*
```

Схема предоставляет значения для следующих типов атрибутов:

- objectClasses (Дополнительная информация приведена в разделе “Классы объектов” на стр. 21.)
- attributeTypes (Дополнительная информация приведена в разделе “Атрибуты” на стр. 22.)
- IBMAttributeTypes (Дополнительная информация приведена в разделе “Атрибут IBMAttributeTypes” на стр. 24.)
- Правила соответствия (Дополнительная информация приведена в разделе “Правила соответствия” на стр. 25).
- Варианты синтаксиса ldap (Дополнительная информация приведена в разделе “Синтаксис атрибута” на стр. 27).

Синтаксис этих определений схемы основан на RFC LDAP версии 3.

Пример записи схемы:

```
objectclasses=( 1.3.6.1.4.1.1466.101.120.111
                NAME 'extensibleObject'
                SUP top AUXILIARY )

objectclasses=(  2.5.20.1
                 NAME 'subschema'
                 AUXILIARY MAY
                     ( dITStructureRules
                    $ nameForms
                    $ ditContentRules
                    $ objectClasses
                    $ attributeTypes
                    $ matchingRules
                    $ matchingRuleUse  ) )
objectclasses=( 2.5.6.1
                NAME 'alias'
                SUP top STRUCTURAL
                MUST aliasedObjectName )

attributeTypes=( 2.5.18.10
                 NAME 'subschemaSubentry'
                 EQUALITY distinguishedNameMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
```

```
                  NO-USER-MODIFICATION
                  SINGLE-VALUE USAGE directoryOperation )
attributeTypes=( 2.5.21.5 NAME 'attributeTypes'
                  EQUALITY objectIdentifierFirstComponentMatch
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.3
                  USAGE directoryOperation )
attributeTypes=( 2.5.21.6 NAME 'objectClasses'
                  EQUALITY objectIdentifierFirstComponentMatch
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.37
                  USAGE directoryOperation
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                  USAGE directoryOperation )

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binary' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Directory String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time' )

matchingRules=( 2.5.13.2 NAME 'caseIgnoreMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
matchingRules=( 2.5.13.0 NAME 'objectIdentifierMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.30 NAME 'objectIdentifierFirstComponentMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.4 NAME 'caseIgnoreSubstringsMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.58 )
```

Информацию схемы можно изменять с помощью API ldap_modify. Дополнительные сведения вы можете найти в разделе “API сервера каталогов”. С помощью DN ″cn=schema″ вы можете добавлять, удалять или заменять типы атрибутов и классы объектов. Дополнительная информация приведена в разделах “Динамическая схема” на стр. 30 и “Управление схемой” на стр. 168. Можно также указать полное описание. Добавляемые или заменяемые записи схемы могут содержать определение LDAP версии 3, расширенное определение атрибута IBM, либо оба определения.

## Поддержка общей схемы

Каталог IBM Directory поддерживает стандартную схему каталога, определяемую следующими документами:

- RFC рабочей группы Internet Engineering Task Force (IETF)  LDAP версии 3, например, RFC 2252 и 2256.
- Directory Enabled Network (DEN) 
- The Common Information Model (CIM) из Desktop Management Task Force (DMTF) 
- The Lightweight Internet Person Schema (LIPS) консорциума Network Application Consortium 

В конфигурацию по умолчанию этой версии LDAP включена поддержка определения схемы LDAP версии 3. Обеспечивается также поддержка определений схем DEN.

IBM предоставляет набор расширенных определений общей схемы, используемых другими приложениями IBM, обращающимися к каталогу LDAP. Эти определения включают в себя:

- Объекты для приложений, реализующих системы типа телефонных справочников, например, eperson, group, country, organization, organization unit and role, locality, state и т.д.
- Объекты для других подсистем, например, для средств учета, служб, служебных точек доступа, для проверки прав доступа, идентификации, средств управления стратегиями защиты и т.д.

## Классы объектов

Класс объектов задает набор атрибутов, описывающих данный объект. Например, если вы создали класс объектов **tempEmployee** , то можно включить в него такие атрибуты временного сотрудника, как **idNumber**, **dateOfHire** или **assignmentLength**. Вы можете добавлять собственные классы объектов, отвечающие требованиям вашей организации. Схема IBM Directory Server содержит ряд базовых типов классов объектов, включая следующие:

- Группы
- Географические объекты
- Организации
- Люди

**Примечание:** Классы объектов, характерные для Directory Server, имеют префикс 'ibm-'.

Классы объектов определяются такими характеристиками, как тип, наследование и атрибуты.

### Тип класса объектов

Класс объектов может относиться к одному из следующих трех типов:

**Структурный:**
Каждая запись может относиться к одному и только к одному структурному классу объектов, определяющему базовое содержимое записи. Этот класс объектов обычно представляет реальный объект. Поскольку все записи должны относиться к какому-либо структурному классу объектов, то это наиболее распространенный тип классов объектов.

**Абстрактный:**
Этот тип применяется в качестве базового класса или шаблона для других (структурных) классов объектов. Он определяет набор атрибутов, общих для нескольких структурных классов объектов. Определение таких структурных классов объектов на базе абстрактного класса позволяет наследовать наборы атрибутов. В этом случае не требуется определять атрибуты отдельно для каждого подчиненного класса объектов.

**Вспомогательный:**
Этот тип указывает дополнительные атрибуты, которые можно связать с записью, относящейся к определенному структурному классу объектов. Несмотря на то, что запись может относиться только к одному структурному классу объектов, он может относиться сразу к нескольким вспомогательным классам объектов.

### Наследование классов объектов

Эта версия сервера каталогов поддерживает наследование классов объектов и определений атрибутов. Новый класс объектов можно определить на базе родительских классов (множественное наследование) и дополнительных или измененных атрибутов.

Каждая запись связывается с одним структурным классом объектов. Все классы объектов являются наследниками абстрактного класса объектов **top**. При этом они могут также быть наследниками других классов объектов. Структура классов объектов определяет список обязательных и допустимых атрибутов для каждой записи. Наследование классов объектов ограничено последовательностью определений классов объектов. Класс объектов может являться наследником только тех классов объектов, которые лежат в иерархии выше него. Например, структура класса объектов для записи person может быть определена в файле LDIF следующим образом:

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
```

В этой структуре organizationalPerson является наследником классов объектов person и top, в то время как класс объектов person является только наследником класса top. Таким образом, при указании для записи класса объекта organizationalPerson эта запись автоматически унаследует обязательные и разрешенные атрибуты родительского класса объектов (в нашем примере - класса объектов person).

Перед обработкой и фиксацией операции обновления схемы проверяются на соответствие иерархии классов схемы.

**Атрибуты**

Каждый класс объектов содержит набор обязательных и дополнительных атрибутов. Обязательные атрибуты - это атрибуты, которые обязательно должны существовать в записях, использующих данный класс объектов. Дополнительные атрибуты - это атрибуты, которые могут присутствовать в записях, использующих данный класс объектов.

# Атрибуты

Каждая запись каталогов имеет набор атрибутов, связанный с ней с помощью класса объектов. Если класс объектов описывает тип информации, хранящейся в записи, то атрибуты содержат фактические данные. Атрибут представляет собой одну или несколько пар имя-значение, содержащих различные элементы данных, такие как имя, адрес или номер телефона. Сервер каталогов представляет данные в виде пар имя-значение, включающих атрибут с описательным именем, например, commonName (cn), и фактические данные, например, John Doe.

Например, запись для пользователя John Doe может содержать следующие пары имя-значение для атрибутов.

```
dn: uid=jdoe, ou=people, ou=mycompany, c=us
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: John Doe
      sn: Doe
givenName: Jack
givenName: John
```

В то время как в схеме уже определены стандартные атрибуты, вы можете создавать, изменять, копировать и удалять определения атрибутов в соответствии с требованиями своей организации.

Дополнительная информация приведена в следующих разделах:


- “Элементы общей подсхемы”
- “Атрибут objectclass” на стр. 23
- “Атрибут attributetypes” на стр. 23
- “Атрибут IBMAttributeTypes” на стр. 24
- “Правила соответствия” на стр. 25
- “Правила индексации” на стр. 26
- “Синтаксис атрибута” на стр. 27


## Элементы общей подсхемы

Для определения грамматики значений атрибутов подсхемы применяются следующие элементы:

- alpha = ’a’ - ’z’, ’A’ - ’Z’
- number = ’0’ - ’9’
- anh = alpha / number / ’-’ / ’;’
- anhstring = 1 * anh
- keystring = alpha [ anhstring ]

- numericstring = 1 * number
- oid = descr / numericoid
- descr = keystring
- numericoid = numericstring *( ″.″ numericstring )
- woid = whsp oid whsp ; набор oids в любом формате (числовые OID или имена)
- oids = woid / ( ″(″ oidlist ″)″ )
- oidlist = woid *( ″$″ woid ) ; дескрипторы объектов, применяемые в качестве имен элементов схемы
- qdescrs = qdescr / ( whsp ″(″ qdescrlist ″)″ whsp )
- qdescrlist = [ qdescr *( qdescr ) ]
- whsp ″'″ descr ″'″ whsp

## Атрибут objectclass

Атрибут objectclasses содержит список поддерживаемых сервером классов объектов. Каждое значение этого атрибута представляет собой отдельное определение класса объектов. Определения классов объектов можно добавлять, удалять и изменять путем внесения соответствующих изменений в атрибут objectclasses записи cn=schema. Значения атрибута objectclasses имеют следующую грамматику, определенную в RFC 2252:

```
ObjectClassDescription = "(" whsp
        numericoid whsp ; Идентификатор класса объектов
        [ "NAME" qdescrs ]
        [ "DESC" qdstring ]
        [ "OBSOLETE" whsp ]
        [ "SUP" oids ] ; Родительский класс объектов
        [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; по умолчанию структурный
        [ "MUST" oids ] ; типы атрибутов
        [ "MAY" oids ] ; типы атрибутов
        whsp ")"
```

Пример определения класса объектов person:

```
( 2.5.6.6 NAME 'person' DESC 'Defines entries that generically represent people. '  STRUCTURAL
SUP top MUST ( cn $ sn ) MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

- OID этого класса 2.5.6.6
- Имя - ″person″
- Это структурный класс объектов
- Является наследником класса объектов ″top″
- Следующие атрибуты являются обязательными: cn, sn
- Следующие атрибуты являются дополнительными: userPassword, telephoneNumber, seeAlso, description

Дополнительная информация об изменении поддерживаемых сервером классов атрибутов приведена в разделе “Управление схемой” на стр. 168.

## Атрибут attributetypes

Атрибут attributetypes содержит список поддерживаемых сервером атрибутов. Каждое значение этого атрибута представляет собой отдельное определение атрибута. Определения атрибутов можно добавлять, удалять и изменять путем внесения соответствующих изменений в атрибут attributetypes записи cn=schema. Значения атрибута attributetypes имеют следующую грамматику, определенную в RFC 2252:

```
AttributeTypeDescription = "(" whsp
        numericoid whsp ; идентификатор типа атрибутов
        [ "NAME" qdescrs ] ; имя, применяемое в AttributeType
        [ "DESC" qdstring ] ; описание
        [ "OBSOLETE" whsp ]
        [ "SUP" woid ] ; производное от этого другого AttributeType
        [ "EQUALITY" woid ; имя правила соответствия
        [ "ORDERING" woid ; имя правила соответствия
        [ "SUBSTR" woid ] ; имя правила соответствия
```

```
        [ "SYNTAX" whsp noidlen whsp ]
        [ "SINGLE-VALUE" whsp ] ; по умолчанию с несколькими значениями
        [ "COLLECTIVE" whsp ] ; по умолчанию не набор
        [ "NO-USER-MODIFICATION" whsp ]; по умолчанию допускает изменение пользователем
        [ "USAGE" whsp AttributeUsage ]; по умолчанию userApplications
      whsp ")"

AttributeUsage =
        "userApplications" /
        "directoryOperation" /
        "distributedOperation" / ; совместное использование DSA
        "dSAOperation" ; зависит от DSA, значение зависит от сервера
```

В правилах соответствия и значениях синтаксиса должны применяться значения, определенные в следующих разделах:

- “Правила соответствия” на стр. 25
- “Синтаксис атрибута” на стр. 27

В схеме можно определять или изменять только атрибуты ″userApplications″. Атрибуты ″directoryOperation″, ″distributedOperation″ и ″dSAOperation″ определяются сервером и имеют специальное значение для работы сервера.

Например, атрибут ″description″ имеет следующее определение:

```
( 2.5.4.13 NAME 'description' DESC 'Attribute common to CIM and LDAP schema to provide lengthy
description of a directory object entry.' EQUALITY caseIgnoreMatch SUBSTR
caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
```

- OID - 2.5.4.13
- Имя - ″description″
- Синтаксис - 1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Дополнительная информация об изменении поддерживаемых сервером типов атрибутов приведена в разделе “Управление схемой” на стр. 168.

## Атрибут IBMAttributeTypes

Атрибут IBMAttributeTypes может применяться для определения информации схемы, выходящей за рамки стандарта LDAP версии 3. Значения IBMAttributeTypes должны соответствовать следующей грамматике:

```
IBMAttributeTypesDescription = "(" whsp
        numericoid whsp
      [ "DBNAME"   qdescrs ]            ; не более 2 имен (таблица, столбец)
      [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
      [ "LENGTH" wlen whsp ]            ; максимальная длина атрибута
      [ "EQUALITY" [ IBMwlen ] whsp ]   ; создать индекс для правила соответствия
      [ "ORDERING" [ IBMwlen ] whsp ]   ; создать индекс для правила соответствия
      [ "APPROX"   [ IBMwlen ] whsp ]   ; создать индекс для правила соответствия
      [ "SUBSTR"   [ IBMwlen ] whsp ]   ; создать индекс для правила соответствия
      [ "REVERSE"  [ IBMwlen ] whsp ]   ; обратный индекс для подстроки
      whsp ")"

   IBMAccessClass =
      "NORMAL"           / ; по умолчанию
      "SENSITIVE"        /
      "CRITICAL"         /
      "RESTRICTED"       /
      "SYSTEM"           /
      "OBJECT"

   IBMwlen = whsp len
```

**Numericoid**

Применяется для связи значения в attributetypes со значением в IBMAttributeTypes.

**DBNAME**

Вы можете указать не более 2 имен, если действительно задано 2 имени. Первым должно быть имя таблицы, применяемой для этого атрибута. Вторым именем должно быть имя столбца, применяемого для полного нормализованного значения атрибута в таблице. Если указано только одно имя, то оно используется и в качестве имени таблицы и в качестве имени столбца. Если имя DBNAME не указано, то в качестве имени будет использоваться первые семнадцать символов имени атрибута (которое должно быть уникальным). Имена таблиц базы данных и названия колонок не могут быть длиннее семнадцати символов.

**ACCESS-CLASS**

Класс доступа для этого типа атрибута. Если ACCESS-CLASS не указан, то по умолчанию применяется класс normal.

**LENGTH**

Максимальная длина этого атрибута. Длина указывается в байтах. На сервере каталогов предусмотрены средства указания длины атрибута. В значении attributetypes строка

```
( attr-oid ... SYNTAX syntax-oid{len} ... )
```

позволяет указать, что attributetype с oid attr-oid имеет заданную максимальную длину.

**EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE**

Если указан любой из этих атрибутов, то для связанно с ним правила соответствия создается индекс. Значение длины позволяет указать ширину индексируемого столбца. Для реализации нескольких правил соответствия применяется единый индекс. Если длина не указана пользователем, то сервер каталогов по умолчанию применяет длину 500 байт. В тех случаях, когда это имеет смысл сервер может также применять меньшую длину, чем запрошена пользователем. Например, если длина индекса превышает максимальную длину атрибута, то длина индекса игнорируется.

## Правила соответствия

Правила соответствия - это инструкции по сравнению строк во время поиска. Эти правила делятся на три категории:

- Равенство
- Упорядочение
- Подстрока

Сервер каталогов поддерживает правила соответствия равенства для всех синтаксисов, кроме двоичного. Для атрибутов двоичного синтаксиса сервер поддерживает только проверку наличия, например ″(jpegphoto=*)″. Для строковых синтаксисов IA5 String и Directory String определения атрибутов уточняются с учетом регистра символов. Например, для атрибута cn применяется правило соответствия caseIgnoreMatch, согласно которому значения ″John Doe″ и ″john doe″ будут равнозначными. В правилах соответствия без учета регистра символов строки сравниваются в верхнем регистре. Алгоритмы обработки символов верхнего регистра подходят не для всех локалей.

Сервер каталогов поддерживает правила соответствия подстрок для атрибутов строковых синтаксисов Directory String, IA5 String и Distinguished Name. В фильтрах поиска для индексации по подстроке несколько символов заменяются символом ″*″. Например, фильтр поиска ″(cn=*smith)″ соответствует всем строкам, оканчивающимся на ″smith″.

Правила соответствия упорядочения поддерживаются синтаксисами Integer, Directory String, IA5 String и Distinguished Name. В строковых синтаксисах упорядочение выполняется на основе простого упорядочения байт в строках кодовой страницы UTF-8. Если атрибут указан без учета регистра символов, то упорядочение выполняется в верхнем регистре. Как указывалось выше, алгоритмы обработки символов верхнего регистра подходят не для всех локалей.

В системе IBM Directory Server поиск по подстрокам и упорядочение заключают в себе соответствующие правила: все синтаксисы с поддержкой индексации по подстроке содержат неявное правило соответствия подстрок, а синтаксисы с поддержкой упорядочения - неявное правило упорядочения. Если атрибуты

| определены без учета регистра символов, то правила для них также работают без учета регистра.

| Правила соответствия равенства | | |
|---|---|---|
| **Правило соответствия** | **OID** | **Синтаксис** |
| caseExactIA5Match | 1.3.6.1.4.1.1466.109.114.1 | Синтаксис Directory String |
| caseExactMatch | 2.5.13.5 IA5 | Синтаксис String |
| caseIgnoreIA5Match | 1.3.6.1.4.1.1466.109.114.2 | Синтаксис IA5 String |
| caseIgnoreMatch | 2.5.13.2 | Синтаксис Directory String |
| distinguishedNameMatch | 2.5.13.1 | DN - отличительное имя |
| generalizedTimeMatch | 2.5.13.27 | Синтаксис Generalized Time |
| ibm-entryUuidMatch | 1.3.18.0.2.22.2 | Синтаксис Directory String |
| integerFirstComponentMatch | 2.5.13.29 | Синтаксис Integer - целое число |
| integerMatch | 2.5.13.14 | Синтаксис Integer - целое число |
| objectIdentifierFirstComponentMatch | 2.5.13.30 | Строка OID. OID - это строка, содержащая цифры (0-9) и десятичные точки (.). |
| objectIdentifierMatch | 2.5.13.0 | Строка OID. OID - это строка, содержащая цифры (0-9) и десятичные точки (.) |
| octetStringMatch | 2.5.13.17 | Синтаксис Directory String |
| telephoneNumberMatch | 2.5.13.20 | Синтаксис Telephone Number |
| uTCTimeMatch | 2.5.13.25 | Синтаксис UTC Time |

| Правила соответствия упорядочения | | |
|---|---|---|
| **Правило соответствия** | **OID** | **Синтаксис** |
| caseExactOrderingMatch | 2.5.13.6 | Синтаксис Directory String |
| caseIgnoreOrderingMatch | 2.5.13.3 | Синтаксис Directory String |
| distinguishedNameOrderingMatch | 1.3.18.0.2.4.405 | DN - отличительное имя |
| generalizedTimeOrderingMatch | 2.5.13.28 | Синтаксис Generalized Time |

| Правила соответствия подстроки | | |
|---|---|---|
| **Правило соответствия** | **OID** | **Синтаксис** |
| caseExactSubstringsMatch | 2.5.13.7 | Синтаксис Directory String |
| caseIgnoreSubstringsMatch | 2.5.13.4 | Синтаксис Directory String |
| telephoneNumberSubstringsMatch | 2.5.13.21 | Синтаксис Telephone Number |

**Примечание:** UTC-Time - это строковый формат времени, определенный в стандартах ASN.1. См. ISO 8601 и X680. Этот синтаксис применяется для хранения значений времени в формате UTC-Time. Обратитесь к разделу “Общее время и время UTC” на стр. 37.

## Правила индексации

Связанные с атрибутами правила индексации позволяют ускорить извлечение информации. Если указан только атрибут, то индексы не создаются. Сервер каталогов поддерживает следующие правила индексации:

- Равенство
- Упорядочение
- Приблизительное равенство

- Подстрока
- Обратное

**Указание правил индексации для атрибутов:** Указание правила индексации для атрибута позволяет управлять созданием и обслуживанием специальных индексов значений атрибутов. Таким образом удается существенно сократить время отклика при выполнении поиска с фильтрами, включающими эти атрибуты. Пять поддерживаемых правил индексации связаны с операциями, выполняемыми фильтром поиска.

**Равенство**

Применяется в следующих операциях поиска:

- equalityMatch '='

Например:

```
"cn = John Doe"
```

**Упорядочение**

Применяется в следующих операциях поиска:

- greaterOrEqual '>='
- lessOrEqual '<='

Например:

```
"sn >= Doe"
```

**Приблизительное равенство**

Применяется в следующих операциях поиска:

- approxMatch '~='

Например:

```
"sn ~= doe"
```

**Подстрока**

Применяется в операциях поиска с использованием синтаксиса подстроки:

- substring '*'

Например:

```
"sn = McC*"
"cn = J*Doe"
```

**Обратный индекс**

Применяется в следующих операциях поиска:

- '*' substring

Например:

```
"sn = *baugh"
```

Для всех атрибутов, которые могут применяться в фильтрах поиска, рекомендуется указывать как минимум индексацию с учетом равенства.

## Синтаксис атрибута

Синтаксис атрибута определяет допустимые значения для этого атрибута. С помощью определения синтаксиса сервер проверяет данные и определяет способ сравнения значений. Например, атрибут ″Boolean″ может содержать только значение ″TRUE″ или ″FALSE″.

Атрибуты могут быть определены как имеющие одно значение или имеющие несколько значений. Если атрибут имеет несколько значений, то эти значения не упорядочиваются, поэтому приложение не должно полагаться на то, что значения атрибута будут возвращены в каком-либо определенном порядке. Если необходимо использовать упорядоченный набор значений, то можно разместить весь список значений в одном значении атрибута:

```
preferences: 1st-pref 2nd-pref 3rd-pref
```

Можно также включить в значение порядковый номер этого значения в последовательности, например:

```
preferences: 2 yyy
preferences: 1 xxx
preferences: 3 zzz
```

Атрибуты с несколькими значениями полезны в тех случаях, когда обращение к записи может осуществляться по нескольким именам. Например, несколько значений имеет атрибут cn (общее имя). Запись может быть определена следующим образом:

```
dn: cn=John Smith,o=My Company,c=US
objectclass: inetorgperson
sn: Smith
cn: John Smith
cn: Jack Smith
cn: Johnny Smith
```

Такое определение позволяет получить одинаковую информацию при поиске как по строке `John Smith`, так и по строке `Jack Smith`.

Двоичные атрибуты могут содержать произвольную последовательность данных, например, фотографию в формате JPEG. По таким атрибутам поиск выполнять нельзя.

Булевские атрибуты содержат строку `TRUE` или `FALSE`.

Атрибуты DN содержат отличительные имена LDAP. Их значения не обязательно должны содержать DN существующих записей, но формат этих значений должен соответствовать синтаксису DN.

Строковые атрибуты типа Directory String содержат строки текста в кодировке UTF-8. Атрибут может учитывать или не учитывать регистр символов при поиске (в соответствии с определенным для этого атрибута правилом соответствия), однако значение всегда возвращается в том виде, в котором оно было первоначально введено.

Атрибуты типа Generalized Time содержат строковое представление даты (как до, так и после 2000 года) и времени GMT с возможностью указания часового пояса. Дополнительные сведения об этих значениях приведены в разделе “Общее время и время UTC” на стр. 37.

Строковые атрибуты IA5 String содержат строки текста в кодировке IA5 (7-разрядная кодировка US ASCII). Атрибут может учитывать или не учитывать регистр символов при поиске (в соответствии с определенным для этого атрибута правилом соответствия), однако значение всегда возвращается в том виде, в котором оно было первоначально введено. Строки типа IA5 String поддерживают применение символов подстановки при поиске.

Целочисленные атрибуты Integer содержат текстовое представление цифрового значения. Например: `0` или `1000`. Значения для атрибутов синтаксиса Integer должны лежать в диапазоне от -2147483648 до 2147483647.

Атрибуты телефонного номера Telephone Number содержат текстовое представление телефонного номера. Сервер каталогов не требует применения какого-либо определенного синтаксиса при указании этих значений. Таким образом, допустимыми будут все следующие значения: `(555)555-5555`, `555.555.5555` и `+1 43 555 555 5555`.

Атрибуты мирового времени UTC Time используют устаревший формат представления даты и времени, применявшийся до 2000 года. Более подробные сведения приведены в разделе “Общее время и время UTC” на стр. 37.

В схеме каталога синтаксис атрибута определяется с помощью объектных идентификаторов (OID), присваиваемых каждому синтаксису. Синтаксисы, поддерживаемые сервером каталогов, и соответствующие им OID приведены в таблице.

| Синтаксис | OID |
|---|---|
| Синтаксис Attribute Type Description | 1.3.6.1.4.1.1466.115.121.1.3 |
| Binary - octet string | 1.3.6.1.4.1.1466.115.121.1.5 |
| Boolean - TRUE/FALSE | 1.3.6.1.4.1.1466.115.121.1.7 |
| Синтаксис Directory String | 1.3.6.1.4.1.1466.115.121.1.15 |
| Синтаксис DIT Content Rule Description | 1.3.6.1.4.1.1466.115.121.1.16 |
| Синтаксис DITStructure Rule Description | 1.3.6.1.4.1.1466.115.121.1.17 |
| DN - отличительное имя | 1.3.6.1.4.1.1466.115.121.1.12 |
| Синтаксис Generalized Time | 1.3.6.1.4.1.1466.115.121.1.24 |
| Синтаксис IA5 String | 1.3.6.1.4.1.1466.115.121.1.26 |
| Описание типа атрибута IBM | 1.3.18.0.2.8.1 |
| Синтаксис Integer - целое число | 1.3.6.1.4.1.1466.115.121.1.27 |
| Синтаксис LDAP Syntax Description | 1.3.6.1.4.1.1466.115.121.1.54 |
| Matching Rule Description | 1.3.6.1.4.1.1466.115.121.1.30 |
| Matching Rule Use Description | 1.3.6.1.4.1.1466.115.121.1.31 |
| Name Form Description | 1.3.6.1.4.1.1466.115.121.1.35 |
| Синтаксис Object Class Description | 1.3.6.1.4.1.1466.115.121.1.37 |
| Строка OID. OID - это строка, содержащая цифры (0-9) и десятичные точки (.). Обратитесь к разделу “Идентификатор объекта (OID)”. | 1.3.6.1.4.1.1466.115.121.1.38 |
| Синтаксис Telephone Number | 1.3.6.1.4.1.1466.115.121.1.50 |
| Синтаксис UTC Time. UTC-Time - это строковый формат времени, определенный в стандартах ASN.1. См. ISO 8601 и X680. Этот синтаксис применяется для хранения значений времени в формате UTC-Time. Обратитесь к разделу “Общее время и время UTC” на стр. 37. | 1.3.6.1.4.1.1466.115.121.1.53 |

## Идентификатор объекта (OID)

Идентификатор объекта (OID) - это строка или последовательность десятичных цифр, однозначно идентифицирующая объект. Такими объектами обычно являются классы объектов или атрибуты.

Если вы не можете выбрать OID, то укажите имя класса или атрибута и добавьте к нему символы **-oid**. Например, если вы создали атрибут tempID, то в качестве OID можно указать значение **tempID-oid**.

Крайне важно, чтобы частные OID присваивались соответствующими официальными организациями. Существует два способа получения официальных OID:

- Зарегистрировать объекты в официальной организации. Такая стратегия может быть удобной, например, при необходимости создания небольшого числа OID.
- Получить в официальной организации ветвь (т.е. поддерево дерева OID) и присвоить собственные OID. Такая стратегия, возможно, окажется предпочтительной в случае необходимости создания множества OID или нестабильности правил присвоения OID.

Американский национальный институт стандартов (ANSI) является в США официальной организацией, осуществляющей регистрацию названий организаций в рамках глобальной программы регистрации, реализуемой Международной организацией по стандартизации (ISO) и Международным союзом телекоммуникаций (ITU). Дополнительную информацию о регистрации названий организаций можно найти на Web-сайте ANSI (www.ansi.org). Ветвь OID ANSI для организаций - 2.16.840.1. При создании новой ветви OID ANSI присваивает номер (NEWNUM): 2.16.840.1.NEWNUM.

В большинстве стран и регионов поддержку реестров OID осуществляют национальные организации по стандартизации. Как и в случае ветви ANSI, обычно это ветви, относящиеся к OID 2.16. Возможно, для поиска официальной организации, осуществляющей регистрацию OID в заданной стране или регионе придется приложить усилия. Действующая в вашей стране национальная организация по стандартизации может быть членом ISO. Названия и контактную информацию о членах ISO можно найти на Web-сайте ISO  (www.iso.ch).

Организация по присвоению идентификаторов Internet (IANA) присваивает номера частным предприятиям, представляющие собой OID ветви 1.3.6.1.4.1. IANA присваивает вновь создаваемому OID номер (NEWNUM) следующим образом: 1.3.6.1.4.1.NEWNUM. Такие номера можно получить на Web-сайте IANA  (www.iana.org).

После присвоения OID вашей организации вы сможете определять собственные OID, добавляя их в конец выделенного вам OID. Допустим, например, что вашей организации присвоен OID 1.1.1. Другим организациям не может быть присвоен OID, начинающийся с символов ″1.1.1″. Вы можете создать диапазон для LDAP, добавив суффикс ″.1″, и получив в итоге OID 1.1.1.1. После этого можно продолжить построение иерархии, выделив диапазон для классов объектов (1.1.1.1.1), типов атрибутов (1.1.1.1.2) и т.д.. В результате атрибуту ″foo″ можно присвоить, например, OID 1.1.1.1.2.34.

## Записи подсхемы

Для сервера существует одна запись подсхемы. Все записи каталога имеют неявный тип атрибута subschemaSubentry. Значение типа атрибута subschemaSubentry представляет собой DN записи подсхемы, соответствующее записи. Все записи, хранящиеся на одном сервере, используют одну и ту же запись подсхемы, а их тип атрибута subschemaSubentry имеет одно и то же значение. Запись подсхемы имеет неизменяемое DN ’cn=schema’.

Запись подсхемы относится к классам объектов ’top’, ’subschema’ и ’IBMsubschema’. Класс объектов ’IBMsubschema’ не имеет атрибутов MUST и имеет один атрибут типа MAY (’IBMattributeTypes’).

## Класс объектов IBMsubschema

Класс объектов IBMsubschema применяется в записях подсхемы только следующим образом:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'IBM specific object class that stores all the attributes and object classes for a given directory
 server.'
SUP 'subschema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

## Запросы к схеме

Для запроса записи подсхемы можно использовать API ldap_search(), как показано в следующем примере:

```
DN           : "cn=schema"
search scope : base
filter       : objectclass=subschema or objectclass=*
```

Этот пример позволяет получить всю схему. Для получения всех значений выбранных типов атрибутов можно воспользоваться параметром attrs в ldap_search. Получить только отдельное значение определенного типа атрибутов нельзя.

Дополнительная информация об API ldap_search приведена в разделе “API сервера каталогов”.

## Динамическая схема

Для динамического изменения схемы можно воспользоваться API ldap_modify с DN ″cn=schema″. За один раз можно добавить, удалить или заменить только одну запись схемы (например, тип атрибутов или класс объектов).

Для удаления записи схемы укажите определяющий эту запись атрибут схемы (objectclasses или attributetypes), а в качестве значения - OID в скобках. Пример удаления атрибута с OID <attr-oid>:

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: ( <attr-oid> )
```

Вы также можете указать полное описание. В любом случае для поиска удаляемой записи схемы применяется правило соответствия objectIdentifierFirstComponentMatch.

Для добавления или замены записи схемы нужно ОБЯЗАТЕЛЬНО указать определение LDAP версии 3 и можно ДОПОЛНИТЕЛЬНО указать определение IBM. В любом случае необходимо указать определения только те записей схемы, к которым должна быть применена операция.

Пример удаления типа атрибута ’cn’ (OID 2.5.4.3) с помощью ldap_modify():

```
LDAPMod  attr;
LDAPMod *attrs[] = { &attr, NULL };
char    *vals [] = { "( 2.5.4.3 )", NULL };
attr.mod_op      = LDAP_MOD_DELETE;
attr.mod_type    = "attributeTypes";
attr.mod_values  = vals;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

Пример добавления нового типа атрибута с OID 20.20.20, являющегося наследником атрибута ″name″ с длиной 20 символов:

```
char    *vals1[] = { "( 20.20.20 NAME 'bar' SUP name )" NULL };
char    *vals2[] = { "( 20.20.20 LENGTH 20 )", NULL };
LDAPMod  attr1;
LDAPMod  attr2;
LDAPMod *attrs[] = { &attr1, &attr2, NULL };
attr1.mod_op = LDAP_MOD_ADD;
attr1.mod_type = "attributeTypes";
attr1.mod_values = vals1;
attr2.mod_op = LDAP_MOD_ADD;
attr2.mod_type = "IBMattributeTypes";
attr2.mod_values = vals2;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

В формате LDIF данный пример выглядел бы следующим образом:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 20.20.20 NAME 'bar' SUP name )
-
add:ibmattributetypes
ibmattributetypes: (20.20.20 LENGTH 20)
```

**Управление доступом**

Динамическое изменение схемы может выполняться только поставщиком копирования или DN администратора.

**Копирование**

При динамическом изменении схемы все вносимые изменения копируются

## Запрещенные изменения схемы

Не все изменения схемы являются разрешенными. Существуют следующие ограничения:

- Все изменения схемы не должны приводить к выходу схемы из согласованного состояния.

- Нельзя удалить тип атрибута, являющийся родительским для другого типа атрибута. Нельзя удалить тип атрибута, указанный для класса объектов как ″MAY″ или ″MUST″.
- Нельзя удалить класс объектов, являющийся родительским для другого класса объектов.
- Нельзя добавить типы атрибутов или классы объектов, ссылающиеся на несуществующие объекты (например, варианты синтаксиса или классы объектов).
- Существующие типы атрибутов и классы объектов нельзя изменять таким образом, чтобы в конечном состоянии они ссылались на несуществующие объекты (например, варианты синтаксиса или классы объектов).
- В определении IBMattributestype новых атрибутов нельзя указывать существующие таблицы базы данных.
- Нельзя удалить атрибуты, используемые в существующих записях каталогов.
- Нельзя изменить длину и синтаксис атрибута.
- Нельзя изменить таблицу базы данных или столбец, связанные с атрибутом.
- Нельзя удалить атрибуты, используемые в определениях существующих классов объектов.
- Нельзя удалить классы объектов, используемые в существующих записях каталогов.

Нельзя вносить в схему изменения, влияющие на работу сервера. Следующие определения схемы являются обязательными для сервера каталогов. Изменять их нельзя.

**Классы объектов:**

- accessGroup
- accessRole
- alias
- os400-usrprf
- referral
- replicaObject
- top

**Атрибуты:**

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName
- createTimestamp
- creatorsName
- description
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- name
- o, organizationName, organization

- objectClass
- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut
- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib
- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc
- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd
- os400-kbdbuf
- os400-langid
- os400-lclpwdmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale
- os400-maxstg
- os400-msgq
- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv

- os400-setjobatr
- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrpprf
- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

**Варианты синтаксиса:**
Все

**Правила соответствия:**
Все

## Проверка схемы

При инициализации сервера файлы схемы считываются и проверяется их согласованность и правильность. В случае обнаружения несоответствий или ошибок сервер не инициализируется и выдается сообщение об ошибке. При динамическом изменении схемы результирующая схема также проверяется на согласованность и правильность. При обнаружении ошибок или несоответствий изменение не выполняется и возвращается сообщение об ошибке. Некоторые проверки выполняются в рамках грамматики (например, тип атрибута может иметь только один родительский тип, а класс объектов может иметь несколько родительских классов).

Для типов атрибутов выполняется проверка следующих требований:

- Два разных типа атрибутов не могут иметь одинаковые имена или OID.
- В иерархии наследования типов атрибутов не должна быть замкнутых циклов.
- Должен быть определен родительский тип атрибута, однако его определение может быть указано позже или в отдельном файле.
- Если тип атрибута является дочерним типом для другого типа, то для обоих типов должно быть указано одинаковое значение USAGE.

- С каждым типом атрибутов связан непосредственно определенный или унаследованный синтаксис.
- Метка NO-USER-MODIFICATION может присваиваться только операционным атрибутам.

Для классов объектов выполняется проверка следующих требований:
- Два разных класса объектов не могут иметь одинаковые имена или OID.
- В иерархии наследования классов объектов не должна быть замкнутых циклов.
- Должен быть определен родительский класс класса объектов, однако его определение может быть указано позже или в отдельном файле.
- Для класса объектов должны быть определены типы атрибутов ″MUST″ и ″MAY″, однако их определения могут быть указаны позже или в отдельном файле.
- Каждый структурированный класс объектов является прямым или косвенным потомком класса объектов top.
- Если у абстрактного типа объектов есть родительские классы, то эти классы также должны быть абстрактными.

**Проверка записи на соответствие схеме**

При добавлении или изменении записи с помощью операции LDAP запись проверяется на соответствие схеме. По умолчанию выполняются все проверки, перечисленные в этом разделе. Однако, путем изменения уровня проверки схемы, вы можете выборочно отключить некоторые проверки. Это можно сделать с помощью Навигатора iSeries, изменив значение поля **Проверка схемы** на странице **База данных/Суффиксы** окна свойств сервера каталогов. Дополнительная информация об атрибутах конфигурации схемы приведена в разделе “Схема конфигурации сервера каталогов” на стр. 236.

При проверке соответствия записи схеме проверяется выполнение следующих условий:

**Классы объектов:**
- Должны иметь по крайней мере одно значение с типом атрибута ″objectClass″.
- Могут иметь любое (в том числе нулевое) количество дополнительных классов объектов. Это не проверка, а просто уточнение. Отключить эту возможность нельзя.
- Могут иметь иметь любое количество абстрактных классов объектов, однако только в результате наследования классов. Это значит, что для каждого абстрактного класса объектов записи существует также структурный или вспомогательный класс объектов, непосредственно или косвенно наследующий от этого абстрактного класса.
- Должны иметь по крайней мере один структурный класс объектов.
- Должны иметь ровно один непосредственный или базовый структурный класс объектов. Это значит, что среди всех структурных классов объектов записи все эти классы должны быть родительскими только для одного класса. Наиболее конкретный производный класс объекта называется ″непосредственным″ или ″базовым структурным″ классом объекта или просто ″структурным″ классом объекта записи.
- Нельзя изменить непосредственный структурный класс объекта (с помощью ldap_modify).
- Для каждого класса объектов записи вычисляется набор всех его непосредственных и прямых родительских классов; если какой-либо из этих классов не указан вместе с записью, то он автоматически добавляется.
- Если включен уровень проверки схемы **Версия 3 (строго)**, то должны быть указаны все структурные родительские классы. Например, для создания класса объектов inetorgperson должны быть указаны следующие классы объектов: person, organizationalperson и inetorgperson.

**Правильность типов атрибутов для записи определяется следующим образом:**
- Набор типов атрибутов MUST для записи вычисляется как объединение наборов типов атрибутов MUST для всех ее классов объектов, включая неявно унаследованные классы. Если набор типов атрибутов MUST записи не является подмножеством набора типов атрибутов, содержащихся в записи, то запись отклоняется.

- Набор типов атрибутов MAY для записи вычисляется как объединение наборов типов атрибутов MAY для всех ее классов объектов, включая неявно унаследованные классы. Если набор типов атрибутов, содержащихся в записи, не является подмножеством объединения наборов типов атрибутов MUST и MAY записи, то запись отклоняется.
- Если какой-либо из определенных для записи типов атрибутов помечен как NO-USER-MODIFICATION, то запись отклоняется.

**Правильность значений типов атрибутов для записи определяется следующим образом:**

- Если какой-либо из содержащихся в записи типов атрибутов является однозначным, но запись содержит несколько значений, то такая запись отклоняется.
- Если синтаксис значения какого-либо из содержащихся в записи типов атрибутов не соответствует синтаксису этого атрибута, то такая запись отклоняется.
- Если длина значения любого из атрибутов любого типа больше, чем максимальная длина этого типа атрибутов, то такая запись отклоняется.

**Правильность DN проверяется следующим образом:**

- Проверяется соответствие синтаксиса формату BNF для DistinguishedNames. В случае несоответствия запись отклоняется.
- Проверяется, все ли типы атрибутов в RDN допустимы для этой записи.
- Проверяется, присутствуют ли в записи значения типов атрибутов, применяемые в RDN.

## Совместимость с iPlanet

Применяемый сервером каталогов анализатор допускает указание значений атрибутов для типов атрибутов схемы (objectClasses и attributeTypes) с применением грамматики iPlanet. Например, descrs и numeric-oids можно указать в одиночных кавычках (как qdescrs). Однако информацию схемы всегда можно получить с помощью ldap_search. После внесения в файл первого динамического изменения значения атрибута (с помощью ldap_modify) весь файл заменяется на файл, в котором значения атрибутов соответствуют спецификации сервера каталогов. Поскольку для файлов и для запросов ldap_modify применяется один и тот же анализатор, то операция ldap_modify, в которой для значений атрибутов применяется грамматика iPlanet, также будет выполнена правильно.

При обращении к записи подсхемы на сервере iPlanet полученная запись может иметь несколько значений, связанных с заданным OID. Например, если какой-либо тип атрибутов имеет два имени (например, ’cn’ и ’commonName’), то описание этого типа атрибутов предоставляется дважды - по одному для каждого имени. сервер каталогов может работать со схемой, в которой описание одного типа атрибутов или класса объектов присутствует несколько раз с одним и тем же описанием (за исключением NAME и DESCR). Однако, когда сервер каталогов публикует схему, он указывает одно описание такого типа атрибутов, в котором перечислены все имена (первым указывается краткое имя). Пример описания атрибута общего имени сервером iPlanet:

```
( 2.5.4.3 NAME 'cn'
  DESC 'Standard Attribute'
   SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

( 2.5.4.3 NAME 'commonName'
  DESC 'Standard Attribute, alias for cn'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Пример описания этого же атрибута сервером каталогов:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

Сервер каталогов поддерживает подтипы. Если вы не хотите, чтобы ’cn’ был подтипом типа name (что является отклонением от стандарта), то можно указать следующее объявление:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )
     DESC 'Standard Attribute'
     SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Первое имя в списке (’cn’) - это предпочитаемое или краткое имя, а все имена, указанные после ’cn’, - это альтернативные имена. С этого момента в схеме или при добавлении записей в каталог можно использовать любые из строк ’2.3.4.3’, ’cn’ и ’commonName’ (а также их вариации, не учитывающие регистр символов).

## Общее время и время UTC

Существуют разные способы обозначения значений дат и времени. Например четвертое февраля 1999 года может быть обозначено следующим образом:

```
2/4/99
4/2/99
99/2/4
4.2.1999
04-FEB-1999
```

и множеством других способов.

На сервере каталогов представление значений времени стандартизировано и серверы LDAP поддерживают два варианта синтаксиса:

- Синтаксис общего времени (Generalized Time), использующий следующий формат:

  ```
  ГГГГММДДЧЧммСС[.|,доли][(+|-ЧЧмм)|Z]
  ```

  Этот формат включает 4 цифры года, по 2 цифры для обозначения месяца, дня, часов, минут и секунд, а также необязательное обозначение долей секунды. Если никаких дополнений нет, то считается, что дата и время заданы в локальном часовом поясе. Для указания того, что применяется значение мирового времени, необходимо добавить символ Z в верхнем регистре. Например:

  ```
  "19991106210627.3"
  ```

  это локальное время, соответствующее 21 часу, 6 минутам и 27,3 секунды 6 ноября 1999 года.

  ```
  "19991106210627.3Z"
  ```

  это мировое время.

  ```
  "19991106210627.3-0500"
  ```

  это локальное время, как и в первом примере, однако оно отстает от мирового времени на 5 часов.

  При указании дробной части секунды обязательно должна быть указана точка или запятая. Для указания смещения часового пояса перед значением часов и минут должен присутствовать символ ’+’ или ’-’.

- Синтаксис мирового времени (Universal Time), использующий следующий формат:

  ```
  ГГММДДЧЧмм[сс][(+ | -)ЧЧмм)|Z]
  ```

  Этот формат включает по 2 цифры для обозначения года, месяца, дня, часов и минут, а также необязательное обозначение долей секунды. Как и в случае GeneralizedTime, можно указать смещение относительно мирового времени. Например, если локальное время - утро 2 января 1999 года, а мировое время - полдень 2 января 1999 года, то значение UTCTime можно указать как

  ```
  "9901021200Z"
  или "9901020700-0500"
  ```

  Если локальное время - утро 2 января 2001 года, а мировое время - полдень 2 января 2001 года, то значение UTCTime можно указать как

  ```
  "0101021200Z"
  или "0101020700-0500"
  ```

  UTCTime содержит только 2 цифры для обозначения года, поэтому применять этот формат не рекомендуется.

Поддерживаются правила соответствия generalizedTimeMatch для равенства и generalizedTimeOrderingMatch для неравенства. Поиск по подстроке не поддерживается. Например, допускаются следующие фильтры:

```
generalized-timestamp-attribute=199910061030
utc-timestamp-attribute>=991006
generalized-timestamp-attribute=*
```

Следующие фильтры недопустимы:

```
generalized-timestamp-attribute=1999*
utc-timestamp-attribute>=*1010
```

## Публикация

i5/OS предоставляет системе возможность публикации некоторых типов информации в каталоге LDAP. Это значит, что система создает и обновляет записи LDAP, соответствующие различным типам данных.

В i5/OS предусмотрена встроенная поддержка публикации следующей информации на сервере LDAP:

**Пользователи**

Если в операционной системе разрешена публикация информации о пользователях, то на сервер каталогов автоматически экспортируются записи из системного каталога рассылки. Для этого применяется API QGLDSSDD. Эта функция синхронизирует данные каталога LDAP с данными системного каталога рассылки. Информация об API QGLDSSDD приведена в разделе “API сервера каталогов” в главе Программирование.

Публикация информации о пользователях полезна в ситуациях, когда необходимо обеспечить возможность поиска с помощью LDAP записей системного каталога рассылки (например, для предоставления доступа к адресной книге LDAP почтовым клиентам POP3 с поддержкой LDAP, таким как Netscape Communicator или Microsoft Outlook Express).

Опубликованная информация о пользователях может также применяться для поддержки идентификации LDAP некоторых пользователей из системного каталога рассылки и других пользователей, добавленных в каталог другими средствами. Опубликованный пользователь имеет атрибут uid, в котором указан пользовательский профайл, и не имеет атрибута userPassword. При получении запроса на подключение для такой записи сервер запрашивает средства защиты операционной системы и проверяет, являются ли значения uid и пароля допустимым именем профайла и паролем пользователя. Этой функцией следует воспользоваться в том случае, если вы хотите применять идентификацию LDAP и хотите, чтобы существующих пользователей можно было идентифицировать с помощью их паролей операционной системы, а пользователей других операционных систем (отличных от i5/OS) можно было добавлять в каталог вручную.

Публиковать пользователей можно и другим способом: брать записи из существующего контрольного списка HTTP и создавать на сервере каталогов соответствующие записи LDAP. Это можно сделать с помощью API QGLDPUBVL. Этот API создает записи каталогов inetOrgPerson с паролями, связанные с записью исходного контрольного списка. API можно запустить один раз, а можно запланировать, чтобы он периодически проверял наличие новых записей и добавлял их на сервер каталогов.

**Примечание:** Этот API поддерживает только записи контрольного списка, созданные для сервера HTTP на основе Apache. Существующие записи на сервере каталогов обновлены не будут. Также не будут обнаружены пользователи, удаленные из контрольного списка.

Как только пользователь будет добавлен в каталог, он получит возможность идентифицироваться в приложениях с проверкой сертификатов и в приложениях с поддержкой идентификации LDAP. Дополнительные сведения об API QGLDPUBVL приведены в разделе Программирование руководства “API сервера каталогов”.

**Системная информация**

Если в операционной системе настроена публикация системной информации на сервере каталогов, то публикуются следующие типы информации:

- Основная информация о компьютере и о выпуске операционной системы.
- Вы также можете выбрать для публикации один или несколько принтеров. В этом случае система будет автоматически синхронизировать каталог LDAP в соответствии с изменениями, вносимыми в системные принтеры.

Допускается публикация следующей информации о принтерах:

- Расположение
- Скорость печати в страницах в минуту
- Поддержка двухсторонней печати и цвета
- Тип и модель
- Описание

Эта информация берется из описания устройства в системе. Пользователи могут руководствоваться этой информацией при выборе принтера. Первоначально информация публикуется в тот момент, когда для принтера включается публикация. Затем, по мере того, как останавливается или запускается загрузчик принтера или изменяется описание устройства, эта информация обновляется.

**Общие принтеры**

При настройке в операционной системе публикации общих принтеров информация о выбранных общих принтерах iSeries NetServer будет публиковаться на настроенном сервере Active Directory. Публикация общих принтеров на сервере Active Directory позволяет пользователям добавлять принтеры iSeries на рабочий стол Windows 2000 с помощью мастера добавления принтера Windows 2000. Для этого при работе с мастером нужно выбрать принтер в каталоге Active Directory Windows 2000. Информация об общих принтерах должна публиковаться на сервере каталогов, поддерживающем схему Active Directory фирмы Microsoft.

**TCP/IP Quality of Service**

На сервере TCP/IP Quality of Service (QOS) можно настроить применение общей стратегии QOS, определенной в каталоге LDAP с помощью схемы IBM. Агент публикации TCP/IP QOS применяется сервером QOS для считывания информации о стратегии; он определяет сервер, идентификационную информацию, а также размещение хранящейся в каталоге информации о стратегии.

Путем определения дополнительных агентов публикации и применения API публикации в каталоге вы также можете создать приложение для публикации или поиска в LDAP других типов информации. Дополнительные сведения приведены в “Публикация информации на сервере каталогов” на стр. 98 и в разделе Программирование руководстваAPI сервера каталогов.

## Копирование

Копирование - это технология, применяемая серверами каталогов для повышения производительности и надежности. Процесс копирования позволяет синхронизировать данные, хранящиеся в нескольких каталогах.

Информация об управлении копированием приведена в разделе “Управление копированием” на стр. 140. Дополнительные сведения о копировании можно найти в следующих разделах:

- “Обзор функции копирования” на стр. 40
- “Терминология функции копирования” на стр. 43
- “Соглашение о копировании” на стр. 44
- “Хранение информации о копировании на сервере” на стр. 45
- “Особенности защиты информации о копировании” на стр. 45

• “Копирование в средах высокой готовности” на стр. 46

## Обзор функции копирования

Копирование позволяет достичь двух основных преимуществ:

- Избыточность информации - на серверах-копиях хранятся резервные копии данных, полученных с серверов-поставщиков.
- Ускорение поиска - запросы на поиск можно выполнять не на одном сервере, а распределить между несколькими серверами с одинаковой информацией. Такой подход позволяет сократить время отклика при обработке запросов.

Отдельные записи каталога идентифицируются как корневые записи копируемых поддеревьев путем добавления к ним класса объектов ibm-replicationContext. Каждое поддерево копируется независимо. Копирование поддерева продолжается по дереву информации каталога (DIT) до тех пор, пока не будут достигнуты листья дерева или другие копируемые поддеревья. После корневого уровня копируемого поддерева добавляются записи с информацией о топологии копирования. Это одна или несколько записей групп копирования, в которых создаются подзаписи копий. С каждой подзаписью копии связано соглашение о копирование, указывающее серверы, которым будет предоставляться копируемая информация, а также идентификационные данные и информация о планировании.

С помощью функции копирования изменение, внесенное в одном каталоге, распространяется во все остальные каталоги. Фактически, изменение, внесенное в одном каталоге, применяется во множестве других каталогов. IBM Directory поддерживает расширенную модель копирования с главными и подчиненными серверами. Поддерживаются следующие новые топологии копирования:

- Копирование поддеревьев дерева информации каталога (DIT) на указанные серверы
- Многоуровневое копирование, называемое также каскадным копированием
- Назначение роли сервера (главный или подчиненный) для поддерева
- Организация нескольких главных серверов (копирование на равноправных серверах).
- Сетевое копирование с помощью шлюзов.

Преимущество копирования поддеревьев заключается в том, что нет необходимости копировать весь каталог целиком. Копия может воспроизводить лишь часть каталога, т.е. поддерево.

В расширенной модели концепция главного сервера и сервера-копии изменилась. Эти термины теперь применяются не к серверам, а к ролям, которые выполняют серверы по отношению к конкретному копируемому поддереву. Сервер может выполнять роль главного сервера для одних поддеревьев и роль копии для других. Термин Главный сервер относится к серверу, который принимает запросы клиентов на обновление копируемого поддерева. Термин Сервер-копия относится к серверу, который принимает запросы на обновление только от других серверов, являющихся поставщиками копируемого поддерева.

Функцией определяются следующие типы серверов: *главный/равноправный*, *каскадный*, *сервер-шлюз* и *сервер-копия*.

*Таблица 1. Роли серверов*

| Каталог | Описание |
|---|---|
| Главный/ равноправный | Главный/равноправный сервер содержит информацию главного каталога, с которого обновления передаются на серверы-копии. Все изменения вносятся на главном сервере, который обеспечивает передачу этих изменений на серверы-копии.<br><br>Может существовать несколько серверов, выполняющих функции главного сервера информации каталога, причем каждый из этих главных серверов должен обеспечивать обновление других главных серверов и серверов-копий. Такая конфигурация называется копированием равноправных серверов. Копирование равноправных серверов позволяет повысить производительность и надежность. Повышение производительности обеспечивается за счет обработки обновлений локальным сервером в крупной распределенной сети. Повышение надежности обеспечивается за счет наличия резервного главного сервера, который может вступить в работу сразу после сбоя основного главного сервера.<br><br>**Примечания:**<br>1. Главные серверы копируют все обновления, полученные от клиентов, но не копируют обновления, полученные от других главных серверов.<br>2. Обновления, внесенные в запись несколькими серверами, могут привести к рассогласованию данных каталога, поскольку механизм разрешения конфликтов не предусмотрен. |
| Каскадное копирование (пересылка) | Каскадный сервер - это сервер-копия, который копирует все полученные изменения. Эта конфигурация отличается от конфигурации с главным/равноправным сервером, который копирует только изменения, вносимые подключенными к нему клиентами. Каскадный сервер может снизить нагрузку на главные серверы в сети с большим количеством разнесенных серверов-копий. |
| Шлюз | Шлюзовое копирование собирает и распределяет информацию по сети с помощью серверов-шлюзов. Основное преимущество шлюзового копирования - уменьшение нагрузки сети. |
| Сервер-копия (только для чтения) | Сервер-копия - это дополнительный сервер, содержащий копию информации каталога. Серверы-копии копируют данные главных серверов (или поддеревьев, копиями которых они являются). Сервер-копия представляет собой резервную копию поддерева. |

В случае сбоя копирования операция повторяется даже в том случае, если главный-сервер перезапущен. Для проверки ошибок копирования можно воспользоваться окном управления очередями в Web-инструменте администрирования каталога.

Вы можете запросить внесение обновлений на сервере-копии, однако фактически запрос на обновление будет передан главному серверу путем возврата перенаправления клиенту. В случае успешного обновления главный сервер передаст обновление серверам-копиям. До тех пор, пока главный сервер не завершит обработку обновления, внесенное изменение не будет отражено на сервере-копии, на котором оно первоначально было запрошено. Изменения копируются в том порядке, в котором они были внесены на главном сервере.

Если вы больше не используете сервер-копию, то необходимо удалить с сервера-поставщика соглашение о копировании. Если этого не сделать, то сервер будет помещать в очередь все обновления и неэффективно использовать память каталога. Кроме того, поставщик будет продолжать пытаться обратиться к отсутствующему серверу-копии и передать ему данные.

### Шлюзовое копирование

Шлюзовое копирование собирает и распределяет информацию по сети с помощью серверов-шлюзов. Основное преимущество шлюзового копирования - уменьшение нагрузки сети. Серверы-шлюзы должны быть главными (с возможностью записи).

На рисунке ниже показана работа шлюзового копирования:
Сеть копирования на рисунке содержит три узла копирования, в каждом из которых есть сервер-шлюз.

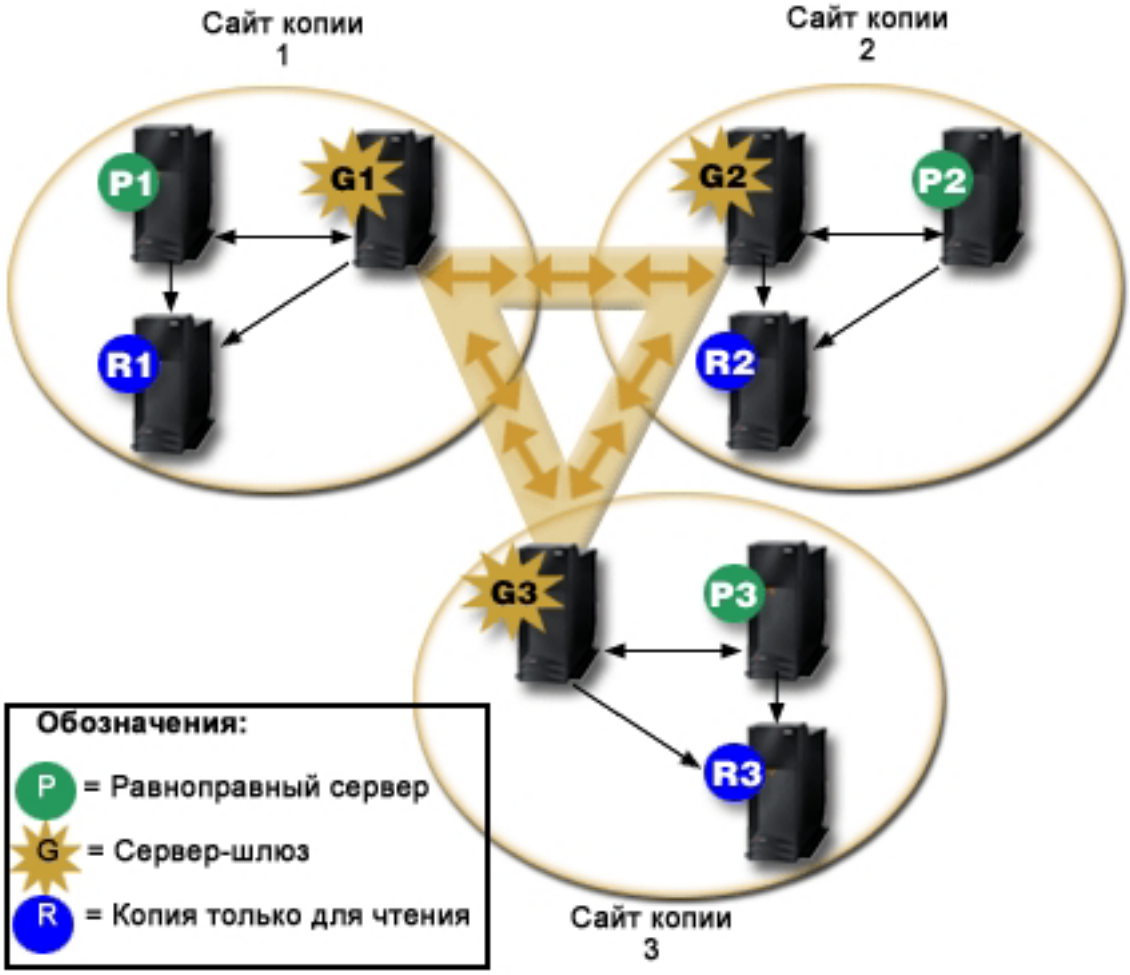



*Рисунок 2. Сеть копирования с серверами-шлюзами*

Сервер-шлюз собирает обновления копирования от главных/равноправных серверов узла копирования, в котором он находится, и рассылает их всем остальным серверам-шлюзам сети копирования. Также он собирает обновления копирования от других серверов-шлюзов сети копирования и рассылает их главным/равноправным серверам и серверам-копиям своего узла копирования.

Для определения, какие обновления рассылать другим серверам-шлюзам в сети копирования, а какие - локальным серверам узла копирования, сервер-шлюз пользуется ИД сервера и ИД приемника.

Для настройки шлюзового копирования следует создать минимум два сервера-шлюза. Создание сервера-шлюза устанавливает узел копирования. Затем следует создать соглашение о копировании между шлюзом, каким-либо главным/равноправным сервером и серверами-копиями, которые планируется включить в этот узел шлюзового копирования.

Серверы-шлюзы должны быть главными (с возможностью записи). При попытке добавить класс объектов-шлюзов ibm-replicaGateway в подзапись, не являющуюся главным сервером, будет выведено сообщение об ошибке.

Создать сервер-шлюз можно двумя способами. Вы можете:

| • Создать новый сервер-шлюз
| • Преобразовать существующий равноправный сервер в сервер-шлюз

| **Примечание:** Очень важно, чтобы на один узел копирования приходился только один сервер-шлюз.

## Терминология функции копирования

В функции копирования применяются следующие термины:

**Каскадное копирование**
Топология копирования с несколькими уровнями серверов. Главный/равноправный сервер копирует данные на набор предназначенных только для чтения серверов пересылки, которые в свою очередь передают копируемые данные на другие серверы. Такая топология позволяет разгрузить главные серверы.

**Сервер-потребитель**
Сервер, получающий копируемые изменения с другого сервера (поставщика).

**Разрешения**
Способ и информация, применяемые сервером-поставщиком при подключении к серверу-потребителю. При простом подключении применяется DN и пароль. Разрешения хранятся в записи, DN которой указано в заданном соглашении о копировании.

**Сервер пересылки**
Сервер пересылки (сервер только для чтения) копирует все изменения, получаемые от главного или равноправного сервера. Получаемые от клиентов запросы на обновление передаются главному или равноправному серверу.

| **Сервер-шлюз**
| Это сервер, который передает весь поток копирования от своего локального узла копирования на
| другие серверы-шлюзы сети копирования. Кроме того, сервер-шлюз получает поток копирования от
| других серверов-шлюзов сети копирования и передает его всем серверам своего локального узла
| копирования. Серверы-шлюзы должны быть главными (с возможностью записи).

**Главный сервер**
Сервер, на котором возможна запись (обновление) выбранного поддерева.

**Вложенное поддерево**
Поддерево, находящееся в копируемом поддереве каталога.

**Равноправный сервер**
Главный сервер, выполняющий свои функции по отношению к данному поддереву наравне с другими главными серверами.

**Группа копий**
Первая запись, созданная в контексте копирования, имеет класс объекта ibm-replicaGroup и представляет собой набор серверов, участвующих в копировании. Она представляет собой удобную точку для настройки ACL, защищающих информацию о топологии копирования. В настоящее время средства администрирования поддерживают в каждом контексте копирования одну группу копий с именем **ibm-replicagroup=default**.

**Подзапись копии**
В записи группы копий можно создать одну или несколько записей с классом объектов ibm-replicaSubentry, по одной для каждого сервера, участвующего в процессе копирования в качестве поставщика. Подзапись копии обозначает роль, которую сервер играет в процессе копирования: главный сервер или сервер только для чтения. Сервер только для чтения может в свою очередь иметь соглашения о каскадном копировании.

**Копируемое поддерево**
Часть DIT, копируемая с одного сервера на другой. Такой подход позволяет копировать выбранное

поддерево на одни серверы и не копировать на другие. На данном сервере выбранное поддерево может допускать запись, в то время как другие поддеревья могут быть предназначены только для чтения.

**Сеть копирования**
Это сеть, состоящая из узлов копирования, связанных между собой.

**Соглашение о копировании**
Хранящаяся в каталоге информация, определяющая ″соединение″ или ″путь копирования″ между двумя серверами. Один из серверов (предоставляющий сведения об изменениях) называется поставщиком, а второй (получающий сведения об изменениях) - потребителем. Соглашение содержит всю информацию, необходимую для установления соединения поставщика с потребителем, и для планирования копирования.

**Контекст копирования**
Указывает корень копируемого поддерева. Для обозначения записи в качестве корня копируемого поддерева к этой записи можно добавить вспомогательный класс объекта ibm-replicationContext. Информация, относящаяся к топологии копирования, хранится в наборе записей, создаваемых на подуровнях контекста копирования.

**Узел копирования**
Узел копирования - это совокупность сервера-шлюза и главного, равноправного сервера или сервера-копии.

**Расписание**
Поддерживается настройка расписания копирования, когда все изменения накапливаются на поставщике, а затем передаются в виде одного пакета. Соглашения о копировании содержат DN записи с информацией расписания.

**Сервер-поставщик**
Сервер, передающий сведения об изменениях другому серверу (потребителю).

## Соглашение о копировании

Соглашение о копировании - это запись каталога с классом объекта **ibm-replicationAgreement**, созданная в подзаписи копии и определяющая параметры копирования с сервера, представленного этой подзаписью, на другой сервер. Эти объекты аналогичны записям replicaObject, применявшимся в предыдущих версиях сервера каталогов. Соглашение о копировании состоит из следующих объектов:

- Описательное имя, указанное в атрибуте имени соглашения.
- URL LDAP, указывающий сервер, номер порта и опцию применения SSL.
- ИД сервера-потребителя, если он известен. Серверы каталогов более ранних версий, чем V5R3, не имеют ИД сервера.
- DN объекта, содержащего идентификационную информацию, применяемую поставщиком для подключения к потребителю.
- Необязательный указатель DN на объект с информацией о расписании копирования. Если этот атрибут отсутствует, то сведения о всех вносимых изменениях передаются сразу же.

В качестве описательного имени может применяться имя сервера-потребителя или любое другое удобное и легко запоминающееся имя.

ИД сервера-потребителя применяется в интерфейсе администрирования для перемещения по элементам топологии. По ИД сервера-потребителя интерфейс может найти соответствующую подзапись и соглашения. Для обеспечения точности данных поставщик при подключении к потребителю получает ИД сервера из корневого DSE и сравнивает его со значением из соглашения. Если ИД серверов не совпадают, то в протокол заносится предупреждающее сообщение.

Поскольку соглашение о копировании также может копироваться, то применяется DN объекта идентификационных данных. Такой подход позволяет сохранять идентификационные данные в некопируемой области каталога. Копирование объектов идентификационных данных (из которых можно

получить идентификационные данные в текстовом виде) может представлять собой серьезную угрозу системе безопасности. Объекты идентификационных данных по умолчанию рекомендуется создавать под суффиксом cn=localhost.

Для каждого поддерживаемого способа идентификации определен собственный класс объектов:

- Простое подключение
- SASL
- Внешний механизм с SSL
- Идентификация Kerberos

Вы можете указать, что часть копируемого поддерева не нужно копировать. Для этого достаточно добавить к корню поддерева вспомогательный класс объекта ibm-replicationContext, не определяя подзаписи копий.

**Примечание:** В Web-инструменте администрирования в тех случаях, когда речь идет об изменениях, ожидающих копирования в соответствии с выбранным соглашением о копировании, такие соглашения называются также очередями.

## Хранение информации о копировании на сервере

Информация о копировании хранится в каталоге в трех местах:

- В конфигурации сервера, содержащей сведения о том, как другие серверы могут идентифицировать себя перед данным сервером для выполнения копирования (например, какие серверы могут выполнять функции поставщиков для данного сервера).
- На верхнем уровне копируемого поддерева. Если корневым уровнем копируемого поддерева является запись ″o=my company″, то непосредственно в этой записи будет создан объект с именем ″ibm-replicagroup=default″ will be created (ibm-replicagroup=default,o=my company). В объекте ″ibm-replicagroup=default″ будут созданы дополнительные объекты, описывающие серверы, на которых должны храниться копии поддерева и соглашений о копировании между серверами.
- Для хранения информации о копировании, применяемой только одним сервером, используется объект ″cn=replication,cn=localhost″. Например, объект, содержащий идентификационные данные сервера-поставщика, необходим только этому серверу-поставщику. Идентификационные данные можно хранить в объекте ″cn=replication,cn=localhost″, обеспечив доступ к ним только данному серверу.
- Для хранения информации о копировании, копируемой на другие серверы, используется объект ″cn=replication, cn=IBMpolicies″.

## Особенности защиты информации о копировании

Ниже приведены сведения о защите следующих объектов:

- ibm-replicagroup=default: Средства управления доступом к этому объекту позволяют указывать, кто может просматривать или изменять хранящуюся в нем информацию о копировании. По умолчанию доступ к этому объекту наследуется от родительского объекта. Для ограничения доступа к информации о копировании рекомендуется явно задать доступ к этому объекту. Например, вы можете определить группу, в которую будут входить пользователи, осуществляющие управление копированием. Эту группу можно указать в качестве владельца объекта ″ibm-replicagroup=default″. При этом другим пользователям доступ к объекту будет запрещен.
- cn=replication,cn=localhost: При работе с этим объектом следует помнить о двух аспектах защиты:
  - Средства управления доступом к этому объекту указывают, кому разрешено просматривать и обновлять хранящиеся в нем объекты. По умолчанию доступ настроен таким образом, что анонимные пользователи могут считывать большую часть информации, за исключением паролей, а добавление, изменение и удаление объектов разрешено только администраторам.
  - Объекты, хранящиеся в ″cn=localhost″, никогда не копируются на другие серверы. В этот контейнер на сервере можно поместить идентификационные данные, применяемые этим сервером для копирования, в результате чего эти данные будут недоступны для других серверов. Другой подход, позволяющий

нескольким серверам использовать одни и те же идентификационные данные, заключается в размещении этих идентификационных данных в объекте ″ibm-replicagroup=default″.

- cn=IBMpolicies: В этот контейнер можно поместить идентификационные данные для копирования, но они будут передаваться всем приемникам данного сервера. Размещение идентификационных данных в cn=replication,cn=localhost считается более безопасным.

## Копирование в средах высокой готовности

Сервер каталогов часто применяется в средах с единым входом в систему, что может привести к однотипным ошибкам. С помощью копирования сервер каталогов можно сделать сервером с высокой готовностью. Для этого есть два способа: распределитель нагрузки IBM и управление IP-адресом. Дополнительные сведения можно найти в разделе 13.2 руководства IBM Redbook IBM WebSphere V5.1 Performance, Scalability, and High Availability. 

## Области и шаблоны пользователей

Применяемые в Web-инструменте администрирования объекты областей и шаблонов избавляют пользователей от необходимости подробно изучать некоторые особенности LDAP.

Область представляет собой набор пользователей и групп. Она содержит информацию о структуре каталога, например, о расположении пользователей и групп. Область определяет расположение пользователей (например, ″cn=users,o=acme,c=us″) и создает пользователей как непосредственные дочерние объекты этой записи (например, пользователь John Doe будет создан как ″cn=John Doe,cn=users,o=acme,c=us″). Вы можете определить несколько областей и присвоить им удобные имена (например, Пользователи Web). Такие имена упростят работу сотрудников, создающих пользователей, и управляющих ими.

Шаблон представляет собой описание пользователя. Он содержит список классов объектов (как структурных, так и вспомогательных), применяемых при создании пользователей. Шаблон позволяет также определить вид панелей, применяемых для создания или изменения пользователей (например, имена вкладок, значения по умолчанию и атрибуты, показанные на каждой вкладке).

При добавлении новой области вы создаете в каталоге объект ibm-realm. Объект ibm-realm хранит все свойства области, например, информацию об определении пользователей и групп, а также о применяемом шаблоне. Объект ibm-realm может указывать на существующую запись каталога, являющуюся родительской записью для пользователей, либо указывать на самого себя (по умолчанию). В последнем случае этот объект является контейнером для хранения новых пользователей. Например, если в каталоге есть контейнер cn=users,o=acme,c=us, то вы можете создать в любом другом месте каталога (например, в контейнере cn=realms,cn=admin stuff,o=acme,c=us) область с именем `users`, в которой в качестве места хранения пользователей и групп будет указан объект cn=users,o=acme,c=us. При этом будет создан объект ibm-realm:

```
dn: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
 objectclass: top
objectclass: ibm-realm
 objectclass: ibm-staticGroup
ibm-realmUserTemplate: cn=users template,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserContainer: cn=users,o=acme,c=us
ibm-realmGroupContainer: cn=users,o=acme,c=us
ibm-realmAdminGroup: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserSearchFilter:
cn: users
```

Если объект cn=users,o=acme,c=us не существует, то вы можете создать в o=acme,c=us область `users`, указывающую на саму себя.

Управление шаблонами пользователей, областями, и группами администраторов областей осуществляет администратор каталога. После создания области управление пользователями и группами этой области могут осуществлять члены группы администраторов области.

Дополнительная информация об управлении областями и шаблонами пользователей приведена в разделе “Управление областями и шаблонами пользователей” на стр. 189.

## Параметры поиска

Для ограничения количества используемых сервером ресурсов администратор может настроить параметры поиска, которые будут ограничивать возможности поиска для пользователей. Для избранных пользователей возможности поиска можно расширить. Ограничение и расширение возможностей поиска делается следующими способами:

**Ограничение поиска**

- Постраничный поиск
- Поиск с сортировкой
- Отключение учета псевдонимов

**Расширение поиска**

- Группы ограниченного поиска

**Постраничный поиск**

Настройка страниц позволяет клиенту управлять объемом данных, возвращаемых в ответ на запрос поиска. Вместо того, чтобы получать сразу все результаты от сервера, клиент может запросить некоторый набор данных (страницу). Следующий запрос вернет следующую страницу результатов, и так далее, пока не будут показаны все результаты или операция не будет отменена. Администратор может ограничить такой поиск, разрешив его только для администраторов.

**Поиск с сортировкой**

Сортировка позволяет клиенту получать результаты поиска, отсортированные на основании заданных критериев, задаваемых ключами сортировки. При этом сортировка выполняется не клиентским приложением, а сервером. Администратор может ограничить такой поиск, разрешив его только для администраторов.

**Отключение учета псевдонимов**

В записи каталога, содержащей классы объектов псевдонимов, или aliasObject, есть атрибут aliasedObjectName, служащий для указания на другую запись каталога. Учет псевдонимах можно указывать только в запросах на поиск. *Учет псевдонимов* означает передачу псевдонима в исходную запись. Если для опции учета псевдонимов установлено значение **всегда** или **поиск**, то время ответа IBM Directory Server на запрос поиска может быть намного длиннее, чем при значении **никогда**, даже если в каталоге нет записей о псевдонимах. Работа функции учета псевдонимов определяется двумя параметрами: опция учета псевдонимов, указанная клиентским запросом на поиск, и опция, настроенная администратором на сервере. Если она настроена, то при отсутствии в каталоге объектов псевдонимов сервер может автоматически пропускать их. Серверная опция учета псевдонимов переопределяет клиентскую. В следующей таблице описывается хэширование учета псевдонимов между клиентом и сервером.

*Таблица 2. Фактический учет псевдонимов в зависимости от параметров клиента и сервера*

| Сервер | Клиент | Фактически |
|---|---|---|
| никогда | любой параметр | никогда |
| всегда | любой параметр | клиентский параметр |
| любой параметр | всегда | серверный параметр |
| поиск | поиск | никогда |
| поиск | поиск | никогда |

**Группы ограниченного поиска**

Администратор может создать группу ограниченного поиска. Эта группа может иметь более гибкие ограничения поиска, чем обычные пользователи. Отдельные члены этой группы (пользователи или другие группы) пользуются менее ограниченным поиском, чем обычные пользователи.

Первая проверка ограничений выполняется при первом запросе на поиск. Если пользователь входит в группу ограниченного поиска, то происходит сравнение ограничений. Если ограничения для группы ограниченного поиска жестче, чем ограничения запроса на поиск, то будут использоваться ограничения запроса. Если ограничения запроса жестче, чем ограничения группы поиска, то будут использоваться ограничения группы поиска. Если ограничения группы поиска не найдены, то будет выполнено сравнение с ограничениями поиска для сервера. Если на сервере ограничения не настроены, то сравнение будет выполняться с серверными ограничениями по умолчанию. Применяться будут всегда меньшие ограничения.

Если пользователь входит в несколько ограниченных ограниченного поиска, то ему будет предоставлен максимальный уровень возможностей для поиска (наименьшие ограничения). Например, пользователь входит в группу поиска 1 с ограничениями: размер поиска до 2000 записей и время поиска до 4000 секунд, и в группу поиска 2 с ограничениями: неограниченный размер поиска и время поиска до 3000 секунд. В результате этот пользователь получает неограниченный размер поиска и время до 4000 секунд.

Группы ограниченного поиска могут храниться либо в контейнере localhost, либо в IBMpolicies. Группы, хранящиеся в IBMpolicies, копируются, а группы в localhost - нет. Одну и ту же группу ограниченного поиска можно хранить одновременно и в localhost, и в IBMpolicies. Если группа не сохранена ни под одним из этих отличительных имен, то сервер проигнорирует ограничительную часть группы и будет рассматривать ее как обычную группу.

Когда пользователь начинает поиск, первыми проверяются записи группы ограниченного поиска в localhost. Если записи для этого пользователя не найдены, то затем проверяется группа ограниченного поиска в IBMpolicies. Если в объекте localhost записи найдены, то группа в IBMpolicies не проверяется. Приоритет групп ограниченного поиска в объекте localhost выше, чем в IBMpolicies.

Дополнительная информация о параметрах поиска приведена в разделах:

- “Настройка параметров поиска” на стр. 136
- “Поиск записей каталога” на стр. 183
- “Управление группами ограниченного поиска” на стр. 130

## Информация о поддержке национальных языков (NLS)

В этом разделе приведены сведения о поддержке национальных языков:

- Серверы LDAP обмениваются данными с клиентами в формате UTF-8. Поддерживаются все символы ISO 10646.
- Для хранения информации в базе данных сервер каталогов применяет метод преобразования UTF-16.
- При сравнении строк на клиенте и сервере не учитывается регистр символов. Алгоритмы обработки символов верхнего регистра подходят не для всех языков (локалей).

Дополнительная информация о UCS-2 приведена в разделе “Глобализация” в главе Планирование.

## Языковые теги

Термин *Языковые теги* обозначает механизм, позволяющий каталогу присваивать кодам языков значения. Эти значения хранятся в каталоге и позволяют клиентам запрашивать каталог с учетом особых требований некоторых языков. Языковой тег входит в описание атрибута. Языковой тег представляет собой строку с префиксом lang-, первый буквенный подтег и необязательные последующие подтеги, разделенные дефисом (-). Последующие подтеги могут представлять собой любую комбинацию буквенно-цифровых символов;

тогда как первый подтег должен состоять только из букв. Длина подтегов может быть любой; совокупная длина всего тега не должна превышать 240 символов. Регистр символов в языковых тегах не учитывается; записи en-us, en-US и EN-US равнозначны. В компонентах DN и RDN языковые теги не поддерживаются. В описании одного атрибута допускается наличие только одного языкового тега.

**Примечание:** Отсюда следует, что языковые теги и уникальные атрибуты являются взаимно исключающими. Если какой-либо атрибут планируется сделать уникальным, то с ним нельзя связывать языковые теги.

Если в каталог добавляются данные при включенных языковых тегах, то их можно использовать при поиске, чтобы выборочно извлечь значения атрибутов на указанных языках. Если в описании какого-либо атрибута, входящего в список запрошенных атрибутов для поиска, содержится языковой тег, то будут возвращены только те значения атрибута записи каталога, язык которых совпадает с этим языковым тегом. То есть, для запроса на поиск:

```
ldapsearch -b "o=ibm,c=us" (objectclass=organization) description;lang-en
```

сервер вернет значения атрибута ″description;lang-en″, а значения атрибутов ″description″ и ″description;lang-fr″ возвращены не будут.

Если атрибут в запросе указан без языкового тега, то будут возвращены все значения атрибута, независимо от языка.

Тип атрибута и языковой тег разделяются точкой с запятой (;).

**Примечание:** Использование точки с запятой разрешено в разделе ″NAME″ объекта AttributeType. Однако, так как этот символ используется для разделения AttributeType и языкового тега, то его использование в разделе ″NAME″ типа атрибута крайне не рекомендуется.

Например, если клиент запрашивает атрибут ″description″, и при этом запись запроса выглядит следующим образом:

```
 objectclass: top
 objectclass: organization
o: Software GmbH
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
postalAddress: Berlin 8001 Germany
postalAddress;lang-de: Berlin 8001 Deutschland
```

, то сервер вернет:

```
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
```

Если в запросе на поиск указан атрибут ″description;lang-de″, то сервер вернет:

```
description;lang-de: Softwareprodukte
```

С помощью языковых тегов в каталогах, поддерживающих работу на нескольких языках, можно хранить многоязычные данные. Например, языковые теги позволяют разработать приложение так, чтобы немецкие клиенты видели только данные с атрибутом lang-de, а французские - данные для атрибута lang-fr.

Определить, включена ли функция языковых тегов, можно с помощью поиска в корневом DSE с атрибутом ″ibm-enabledCapabilities″.

```
ldapsearch -b "" -s base objectclass=* ibm-enabledCapabilities
```

Если возвращен идентификатор ″1.3.6.1.4.1.4203.1.5.4″, то функция включена.

Если поддержка языковых тегов не включена, то все операции LDAP, связанные с языковыми тегами, будут отклонены с сообщением об ошибке.

Языковые теги можно связывать не со всеми атрибутами. Определить, допускает ли данный атрибут языковые теги, можно с помощью команды ldapexop:

- Для атрибутов, поддерживающих языковые теги: `ldapexop -op getattributes -attrType language_tag -matches true`
- Для атрибутов, не поддерживающих языковые теги: `ldapexop -op getattributes -attrType language_tag -matches false`

Дополнительная информация приведена в разделе “Добавление записи, содержащей языковые теги” на стр. 180.

## Переадресация в каталоге LDAP

Переадресация позволяет нескольким серверам каталогов работать совместно. Если запрашиваемое клиентом DN находится в другом каталоге, сервер может автоматически отправить (переадресовать) запрос на другой сервер LDAP.

Сервер каталогов поддерживают два типа переадресации. Можно указать сервер переадресации по умолчанию, на который серверы LDAP будут переадресовывать все запросы клиентов относительно DN, отсутствующих в каталоге. Кроме того, с помощью клиента LDAP можно добавить на сервер каталогов записи, содержащие ссылку objectClass. Таким образом можно настроить серверы для переадресации запросов к определенным DN.

**Примечание:** На сервере каталогов объекты переадресации должны содержать только атрибуты отличительного имени (`dn`), класса объекта (`objectClass`) и переадресации (`ref`). Применение этого ограничения продемонстрировано в примере “ldapsearch” на стр. 219.

Серверы переадресации тесно связаны с серверами-копиями. Так как клиенту запрещено изменять данные на серверах-копиях, сервер-копия переадресует все запросы на изменение данных на главный сервер.

## Транзакции

Сервер каталогов можно настроить таким образом, чтобы клиенты могли применять транзакции. (Дополнительная информация о настройке параметров транзакций приведена в разделе “Настройка параметров транзакций” на стр. 125.) Транзакция представляет собой группу операций с каталогом LDAP, объединенных в единое целое. Результаты выполнения отдельных операций LDAP, составляющих транзакцию, сохраняются только после успешного завершения всех операций транзакции и ее фиксации. При сбое одной из операций или отмене транзакции отменяются и все остальные операции транзакции. Эта возможность позволяет пользователям организованно выполнять операции на сервере LDAP. Например, пользователь может настроить на клиенте транзакцию для удаления нескольких записей каталога. Если в процессе обработки транзакции соединение между клиентом и сервером будет разорвано, то ни одна из записей не будет удалена. Таким образом, пользователь сможет просто запустить транзакцию еще раз, не проверяя, какие записи были удалены.

В транзакции могут входить следующие транзакции LDAP:

- добавить
- изменить
- изменить RDN
- удалить

**Примечание:** Не включайте в транзакции изменения схемы каталогов (суффикс cn=schema). Формально такие операции можно добавить в транзакцию, однако их невозможно отменить в случае сбоя транзакции. Это может привести к непредвиденным неполадкам сервера каталогов.

## Защита сервера каталогов

Вопросы защиты сервера каталогов описаны в следующих разделах:

- “Контроль”
- “Поддержка протоколов SSL и TLS на сервере каталогов”
- “Идентификация Kerberos на сервере каталогов” на стр. 52
- “Группы и роли” на стр. 53
- “Права доступа администратора” на стр. 59
- “Proxy-идентификация” на стр. 60
- “Списки управления доступом” на стр. 60
- “Принадлежность объектов каталога LDAP” на стр. 72
- “Стратегия управления паролями” на стр. 73
- “Идентификация” на стр. 76
- “Предотвращение отказа в обслуживании” на стр. 80

**Связанные концепции**

“Управление свойствами защиты” на стр. 161

## Контроль

Сервер каталогов поддерживает средства контроля из подсистемы защиты i5/OS. Возможен контроль следующих операций:

- Подключение к серверу каталогов и отключение от него.
- Изменения прав доступа к объектам каталога LDAP.
- Изменение принадлежности объектов каталога LDAP.
- Создание, удаление, поиск и изменение объектов каталога LDAP.
- Изменения пароля администратора и обновление отличительных имен (DN)
- Изменения паролей пользователей.
- Импорт и экспорт файлов.

Возможно, для включения контроля за записями каталога потребуется изменить параметры контроля. Если системное значение QAUDCTL равно *OBJAUD, функцию контроля за объектами можно включить с помощью Навигатора. Дополнительная информация о контроле приведена в разделе *Справочник по защите*

 или в разделе “Контроль защиты”.

## Поддержка протоколов SSL и TLS на сервере каталогов

Для защиты соединений с сервером каталогов можно применять протоколы SSL и TLS.

SSL - это стандартный протокол, применяемый для защиты данных в сети Internet. SSL может применяться для защиты соединений с клиентами LDAP и серверами-копиями. Для повышения надежности защиты соединения помимо идентификации сервера может применяться идентификация клиента. В этом случае перед установлением соединения с сервером клиент должен предъявить сертификат, идентифицирующий клиент.

Для применения SSL в системе должен быть установлен Диспетчер цифровых сертификатов (DCM), компонент 34 операционной системы i5/OS. DCM предоставляет интерфейс для создания и управления

цифровыми сертификатами и хранилищами сертификатов. Информация о цифровых сертификатах и работе с DCM приведена в разделе “Диспетчер цифровых сертификатов”. Сведения о поддержке SSL на серверах iSeries вы можете найти в разделе “Secure Sockets Layer (SSL)”.

TLS является преемником SSL. Этот протокол использует те же технологии шифрования, но поддерживает больше алгоритмов. Информация о поддержке TLS на сервере iSeries приведена в разделе Поддерживаемые протоколы SSL и TLS. С помощью TLS сервер может обмениваться данными с клиентом как по защищенному, так и по незащищенному каналу по стандартному порту 389. Для установки защищенного соединения служит расширенная операция StartTLS.

Для настройки TLS в системе клиента должны соблюдаться следующие условия:

1. На сервере каталогов должна быть настроена работа с протоколом TLS или SSLTLS. См. раздел “Включение SSL и TLS на сервере каталогов” на стр. 165.
2. В утилитах командной строки клиента следует указывать опцию -Y.

**Примечание:** TLS и SSL являются взаимоисключающими. Вызов запроса на запуск TLS (опция -Y) по порту SSL приведет к появлению ошибок.

Клиент может установить соединение по защищенному порту (636) как с помощью TLS, так и с помощью SSL. StartTLS - это функция LDAP, позволяющая установить защищенное соединение поверх существующего незащищенного (порт 389). По сути, StartTLS (или утилиту командной строки -Y) можно применять только со стандартным незащищенным портом (389); для защищенного соединения функцию StartTLS применять нельзя.

Дополнительная информация приведена в разделе “Включение SSL и TLS на сервере каталогов” на стр. 165.

## Идентификация Kerberos на сервере каталогов

Сервер каталогов поддерживает идентификацию Kerberos. Kerberos - это протокол сетевой идентификации, обеспечивающий надежную идентификацию приложений клиент-сервер с помощью шифрования с личным ключом.

Для включения идентификации Kerberos следует настроить службу сетевой идентификации.

Функция идентификации Kerberos сервера каталогов поддерживает механизм GSSAPI SASL. Он дает возможность применять идентификацию Kerberos при работе с сервером каталогов как клиентам LDAP Windows 2000, так и клиентам сервера каталогов.

**Имя субъекта Kerberos**, применяемое сервером, имеет следующий вид:

```
имя-службы/имя-хоста@область
```

`имя-службы` - ldap (в нижнем регистре), `имя-хоста` - полное имя TCP/IP системы, а `область` - область, заданная по умолчанию в конфигурации Kerberos системы.

Например, для системы `my-as400` в домене TCP/IP `acme.com` с областью Kerberos по умолчанию `ACME.COM` имя субъекта Kerberos для сервера LDAP будет равно `ldap/my-as400.acme.com@ACME.COM`. Область Kerberos по умолчанию указана в директиве default_realm (default_realm = ACME.COM) файла конфигурации Kerberos (по умолчанию это файл /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf). Если область по умолчанию не задана, то на сервере каталогов нельзя настроить функцию идентификации Kerberos.

Если применяется идентификация Kerberos, то сервер каталогов связывает с соединением отличительное имя (DN), которое определяет права доступа к данным каталога. DN может выбираться одним из следующих способов:

- Сервер может создать DN на основе ИД Kerberos. При этом на основе идентификатора Kerberos в формате субъект@область создается DN в формате ibm-kn=субъект@область. ibm-kn= эквивалентно ibm-kerberosName=.

- Сервер может выполнять поиск отличительного имени (DN) в каталоге, содержащем запись для субъекта и области Kerberos. При выборе этого варианта сервер выполняет поиск в каталоге записи, содержащей заданный идентификатор Kerberos.

У вас должен быть файл таблицы ключей (keytab), содержащий ключ для субъекта службы LDAP. Дополнительная информация о реализации Kerberos на сервере iSeries приведена в разделе Служба сетевой идентификации справочной системы Information Center. В разделе Настройка службы сетевой идентификации приведены инструкции по добавлению информации в файлы таблицы ключей.

## Группы и роли

Группа представляет собой список или набор имен. Группа может применяться для управления доступом в атрибутах **aclentry**, **ibm-filterAclEntry** и **entryowner**, либо в других случаях, зависящих от конкретного приложения, например, в списке рассылки. См. раздел “Списки управления доступом” на стр. 60. Группы могут быть статическими, динамическими и вложенными. Информация о работе с группами приведена в разделе “Управление пользователями и группами” на стр. 186.

Роли аналогичны группам в том смысле, что они также представлены объектами каталога. Кроме того, роли содержат списки DN групп.

Дополнительная информация приведена в следующих разделах:



### Статические группы

Состав статических групп определяется с помощью структурных классов объектов **groupOfNames**, **groupOfUniqueNames**, **accessGroup** и **accessRole**, либо с помощью вспомогательного класса объектов **ibm-staticgroup**. Статическая группа, созданная с помощью структурных классов объектов **groupOfNames** и **groupOfUniqueNames** должна иметь по крайней мере один элемент. Группа, созданная с помощью структурного класса объектов **accessGroup** или **accessRole** может быть пустой. Статическую группу можно также определить с помощью вспомогательного класса объектов **ibm-staticGroup**. Такая группа не требует наличия атрибута **member**, а значит, может быть пустой.

Типичный пример группы:

```
DN: cn=Dev.Staff,ou=Austin,c=US
objectclass: accessGroup
 cn: Dev.Staff
 member: cn=John Doe,o=IBM,c=US
 member: cn=Jane Smith,o=IBM,c=US
 member: cn=James Smith,o=IBM,c=US
```

Каждый объект группы содержит атрибут с несколькими значениями, представляющими собой DN элементов группы.

При удалении группы доступа эта группа также удаляется из всех ACL, в которых она применялась.

### Динамические группы

Состав динамических групп определяется несколько иначе, чем в статических группах. Вместо перечисления отдельных элементов группы состав динамических групп определяется с помощью операций поиска LDAP.

Для определения операции поиска с применением упрощенного синтаксиса URL LDAP в динамической группе применяется структурный класс объектов **groupOfURLs** (или вспомогательный класс объектов **ibm-dynamicGroup**) и атрибут **memberURL**.

```
ldap:///<базовое DN поиска> ? ? <область поиска> ? <фильтр поиска>
```

**Примечание:** Как показано в примере, имя хоста может отсутствовать. Все остальные параметры соответствуют обычному синтаксису URL LDAP. Каждое поле параметра должно отделяться символом ?, даже если параметр не указан. Обычно между базовым DN и областью поиска указывается список возвращаемых атрибутов. Кроме того, этот параметр не применяется сервером при определении состава динамических групп, поэтому его можно не указывать. Однако, разделитель**?** по-прежнему должен присутствовать.

где:

**базовое DN поиска**
Точка, с которой начинается поиск в каталоге. Это может быть суффикс или корневая запись каталога, например, **ou=Austin**. Это обязательный параметр.

**область поиска**
Задает область поиска. По умолчанию применяется базовый поиск.

**Базовый поиск**
Возвращает информацию только о базовом DN, указанном в URL.

**one** Возвращает информацию только о записях, находящихся на следующем уровне после базового DN, указанного в URL. Базовая запись не включается.

**sub** Возвращает информацию о записях, находящихся на всех уровнях поддерева, включая базовое DN.

**фильтр поиска**
Фильтр, который необходимо применить к записям в области поиска. Информация о синтаксисе фильтра поиска приведена в разделе “Опции фильтра ldapsearch” на стр. 223. Значение по умолчанию: objectclass=*

Поиск элементов динамических групп всегда выполняется только на самом сервере, поэтому в отличие от полного URL LDAP имя хоста и номер порта никогда не указываются, в качестве протокола всегда указывается **ldap** (и никогда **ldaps**). Атрибут **memberURL** может содержать URL любого типа, но сервер определяет членство в динамических группах только по атрибутам **memberURL**, начинающимся с символа **ldap:**///.

**Примеры**

Единственная запись, в которой применяется базовая область поиска по умолчанию и фильтр по умолчанию, равный objectclass=*:

```
ldap:///cn=John Doe, cn=Employees, o=Acme, c=US
```

Все записи, находящиеся на один уровень ниже записи cn=Employees, фильтр по умолчанию - objectclass=*:

```
ldap:///cn=Employees, o=Acme, c=US??one
```

Все записи, находящиеся на более низких уровнях, чем o-Acme с objectclass=person:

```
ldap:///o=Acme, c=US??sub?objectclass=person
```

В зависимости от классов объектов, применяемых при определении записей пользователей, эти записи могут не содержать атрибутов, необходимых для определения членства в динамических группах. Вы можете добавить к записям пользователей атрибут **ibm-group**, воспользовавшись вспомогательным классом объектов **ibm-dynamicMember**. Этот атрибут позволяет добавлять к записям пользователей произвольные значения, которые могут применяться в качестве целевых значений фильтров динамических групп. Например:

Элементами этой динамической группы являются все записи, непосредственно находящиеся под записью cn=users,ou=Austin, и имеющие атрибут ibm-group, равный GROUP1:

```
dn: cn=GROUP1,ou=Austin
 objectclass: groupOfURLs
 cn: GROUP1
 memberURL: ldap:///cn=users,ou=Austin??one?(ibm-group=GROUP1)
```

Пример элемента группы cn=GROUP1,ou=Austin:

```
dn: cn=Group 1 member, cn=users, ou=austin
      objectclass: person
 objectclass: ibm-dynamicMember
 sn: member
 userpassword: memberpassword
 ibm-group: GROUP1
```

## Вложенные группы

Вложенные группы позволяют создавать иерархические структуры, используемые для организации наследуемого членства в группах. Вложенная группа представляет собой дочернюю записью группы, DN которой указан в атрибуте записи родительской группы. Родительская группа создается путем добавления к одному из структурных классов объектов групп(**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** или **groupOfURLs**) вспомогательного класса объектов **ibm-nestedGroup**. После добавления вложенной группы можно указать произвольное количество атрибутов **ibm-memberGroup**, значения которых будут содержать имена DN вложенных дочерних групп. Например:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
 objectclass: groupOfNames
 objectclass: ibm-nestedGroup
 objectclass: top
 cn: Group 2
 description: Group composed of static, and nested members.
 member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=IBM, c=US
 ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=IBM, c=US
```

Появление замкнутых циклов в иерархии вложенных групп недопустимо. Если будет выявлено, что выполнение операции над вложенной группой приведет к появлению циклических ссылок (как непосредственных, так и путем наследования), то это будет считаться нарушением ограничений и операция выполнена не будет.

## Смешанные группы

Любой структурный класс объектов группы можно расширить таким образом, чтобы членство в группе определялось как совокупность членства в статических, динамических и вложенных группах. Например:

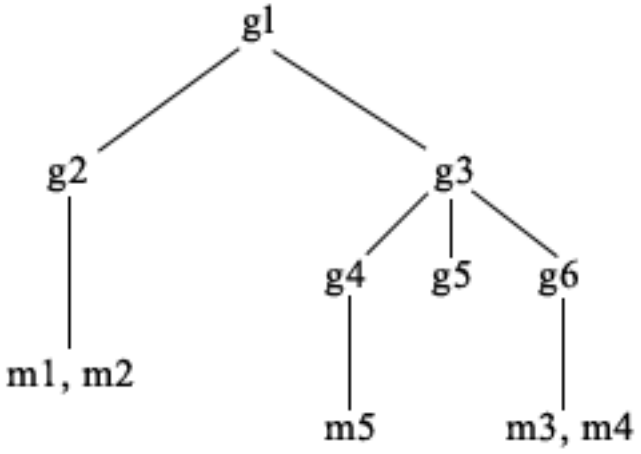
```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
 objectclass: groupOfURLs
 objectclass: ibm-nestedGroup
 objectclass: ibm-staticGroup
 objectclass: top
 cn: Group 10
 description: Group composed of static, dynamic, and nested members.
 memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
 ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=IBM, c=US
 member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=IBM, c=US
```

## Определение членства в группах

Для определения членства в группах может применяться два операционных атрибута. Для данной записи группы операционный атрибут **ibm-allMembers** позволяет получить полный список элементов групп, включая статические, динамические и вложенные группы. Для данной записи пользователя с помощью операционного атрибута **ibm-allGroups** можно получить полный список групп (включая родительские группы), в состав которых входит пользователь.

В зависимости от настройки ACL для данных, в ответе на запрос может быть возвращено лишь подмножество всех запрошенных данных. Обращаться к операционным атрибутам **ibm-allMembers** и **ibm-allGroups** могут любые пользователи, однако возвращаемый набор данных включает сведения лишь о тех записях и атрибутах LDAP, к которым у запрашивающего пользователя есть права доступа. Для просмотра списка статических элементов групп пользователь, обращающийся к атрибуту **ibm-allMembers** или **ibm-allGroups**, должен иметь доступ к значениям атрибутов **member** или **uniquemember** для группы и вложенных групп, а для просмотра динамических элементов групп должен иметь возможность выполнять операции поиска, указанные в значениях атрибута **memberURL**. Примеры:

**Примеры иерархии**




В этом примере **m1** и **m2** указаны в атрибуте member группы **g2**. Согласно списку ACL группы **g2**, для пользователя **user1** доступ к атрибуту member разрешен, а для пользователя **user2** - запрещен. Запись LDIF для группы **g2**:

```
dn: cn=g2,cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g2
member: cn=m1,cn=users,o=ibm,c=us
member: cn=m2,cn=users,o=ibm,c=us
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us:normal:rsc:at.member:deny:rsc
```

Запись **g4** использует aclentry по умолчанию, что позволяет считывать атрибут member как пользователю **user1**, так и пользователю **user2**. Запись LDIF для группы **g4**:

```
dn: cn=g4, cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g4
member: cn=m5, cn=users,o=ibm,c=us
```

Запись **g5** описывает динамическую группу, два элемента которой определяются атрибутом memberURL. Запись LDIF для группы **g5**:

```
dn: cn=g5, cn=groups,o=ibm,c=us
objectclass: container
objectclass: ibm-dynamicGroup
cn: g5
memberURL: ldap:///cn=users,o=ibm,c=us??sub?(|(cn=m3)(cn=m4))
```

Записи **m3** и **m4** входят в группу **g5**, поскольку они соответствуют **memberURL**. Согласно списку ACL для записи **m3**, пользователям **user1** и **user2** поиск выполнять разрешено. ACL для записей **m4** запрещает пользователю **user2** выполнять поиск. Запись LDIF для **m4**:

```
dn: cn=m4, cn=users,o=ibm,c=us
objectclass: person
cn: m4
sn: four
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us
```

**Пример 1:**

Пользователь User1 выполняет поиск для просмотра списка всех элементов группы **g1**. У пользователя User1 есть доступ ко всем элементам группы, поэтому будет возвращен полный список.

```
ldapsearch -D cn=user1,cn=users,o=ibm,c=us -w user1pwd -s base -b cn=g1,
           cn=groups,o=ibm,c=us objectclass=* ibm-allmembers


cn=g1,cn=groups,o=ibm,c=us
ibm-allmembers: CN=M1,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M2,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M4,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

**Пример 2:**

Пользователь User2 выполняет поиск для просмотра списка всех элементов группы **g1**. У пользователя User2 нет прав доступа к элементам **m1** и **m2**, поскольку у него нет доступа к атрибуту member группы **g2**. У пользователя User2 есть доступ к атрибуту member группы **g4**, а значит, есть доступ и к элементу **m5**. User2 может выполнять в memberURL **g5** поиск записи **m3** и видеть эту запись в полученном списке, но не может выполнять поиск **m4**.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=g1,
           cn=groups,o=ibm,c=us objectclass=* ibm-allmembers


cn=g1,cn=groups,o=ibm,c=us
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

**Пример 3:**

Пользователь User2 выполняет поиск с целью определить, является ли **m3** элементом группы **g1**. У пользователя User2 есть права доступа для выполнения поиска, поэтому в результате операции будет возвращена информация о том, что **m3** является элементом группы **g1**.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=m3,
           cn=users,o=ibm,c=us objectclass=* ibm-allgroups


cn=m3,cn=users,o=ibm,c=us
ibm-allgroups: CN=G1,CN=GROUPS,O=IBM,C=US
```

**Пример 4:**

Пользователь User2 выполняет поиск с целью определить, является ли **m1** элементом группы **g1**. У пользователя User2 нет прав доступа к атрибуту member, поэтому в результате выполнения поиска сведения о том, что **m1** является элементом группы **g1**, получены не будут.

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b
           cn=m1,cn=users,o=ibm,c=us objectclass=* ibm-allgroups


cn=m1,cn=users,o=ibm,c=us
```

## Классы объектов групп для вложенных и динамических групп

**ibm-dynamicGroup**

Этот вспомогательный класс объектов допускает применение дополнительного атрибута **memberURL**. Используя его со структурным классом, например, **groupOfNames**, вы можете создавать смешанные группы, включающие как статические, так и динамические элементы.

**ibm-dynamicMember**

Этот вспомогательный класс объектов допускает применение дополнительного атрибута **ibm-group**. Он применяется в качестве атрибута фильтра при создании динамических групп.

**ibm-nestedGroup**

Этот вспомогательный класс объектов допускает применение дополнительного атрибута **ibm-memberGroup**. Используя его со структурным классом, например, **groupOfNames**, вы можете создавать дочерние группы, вложенные в родительские группы.

**ibm-staticGroup**

Этот вспомогательный класс объектов допускает применение дополнительного атрибута **member**. Используя его со структурным классом, например, **groupOfURLs**, вы можете создавать смешанные группы, включающие как статические, так и динамические элементы.

**Примечание:** Класс **ibm-staticGroup** - это единственный класс, для которого атрибут **member** является *необязательным*. Все остальные классы, использующие атрибут **member**, требуют наличия хотя бы одного члена в группе.

## Типы атрибутов групп

**ibm-allGroups**

Показывает список всех групп, в состав которых входит запись. Запись может быть включена в состав группы как напрямую, с помощью атрибута **member**, **uniqueMember** или **memberURL**, так и косвенно, с помощью атрибута **ibm-memberGroup**. Этот предназначенный **только для чтения** операционный атрибут нельзя применять в фильтрах поиска. Атрибут **ibm-allGroups** можно применять в запросах сравнения, позволяющих определить, входит ли элемент в выбранную группу. Следующий пример позволяет определить, является ли запись ″cn=john smith,cn=users,o=my company″ элементом группы ″cn=system administrators, o=my company″:

```
rc = ldap_compare_s(ld, "cn=john smith,cn=users,o=my company, "ibm-allgroups",
    "cn=system administrators,o=my company");
```

**ibm-allMembers**

Показывает все элементы группы. Запись может быть включена в состав группы как напрямую, с помощью атрибута **member**, **uniqueMember** или **memberURL**, так и косвенно, с помощью атрибута **ibm-memberGroup**. Этот предназначенный **только для чтения** операционный атрибут нельзя применять в фильтрах поиска. Атрибут **ibm-allMembers** можно применять в запросах сравнения, позволяющих определить, входит ли DN в выбранную группу. Следующий пример позволяет определить, является ли запись ″cn=john smith,cn=users,o=my company″ элементом группы ″cn=system administrators, o=my company″:

```
rc = ldap_compare_s(ld, "cn=system administrators,o=my company, "ibm-allmembers",
    "cn=john smith,cn=users,o=my company");
```

**ibm-group**

Этот атрибут применяется вспомогательным классом **ibm-dynamicMember**. Он позволяет определять произвольные значения, управляющие вхождением записи в динамические группы. Например, добавив значение ″Bowling Team″, вы можете включить запись в любой **memberURL** с фильтром ″ibm-group=Bowling Team″.

**ibm-memberGroup**

Этот атрибут применяется вспомогательным классом **ibm-nestedGroup**. Он определяет дочерние группы, связанные с записью родительской группы. При обработке ACL, а также операционных атрибутов **ibm-allMembers** и **ibm-allGroups** элементы всех дочерних групп считаются элементами родительской группы. Сами дочерние группы *не* являются элементами родительской группы. Членство во вложенных группах является рекурсивным.

**member**

Указывает отличительные имена всех элементов группы. Например: `member: cn=John Smith, dc=ibm, dc=com`.

**memberURL**

Указывает URL, связанные с каждым из членов группы. Могут применяться URL любого типа. Например: `memberURL: ldap:///cn=jsmith,dc=ibm,dc=com`.

**uniquemember**

Указывает группу связанных с записью имен, причем наличие у каждого имени атрибута uniqueIdentifier делает это имя уникальным. Значение атрибута uniqueMember представляет собой DN, за которым следует uniqueIdentifier. Например: `uniqueMember: cn=John Smith, dc=ibm, dc=com 17`.

### Роли

Предоставление доступа на основе ролей является важным дополнением к средствам управления доступом на основе групп. Выполняя определенную роль, вы получаете все права доступа, необходимые для выполнения связанных с этой ролью операций. В отличие от группы, для роли применяется неявно заданный набор прав доступа. Не существует никаких встроенных предположений относительно того, какие права доступа предоставляются или аннулируются при включении пользователя в группу.

Роли аналогичны группам в том смысле, что они также представлены объектами каталога. Кроме того, роли содержат списки DN групп. Роли, используемые для управления доступом, должны иметь класс объектов 'AccessRole'. Класс объектов 'Accessrole' является подклассом 'GroupOfNames'.

Например, если существует набор DN 'sys admin', то самой естественной первой реакцией будет рассмотрение этих DN как группы 'sys admin group' (поскольку именно группы и пользователи представляют собой наиболее часто встречающиеся атрибуты прав доступа). Однако, поскольку существуют определенные наборы прав доступа, которые логично было бы предоставлять элементам набора DN 'sys admin', то правильнее было бы определить такой набор как роль 'sys admin role'.

## Права доступа администратора

IBM Directory Server поддерживает следующие типы прав доступа администратора:

- **Спроецированный администратор i5/OS:** Клиент, идентифицированный как спроецированный пользователь (запись LDAP, представляющая собой профайл пользователя операционной системы) со специальными правами доступа *ALLOBJ и *IOSYSCFG. Этот клиент имеет право на изменение конфигурации каталога с помощью интерфейсов LDAP (поддерево cn=configuration или Web-инструмент администрирования, задача ″Администрирование сервера″), а также может действовать как администратор LDAP для других записей каталогов (записи, хранящиеся в одном из суффиксов DB2 или в схеме). Только спроецированным администраторам i5/OS разрешено изменять конфигурацию сервера.
- **Администратор LDAP:** В системе IBM Directory Server ИД (DN) одного пользователя можно настроить главным администратором сервера LDAP. В iSeries также есть возможность создания администратора LDAP на основе профайла спроецированного пользователя операционной системы. Администратор сервера LDAP может выполнять целый ряд административных задач, например, управление копированием, схемами и записями каталогов. Дополнительная информация приведена в разделе “Предоставление спроецированным пользователям администраторских прав доступа” на стр. 128.
- **Группа администраторов:** Спроецированный администратор i5/OS может включить несколько пользователей в группу администраторов. Члены этой группы также могут выполнять ряд задач, поскольку у них те же права доступа, что и у администратора сервера LDAP.

  **Примечание:** При использовании Web-инструмента администрирования задачи, не указанные для группы администраторов явно, будут отключены.

Администратор LDAP или члены группы администраторов могут выполнять следующие задачи администрирования:

- Изменять собственные пароли
- Завершать соединения
- Применять и изменять стратегию управления паролями, за исключением шифрования паролей, которое разрешается выполнять только спроецированному администратору i5/OS.

- Управлять уникальными атрибутами
- Управлять схемой сервера
- Управлять копированием, за исключением настройки параметров копирования (в том числе DN подключения главного сервера, пароль и стандартная переадресация), выполнение которой разрешено только спроецированному администратору i5/OS.

Информация о создании группы администраторов приведена в разделе “Работа с группой администраторов” на стр. 129.

## Proxy-идентификация

Proxy-идентификация - это особый вид идентификации. С помощью механизма Proxy-идентификации клиентское приложение может подключиться к каталогу со своим идентификатором, и при этом получает возможность действовать в этом каталоге от имени другого пользователя. Некоторый набор доверенных приложений и ряд пользователей может обращаться к серверу каталогов от имени нескольких пользователей.

Члены группы Proxy-идентификации могут выступить от имени любого пользователя, за исключением администратора и членов группы администраторов.

Группы Proxy-идентификации могут храниться либо в контейнере localhost, либо в IBMpolicies. Группа, хранящаяся в IBMpolicies, копируется, а группа в localhost - нет. Одну и ту же группу можно сохранить одновременно и в localhost, и в IBMpolicies. Если группа не сохранена ни под одним из этих отличительных имен, то сервер проигнорирует часть Proxy этой группы и будет рассматривать ее как обычную группу.

Например, клиентское приложение, client1 подключается к серверу каталогов с высоким уровнем прав доступа. Этому приложению посылает запрос пользователь UserA, права доступа которого ограничены. Если клиент входит в группу Proxy-идентификации, то он может передать запрос не от имени client1, а от имени UserA, права доступа которого более ограничены. То есть вместо того, чтобы выполнить запрос от client1, сервер приложений может обращаться только к той информации и выполнять только те действия, которые разрешены пользователю UserA. Сервер приложений выполняет запрос от имени (или в качестве посредника) пользователя UserA.

**Примечание:** Значение атрибута member должно быть указано в виде DN. В противном случае будет выведено сообщение Недопустимый синтаксис DN. Группа Proxy-идентификации не может содержать вложенных групп.

Также в группу Proxy-идентификации не может входить администратор или члены группы администраторов. Всякий раз при выполнении действия с применением Proxy-идентификации в протокол контроля заносятся и DN подключения, и DN proxy.

Дополнительная информация приведена в разделе “Управление группой Proxy-идентификации” на стр. 132.

## Списки управления доступом

Списки управления доступом (ACL) предназначены для защиты информации, хранящейся в каталоге LDAP. С помощью ACL администраторы могут ограничивать доступ к различным частям каталога или к отдельным его записям. С помощью ACL можно управлять изменениями, вносимыми в любые записи и атрибуты каталога. ACL для данной записи или атрибута может быть задан явно или унаследован от родительской записи.

Стратегию управления доступом лучше всего разрабатывать таким образом, чтобы можно было создать группы пользователей, которые затем будут применяться при настройке доступа к объектам и атрибутам. Принадлежность и права доступа следует задавать на как можно более высоком уровне дерева, обеспечив наследование прав доступа ко всем объектам более низкого уровня.

Связанные с управлением доступом операционные атрибуты, такие как entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource и aclPropagate, являются необычными в том смысле, что они логически связаны с каждым объектом, но могут иметь значения, зависящие от объектов, находящихся на более высоких уровнях иерархии. Значения этих атрибутов могут быть заданы явно или унаследованы.

Модель управления доступом определяет два набора атрибутов: Информация управления доступом (ACI) и информация entryOwner. ACI определяет права доступа, которые предоставляются определенным субъектам по отношению к заданным объектом для выполнения определенных операций. К определению ACI применяются атрибуты aclEntry и aclPropagate. Информация entryOwner указывает, какие субъекты могут определять ACI для связанного с этой информацией объекта записи. К определению entryOwner применяются атрибуты entryOwner и ownerPropagate.

Существует два типа списков управления доступом: ACL с фильтрами и ACL без фильтров. ACL без фильтров явно применяются к той записи каталога, в которой они находятся, и могут распространятся либо только на эту запись, либо на все ее дочерние записи. В ACL с фильтрами для определения объектов, к которым должны применяться права доступа, используется сравнение на основе фильтра объектов.

С помощью ACL администраторы могут ограничивать доступ к различным частям каталога, отдельным записям, а также, на основании имен или классов доступа атрибутов, - к атрибутам записей. С каждой записью каталога LDAP связан набор ACI. В соответствии с моделью LDAP, информация ACI и entryOwner представляется в виде пар атрибут-значение. Для управления этими значениями применяется синтаксис LDIF. Поддерживаемые атрибуты:

- aclEntry
- aclPropagate
- ibm-filterAclEntry
- ibm-filterAclInherit
- entryOwner
- ownerPropagate

Информация о работе с ACL приведена в разделе “Управление списками управления доступом (ACL)” на стр. 197. Дополнительную информацию вы можете найти в следующих разделах:


- “ACL с фильтрами”
- “Синтаксис атрибутов управления доступом” на стр. 62
- “AclEntry и ibm-filterAclEntry” на стр. 63
- “EntryOwner” на стр. 65
- “Наследование” на стр. 65
- “Вычисление прав доступа” на стр. 66
- “Определение ACI и владельцев записи” на стр. 68
- “Изменение значения ACI и владельца записи” на стр. 69
- “Удаление значения ACI/владельца записи” на стр. 71
- “Получение значения ACI/владельца записи” на стр. 72
- “Особенности копирования поддерева” на стр. 72


## ACL с фильтрами

В ACL с фильтрами для определения объектов, к которым должны применяться права доступа, используется сравнение на основе фильтра объектов.

ACL с фильтрами наследуются всеми объектами поддерева, соответствующими заданному условию сравнения. В связи с этим атрибут aclPropagate, применяемый для прекращения наследования ACL без фильтров, не применяется по отношению к новым ACL с фильтрами.

По умолчанию ACL с фильтрами накапливают права доступа от включенной записи наименьшего уровня вверх по цепочке предков, до включенной записи наивысшего уровня в дереве информации о каталоге (DIT). Действующие права доступа вычисляются как объединение разрешений или запретов для всех записей, отвечающих условиям фильтра. Однако в этом алгоритме есть одно исключение. Для совместимости с функцией копирования поддерева, а также для обеспечения более надежного контроля со стороны администратора накопление прав доступа ограничивается сверху атрибутом ceiling.

Вместо объединения новых средств управления ACL с фильтрами и уже существующих ACL без фильтров, для поддержки ACL без фильтров были добавлены новые атрибуты управления доступом. Поддерживаемые атрибуты:

- ibm-filterAclEntry
- ibm-filterAclInherit

Атрибут ibm-filterAclEntry имеет тот же формат, что и aclEntry, плюс компонент фильтра объектов. Связанный атрибут ceiling - это ibm-filterAclInherit. Значение по умолчанию равно true. Если значение равно false, то накопление прерывается.

## Синтаксис атрибутов управления доступом

Каждым из этих атрибутов можно управлять с помощью записи в формате LDIF. Синтаксис новых атрибутов ACL с фильтрами представляет собой видоизмененную версию синтаксиса уже существующих атрибутов ACL без фильтров. Ниже приведено описание синтаксиса атрибутов ACI и entryOwner в формате BNF.

```
<aclEntry> ::=  <субъект> [ ":"  <права доступа> ]

<aclPropagate> ::=  "true" | "false"
<ibm-filterAclEntry> ::=  <субъект>  ":" <фильтр объектов>  [ ":"  <права доступа> ]

<ibm-filterAclInherit> ::=  "true" | "false"
<entryOwner> ::=  <субъект>

<ownerPropagate> ::= "true" | "false"

<субъект> ::= <тип Dn субъекта> ':' <Dn субъекта> |
                       <псевдо Dn>

<тип Dn субъекта> ::= "role" | "group" | "access-id"

<Dn субъекта> ::= <DN>

<DN> ::= отличительное имя в соответствии с RFC 2251, раздел 4.1.3.

<псевдо Dn> ::= "group:cn=anybody" | "group:cn=authenticated" |
                         "access-id:cn=this"
<фильтр объектов> ::= строка фильтра поиска в соответствии с RFC 2254, раздел 4
                               (расширенное сравнение не поддерживается)
<права доступа> ::= <список доступа> [":" <права доступа> ]

<список доступа> ::=  <доступ к объекту> | <доступ к атрибуту> |
                           <доступ к классу атрибутов>

<доступ к объекту> ::= "объект:" [<действие> ":"]  <права доступа к объекту>

<действие> ::= "grant" | "deny"

<права доступа к объекту> ::=  <право доступа к объекту> [ <права доступа к объекту> ]

<право доступа к объекту> ::= "a" | "d" |  ""

<права доступа к атрибуту> ::= "at." <имя атрибута> ":" [<действие> ":"]
                                    <права доступа к атрибуту>
```

```
<имя атрибута> ::= имя attributeType в соответствии с RFC 2251, раздел 4.1.4.
                       (OID или алфавитно-цифровая строка, начинающаяся с буквы,
                        допустимы символы "-" и ";")

<права доступа к атрибуту> ::=  <право доступа к атрибуту>
                                  [<права доступа к атрибуту>]

<право доступа к атрибуту> ::=  "r" | "w" | "s" | "c" |  ""

<доступ к классу атрибутов> ::= <класс> ":" [<действие> ":"]
                                   <права доступа к атрибуту>

<класс> ::= "normal" | "sensitive" | "critical" | "system" | "restricted"
```

## AclEntry и ibm-filterAclEntry

**Субъект:** Субъект (т.е. некто, запрашивающий доступ к объекту для выполнения определенной операции) представляет собой сочетание типа DN (отличительного имени) и собственно DN. Допустимые типы DN: access-id, Group и Role.

DN указывает конкретный ИД доступа (access-id), роль (role) или группу (group). Пример субъекта: access-id: cn=personA, o=IBM или group: cn=deptXYZ, o=IBM.

Поскольку двоеточие ( : ) применяется в качестве разделителя полей, то DN, содержащие символы двоеточия, должны быть заключены в двойные кавычки ( “” ). Если DN уже содержит символы двойных кавычек, то перед этими символами следует указать обратную косую черту (\).

Для управления доступом можно применять любые определенные в каталоге группы.

**Примечание:** Для управления доступом можно применять любые сочетания структурных классов объектов **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** или **groupOfURLs**, а также вспомогательных классов объектов **ibm-dynamicGroup** и **ibm-staticGroup**.

Еще одним типом DN, применяемым в модели управления доступом, является роль. Несмотря на то, что роли и группы реализованы очень похоже, лежащие в их основе концепции различаются. Когда для пользователя задается роль, то существует неявное предположение о том, что все права доступа, необходимые для выполнения связанных с этой ролью операций, уже настроены. В случае членства в группе нет никаких предварительных предположений о том, какие права доступа могут быть предоставлены (или аннулированы) при включении пользователя в группу.

Роли аналогичны группам в том смысле, что они также представлены объектами каталога. Кроме того, роли содержат списки DN групп. Роли, используемые для управления доступом, должны иметь класс объектов **AccessRole**.

**Псевдо DN:** В каталоге LDAP предусмотрено несколько псевдо DN. Они применяются для обозначения большого числа DN, имеющих общие характеристики по отношению либо к выполняемой операции, либо к объекту, над которым выполняется эта операция.

В настоящее время определено три псевдо DN:

**group:cn=anybody**
: Относится ко всем субъектам, в том числе и к не идентифицированным. В эту группу автоматически включаются все пользователи.

**group:cn=authenticated**
: Относится ко всем DN, для которых была успешно выполнена идентификация в каталоге. Способ идентификации при этом не учитывается.

**access-id:cn=this**

Относится к DN подключения, которое соответствует DN целевого объекта, над которым выполняется операция.

**Фильтр объектов:** Этот параметр относится только к ACL с фильтрами. В качестве формата фильтра объектов применяется строка поиска в соответствии с RFC 2254. Поскольку целевой объект уже известен, то фактически строка не используется для поиска. Вместо этого к рассматриваемому объекту применяется операция сравнения на основе фильтра, позволяющая определить, применим ли к нему данный набор значений ibm-filterAclEntry.

**Права доступа:** Права доступа могут применяться как к объекту в целом, так и к его отдельным атрибутам. Права доступа LDAP дискретны. Это значит, что предоставление какого-либо одного права не означает предоставления другого права. Права доступа можно сочетать, обеспечивая предоставление наборов прав доступа в соответствии с описанными ниже правилами. В качестве прав доступа может быть указано пустое значение, означающее, что данному субъекту права доступа к целевому объекту не предоставлены. Права доступа включают в себя три части:

**Действие:**

Допустимые значения: **grant** (разрешить) и **deny** (запретить).Если это поле отсутствует, то по умолчанию применяется значение **grant**.

**Разрешения:**

Существует шесть основных операций, которые можно выполнить над объектом каталога. Эти операции образуют следующий базовый набор разрешений ACI: добавление записи, удаление записи, считывание значения атрибута, запись значения атрибута, поиск атрибута и сравнение значения атрибута.

Возможные разрешения для атрибутов: чтение ( r ), запись ( w ), поиск ( s ) и сравнение ( c ). Кроме того, существуют разрешения для объектов, применяемые к записи в целом. Это разрешения на добавление дочерних записей ( a ) и удаление записи ( d ).

В следующей таблице перечислены разрешения, необходимые для выполнения каждой из операций LDAP.

| **Операция** | **Необходимые разрешения** |
|---|---|
| ldapadd | добавление (для родительской записи) |
| ldapdelete | удаление (для объекта) |
| ldapmodify | запись (для изменяемых атрибутов) |
| ldapsearch | • поиск, чтение (для атрибутов в RDN)<br>• поиск (для атрибутов, указанных в фильтре поиска)<br>• поиск (для атрибутов, возвращаемых только в виде имен)<br>• поиск, чтение (для атрибутов, возвращаемых со значениями) |
| ldapmodrdn | запись (для атрибутов RDN) |
| ldapcompare | сравнение (для сравниваемых атрибутов) |

**Примечание:** В операциях поиска у субъекта должны быть права доступа на поиск для всех атрибутов, указанных в фильтре поиска; в противном случае возвращается пустой список результатов. Для того чтобы операция поиска вернула набор записей, у субъекта должны быть права доступа на поиск и чтение для всех атрибутов в RDN возвращаемых записей.

**Целевая область прав доступа:**

Права доступа могут применяться к объекту в целом (например, права на добавление дочерней

записи или права на удаление записи), к отдельным атрибутам записи, либо к группам атрибутов (классы доступа к атрибутам) в соответствии с приведенной ниже информацией.

Атрибуты, требующие предоставления одинаковых прав доступа, группируются в классы. Соответствие между атрибутами и классами задается в файле схемы каталога. Эти классы являются дискретными: доступ к одному классу не означает неявного предоставления доступа к другому классу. Права доступа задаются по отношению ко всему классу доступа. Права доступа, указанные для какого-либо класса атрибутов, действуют по отношению ко всем атрибутам из этого класса доступа (если для отдельных атрибутов явно не заданы другие права доступа).

IBM определяет три класса, применяемые при определении прав доступа к пользовательским атрибутам: **normal**, **sensitive** и **critical**. Например, атрибут **commonName** относится к классу normal, а атрибут userpassword - к классу critical. Если не указано обратное, то пользовательские атрибуты относятся к классу доступа normal.

Определено также еще два класса доступа: system и restricted. К классу system относятся следующие атрибуты:

- **creatorsName**
- **modifiersName**
- **createTimestamp**
- **modifyTimestamp**
- **ownerSource**
- **aclSource**

Эти атрибуты обслуживаются сервером LDAP и пользователи каталогов имеют доступ к ним только для чтения. Атрибуты **OwnerSource** и **aclSource** описаны в разделе Наследование (см. “Наследование”).

К классу restricted относятся атрибуты, применяемые средствами управления доступом:

- **aclEntry**
- **aclPropagate**
- **entryOwner**
- **ownerPropagate**
- **ibm-filterAclEntry**
- **ibm-filterAclInherit**
- **ibm-effectiveAcl**

Права на чтение атрибутов этого класса есть у всех пользователей, но создавать, изменять и удалять атрибуты могут только пользователи **entryOwner**.

**Примечание:** Атрибут **ibm-effectiveAcl** допускает только чтение.

## EntryOwner

У владельцев записей (EntryOwner) есть полный набор прав доступа к объектам, позволяющий выполнять любые операции независимо от aclEntry. Кроме того, владельцы записей являются единственными субъектами, которые могут управлять записями aclEntry для объекта. EntryOwner - это субъект управления доступом, который может быть отдельным пользователем, группой или ролью.

**Примечание:** По умолчанию администратор каталога является владельцем всех объектов каталога и принадлежность записи администратору (entryOwnership) отменить нельзя.

## Наследование

Записи, в которых присутствует aclEntry, считаются записями с явной **aclEntry**. Аналогично, если для какой-либо записи указан **entryOwner**, то считается, что такая запись имеет явно указанного владельца. Эти два понятия не следует путать, поскольку запись с явным владельцем может иметь или не иметь явно

указанную **aclEntry**, а у записи с явной **aclEntry** может быть явный владелец. Если у записи нет какого-либо из этих значений, то отсутствующее значение наследуется от родительского узла дерева каталога.

Явно указанные значения **aclEntry** и **entryOwner** применяются к той записи, в которой они указаны. Кроме того, значение может применяться ко всем потомкам, не имеющим явно указанного значения. Такие значения считаются наследуемыми, поскольку они наследуются потомками в структуре каталога. Наследование каждого значения продолжается до тех пор, пока не встретится другое явное значение.

**Примечание:** Порядок наследования ACL с фильтрами отличается от порядка наследования ACL без фильтров. Их действие распространяется на все объекты поддерева, отвечающие условию сравнения. Дополнительная информация о различиях приведена в разделе “ACL с фильтрами” на стр. 61.

Значения **AclEntry** и **entryOwner** могут применяться только к одной конкретной записи (если значение propagation равно ″false″) или к записи и связанным с ней поддеревом (если значение propagation равно ″true″). Несмотря на то, что наследование выполняется как для **aclEntry**, так и для **entryOwner**, наследование этих значений никак не связано друг с другом.

Атрибуты **aclEntry** и **entryOwner** поддерживают указание нескольких значений, однако атрибуты propagation (**aclPropagate** и **ownerPropagate**) могут иметь только одно значение, действующее для всех значений атрибутов **aclEntry** или **entryOwner** данной записи.

Системные атрибуты **aclSource** и **ownerSource** содержат DN действующего узла, начиная с которого начинается применение **aclEntry** или **entryOwner** соответственно.Если такой узел не существует, то применяется значение **default**.

Действующие права доступа к объекту определяются с помощью следующих правил:

- Если для объекта явно указан набор атрибутов управления доступом, то именно они определяют права доступа к объекту.
- Если явно определенные атрибуты управления доступом отсутствуют, то выполняется поиск по более высоким уровням иерархии дерева до тех пор, пока не будет найден родительский узел с установленными атрибутами управления доступом.
- Если такой узел не найден, то субъекту предоставляются описанные ниже права доступа по умолчанию.

Владельцем записи является администратор каталога. Элементам псевдогруппы cn=anybody (все пользователи) предоставляются права доступа на чтение, поиск и сравнение атрибутов с классом доступа `normal`.

## Вычисление прав доступа

Выполнение каждой конкретной операции над целевым объектом разрешается или запрещается в зависимости от DN подключения субъекта. Процесс определения прав доступа прекращается сразу после определения прав доступа.

Сначала выполняется поиск действующего определения **entryOwnership** и **ACI**, проверка принадлежности записи, а затем - проверка значений ACI объекта.

ACL с фильтрами накапливают права доступа от записи самого низкого уровня вверх по цепочке предков, до записи самого высокого уровня в иерархии DIT. Действующие права доступа вычисляются как объединение разрешений или запретов для всех записей, отвечающих условиям фильтра. Для вычисления действующих прав доступа ACL с фильтрами применяется существующий набор правил уточнения и сочетания.

В пределах одной записи каталога атрибуты с фильтрами и без фильтров являются взаимно исключающими. Одновременное указание в записи атрибутов обоих типов недопустимо и является нарушением ограничений. При выявлении такой ситуации в ходе создания или обновления записи каталога операция не выполняется.

При вычислении действующих прав доступа режим вычисления определяется первым типом ACL, обнаруженным в цепочке предков целевого объекта. В режиме с фильтром все ACL без фильтров, обнаруженные в ходе вычисления действующих прав доступа, игнорируются. Аналогично, в режиме без фильтра игнорируются все обнаруженные в ходе вычисления ACL с фильтрами.

Для того чтобы ограничить накопление списков ACL с фильтрами при вычислении действующих прав доступа, в любой записи между самым нижним и самым верхним вхождением **ibm-filterAclEntry** в рассматриваемом поддереве можно указать атрибут **ibm-filterAclInherit** со значением ″false″. При этом подмножество атрибутов **ibm-filterAclEntry**, находящихся на более высоких уровнях иерархии, будет игнорироваться.

Если в режиме ACL с фильтрами ACL с фильтрами не применяются, то используется ACL по умолчанию (cn=anybody предоставляется доступ для чтения, поиска и сравнения атрибутов с классом доступа `normal`). Такая ситуация возможна в том случае, когда запрашиваемая запись не соответствует ни одному из фильтров, указанных в значениях **ibm-filterAclEntry**. Если вы не хотите, чтобы применялись указанные права доступа по умолчанию, то можно указать например следующий ACL фильтра по умолчанию:

```
ibm-filterAclEntry: group:cn=anybody:(objectclass=*):
```

В этом примере доступ будет по умолчанию запрещен. Для предоставления нужных прав доступа вы можете внести соответствующие изменения.

По умолчанию администратор каталога и главный или равноправный сервер (в случае копирования) имеет все права доступа ко всем объектам каталога, за исключением прав доступа на запись системных атрибутов. Все остальные владельцы записей (**entryOwner**) имеют все права доступа к принадлежащим им объектам, также за исключением прав доступа на запись системных атрибутов. У всех пользователей есть права доступа на чтение системных и ограниченных атрибутов. Изменить эти права доступа нельзя. Если у запрашивающего субъекта есть **entryOwnership** (т.е. он является владельцем записи), то права доступа определяются указанными выше значениями по умолчанию и вычисление прав доступа прекращается.

Если запрашивающий субъект не является владельцем записи, то проверяются значения ACI записей объекта. Права доступа к целевому объекту в соответствии с ACI определяются с помощью правил уточнения и сочетания.

**Правило уточнения**

При принятии решения о предоставлении или не предоставлении пользователю доступа применяются наиболее точные определения aclEntry. При этом применяется следующая иерархия уровней точности:

- Access-id является более точным, чем группа или роль. Группы и роли равнозначны.
- На одном уровне **dnType** права доступа уровня отдельных атрибутов являются более точными, чем права доступа уровня класса атрибутов.
- На одном уровне атрибута или класса атрибутов действие **deny** (запретить) является более точным, чем действие **grant** (разрешить).

**Правило сочетания**

Предоставленные субъектам права доступа с одинаковым уровнем точности сочетаются друг с другом. Если определить доступ в рамках одного уровня точности нельзя, то применяются определения прав доступа более общего уровня. Если после применения всех определенных ACI права доступа вычислить по-прежнему невозможно, то доступ запрещается.

**Примечание:** Если в ходе вычисления прав доступа были обнаружены **aclEntry** уровня access-id, то при дальнейшем вычислении прав доступа aclEntry уровня группы не учитываются. Исключением является случай, когда все **aclEntry**, соответствующие уровню access-id, определены в cn=this; в этом случае при вычислении используются также **aclEntry** уровня группы.

Другими словами, если в пределах записи объекта определенная запись ACI содержит DN субъекта access-id, совпадающее с DN подключения, то права доступа определяются на основе этой записи aclEntry. Если для одного DN субъекта определены права доступа уровня атрибутов, то они имеют более высокий приоритет, чем права доступа уровня класса атрибутов. Если в пределах определения прав доступа уровня атрибута или уровня класса атрибутов указаны конфликтующие права доступа, то запрет имеет более высокий приоритет, чем разрешение.

**Примечание:** Указанное в качестве прав доступа значение null запрещает указывать более точные определения прав доступа.

Если права доступа по-прежнему невозможно вычислить и все найденные соответствующие aclEntry определены в ″cn=this″, то проверяется членство в группах. Если пользователь входит в состав нескольких групп, то его права доступа будут определяться сочетанием прав доступа в этих группах. Кроме того, пользователь автоматически включается в группу cn=Anybody и, если он прошел идентификацию, - в группу cn=Authenticated. Если для этих групп определены права доступа, то они предоставляются пользователю.

**Примечание:** Сведения о членстве в группах и ролях определяются в момент подключения и считаются действительными либо до момента следующего подключения, либо до момента получения запроса на отключение. Вложенные группы и роли, то есть группы и роли, определенные как элементы других групп и ролей, не учитываются ни при определении членства в группах, ни при вычислении прав доступа.

Допустим, например, что атрибут attribute1 относится к классу атрибутов sensitive, пользователь cn=Person A, o=IBM входит в состав групп group1 и group2, и при этом определены следующие записи aclEntry:

1. aclEntry: access-id: cn=Person A, o=IBM: at.attributel:grant:rsc:sensitive:deny:rsc
2. aclEntry: group: cn=group1,o=IBM:critical:deny:rwsc
3. aclEntry: group: cn=group2,o=IBM:critical:grant:r:normal:grant:rsc

Пользователю будут предоставлены следующие права доступа:

- Права доступа ’rsc’ к атрибуту attribute1, (основания: 1. определение уровня атрибута имеет более высокий приоритет, чем определение уровня класса атрибутов).
- Доступ к другим атрибутам класса sensitive целевого объекта будет запрещен (основание: 1).
- Другие права доступа предоставлены не будут (2 и 3 НЕ учитываются при вычислении прав доступа).

Рассмотрим другой пример со следующими записями aclEntry:

1. aclEntry: access-id: cn=this: sensitive
2. aclEntry: group: cn=group1,o=IBM:sensitive:grant:rsc:normal:grant:rsc

Пользователю будут предоставлены следующие права доступа:

- Доступ к атрибутам класса sensitive предоставлен не будет (основание: 1. указанное в access-id значение Null запрещает включать права доступа к атрибутам класса sensitive из group1).
- Права доступа ’rsc’ к атрибутам класса normal (основание: 2).

## Определение ACI и владельцев записи

Ниже приведено два примера настройки административного субдомена. В первом примере рассматривается один пользователь, который будет являться владельцем (entryOwner) всего домена. Во втором примере таким владельцем является группа.

```
entryOwner: access-id:cn=Person A,o=IBM
ownerPropagate: true

entryOwner: group:cn=System Owners, o=IBM
ownerPropagate: true
```

В следующем примере продемонстрировано предоставление access-id ″cn=Person 1, o=IBM″ прав доступа на чтение, поиск и сравнение для атрибута attribute1. Эти права доступа относятся ко всем узлам поддерева,

включая узел, содержащий данный ACI, а также все узлы более низкого уровня, соответствующие фильтру сравнения ″(objectclass=groupOfNames)″. Накопление соответствующих атрибутов ibm-filteraclentry родительских узлов прервано на этой записи путем присвоения атрибуту ibm-filterAclInherit значения ″false″.

```
ibm-filterAclEntry: access-id:cn=Person 1,o=IBM:(objectclass=groupOfNames):
                    at.attribute1:grant:rsc

ibm-filterAclInherit: false
```

В следующем примере рассмотрено предоставление группе ″cn=Dept XYZ, o=IBM″ прав доступа на чтение, поиск и сравнение атрибута attribute1. Права доступа относятся ко всему поддереву, начиная от узла, содержащего данный ACI.

```
aclEntry: group:cn=Dept XYZ,o=IBM:at.attribute1:grant:rsc
aclPropagate: true
```

В следующем примере показано, как разрешить роли ″cn=System Admins,o=IBM″ добавление дочерних объектов данного узла, а также чтение, поиск и сравнение атрибута attribute2 и атрибутов класса critical. Права доступа применяются только к узлу, содержащему данный ACI.

```
aclEntry: role:cn=System Admins,o=IBM:object:grant:a:at.
         attribute2:grant:rsc:critical:grant:rsc
aclPropagate: false
```

## Изменение значения ACI и владельца записи

**Modify-replace**

Атрибут Modify-replace работает так же, как и все остальные атрибуты. Если значение атрибута не существует, то оно создается. Если значение атрибута существует, то оно заменяется.

Допустим, для записи существуют следующие ACI:

```
aclEntry: group:cn=Dept ABC,o=IBM:normal:grant:rsc
aclPropagate: true
```

Внесем следующие изменения:

```
dn: cn=some entry
changetype: modify
replace: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

Результирующий ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclPropagate: true
```

Значения ACI для Dept ABC во время замены будут утрачены.

Допустим, для записи существуют следующие ACI:

```
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):normal
                  :grant:rsc ibm-filterAclInherit: true
```

Внесем следующие изменения:

```
dn: cn=some entry
changetype: modify
replace: ibm-filterAclEntry
           ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
dn: cn=some entry
changetype: modify
replace: ibm-filterAclInherit
ibm-filterAclInherit: false
```

Результирующий ACI:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
       :grant:rsc ibm-filterAclInherit: false
```

Значения ACI для Dept ABC во время замены будут утрачены.

**Modify-add**

Если во время выполнения операции ldapmodify-add ACI или entryOwner не существует, то создаются ACI или entryOwner с заданными значениями. Если ACI или entryOwner существует, то указанные значения ACI или entryOwner добавляются. Допустим, например, что существует следующий ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

Внесем следующее изменение:

```
dn: cn=some entry
changetype: modify
add: aclEntry
aclEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

Будет получена следующая aclEntry с несколькими значениями:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

Допустим, например, что существует следующий ACI:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
```

Внесем следующее изменение:

```
dn: cn=some entry
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC)
                  :at.attribute1:grant:rsc
```

Будет получена следующая aclEntry с несколькими значениями:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):at.attribute1
                  :grant:rsc
```

Базовыми блоками являются права доступа для атрибута или класса атрибутов, а действия считаются уточняющими спецификаторами. Если одно и то же значение прав доступа указано несколько раз, то сохраняется только одно значение. Если одно и то же значение прав доступа добавлено несколько раз с разными действиями, то применяется последнее указанное действие. Если результирующее поле прав доступа пусто (″″), то это значение устанавливается равным null и применяется действие **grant**.

Допустим, например, что существует следующий ACI:

```
aclEntry: group:cn=Dept XYZ,O=IBM:normal:grant:rsc
```

Внесем следующее изменение:

```
dn: cn=some entry
changetype: modify
add: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:normal:deny:r:critical:deny::sensitive
        :grant:r
```

Будет получена следующая aclEntry:

```
aclEntry: group:cn=Dept XYZ,O=IBM:normal:grant:sc:normal:deny:r:critical
        :grant::sensitive:grant:r
```

Допустим, например, что существует следующий ACI:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,O=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
```

Внесем следующее изменение:

```
dn: cn=some entry
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :deny:r:critical:deny::sensitive:grant:r
```

yields an aclEntry of:

```
ibm-filterAclEntry: group:cn=Dept XYZ,O=IBM:(cn=Manager XYZ):normal
                  :grant:sc:normal:deny:r:critical:grant::sensitive
                  :grant:r
```

**Modify-delete**

Для удаления конкретного значения ACI применяется обычный синтаксис ldapmodify-delete.

Рассмотрим следующую ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rwsc

dn: cn = some entry
changetype: modify
delete: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
```

Оставшаяся на сервере ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rwsc
```

Рассмотрим следующую ACI:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
                  :grant:ad
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rwsc

dn: cn = some entry
changetype: modify
delete: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
                  :grant:ad
```

Оставшаяся на сервере ACI:

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rwsc
```

Удаление несуществующего значения ACI или entryOwner не приведет к внесению каких-либо изменений в ACI или entryOwner. При этом будет возвращен код указывающий, что значение атрибута не существует.

## Удаление значения ACI/владельца записи

Операция ldapmodify-delete позволяет удалить entryOwner с помощью следующего синтаксиса:

```
dn: cn = some entry
changetype: modify
delete: entryOwner
```

В данном случае рассматриваемая запись больше не будет иметь явного владельца (entryOwner). ownerPropagate также будет автоматически удален. В результате данная запись унаследует entryOwner от родительского узла дерева в соответствии с действующими правилами наследования.

Аналогичным образом можно полностью удалить aclEntry:

```
dn: cn = some entry
changetype: modify
delete: aclEntry
```

Удаление из записи последнего значения ACI или entryOwner - это не то же самое, что удаление ACI или entryOwner. Запись может содержать ACI или entryOwner без значений. В этом случае при запросе ACI или entryOwner клиенту не возвращается никакое значение как для текущего, так и для всех дочерних узлов вплоть до узла, на котором значение будет переопределено. Для того чтобы избежать появления никому не принадлежащих записей, у администратора каталога всегда есть полный доступ ко всем записям, даже если у этой записи существует пустое значение ACI или entryOwner.

### Получение значения ACI/владельца записи

Действующие значения ACI или entryOwner можно получить путем простого указания в операции поиска нужного атрибута ACL или entryOwner, например:

```
ldapsearch -b "cn=object A, o=ibm" -s base "objectclass=*"
    aclentry aclpropagate aclsource entryowner ownerpropagate ownersource
    ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl
```

Этот запрос вернет всю информацию ACL или entryOwner, применяемую при вычислении прав доступ к объекту A. Обратите внимание, что возвращаемые значения могут выглядеть несколько иначе, чем при первоначальном определении. Однако возвращенные значения будут эквивалентны своему первоначальному формату.

Поиск только по атрибуту ibm-filterAclEntry вернет только значения, относящиеся к содержащей его записи.

Для просмотра накопленных действующих значений доступа применяется предназначенный только для чтения операционный атрибут ibm-effectiveAcl. Запрос на поиск по атрибуту ibm-effectiveAcl вернет действующие права доступа к целевому объекту, вычисленные на основании ACL с фильтрами или без фильтров, в зависимости от конкретной структуры DIT.

Поскольку ACL с фильтрами могут быть получены от нескольких родительских объектов, то для просмотра списка всех исходных родительских объектов можно выполнить поиск по атрибуту aclSource.

### Особенности копирования поддерева

Для включения в процесс копирования поддерева средств управления доступом на основе фильтров на одном уровне с записью ibm-replicationContext или на более низком уровне должен присутствовать атрибут ibm-filterAclEntry.

Поскольку получить сведения о правах доступа родительских записей, находящихся в иерархии выше копируемого поддерева, невозможно, то в записи ibm-replicationContext должен быть указан атрибут ibm-filterAclInherit со значением **false**.

## Принадлежность объектов каталога LDAP

У любого объекта каталога LDAP есть, по крайней мере, один владелец. Владелец может удалить объект. Владельцу наравне с администратором разрешено изменять свойства принадлежности и атрибуты списка управления доступом (ACL) объекта. Принадлежность объекта может наследоваться или задаваться явно. Таким образом, принадлежность объекта можно задать одним из следующих способов:

- Явно задать принадлежность объекта.
- Указать, что объекты наследуют список владельцев от объектов более высокого уровня в иерархии каталога LDAP.

Сервер каталогов позволяют определить несколько владельцев для одного объекта. Кроме того, объект может принадлежать сам себе. Для этого в список владельцев объекта добавляется специальное DN `cn=this`. Предположим, что владельцем объекта `cn=A` является `cn=this`. Любой пользователь, подключившийся к серверу как `cn=A`, будет считаться владельцем объекта `cn=A`.

Дополнительная информация о работе со свойствами принадлежности приведена в разделе “Управление записями каталога” на стр. 179.

## Стратегия управления паролями

При использовании серверов LDAP для идентификации важно обеспечить поддержку сервером LDAP стратегий управления паролями, включая контроль сроков действия паролей, числа неудачных попыток входа в систему и правил выбора паролей. На сервере каталогов можно настраивать все три перечисленных типа стратегий. Стратегия применяется ко всем записям каталога с атрибутом userPassword. Определять разные стратегии для различных наборов пользователей нельзя. На сервере каталогов предусмотрен также механизм информирования клиентов о ситуациях, связанных со стратегией управления паролем (например, об истечении срока действия пароля через три дня), а также набор операционных атрибутов, с помощью которых администраторы могут, например, выполнять поиск пользователей с истекшим сроком действия паролей или с блокированными учетными записями.

Дополнительная информация о работе со свойствами стратегии управления паролями приведена в разделе “Управление паролями” на стр. 161.

**Настройка**

Существуют следующие варианты настройки параметров сервера, связанных с управлением паролями:

- Глобальное включение или выключение стратегии управления паролями
- Правила изменения пароля, включая:
  - Возможность изменения паролей пользователями. Обратите внимания, что эта стратегия применяется в дополнение к уже действующим средствам управления доступом. Таким образом, средства управления доступа должны предоставлять пользователю возможность изменения атрибута userPassword, а стратегия управления паролем должна разрешать пользователям изменять свои пароли. Если эта стратегия выключена, то пользователи не могут изменять свои пароли. В этом случае изменить пароль записи сможет только администратор или другой пользователь с правами доступа на изменение атрибута userPassword.
  - Необходимость изменения паролей после сброса. Если эта стратегия включена, то после изменения пароля кем-либо кроме самого пользователя пароль помечается как сброшенный и перед выполнением каких-либо других операций с каталогом пользователь должен изменить свой пароль. Операция подключения со сброшенным паролем выполняется как обычно. Для получения уведомления о необходимости изменения сброшенного пароля приложение должно поддерживать стратегию управления паролями.
  - Запрос у пользователей старого пароля при изменении пароля. Если включена эта стратегия, то пароль можно изменить только с помощью запроса, в котором предусмотрено удаление атрибута userPassword (со старым значением) и добавление нового значения userPassword. Тем самым возможность изменения пароля предоставляется только тем пользователям, которые знают текущий пароль. Администратор или другой пользователь с правами доступа на изменение атрибута userPassword также сможет в любой момент задать пароль.
- Правила истечения срока действия пароля, включая:
  - Срок действия паролей или не ограничен или ограничен определенным интервалом времени с момента последнего изменения.
  - Включение или выключение предупреждения пользователей о завершении срока действия пароля через определенное время. Для получения предупреждения о скором завершении срока действия пароля приложение должно поддерживать стратегию управления паролями.
  - Возможность настройки числа входов в систему, разрешенных пользователю после истечения срока действия его пароля. Приложения с поддержкой стратегии управления паролями будут получать уведомления об оставшемся числе входов в систему. Если вход в систему после истечения срока действия пароля запрещен, то пользователь не сможет пройти идентификацию или самостоятельно изменить свой истекший пароль.
- Правила проверки пароля, включая:

– Настраиваемый размер хронологии паролей, позволяющий серверу сохранять N последних паролей и запрещающий пользователям указывать уже применявшиеся пароли.
– Проверка синтаксиса паролей, включая настройку действий сервера при хэшировании паролей. При этом сервер может игнорировать стратегию в случае выполнения любого из следующих условий:
  - На сервере хранятся хэшированные пароли.
  - Клиент предоставляет серверу хэшированный пароль (такая ситуация возможна при передаче записей между серверами с помощью файла LDIF, когда исходный сервер использует хэшированные пароли).

  В этих случаях применение сервером всех синтаксических правил может оказаться невозможным. Поддерживаются следующие синтаксические правила: минимальная длина, минимальное число букв, минимальное число цифр или специальных символов, число повторяющихся символов, число символов нового пароля, отличающихся от символов старого пароля.

• Правила обработки неудачных попыток входа в систему, включая:
– Ограничение минимального времени между операциями изменения пароля, не позволяющее пользователям быстро перебрать ограниченный набор паролей и снова установить старый пароль.
– Ограничение максимального числа неудачных попыток входа в систему перед блокировкой учетной записи.
– Настраиваемый интервал блокировки пароля. Через указанное время работа с ранее заблокированной учетной записью может быть возобновлена. Эта возможность поможет обезопасить систему от атак хакеров, пытающихся подобрать пароль, не создавая при этом неудобств для пользователей, забывших свой пароль.
– Настраиваемый интервал отслеживания сервером числа неудачных попыток входа в систему. Если максимальное число неудачных попыток входа в систему будет достигнуто за указанный интервал времени, то учетная запись блокируется. По истечении заданного времени сервер сбрасывает информацию о предыдущих неудачных попытках входа в систему с помощью данной учетной записи.

Параметры стратегии управления паролями хранятся на сервере каталогов в объекте ″cn=pwdpolicy″, который выглядит следующим образом:

```
cn=pwdpolicy objectclass=container objectclass=pwdPolicy
objectclass=ibm-pwdPolicyExt
objectclass=top
cn=pwdPolicy
pwdExpireWarning=0
pwdGraceLoginLimit=0
passwordMaxRepeatedChars=0
pwdSafeModify=false
pwdattribute=userpassword
pwdinhistory=0
pwdchecksyntax=0
passwordminotherchars=0
passwordminalphachars=0
pwdminlength=0
passwordmindiffchars=0
pwdminage=0
pwdmaxage=0
pwdallowuserchange=true
pwdlockoutduration=0
ibm-pwdpolicy=true
pwdlockout=true
pwdmaxfailure=2
pwdfailurecountinterval=0
pwdmustchange=false
```

**Приложения с поддержкой стратегии управления паролями**

Предусмотренная на сервере Directory Server for iSeries поддержка стратегии управления паролями включает в себя ряд управляющих функций LDAP, которые можно применять в приложениях с поддержкой стратегии управления паролями для получения уведомлений о различных ситуациях, связанных с управлением паролями.

Приложения могут получать уведомления о следующих ситуациях:

- Врем, оставшееся до завершения срока действия пароля
- Число оставшихся попыток входа в систему после истечения срока действия пароля

Приложения могут также получать информацию о следующих ошибках:

- Истек срок действия пароля
- Учетная запись блокирована
- Пароль сброшен и его необходимо изменить
- Пользователю запрещено изменять свой пароль
- При изменении пароля необходимо указать старый пароль
- Новый пароль не соответствует синтаксическим правилам
- Новый пароль слишком короткий
- Пароль недавно уже изменялся
- Новый пароль недавно уже применялся

Применяется два управляющих элемента. Управляющий элемент запроса функции управления паролями позволяет сообщить серверу, что приложение должно получать информацию о ситуациях, связанных с управлением паролями. Этот управляющий элемент применяться приложением во всех операциях, в которых приложение должно получать такую информацию. Обычно это запрос на первоначальное подключение и все запросы на изменение пароля. При наличии управляющего элемента запроса функции управления паролями сервер в случае обнаружения любой из перечисленных выше ситуаций возвращает управляющий элемент ответа функции управления паролями.

В число API клиента сервера каталогов входят API, позволяющие обращаться к этим функциям из приложений на C. Это следующие API:

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

Для приложений, не использующих такие API, управляющие элементы описаны ниже. Для работы с этими управляющими элементами необходимо применять возможности, обеспечиваемые API клиента LDAP. Например, в интерфейсе Java Naming and Directory Interface (JNDI) предусмотрена встроенная поддержка некоторых стандартных управляющих элементов, а также предусмотрена среда поддержки тех управляющих элементов, которые не распознаются JNDI непосредственно.

**Управляющий элемент запроса функции управления паролями**

```
Имя: 1.3.6.1.4.1.42.2.27.8.5.1
Критичность управления: FALSE
Управляющее значение: Нет
```

**Управляющий элемент ответа функции управления паролями**

```
Имя: 1.3.6.1.4.1.42.2.27.8.5.1 (как в запросе)
Критичность управления: FALSE
Управляющее значение: Значение в кодировке BER, определенное в ASN.1 следующим образом:
  PasswordPolicyResponseValue ::= SEQUENCE {
  warning [0] CHOICE OPTIONAL {
  timeBeforeExpiration [0] INTEGER (0 .. MaxInt),
  graceLoginsRemaining [1] INTEGER (0 .. maxInt) }
  error  [1] ENUMERATED OPTIONAL {
  passwordExpired   (0),
```

```
accountLocked    (1),
changeAfterReset   (2),
passwordModNotAllowed (3),
mustSupplyOldPassword (4),
invalidPasswordSyntax (5),
passwordTooShort   (6),
passwordTooYoung   (7),
passwordInHistory   (8) } }
```

Как и другие элементы протокола LDAP, кодировка BER использует неявные теги.

**Операционные атрибуты стратегии управления паролями**

Для каждой записи, имеющей атрибут userPassword, сервер каталогов поддерживает набор операционных атрибутов. Пользователи с необходимыми правами доступа могут выполнять поиск по этим атрибутам. Кроме того, эти атрибуты могут использоваться в фильтрах поиска и возвращаться в ответе на поисковый запрос. Это следующие атрибуты.

- pwdChangedTime - Атрибут GeneralizedTime, содержащий время последнего изменения пароля.
- pwdAccountLockedTime - Атрибут GeneralizedTime, содержащий время блокировки учетной записи. Если учетная запись не блокирована, то этот атрибут отсутствует.
- pwdExpirationWarned - Атрибут GeneralizedTime, содержащий время первой отправки клиенту предупреждения о завершении срока действия пароля.
- pwdFailureTime - Многозначный атрибут GeneralizedTime, содержащий моменты времени, соответствующие последовательным неудачным попыткам входа в систему. Если последняя попытка входа в систему была удачной, то этот атрибут отсутствует.
- pwdGraceUseTime - Многозначный атрибут GeneralizedTime, содержащий моменты времени, соответствующие предыдущим входам в систему после истечения срока действия пароля.
- pwdReset - Атрибут Boolean, содержащий значение TRUE в том случае, если пароль был сброшен и пользователь должен его изменить.
- ibm-pwdAccountLocked - Булевский атрибут, обозначающий, что учетная запись заблокирована администратором.

**Копирование стратегии управления паролями**

Информация о стратегии управления паролями передается серверами-поставщиками серверам-потребителям. Изменения записи cn=pwdpolicy копируются также, как глобальные изменения, например, изменения схемы. Информация о состоянии стратегии управления паролями для отдельных записей также копируется, поэтому, например, в случае блокировки записи на сервере-поставщике, это действие будет воспроизведено и на всех серверах-копиях. Однако изменения состояния стратегии управления паролями, внесенные на серверах-копиях, предназначенных только для чтения, не воспроизводятся на других серверах.

## Идентификация

Управление доступом на сервере каталогов осуществляется на основании отличительного имени (DN), связанного с данным соединением. DN устанавливается в результате подключения к серверу каталогов (входа в систему).

При первоначальной настройке сервера каталогов для идентификации могут применяться следующие имена:

- Anonymous
- Администратор каталога (по умолчанию cn=administrator)
- Профайл спроецированного пользователя i5/OS (см. раздел “Спроецированная база данных операционной системы” на стр. 80)

Для того чтобы нескольким пользователям не приходилось работать с одной учетной записью администратора каталога, рекомендуется создать дополнительные записи пользователей, которым можно будет предоставить права доступа на управление различными частями каталога.

| Дополнительная информация приведена в разделе “Управление пользователями” на стр. 186.

С точки зрения LDAP существуют следующие среды идентификации:

- Простое подключение, когда приложение предоставляет DN и соответствующий ему пароль в простом текстовом формате
| • Подключение SASL, когда применяются дополнительные способы идентификации, включая CRAM-MD5,
| DIGEST-MD5, EXTERNAL, GSSAPI и OS400-PRFTKN.

**Простое подключение, DIGEST-MD5 и CRAM-MD5**

В случае простого подключения клиент должен указать DN существующей записи LDAP и пароль, соответствующий значению атрибута userPassword этой записи. Допустим, например, что вы создали для пользователя John Smith следующую запись:

```
sample.ldif:
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
cn: John Smith
        sn: smith
        userPassword: mypassword

ldapadd -D cn=administrator -w secret -f sample.ldif
```

После этого вы сможете использовать DN ″cn=John Smith,cn=users,o=acme,c=us″ в средствах управления доступом или включить это DN в состав группы.

Атрибут userPassword можно указать для нескольких стандартных классов объектов, включая, но не ограничиваясь этим, следующие классы: person, organizationalperson, inetorgperson, organization, organizationalunit и т.д.

В паролях сервера каталогов учитывается регистр символов. Если вы создадите запись, в которой атрибуту userPassword присвоено значение `secret`, то при попытке подключения с паролем `SECRET` будет выдано сообщение об ошибке.

При простом подключении клиент в составе запроса на подключение отправляет серверу пароль в текстовом виде. При такой передаче возможен перехват пароля на уровне протокола. Для защиты пароля следует применять соединение SSL (вся информация, передаваемая по соединениям SSL, шифруется). Кроме того, может применяться способ идентификации DIGEST-MD5 или SASL CRAM-MD5.

Для применения способа идентификации CRAM-MD5 необходимо, чтобы у сервера был доступ к паролю в текстовом виде (т.е. должна быть установлена опция защиты пароля `none`, что означает хранение пароля в незашифрованном виде и возможность его получения в текстовом формате с помощью операции поиска), и чтобы значение QRETSVRSEC (сохранение данных защиты сервера) было равным 1 (Сохранять данные). Клиент отправляет серверу значение DN. Сервер извлекает значение атрибута userPassword для записи и генерирует случайную строку. Затем эта случайная строка передается клиенту. После этого и клиент и сервер хэшируют эту случайную строку, используя пароль в качестве ключа, а затем клиент передает полученный результат серверу. Если хэшированные строки совпадают, то запрос на подключение считается успешным, причем пароль серверу не передается.

| Способ DIGEST-MD5 аналогичен способу CRAM-MD5. Для его применения тоже необходимо, чтобы у
| сервера был доступ к паролю в текстовом виде (для опции защиты пароля установлено значение `none`), и
| чтобы системное значение QRETSVRSEC было равным 1. Для DIGEST-MD5 необходимо, чтобы клиент
| отправлял на сервер не DN, а имя пользователя. Для того, чтобы способ DIGEST-MD5 мог применять

обычный пользователь (не администратор), необходимо, чтобы в каталоге не было других записей с тем же именем пользователя. Остальные отличия способа DIGEST-MD5 заключаются в большем количестве параметров конфигурации: область сервера, атрибут имени пользователя и пароль администратора. iSeries позволяет пользователям подключаться в качестве спроецированных или опубликованных пользователей, когда сервер сверяет предоставленный пароль с паролем в пользовательском профайле в системе. Так как текстовый пароль, используемый в пользовательских профайлах, недоступен серверу, то способ DIGEST-MD5 неприменим для спроецированных или опубликованных пользователей.

Дополнительная информация приведена в разделе “Настройка идентификации DIGEST-MD5 на сервере каталогов” на стр. 168.

**Подключение опубликованных пользователей**

Сервер каталогов может работать с записями LDAP, пароли которых совпадают с паролями соответствующих пользовательских профайлов той же операционной системы. Для этого запись должна отвечать следующим требованиям:

- У записи должен быть атрибут UID, значение которого должно совпадать с именем пользовательского профайла операционной системы.
- В записи не должно быть атрибута userPassword

Когда сервер получает запрос на подключение для записи, имеющей атрибут UID, но не имеющей атрибута userPassword, то сервер обращается к подсистеме защиты операционной системы и проверяет, является ли указанное значение UID допустимым именем пользовательского профайла, а указанный пароль - паролем этого профайла. Такие записи называются опубликованными пользователями, поскольку они создаются при публикации на сервере LDAP записей системного каталога рассылки (SDD).

**Подключение спроецированных пользователей**

Запись LDAP, соответствующая пользовательскому профайлу операционной системы, называется спроецированным пользователем. DN спроецированного пользователя вместе с правильным паролем соответствующего пользовательского профайла позволяют выполнить подключение к каталогу. Например, для пользователю JSMITH системы my-system.acme.com может соответствовать следующее DN:

```
os400-profile=JSMITH,cn=accounts,os400-sys=my-system.acme.com
```

**Подключение SASL EXTERNAL**

Если для идентификации клиентов применяется соединение SSL или TLS (например, у клиента есть частный сертификат), то можно воспользоваться способом идентификации SASL EXTERNAL. При таком способе идентификации в случае подключения SSL сервер получает сведения о клиенте из внешнего источника. Сервер получает общую часть сертификата клиента (передаваемую серверу в ходе установления соединения SSL) и извлекает соответствующее DN субъекта. Затем сервер LDAP связывает это DN с подключением.

Допустим, например, что сертификат выдан следующему пользователю:

```
common name: John Smith
organization unit: Engineering
organization: ACME
locality: Minneapolis
state: MN
country: US
```

В этом случае может применяться следующее DN субъекта:

```
cn=John Smith,ou=Engineering,o=acme,l=Minneapolis,st=MN,c=US
```

Обратите внимание, что элементы cn, ou, o, l, st и c применяются в том же порядке, в котором они составляют DN субъекта.

**Подключение SASL GSSAPI**

Механизм подключения SASL GSSAPI позволяет выполнять идентификацию с помощью паспорта Kerberos. Эта возможность полезна в случае, когда клиент выполнил KINIT или другой вид идентификации Kerberos (например, вход в систему домена Windows 2000). В этом случае сервер проверяет паспорт клиента, а затем получает имя области и имя субъекта Kerberos; например, субъект jsmith в области acme.com обычно обозначается как jsmith@acme.com. Сервер можно настроить таким образом, чтобы он связывал эти сведения с DN одним из следующих двух способов:

- Путем формирования псевдо DN в формате ibm-kn=jsmith@acme.com
- Путем поиска записи, имеющей вспомогательный класс ibm-securityidentities и значение altsecurityidenties в формате KERBEROS:<субъект>@<область>.

Запись для субъекта jsmith@acme.com может выглядеть следующим образом:

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
objectclass: ibm-securityidentities
cn: John Smith
sn: Smith
altsecurityidentities: kerberos:jsmith@acme.com
```

Информация о включении идентификации Kerberos приведена в разделе “Включение идентификации Kerberos на сервере каталогов” на стр. 167.

**Подключение OS400-PRFTKN**

Механизм подключения OS400-PRFTKN SASL применяется для идентификации на сервере с помощью ключа профайла (см. описание Generate Profile Token API). При использовании такого механизма сервер проверяет ключ профайла и связывает с подключением DN спроецированного пользовательского профайла (например, os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Если у приложения уже есть ключ профайла, то для простого подключения механизм не обращается повторно за именем и паролем пользовательского профайла. Для применения этого механизма используется API ldap_sasl_bind s с указанием значения null в качестве DN, `OS400-PRFTKN` в качестве механизма и с двоичными данными в формате berval с 32-байтовым ключом профайла в качестве идентификационных данных. При обращении к серверу каталогов с помощью API LDAP системы i5/OS или утилит командной строки QSH (например, ldapsearch) пароль можно опустить. При этом клиентские API будут идентифицироваться на сервере в качестве текущего пользовательского профайла для задания. Например:

```
> ldapsearch -m OS400-PRFTKN -b "o=ibm,c=us" "(uid=johndoe)"
```

выполняет поиск прав доступа в текущем пользовательском профайле, как если бы вы применили:

```
> ldapsearch -D os400-profile=myprofile,cn=accounts,os400-sys=mysystem -w mypassword -b
"o=ibm,c=us" "(uid=johndoe)"
```

**Применение LDAP в качестве службы идентификации**

LDAP очень часто применяется в качестве службы идентификации. Например, вы можете настроить идентификацию с помощью LDAP на Web-сервере. Настроив идентификацию с помощью LDAP на нескольких Web-серверах (или других приложениях), вы сможете поддерживать единый реестр пользователей этих приложений, а не определять пользователей заново для каждого нового приложения или экземпляра Web-сервера.

Как работает такая система? Web-сервер запрашивает у пользователя имя и пароль. Затем Web-сервер берет эту информацию и выполняет в каталоге LDAP поиск записи с указанным именем пользователя (например, вы можете настроить Web-сервер таким образом, чтобы в имя пользователя рассматривалось как атрибут LDAP ’uid’ или ’mail’). Если будет найдена ровно одна запись, то Web-сервер отправляет серверу запрос на

подключением с использованием DN только что найденной записи и указанного пользователем пароля. Если подключение выполняется успешно, значит идентификацию пользователя можно считать завершенной. Для защиты паролей от перехвата на уровне протокола можно применять соединения SSL.

Web-сервер может также сохранять сведения о применявшемся DN, позволяя приложению использовать это DN, например, для хранения каких-либо данных в этой записи, в другой записи или в отдельной базе данных, использующей DN в качестве ключа для поиска информации.

Вместо запроса на подключение часто также применяется операция сравнения LDAP. Например: `ldap_compare(ldap_session, dn, "userPassword", enteredPassword)`. Таким образом приложение может использовать только один сеанс LDAP, а не запускать и не завершать отдельный сеанс для каждого запроса на идентификацию.

## Предотвращение отказа в обслуживании

Сервер каталогов поддерживает защиту от следующих типов атак отказа в обслуживании:

- Клиенты, которые пересылают данные медленно, частично, либо не пересылают вообще
- Клиенты, которые не читают результатов данных или читают медленно
- Клиенты, которые не подключаются
- Клиенты, запросы которых порождают длительно выполняющиеся запросы к базе данных
- Клиенты, которые подключаются анонимно
- Загрузка сервера, мешающая администратору выполнять задачи администрирования сервера

Сервер каталогов дает администратору несколько вариантов защиты от атак отказа в обслуживании. Даже если сервер занят длительно выполняющейся операцией, администратор всегда может получить к нему доступ через аварийную нить. Кроме этого, контроль над доступом к серверу для администратора сохраняется, включая возможность отключения клиентов с конкретными IP-адресами или DN подключения, а также возможность запрещения анонимного доступа к серверу. Для того чтобы включить на сервере защиту от атак отказа в обслуживании, существуют и другие параметры конфигурации.

Дополнительная информация приведена в разделе:

- “Управление соединениями сервера” на стр. 122
- “Управление свойствами соединения” на стр. 123

# Спроецированная база данных операционной системы

Спроецированная база данных системы обеспечивает преобразование объектов i5/OS в записи дерева каталогов LDAP. Спроецированные объекты являются LDAP-представлениями объектов операционной системы, а не записями базы данных сервера LDAP. В записи дерева каталога проецируются только объекты пользовательских профайлов. Преобразование объектов пользовательских профайлов называется спроецированной базой данных пользователей операционной системы.

Операции LDAP преобразуются в функции операционной системы. Таким образом, для выполнения операций LDAP над объектами операционной системы применяются системные функции. Все операции LDAP с пользовательскими профайлами выполняются под управлением пользовательского профайла, связанного с соединением клиента.

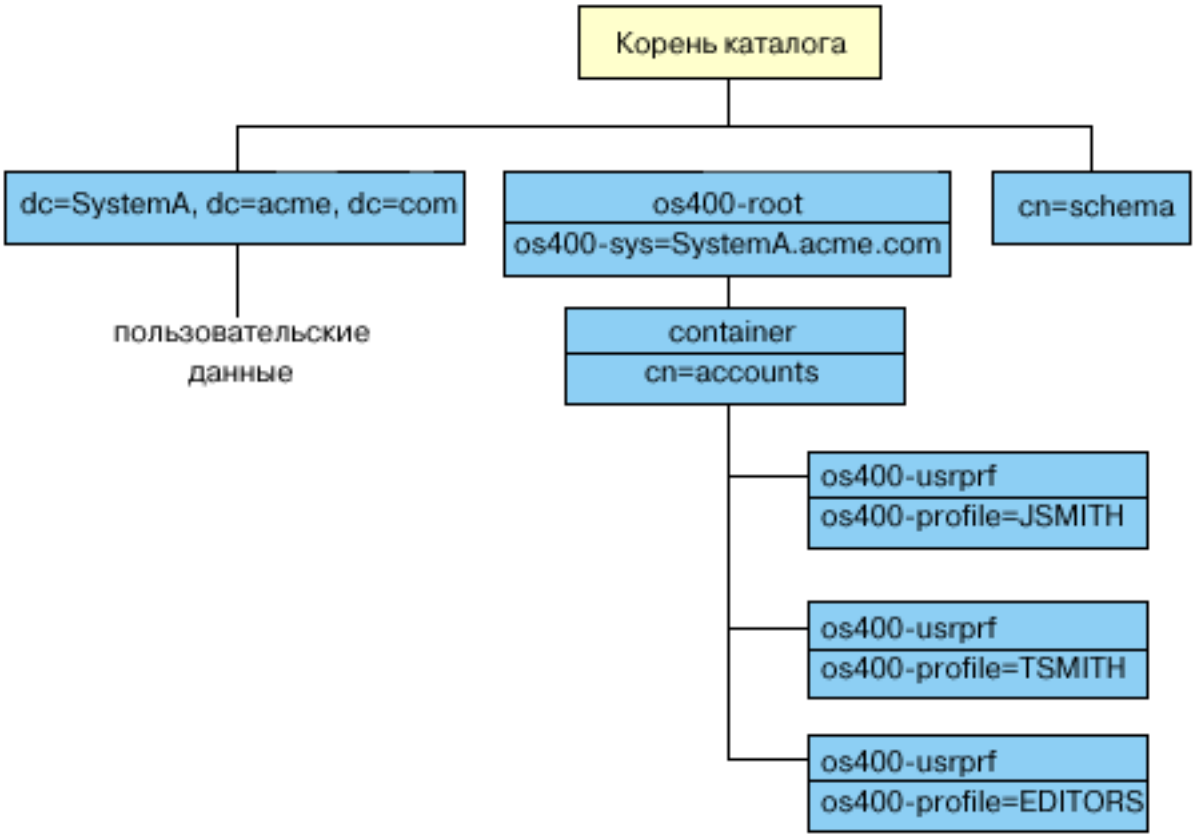
Более подробные сведения о спроецированной базе данных операционной системы приведены в следующих разделах:

- “Дерево информации каталога спроецированных пользователей” на стр. 81
- “Операции LDAP” на стр. 81
- “DN подключения администратора и копии” на стр. 85
- “Схема спроецированного пользователя” на стр. 86

## Дерево информации каталога спроецированных пользователей

На приведенном ниже рисунке показан пример дерева информации каталога (DIT) спроецированной базы данных пользователей. На рисунке изображены как профайлы отдельных пользователей, так и профайлы групп. JSMITH и TSMITH - пользовательские профайлы, связанные с идентификатором группы (GID) GID=*NONE (или 0); EDITORS - это профайл группы, связанный с ненулевым GID.

Суффикс dc=SystemA,dc=acme,dc=com указан на рисунке в качестве примера. Этот суффикс представляет текущую базу данных, управляющую другими записями LDAP. Суффикс cn=schema представляет текущую общую схему всего сервера.




Корнем дерева является суффикс, по умолчанию равный `os400-sys=`*`SystemA.acme.com`*, где *`SystemA.acme.com`* - имя системы. Класс объекта - `os400-root`. Хотя DIT нельзя изменить или удалить, можно изменить конфигурацию суффикса системных объектов. Однако при этом следует убедиться в том, что суффикс не указан в ACL или других объектах, в которые придется вносить изменения при изменении суффикса.

На предыдущем рисунке контейнер cn=accounts показан под корневой записью каталога. Этот объект нельзя изменить. Контейнер помещается на этом уровне для другой информации или объектов, которые операционная система может спроецировать в будущем. Под контейнером cn=accounts расположены пользовательские профайлы, спроецированные в виде `objectclass=os400-usrprf` . Эти пользовательские профайлы являются спроецированными пользовательскими профайлами и хранятся в LDAP в формате `os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com` .

## Операции LDAP

Спроецированные пользовательские профайлы могут применяться при выполнении перечисленных ниже операций LDAP.

**Подключение**

Клиент LDAP может указать спроецированный пользовательский профайл при подключения к серверу LDAP (во время идентификации). Для этого нужно задать пароль пользовательского профайла i5/OS и DN спроецированного пользовательского профайла в качестве DN подключения. Пример DN, указанного в запросе на подключение: `os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com`.

Для получения доступа к спроецированной базе данных клиент должен подключиться как спроецированный пользователь.

Для идентификации спроецированных пользователей на сервере каталогов существует также два дополнительных механизма:

- Подключение GSSAPI SASL. Если в операционной системе настроено применение преобразования идентификаторов в рамках предприятия (EIM), то сервер каталогов запрашивает EIM и определяет, есть ли связь между локальным пользовательским профайлом и исходным идентификатором Kerberos. При наличии такой связи сервер связывает пользовательский профайл с подключением и применяет его для обращения к проецируемому системному объекту. Дополнительная информация о EIM приведена в разделе EIM.
- Подключение OS400-PRFTKN SASL. Для идентификации на сервере каталогов может применять ключ профайла. Сервер связывает с подключением профайл этого ключа.

Сервер выполняет все операции от имени этого пользовательского профайла. DN спроецированного пользовательского профайла можно задать в ACL LDAP наравне с другими DN записей LDAP. Если в запросе на подключения указан спроецированный пользовательский профайл, то доступен только простой способ подключения.

**Поиск**

Спроецированная база данных системы поддерживает некоторые основные фильтры поиска. В фильтрах поиска можно указывать атрибуты objectclass, os400-profile и os400-gid. Значение атрибута os400-profile может содержать символы подстановки. Для атрибута os400-gid можно указать только значение `(os400-gid=0)`, соответствующее отдельному пользовательскому профайлу, или `!(os400-gid=0)`, соответствующее профайлу группы. В ходе поиска можно получить значения всех атрибутов пользовательского профайла, за исключением пароля и другой конфиденциальной информации.

Некоторые фильтры возвращают только значения атрибутов DN objectclass и os400-profile. Для получения более подробной информации необходимо выполнить дополнительную операцию поиска.

Приведенная ниже таблица содержит описание операций поиска в спроецированной базе данных системы.

*Таблица 3. Операции поиска для спроецированной базы данных системы*

| Запрошенный поиск | База поиска | Область поиска | Фильтр поиска | Комментарии |
|---|---|---|---|---|
| Возвратить информацию об os400-sys=SystemA, (необязательно) вложенных контейнерах и (необязательно) объектах в этих контейнерах. | os400-sys= SystemA.acme.com | base, sub или one | objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf | Возвращает атрибуты и соответствующие значения с учетом указанной области и фильтра. Внутренние атрибуты и их значения возвращаются для суффикса системных объектов и вложенного контейнера. |

*Таблица 3. Операции поиска для спроецированной базы данных системы (продолжение)*

| Запрошенный поиск | База поиска | Область поиска | Фильтр поиска | Комментарии |
|---|---|---|---|---|
| Возвратить все пользовательские профайлы. | cn=accounts, os400-sys= SystemA.acme.com | one или sub | os400-gid=0 | Для спроецированных пользовательских профайлов возвращаются только DN и значения атрибутов objectclass и os400-profile. В случае, если указаны другие фильтры, возвращается значение LDAP_UNWILLING_ TO_PERFORM. |
| Возвратить все группы. | cn=accounts, os400-sys= SystemA.acme.com | one или sub | (!(os400-gid=0)) | Для спроецированных пользовательских профайлов возвращаются только DN и значения атрибутов objectclass и os400-profile. В случае, если указаны другие фильтры, возвращается значение LDAP_UNWILLING_ TO_PERFORM. |
| Возвратить все пользовательские профайлы и профайлы групп. | cn=accounts, os400-sys= SystemA.acme.com | one или sub | os400-profile=* | Для спроецированных пользовательских профайлов возвращаются только DN и значения атрибутов objectclass и os400-profile. В случае, если указаны другие фильтры, возвращается значение LDAP_UNWILLING_ TO_PERFORM. |
| Возвратить информацию о конкретном пользовательском профайле или профайле группы, например, о пользовательском профайле JSMITH. | cn=accounts, os400-sys= SystemA.acme.com | one или sub | os400-profile=JSMITH | Можно получить и другие атрибуты. |
| Возвратить информацию о конкретном пользовательском профайле или профайле группы, например, о пользовательском профайле JSMITH. | os400-profile=JSMITH, cn=accounts, os400-sys= SystemA.acme.com | bas, sub или one | objectclass=os400-usrprf objectclass=* os400-profile=JSMITH | Можно получить и другие атрибуты. Хотя в качестве области поиска можно указать один уровень, ни одно значение не будет найдено, так как в дереве информации каталога нет записей, вложенных в пользовательский профайл JSMITH. |

*Таблица 3. Операции поиска для спроецированной базы данных системы (продолжение)*

| Запрошенный поиск | База поиска | Область поиска | Фильтр поиска | Комментарии |
|---|---|---|---|---|
| Возвратить все пользовательские профайлы и профайлы групп, начинающиеся с буквы A. | cn=accounts, os400-sys= SystemA.acme.com | one или sub | os400-profile=A* | Для спроецированных пользовательских профайлов возвращаются только DN и значения атрибутов objectclass и os400-profile. В случае, если указаны другие фильтры, возвращается значение LDAP_UNWILLING_ TO_PERFORM. |
| Возвратить все профайлы групп, начинающиеся с буквы G. | cn=accounts, os400-sys= SystemA.acme.com | one или sub | (&(!(os400-gid=0)) (os400-profile=G*)) | Для спроецированных пользовательских профайлов возвращаются только DN и значения атрибутов objectclass и os400-profile. В случае, если указаны другие фильтры, возвращается значение LDAP_UNWILLING_ TO_PERFORM. |
| Возвратить все пользовательские профайлы, начинающиеся с буквы A. | cn=accounts, os400-sys= SystemA.acme.com | one или sub | (&(os400-gid=0) (os400-profile=A*)) | Для спроецированных пользовательских профайлов возвращаются только DN и значения атрибутов objectclass и os400-profile. В случае, если указаны другие фильтры, возвращается значение LDAP_UNWILLING_ TO_PERFORM. |

**Сравнение**

Операция сравнения LDAP позволяет сравнивать значения атрибутов спроецированных пользовательских профайлов. Сравнивать атрибуты os400-aut и os400-docpwd нельзя.

**Добавление и изменение**

Пользовательские профайлы можно добавлять и изменять с помощью соответствующих операций LDAP.

**Удаление**

Пользовательские профайлы можно удалять с помощью соответствующей операции LDAP. Способ обработки параметров DLTUSRPRF, OWNOBJOPT и PGPOPT в новой версии определяется двумя управляющими значениями сервера LDAP. Эти значения можно задать в операции удаления LDAP. Дополнительная информация об обработке этих параметров приведена в описании команды Удалить пользовательский профайл (DLTUSRPRF).

Ниже указаны управляющие значения и соответствующие идентификаторы объектов (OID), которые клиент LDAP может задать в операции удаления.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Управляющее значение представляет собой строку в следующем формате:
  - controlValue ::= ownObjOpt [ newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  Управляющее значение ownObjOpt указывает действие, выполняемое в случае, если пользовательскому профайлу принадлежат объекты. Значение *NODLT указывает, что в этом случае пользовательский профайл не будет удален. Значение *DLT указывает, что следует удалить объекты, принадлежащие этому пользовательскому профайлу, а значение *CHGOWN указывает, что следует присвоить эти объекты другому профайлу.

  Значение newOwner задает пользовательский профайл, которому будут присвоены объекты, принадлежащие удаляемому профайлу. Это значение необходимо указать в том случае, если значение ownObjOpt равно *CHGOWN.

  Примеры управляющих значений:
  - *NODLT: указывает, что профайл, владеющий объектами, нельзя удалять
  - *CHGOWN SMITH: указывает, что объекты следует присвоить пользовательскому профайлу SMITH.
- Идентификатор объекта (OID) определен в файле ldap.h как LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Управляющее значение представляет собой строку в следующем формате:

    controlValue ::=pgpOpt [ newPgp [ newPgpAut ] ]
    pgpOpt ::= *NOCHG / *CHGPGP
    newPgp ::= *NONE / имя-пользовательского-профайла
    newPgpAut ::= *OLDPGP / *PRIVATE / *ALL / *CHANGE / *USE / *EXCLUDE

    Значение pgpOpt задает действие, выполняемое в случае, если удаляемый пользовательский профайл является основной группой для каких-либо объектов. Если указано значение *CHGPGP, то требуется задать значение newPgp. Значение newPgp задает имя профайла основной группы, либо *NONE. Если задан новый профайл основной группы, то можно указать и значение newPgpAut. Значение newPgpAut задает права доступа к объектам, которые предоставляются новой основной группе.

  Примеры управляющих значений:
  - *NOCHG: указывает, что профайл, являющийся основной группой для объектов, удалять нельзя.
  - *CHGPGP *NONE: указывает, что основная группа объектов будет удалена.
  - *CHGPGP SMITH *USE: указывает, что следует назначить основной группой пользовательский профайл SMITH и присвоить основной группе права доступа *USE.

  Если в операции удаления не указано одно из этих управляющих значений, то применяются текущие значения по умолчанию, заданные для команды QSYS/DLTUSRPRF.

**ModRDN**

Переименовать спроецированный пользовательский профайл нельзя, так как эта операция не поддерживается операционной системой.

**API импорта и экспорта**

API QgldImportLdif и QgldExportLdif не поддерживают импорт и экспорт данных в спроецированной базе данных системы.

## DN подключения администратора и копии

В качестве DN подключения копии или администратора можно указать спроецированный пользовательский профайл. В этом случае будет применяться пароль этого пользовательского профайла. Спроецированные

пользовательские профайлы могут выступать в роли администраторов LDAP, если им предоставлены права доступа к идентификатору функции Администратор сервера каталогов (QIBM_DIRSRV_ADMIN). Права доступа к функции администратора можно предоставить нескольким пользовательским профайлам.

Дополнительная информация приведена в разделе “Права доступа администратора” на стр. 59.

### Схема спроецированного пользователя

Классы объектов и атрибуты из спроецированной базы данных содержатся в общей схеме всего сервера. Имена атрибутов LDAP задаются в формате `os400-`*`nnn`*, где в качестве *`nnn`* обычно применяется ключевое слово атрибута в командах пользовательских профайлов.Например, атрибут os400-usrcls соответствует параметру USRCLS команды CRTUSRPRF. Значения атрибутов соответствуют значениям параметров команд CRTUSRPRF и CHGUSRPRF, либо значениям, отображаемым при просмотре пользовательских профайлов. Просмотреть определения класса объектов os400-usrprf и связанных с ним атрибутов os400-xxx можно с помощью Web-инструмента администрирования или с помощью другого приложения.

## Сервер каталогов и поддержка журналов в i5/OS

Для хранения информации сервер каталогов использует поддержку базы данных i5/OS. При добавлении записей каталога в базу данных сервер каталогов применяет управление фиксацией. Для этого необходима поддержка журналов i5/OS.

При первом запуске сервера или функции импорта LDIF создаются следующие объекты:

- Журнал
- Получатель журнала
- Необходимые таблицы базы данных

Журнал QSQJRN создается в настроенной библиотеке базы данных. Получатель журнала QSQJRN0001 сначала создается в настроенной библиотеке базы данных.

Вы можете изменить значения параметров по умолчанию с учетом параметров среды, размера и структуры каталога, а также стратегии сохранения и восстановления. В частности, может потребоваться изменить параметры работы с объектами и применяемые пороговые значения размера. При необходимости можно изменить параметры ведения журнала. Конфигурация LDAP по умолчанию предполагает удаление старых получателей журналов. Если настроена функция ведения протокола изменений, и необходимо сохранять старые получатели журналов, выполните в командной строке следующую команду:

```
CHGJRN JRN(QUSRDIRCL/QSQJRN) DLTRCV(*NO)
```

Если настроена функция ведения протокола изменений, то старые получатели журнала можно удалить с помощью следующей команды:

```
CHGJRN JRN(QUSRDIRCL/QSQJRN)  DLTRCV(*YES)
```

Информация о командах работы с журналами приведена в описании “команд OS/400” в главе Программирование.

## Уникальные атрибуты

Функция уникальных атрибутов гарантирует, что значения заданных атрибутов всегда будут уникальными в пределах каталога. Такие атрибуты можно указывать только в двух записях: cn=uniqueattribute,cn=localhost и cn=uniqueattribute,cn=IBMpolicies. Результаты поиска для таких атрибутов будут уникальными только для базы данных конкретного сервера. Результаты поиска, включающие результаты переадресации, не обязательно будут уникальными.

**Примечание:** Не могут быть уникальными двоичные и операционные атрибуты, атрибуты конфигурации и атрибуты классов объектов.

Уникальными можно настроить не все атрибуты. Определить поддержку уникальности для атрибута можно с помощью команды ldapexop:

- Для атрибутов, которые могут быть уникальными: `ldapexop -op getattributes -attrType unique -matches true`
- Для атрибутов, которые не могут быть уникальными: `ldapexop -op getattributes -attrType unique -matches false`

Дополнительная информация об уникальных атрибутах приведена в разделе “Управление уникальными атрибутами” на стр. 133.

## Операционные атрибуты

Существует несколько атрибутов, которые имеют для сервера каталогов особое значение и называются операционными атрибутами. Эти атрибуты обслуживаются сервером и либо отражают информацию об управляемых сервером записях, либо влияют на работу самого сервера. Эти атрибуты имеют следующие особенности:

- Эти атрибуты не возвращаются операциями поиска, если они не были явно (по имени) указаны в запросе.
- Атрибуты не относятся к какому-либо классу объектов. Записи, с которыми связаны атрибуты, определяет сервер.

Сервер каталогов поддерживает следующие наборы операционных атрибутов:

- в каждой записи содержатся атрибуты creatorsName, createTimestamp, modifiersName, modifyTimestamp. Они содержат DN подключения и время первоначального создания или последнего изменения записи. Эти атрибуты можно указывать в фильтрах поиска, например, для поиска всех записей, измененных после определенного момента времени. Пользователи не могут изменять значения этих атрибутов. Эти атрибуты копируются на сервер-потребитель, а также импортируются и экспортируются в файлы LDIF.
- ibm-entryuuid. Присутствует у каждой записи, созданной сервером V5R3 или более позднего выпуска. Этот атрибут представляет собой универсальный уникальный строковый идентификатор, присваиваемый сервером каждой записи при ее создании. Он полезен в ситуациях, когда приложения должны различать записи с одинаковыми именами, находящиеся на разных серверах. Для генерации идентификаторов, уникальных среди всех записей на всех серверах применяется алгоритм DCE UUID, использующий системное время, адрес адаптера и другую информацию.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. Дополнительная информация приведена в разделе “Списки управления доступом” на стр. 60.
- hasSubordinates. Есть у каждой записи. Имеет значение TRUE, если у этой записи есть подчиненные объекты.
- numSubordinates. Есть у каждой записи и содержит число ее дочерних записей.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory. Дополнительная информация приведена в разделе “Стратегия управления паролями” на стр. 73.
- subschemasubentry - Есть у каждой записи. Указывает размещение схемы для данной части дерева. Этот атрибут полезен для серверов с несколькими схемами, когда необходимо найти схему, применяемую в данной части дерева.

Полный список операционных атрибутов можно получить с помощью команды: `ldapexop -op getattributes -attrType operational -matches true`.

## Кэши сервера

Кэши LDAP - это буферы для быстрого сохранения в памяти информации LDAP: запросов, ответов и данных идентификации пользователей. Настройка кэшей LDAP может значительно повысить быстродействие.

Поиск с обращением к кэшу LDAP гораздо быстрее, чем поиск с подключением к DB2, даже если информация в DB2 кэшируется. Именно поэтому настройка кэшей LDAP значительно повышает производительность - не нужно вызывать базу данных. Особенно полезны кэши LDAP для приложений, в которых часто требуется загружать повторяющуюся кэшированную информацию.

В следующих разделах описываются кэши LDAP по видам и приводится информация по определению оптимальной настройки каждого кэша под конкретные нужды .

- “Кэш атрибутов”
- “Кэш фильтра” на стр. 89
- “Кэш записей” на стр. 89
- “Кэш ACL” на стр. 89

Информация о настройке кэша приведена в разделе “Настройка параметров производительности” на стр. 137.

## Кэш атрибутов

Главное достоинство кэша атрибутов - обработка фильтров в памяти, а не в базе данных. Еще одно преимущество - обновление кэша после каждой операции LDAP: добавления, удаления, изменения или операции modrdn.

При принятии решения о том, какие атрибуты требуется сохранять в памяти, следует учесть:

- Объем свободной памяти на сервере
- Размер каталога
- Типы фильтров поиска, с которыми обычно работает приложение

**Примечание:** Диспетчер кэша атрибутов поддерживает простые фильтры: фильтры точного соответствия и фильтры наличия. Также поддерживаются сложные фильтры - конъюнктивные и дизъюнктивные, причем составляющие их фильтры могут быть фильтрами точного соответствия, наличия, или, в свою очередь, тоже конъюнктивными или дизъюнктивными.

В кэш атрибутов можно добавлять не все атрибуты. Определить, можно ли добавить данный атрибут в кэш, позволяет команда ldapexop:

- Для атрибутов, которые можно добавить: `ldapexop -op getattributes -attrType attribute_cache -matches true`
- Для атрибутов, которые нельзя добавить: `ldapexop -op getattributes -attrType attribute_cache -matches false`

Кэширование атрибутов можно настроить вручную или автоматически. Для того чтобы настроить кэширование атрибутов вручную, администратору следует выполнить поиск по cn=monitor и определить, для каких атрибутов кэширование важнее всего. В результате этого поиска будет получена последняя информация, содержащая список кэшируемых атрибутов, объем памяти, требуемый для кэширования каждого атрибута, общий объем памяти, занимаемый кэшем атрибутов, настроенный объем памяти для кэша атрибутов и список атрибутов, наиболее часто запрашиваемых в поиске. С помощью этих сведений администратор может изменить максимальный объем памяти для кэша атрибутов, а также, при необходимости, может в любое время менять кэшируемые атрибуты - на основе периодического поиска по cn=monitor.

Также администратор может настроить автоматическое кэширование атрибутов. При автоматическом кэшировании сервер каталогов отслеживает сочетания атрибутов, которые наиболее важно сохранить в кэше. Размер кэша определяет администратор. Затем сервер периодически обновляет кэш. Период обновления также указывается администратором.

## Кэш фильтра

Когда клиент запрашивает данные, а диспетчер кэша атрибутов не может обработать этот запрос в памяти, запрос идет в кэш фильтра. В этом кэше содержатся сохраненные ИД записей. Как только запрос попадает в кэш фильтра, может произойти следующее:

- **В кэше фильтра найдены ИД, соответствующие параметрам фильтра, используемого в запросе.** В этом случае список этих ИД отправляется в кэш записей.
- **Соответствующие ИД записей не найдены в кэше фильтра.** В этом случае для обработки запроса необходимо искать нужные данные в DB2.

Для определения максимального размера кэша фильтра запустите задачу с разными размерами кэша и измерьте разницу в операциях в секунду.

Количество записей, которые можно добавить в кэш, задает переменная конфигурации кэша фильтра bypass limit. Например, если значение bypass limit равно 1000, то фильтр поиска, которому соответствует больше тысячи записей, не будет добавлен в кэш. Такой подход препятствует добавлению в кэш больших фильтров, которые могут записаться на место важных сохраненных записей. Для определения оптимального значения переменной bypass limit для конкретной задачи запустите задачу несколько раз и измерьте производительность.

## Кэш записей

В кэше записей содержатся данные о записях. Сначала в кэш записей посылается ИД записи. Если в кэше найдена запись с таким ИД, то она возвращается клиенту. В противном случае запрос ищет соответствующие записи в базе данных DB2.

Для определения максимального размера кэша записей запустите задачу с разными размерами кэша и замерьте разницу в операциях в секунду.

## Кэш ACL

В кэше ACL хранится информация об управлении доступом, например, владелец записи, права доступа для последних вызванных записей. Этот кэш предназначен для повышения быстродействия при определении разрешенных операций для записи: добавления, удаления, изменения и поиска. Если запись в кэше ACL не найдена, то информация об управлении доступом к этой записи берется из базы данных. Для подбора подходящего размера кэша ACL оцените быстродействие сервера при выполнении типичных задач с разными размерами кэша.

---

# Элементы управления и расширенные операции

**Управляющие элементы**

Управляющие элементы предоставляют серверу дополнительную информацию, которая определяет способ интерпретации сервером полученного запроса. Например, в запросе LDAP на удаление можно задать управляющий элемент `удалить поддерево`, указывающий, что сервер должен удалить не только данную запись, но и все ее дочерние записи. Управляющий элемент состоит из трех частей:

- Тип управляющего элемента, т.е. его OID.
- Индикатор критичности, указывающий, какие действия сервер должен предпринять в том случае, если он не поддерживает этот управляющий элемент. Это булевское значение. Значение FALSE указывает, что управляющий элемент не критичен и его можно проигнорировать, если он не поддерживается сервером. Значение TRUE указывает, что управляющий элемент критичен и если он не поддерживается сервером, то запрос обработан не будет и будет выдано сообщение об ошибке неподдерживаемого критичного расширения.
- Необязательное управляющее значение, которое содержит данные, связанные с этим управляющим элементом. Содержимое управляющего значения задается в формате ASN.1. Само значение представляет собой управляющие данные в кодировке BER.

**Расширенные операции**

Расширенные операции позволяют выполнять операции, выходящие за рамки стандартных операций LDAP. Например, расширенные операции позволяют объединить набор операций в единую транзакцию. Расширенная операция состоит из следующих элементов:

- Имя запроса, т.е. OID данной операции.
- Необязательное значение запроса, которое содержит данные, связанные с операцией. Содержимое значения запроса задается в формате ASN.1. Само значение представляет собой данные запроса в кодировке BER.

Расширенные операции обычно имеют расширенный ответ. Ответ состоит из следующих элементов:

- Компоненты стандартного результата операции LDAP (код ошибки, DN и сообщение об ошибке)
- Имя ответа, т.е. OID, идентифицирующий тип ответа
- Необязательное значение ответа, которое содержит связанные с ответом данные. Содержимое значения ответа задается в формате ASN.1. Само значение представляет собой данные ответа в кодировке BER.

Полный список управляющих функций и расширенных операций с объектными ИД и описаниями приведен в разделе “Идентификаторы объектов (OID)” на стр. 280.

# Глава 5. Сервер каталогов - Введение

Сервер каталогов автоматически устанавливается при установке i5/OS. При этом создается конфигурация по умолчанию. Для того чтобы начать работу с сервером каталогов, выполните следующие действия:

1. Если вы устанавливаете выпуск V5R4 и в предыдущем выпуске использовали сервер каталогов, то ознакомьтесь со сведениями о миграции. Дополнительная информация приведена в разделе “Особенности миграции”.
2. Составьте план установки и настройки сервера каталогов. Дополнительная информация приведена в разделе “Планирование конфигурации сервера каталогов” на стр. 96.
3. Для настройки сервера каталогов запустите мастер настройки. Дополнительная информация приведена в разделе “Настройка сервера каталогов” на стр. 97.
4. Запустите сервер. Дополнительная информация приведена в разделе “Запуск/останов сервера каталогов” на стр. 120.
5. С помощью Web-инструмента администрирования создайте или отредактируйте каталог LDAP. Дополнительная информация приведена в разделе “Web-администрирование” на стр. 105.
6. Дополнительные сведения о выполнении различных задач сервера каталогов приведены в разделе Глава 7, “Администрирование сервера каталогов”, на стр. 119.

## Особенности миграции

Сервер каталогов автоматически устанавливается при установке i5/OS. При первом запуске сервер автоматически преобразует все существующие данные о конфигурации. В связи с этим при первом запуске сервера возможна довольно продолжительная задержка.

**Примечание:** При установке и первоначальной настройке сервера выполняется преобразование конфигурации и файлов схемы. Если конфигурация и файлы схемы в каталоге /qibm/userdata/os400/dirsrv были восстановлены из резервной копии предыдущего выпуска, то по окончании первоначальной настройки сервера схема и конфигурация нового выпуска наложится на файлы от предыдущего, которые при этом повторно не преобразуются. Восстановление схемы и конфигурации предыдущего выпуска после преобразования могут привести к невозможности запуска сервера и другим непредсказуемым последствиям. Если требуется сохранить предыдущую конфигурацию и схему, то сохраняйте эти данные после успешного запуска сервера.

Если вы работали с сервером каталогов в V5R3 или V5R21, то обратитесь к разделу “Преобразование данных в V5R4 из V5R3 или V5R2”.

Если вы работали с сервером каталогов в V4R4, V4R5 или V5R1, то можно преобразовать данные в формат V5R4. Дополнительная информация приведена в разделе “Перенос данных из V4R4 ,V4R5 или V5R1 в V5R4” на стр. 92.

При наличии сети копирующих серверов обратитесь за дополнительной информацией к разделу “Миграция сети копирующих серверов” на стр. 93.

При использовании Kerberos обратитесь к разделу “Изменение имени службы Kerberos” на стр. 95.

## Преобразование данных в V5R4 из V5R3 или V5R2

В сервере каталогов i5/OS V5R4 появился целый ряд новых функций и возможностей. Внесенные изменения относятся как к серверу каталогов LDAP, так и к графическому пользовательскому интерфейсу Навигатора. Для работы с новыми функциями графического интерфейса необходимо установить Навигатор в системе,

подключенной к серверу iSeries по TCP/IP. Навигатор является компонентом продукта iSeries Access для Windows. Если в системе установлена более ранняя версия Навигатора, обновите ее до версии V5R4.

К выпуску i5/OS V5R4 можно непосредственно перейти от версий V5R2 и V5R3. При переходе к i5/OS V5R4 данные каталога и файлы схемы каталога автоматически преобразуются в формат V5R4.

При переходе к i5/OS V5R4 необходимо обратить внимание на следующие особенности:

- При переходе к выпуску V5R4 сервер каталогов автоматически преобразует файлы схемы в формат V5R4, а старые файлы схемы удаляются. Однако если файлы схемы были удалены или переименованы, то преобразование выполнено не будет. В этом случае будет показано сообщение об ошибке, либо сервер каталогов будут считать, что эти файлы уже преобразованы.
- После перехода к V5R4 вначале следует запустить сервер для преобразования существующих данных, и лишь затем импортировать новые данные. Импортировать данные, не запуская сервер, может только пользователь со специальными правами доступа. Сервер каталогов преобразует данные каталога в формат V5R4 при первом запуске сервера или импорте файла LDIF. Планируя процедуру перехода к новой версии, отведите время на выполнение этой операции.
- После перехода к новой версии сервер каталогов LDAP будет автоматически запускаться вместе с TCP/IP. Для того чтобы запретить автоматический запуск сервера, измените соответствующий параметр с помощью Навигатора.

## Перенос данных из V4R4 ,V4R5 или V5R1 в V5R4

К выпуску i5/OS V5R4 нельзя непосредственно перейти от V4R4, V4R5 или V5R1. Если вы хотите перейти от этих выпусков к V5R4, то можно воспользоваться любой из следующих процедур:

- “Переход от версий V4R4, V4R5 или V5R1 к промежуточному выпуску”
- “Сохранение библиотеки базы данных и установка выпуска V5R4” на стр. 93

При обновлении версии V4R4 необходимо обратить внимание на следующие особенности:

- V4R4 и более ранние выпуски сервера каталогов не принимали в расчет часовые пояса при создании записей системного времени. Начиная с версии V4R5, часовые пояса учитываются во всех операциях добавления и изменения записей каталога. По этой причине при переходе от выпуска V4R4 и более ранних выпусков сервер каталогов изменяет существующие атрибуты `createtimestamp` и `modifytimestamp` в соответствии с фактическим часовым поясом. При этом значение часового пояса, заданное на сервере iSeries, вычитается из значений системного времени, хранящихся в каталоге. В случае, если текущий часовой пояс отличается от значения, применявшегося в момент создания или изменения записей, новые значения системного времени не будут соответствовать исходному часовому поясу.
- При переходе от выпуска V4R4 или более раннего выпуска учтите, что данные каталога будут занимать примерно вдвое больше памяти. Это обусловлено тем, что в V4R4 и более ранних версиях сервер каталогов поддерживал только набор символов IA5 и хранил данные в CCSID 37 (однобайтный формат). В настоящий момент сервер каталогов поддерживает полный набор символов ISO 10646. После обновления вначале следует запустить сервер для преобразования существующих данных, и лишь затем импортировать новые данные. Импортировать данные, не запуская сервер, может только пользователь со специальными правами доступа.

### Переход от версий V4R4, V4R5 или V5R1 к промежуточному выпуску

Несмотря на то, что непосредственный переход от версий V4R4, V4R5 и V5R1 к версии V5R4 не поддерживается, доступны следующие варианты обновления:

- переход от выпуска V4R4 или V4R5 к выпуску V5R1
- переход от выпуска V4R5 или V5R1 к выпуску V5R2
- переход от выпуска V5R1 или V5R2 к выпуску V5R3
- переход от выпуска V5R2 или V5R3 к выпуску V5R4

Одним из способов обновления сервера каталогов является переход к промежуточному выпуску (V5R2 или V5R3), а затем - к V5R4. Более подробные сведения об установке i5/OS приведены в разделе *Установка*

*программ* . Выполните переход с помощью следующей процедуры. Схема должна преобразоваться автоматически. После каждой установки проверьте наличие изменений схемы.

1. В случае V4R4: установите выпуск V5R1. Затем установите V5R3.
2. В случае V4R5: установите V5R1 или V5R2. Если вы установили V5R1, то затем устанавливайте V5R2 или V5R3.
3. В случае V5R1: установите V5R3.
4. В случае V5R2 или V5R3: установите V5R4.
5. Запустите сервер каталогов, если он еще не запущен.

### Сохранение библиотеки базы данных и установка выпуска V5R4

Для того чтобы перейти к новому выпуску сервера каталогов, можно сохранить библиотеку базы данных, с которой работает сервер каталогов V4R4 или V4R5, а затем восстановить ее после установки V5R4. При этом не приходится устанавливать промежуточный выпуск. Однако в ходе этой процедуры не переносятся параметры сервера, поэтому их придется настроить заново. Более подробные сведения об установке i5/OS приведены в разделе *Установка программ* . Для перехода к новой версии продукта выполните следующие действия:

1. Запишите изменения, внесенные в файлы схемы в каталоге /QIBM/UserData/OS400/DirSrv. Файлы схемы не переносятся автоматически, поэтому все изменения потребуется заново внести вручную.Если изменения были внесены в схему с помощью файлов LDIF и утилиты ldapmodify, то найдите эти файлы, чтобы воспользоваться ими после перехода к новому выпуску. Для просмотра конкретного атрибута или определения класса объектов можно воспользоваться инструментом управления каталогами или Web-инструментом администрирования (из другой системы V5R4). Если изменение заключается только в добавлении новых атрибутов или классов объектов, то скопируйте файл /qibm/userdata/os400/dirsrv/v3.modifiedschema. Этот файл пригодится при построении файла LDIF, содержащего изменения схемы. Дополнительная информация приведена в разделе “Схема” на стр. 18.
2. Запишите параметры конфигурации, заданные в свойствах сервера каталогов, в том числе имя библиотеки базы данных.
3. Сохраните библиотеку базы данных, указанную в конфигурации сервера каталогов. Если вы настраивали протокол изменений, то нужно будет также сохранить библиотеку QUSRDIRCL.
4. Запишите параметры конфигурации публикации. Публикацию конфигурации (кроме данных о пароле) можно просмотреть с помощью Навигатора, выбрав вкладку **Службы каталогов** раздела **Свойства** системы.
5. Установите в системе i5/OS выпуск V5R4.
6. Настройте сервер каталогов с помощью EZ-Setup.
7. Восстановите библиотеку базы данных, сохраненную на шаге 3. Если на шаге 3 вы сохраняли библиотеку QUSRDIRCL, то восстановите ее.
8. С помощью Навигатора внесите изменения в конфигурацию сервера каталогов. Укажите библиотеку базы данных, которая была настроена ранее и которую вы восстановили на предыдущих шагах.
9. С помощью Навигатора восстановите конфигурацию функции публикации.
10. Перезапустите сервер каталогов.
11. С помощью Web-инструмента администрирования внесите в файл схемы изменения, записанные на шаге 1.

## Миграция сети копирующих серверов

При первом запуске главный сервер преобразует хранящуюся в каталоге информацию об управлении копированием. Записи с классом объектов replicaObject в поддереве cn=localhost заменяются на записи новой модели копирования (дополнительная информация приведена в разделе “Копирование” на стр. 39). На главном сервере настраивается копирование всех суффиксов каталога. Создаются записи соглашений о

копировании с атрибутом ibm-replicationOnHold, равным true. Тем самым обеспечивается возможность накопления внесенных на главном сервере изменений до того момента, пока сервер-копия не будет готов к их обработке.

Все эти запись образуют топологию копирования. Новый главный сервер может работать с серверами-копиями предыдущего выпуска; при этом данные, относящиеся к функциям нового выпуска, не будут копироваться на серверы предыдущих выпусков. Вы должны экспортировать с главного сервера записи топологии копирования и добавить их на каждый обновленный сервер-копию. Для экспорта воспользуйтесь инструментом командной строки Qshell “ldapsearch” на стр. 219 и сохраните вывод в файле. Команда поиска должна выглядеть примерно следующим образом:

```
ldapsearch -h хост-главного-сервера -p порт-главного-сервера \
 -D DN-администратора-главного-сервера -w пароль-администратора-главного-сервера \
 -b ibm-replicagroup=default,DN-записи-суффикса \
 -L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
     > replication.topology.ldif
```

Эта команда создаст в текущем рабочем каталоге файл LDIF с именем replication.topology.ldif. Файл будет содержать только новые записи.

**Примечание:** Не включайте следующие суффиксы:

- cn=changelog
- cn=localhost
- cn=pwdpolicy
- cn=schema
- cn=configuration

Включать следует только суффиксы, созданные пользователем.

Повторите команду на главном сервере для каждого суффикса, но вместо “>” указывайте символы “>>”, позволяющие добавить результаты очередной операции поиска в конец файла вывода. После заполнения файла скопируйте его на серверы-копии.

После обновления серверов-копий добавьте на них полученный файл; не добавляйте файл на серверы предыдущей версии. Перед добавлением файла необходимо перезапустить сервер.

Для запуска сервера выберите в Навигаторе пункт **Запустить** . Дополнительная информация приведена в разделе “Запуск/останов сервера каталогов” на стр. 120.

Для останова сервера выберите в Навигаторе пункт **Остановить**. Дополнительная информация приведена в разделе “Запуск/останов сервера каталогов” на стр. 120.

При добавлении файла на сервер-копию убедитесь, что этот сервер не работает. Добавить данные можно с помощью опции Навигатора **Импортировать файл**.

После загрузки записей топологии копирования запустите сервер-копию и возобновите копирование. Возобновить копирование можно одним из следующих способов:

- На главном сервере выберите в Web-инструменте администрирования опцию **Управление очередями** в разделе **Управление копированием**.
- Воспользуйтесь утилитой командной строки **ldapexop**. Например:

  ```
  ldapexop -h хост-главного-сервера -p порт-главного-сервера \
   -D DN-администратора-главного-сервера \
  -w пароль-администратора-главного-сервера \
   -op controlrepl -action resume -ra DN-соглашения-о-копировании
  ```

  Эта команда возобновит копирование для сервера, определенного в записи с указанным DN.

Для того чтобы определить, какое DN соглашения о копировании соответствует серверу-копии, просмотрите файл replication.topology.ldif. Главный сервер заносит в протокол сообщение о том, что запущено копирование для этого сервера копии, а также предупреждение о том, что ИД сервера-копии в соглашении не соответствует ИД сервера-копии. Для применения правильного ИД сервера в соглашении о копировании перейдите в раздел **Управление копированием** в Web-инструменте администрирования или воспользуйтесь утилитой командной строки **ldapmodify**. Например:

```
ldapmodify -c -h хост-главного-сервера -p порт-главного-сервера \
 -D DN-администратора-главного-сервера -w пароль-администратора-главного-сервера
dn: DN-соглашения-о-копировании
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: ИД-сервера-копии
```

Эти команды можно вводить непосредственно в командной строке или сохранить их в файле LDIF, а затем указать этот файл в команде с помощью опции **-i** *файл*. Для прерывания команды можно воспользоваться функцией **Прервать предыдущий запрос**.

Миграция сервера-копии завершена.

Для того чтобы продолжить работу с сервером-копией предыдущего выпуска также необходимо возобновить копирование с помощью утилиты командной строки **ldapexop** или с помощью опции **Управление копированием** в Web-инструменте администрирования для этой копии. Если миграция сервера-копии предыдущего выпуска была выполнена позже, то для синхронизации данных каталога воспользуйтесь утилитой командной строки **ldapdiff**. При этом на сервере-копии будут обновлены все записи и атрибуты, которые не была скопированы.

## Изменение имени службы Kerberos

Начиная с версии V5R3, изменилось имя службы идентификации GSSAPI (Kerberos), применяемое в API клиентов и сервера каталогов. Новое имя несовместимо с именем службы, применявшимся до V5R3 (это изменение присутствует также в V5R2M0 PTF 5722SS1-SI08487).

До выпуска V5R3 в API клиентов и сервера каталогов имя службы при использовании механизма идентификации GSSAPI (Kerberos) указывалось в формате `LDAP/имя-хоста-dns@область-Kerberos`. Это имя не соответствует стандартам идентификации GSSAPI, в которых требуется, чтобы имя субъекта начиналось со строки ″ldap″ в нижнем регистре. В результате API клиентов и сервера каталогов не всегда могли взаимодействовать с продуктами других поставщиков. В частности, такая ситуация возникала в том случае, если в центре рассылки ключей Kerberos (KDC) в именах субъектов учитывался регистр символов. Вместе с операционной системой поставляется пример клиента, использующего правильное имя службы - это широко распространенный API клиента LDAP Java, комплекс связи LDAP для JNDI.

В V5R3M0 имя службы изменено в соответствии со стандартами. При этом, однако, возникли новые проблемы совместимости.

- После установки этого выпуска будет невозможно запустить сервер каталогов, на котором настроена идентификация GSSAPI. Это связано с использованием в файле keytab сервера идентификационных данных со старым именем службы (LDAP/mysys.ibm.com@IBM.COM), в то время как сервер требует применения нового имени службы (ldap/mysys.ibm.com@IBM.COM).
- Сервер каталогов или приложение LDAP, использующие API LDAP V5R3M0 в ряде могут не пройти идентификацию при взаимодействии со старыми серверами и клиентами OS/400. Для исправления этой ситуации выполните следующие действия:
  1. Если в KDC учитывается регистр символов в именах субъектов, то создайте учетную запись с правильным именем службы (ldap/mysys.ibm.com@IBM.COM).
  2. Обновите файл keytab сервера каталогов, указав в нем идентификационные данные с новым именем службы. При этом рекомендуется также удалить старые идентификационные данные. Для обновления файла keytab можно воспользоваться утилитой Qshell keytab. По умолчанию сервер каталогов

использует файл /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. Мастер службы сетевой идентификации (Kerberos) V5R3M0 в Навигаторе iSeries также создает записи keytab с новым именем службы.

3. В системах V5R2M0 OS/400, в которых применяется GSSAPI, пакет PTF 5722SS1-SI08487.

Вы также можете продолжать использование в API клиентов и сервера каталогов старое имя службы. Такой подход возможен, например, при использовании идентификации Kerberos в смешанной сети, включающей как системы с PTF, так и системы без PTF. В этом случае необходимо установить переменную среды LDAP_KRB_SERVICE_NAME. Установить переменную среды для всей системы (для настройки имени службы на всем сервере) можно с помощью следующей команды:

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

эту же операцию можно выполнить с помощью QSH (для работы с утилитами LDAP, запускаемыми в этом сеансе QSH):

```
export LDAP_KRB_SERVICE_NAME=1
```

## Планирование конфигурации сервера каталогов

Перед установкой сервера каталогов и настройкой каталога LDAP необходимо продумать структуру и параметры каталога. Обратите внимание на следующие параметры:

- **Организация каталога**. Продумайте структуру каталога и определите, какие суффиксы и атрибуты будет применять сервер. Дополнительная информация приведена в разделах “Рекомендуемые способы работы со структурой каталогов” на стр. 103, “Каталоги” на стр. 9, “Суффикс (контекст имен)” на стр. 17 и “Атрибуты” на стр. 22.
- **Определите размер будущего каталога**. Исходя из этого размера можно оценить необходимый объем памяти. Размер каталога зависит от следующих параметров:
  - Число атрибутов в схеме каталога.
  - Число записей на сервере.
  - Тип информации, хранящейся на сервере.

  Например, пустой каталог, применяющий схему сервера каталогов по умолчанию, занимает приблизительно 10 Мб дискового пространства. Каталог со схемой по умолчанию, содержащий 1000 записей со стандартной информацией о сотрудниках компании, занимает примерно 30 Мб. Фактический размер каталога зависит от выбранных атрибутов. Необходимый объем памяти значительно возрастет, если вы планируете хранить в каталоге большие объекты, например, изображения.
- **Выберите необходимые средства защиты**.

  Сервер каталогов допускает применение стратегии управления паролями, гарантирующей периодическое изменение паролей пользователями, а также соответствие паролей предъявляемым в организации требованиям.

  Для защиты каналов связи сервер каталогов поддерживает применение протоколов SSL, TSL и цифровых сертификатов. Поддерживается также идентификация Kerberos.

  Сервер каталогов позволяет настраивать доступ к объектам каталога с помощью списков управления доступом (ACL). Для защиты каталога можно также воспользоваться системными средствами контроля за действиями.

  Необходимо выбрать стратегию управления паролями.
- **Выберите DN и пароль администратора**. DN администратора по умолчанию `cn=administrator`. Это единственный идентификатор, у которого после первоначальной настройки сервера есть права доступа на создание и изменение записей каталога. Вы можете воспользоваться DN администратора по умолчанию или выбрать другое DN. Необходимо также задать пароль для DN администратора.
- **Установите программное обеспечение, необходимое для Web-инструмента администрирования сервера каталогов**. Для работы с Web-инструментом администрирования сервера каталогов на сервере iSeries должны быть установлены следующие продукты:
  - IBM HTTP Server for iSeries (5722-DG1)

– IBM WebSphere Application Server - Express (5722-IWE - базовый компонент и компонент 2)

Дополнительная информация о продуктах IBM HTTP Server for iSeries и IBM WebSphere Application Server - Express приведена в разделе IBM HTTP Server.

## Настройка сервера каталогов

1. Если в системе не была настроена публикация информации на другом сервере LDAP, и на сервере DNS TCP/IP не определены серверы LDAP, то сервер каталогов автоматически устанавливается с ограниченной конфигурацией по умолчанию. Дополнительная информация приведена в разделе “Конфигурация сервера каталогов по умолчанию” на стр. 98. Вы можете настроить отдельные параметры сервера каталогов с помощью мастера. Этот мастер можно запустить как в процессе настройки EZ-Setup, так и позже - с помощью Навигатора. Этот мастер позволяет выполнить первоначальную настройку сервера каталогов. Кроме того, с его помощью можно изменить конфигурацию сервера каталогов.

   **Примечание:** При изменении конфигурации сервера с помощью этого мастера настройка сервера начинается с самого начала. Первоначальная конфигурация не изменяется, а удаляется. Однако данные каталога не удаляются, а сохраняются в библиотеке, выбранной при установке (по умолчанию QUSRDIRDB). Протокол изменений также сохраняется без изменений (по умолчанию - в библиотеке QUSRDIRCL).

   Для того чтобы начать установку ″с нуля″ перед запуском мастера необходимо очистить эти две библиотеки.

   Для того чтобы изменить конфигурацию сервера каталогов, а не очистить ее полностью, щелкните правой кнопкой мыши на пункте **Каталог** и выберите опцию **Свойства**. При этом исходная конфигурация будет сохранена.

   Для настройки сервера необходимы специальные права доступа *ALLOBJ и *IOSYSCFG. Для настройки функции контроля за действиями дополнительно потребуются специальные права доступа *AUDIT.
2. Для запуска Мастера настройки сервера каталогов выполните следующие действия:
   a. В Навигаторе откройте **Сеть**.
   b. Откройте **Серверы**.
   c. Выберите **TCP/IP**.
   d. Щелкните правой кнопкой мыши на пункте **IBM Directory Server** и выберите **Настроить**.

      **Примечание:** Если сервер каталогов уже настроен, выберите опцию **Изменить конфигурацию** вместо опции **Настроить**.
3. Настройте сервер каталогов, следуя указаниям мастера.

   **Примечание:** Возможно, потребуется разместить библиотеку, содержащую данные каталога, в пользовательском пуле вспомогательной памяти (ASP), а не в системном ASP. Обратите внимание, что эту библиотеку нельзя поместить в независимый ASP. В противном случае вам не удастся настроить, изменить конфигурацию или запустить сервер, связанный с этой библиотекой.
4. По завершении работы мастера будет создана базовая конфигурация сервера каталогов. Если в системе применяется продукт Lotus Domino, то порт 389 (порт сервера LDAP по умолчанию) может быть уже занят функцией LDAP Domino. Выполните одно из следующих действий:
   - Измените порт, применяемый Lotus Domino. Дополнительная информация приведена в разделе Электронная почта главы “ Применение хоста LDAP Domino и сервера каталогов в одной системе iSeries”.
   - Измените порт, применяемый сервером каталогов. Дополнительная информация приведена в разделе “Изменение номера порта или IP-адреса” на стр. 126.
   - Используйте точные IP-адреса. Дополнительная информация приведена в разделе “Изменение номера порта или IP-адреса” на стр. 126.

5. Создайте запись, соответствующую суффиксу или суффиксам, которые вы настроили. Дополнительная информация приведена в разделе “Добавление и удаление суффиксов сервера каталогов” на стр. 127.

Перед тем, как продолжить работу, вы можете также выполнить одну или все следующие операции:
- Импорт данных на сервер (см. раздел “Импорт и экспорт файла LDIF” на стр. 100).
- Включение защиты SSL (см. раздел “Включение SSL и TLS на сервере каталогов” на стр. 165).
- Включение идентификации Kerberos (см. раздел “Включение идентификации Kerberos на сервере каталогов” на стр. 167).
- Настройка переадресации (см. раздел “Выбор сервера каталогов для переадресации” на стр. 126).

## Конфигурация сервера каталогов по умолчанию

Сервер каталогов автоматически устанавливается при установке i5/OS. При этом создается конфигурация по умолчанию. Сервер каталогов применяет конфигурацию по умолчанию, если выполнены следующие условия:

- Администратор не запускал мастер настройки сервера каталогов и не изменял параметры на странице Свойства.
- На сервере каталогов не настроена публикация.
- Сервер каталогов не может найти информацию об LDAP на сервере DNS.

При работе сервера каталогов с конфигурацией по умолчанию:

- Сервер каталогов автоматически запускается вместе с TCP/IP.
- Создается администратор по умолчанию - cn=Administrator. Устанавливается пароль, применяемый для выполнения внутренних операций. Другой пароль администратора можно задать на странице свойств сервера каталогов.
- Создается суффикс по умолчанию на основе имени хоста системы. Кроме того, на основе этого имени создается суффикс объектов системы. Например, если имя системы - mary.acme.com, то будет создан суффикс dc=mary,dc=acme,dc=com.
- Сервер каталогов по умолчанию применяет библиотеку данных QUSRDIRDB. Она создается в системном ASP.
- Сервер применяет порт 389 для незащищенных соединений. Если для LDAP задан цифровой сертификат, то включается опция применения SSL. Для защищенных соединений применяется порт 636.

## Заполнение каталога

Заполнить каталог можно множеством способов. Дополнительная информация приведена в следующих разделах:

- “Публикация информации на сервере каталогов”
- “Импорт и экспорт файла LDIF” на стр. 100
- “Копирование пользователей из контрольного списка сервера HTTP на сервер каталогов” на стр. 101

## Публикация информации на сервере каталогов

Систему можно настроить для публикации определенной информации на локальном или удаленном сервере каталогов. При изменении информации с помощью Навигатора в i5/OS система автоматически публикует эту информацию на сервере каталогов. Публикуемая информация может включать системные сведения (системы и принтеры), информацию об общих принтерах, пользователях, а также стратегии QoS TCP/IP (см. раздел “Публикация” на стр. 38).

Если родительское DN, в котором публикуются данные, не существует, то сервер каталогов автоматически создает это DN. В системе также могут быть установлены другие приложения i5/OS, публикующие информацию в каталоге LDAP. Кроме того, пользовательские программы могут публиковать в каталоге LDAP информацию других типов с помощью интерфейсов прикладных программ (API).

**Примечание:** Информацию об i5/OS можно публиковать на сервере каталогов, работающем в другой операционной системе, если на этом сервере применяется схема IBM.

Для настройки в операционной системе i5/OS функции публикации информации на сервере каталогов выполните следующие действия:

1. В Навигаторе щелкните правой кнопкой мыши на значке системы и выберите пункт **Свойства**.
2. Перейдите на страницу **Сервер каталогов**.
3. Выберите типы информации, которую требуется публиковать.

   **Совет:**

   Выберите все типы информации, которые планируется публиковать на одном сервере каталогов. Навигатор будет применять значения, заданные при настройке публикации одного типа информации, в качестве значений по умолчанию при настройке остальных типов.
4. Нажмите кнопку **Сведения**.
5. Отметьте опцию **Публиковать системную информацию**.
6. Укажите **Способ идентификации** для сервера и задайте идентификационную информацию.
7. Нажмите кнопку **Изменить** напротив поля **(Активный) Сервер каталогов**. В появившемся окне введите имя сервера каталогов, на котором будет публиковаться информация i5/OS, затем нажмите **OK**.
8. В поле **DN** введите родительское отличительное имя (DN), в которое будет добавлена информация на сервере каталогов.
9. Заполните поля на панели **Соединение с сервером**, руководствуясь текущими параметрами конфигурации.

   **Примечание:** Для публикации информации i5/OS на сервере каталогов с применением SSL или Kerberos сначала необходимо настроить поддержку соответствующего протокола на сервере каталогов. Дополнительная информация об SSL и Kerberos приведена в разделе “Идентификация Kerberos на сервере каталогов” на стр. 52.
10. Если сервер каталогов не применяет порт, заданный по умолчанию, укажите правильный номер порта в поле **Порт**.
11. Нажмите кнопку **Проверить**, чтобы убедиться, что родительское DN существует на сервере и информация о соединении указана верно. Если указанный путь в каталоге не существует, то появится окно диалога с предложением создать его.

    **Примечание:** Если родительское DN не существует, и вы его не создадите, то публикация не будет выполнена.
12. Нажмите кнопку **OK**.

**Примечание:** Информацию i5/OS можно опубликовать на сервере каталогов LDAP, работающем в другой операционной системе. Информация о системе и пользователях должна публиковаться на сервере каталогов, применяющем схему, совместимую со схемой сервера IBM Directory Server. Дополнительная информация о схеме каталога IBM приведена в разделе “Схема IBM Directory Server” на стр. 19.

### API для публикации информации i5/OS на сервере каталогов

Сервер каталогов обеспечивает встроенную поддержку, позволяющую публиковать информацию о пользователях и системе. Соответствующие опции показаны на странице **Сервер каталогов** окна **Свойства** системы. С помощью API настройки и публикации сервера LDAP можно создавать программы i5/OS для публикации информации других типов. Эти типы информации также показаны на странице **Сервер каталогов**. Первоначально опции публикации этих типов информации выключены, как и опции публикации пользовательской и системной информации. Для их настройки применяется та же процедура. Программа, добавляющая данные в каталог LDAP, называется агентом публикации. Тип публикуемой информации, указанный на странице **Сервер каталогов**, служит именем агента.

В пользовательских приложениях могут применяться следующие API публикации:

**QgldChgDirSvrA**
Сначала приложение добавляет имя агента в виде выключенной опции, применяя формат CSVR0500. Пользователи приложения должны перейти на страницу сервера каталогов в программе Навигатор и настроить соответствующий агент публикации. Примерами имен агентов могут служить имена системных и пользовательских агентов, которые по умолчанию указываются на странице **Сервер каталогов**.

**QgldLstDirSvrA**
Формат LSVR0500 этого API позволяет получить список агентов, доступных в настоящий момент в системе.

**QgldPubDirObj**
Этот API служит для публикации данных.

Более подробная информация об этих API приведена в разделе Простой протокол доступа к каталогам (LDAP) справочной системы iSeries Information Center, относящемся к категории Программирование.

## Импорт и экспорт файла LDIF

**Импорт файла LDIF**

Для переноса информации между серверами каталогов применяются файлы в формате обмена данными LDAP (LDIF). Дополнительная информация приведена в разделе “Формат обмена данными LDAP (LDIF)” на стр. 234. Перед выполнением этой операции передайте файл LDIF на сервер iSeries как потоковый файл.

Для того чтобы импортировать файл LDIF на сервер каталогов, выполните следующие действия:
1. Если сервер каталогов запущен, остановите его. Информация о завершении работы сервера каталогов приведена в разделе “Запуск/останов сервера каталогов” на стр. 120.
2. В Навигаторе откройте **Сеть**.
3. Откройте **Серверы**.
4. Выберите **TCP/IP**.
5. Щелкните правой кнопкой мыши на пункте **IBM Directory Server** и выберите **Сервис**, затем **Импортировать файл**.

   Выбрав опцию **Скопировать импортированные данные**, вы можете также указать, что при следующем запуске сервер должен скопировать только что импортированные данные. Эта возможность полезна при добавлении новых записей в уже существующее дерево на главном сервере. Если вы импортируете данные для инициализации сервера-копии (или равноправного сервера), то копирование данных обычно не включается, поскольку соответствующие данные могут уже существовать на серверах, для которых данный сервер является поставщиком.

**Примечание:** Для импорта файлов LDIF можно также воспользоваться утилитой ldapadd (см. раздел “ldapmodify и ldapadd” на стр. 203).

**Экспорт файла LDIF**

Для переноса информации между серверами каталогов применяются файлы в формате обмена данными LDAP (LDIF). Дополнительная информация приведена в разделе “Формат обмена данными LDAP (LDIF)” на стр. 234. В файл LDIF можно экспортировать весь каталог LDAP или его часть.

Для того чтобы экспортировать файл LDIF с сервера каталогов, выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **IBM Directory Server** и выберите **Сервис**, затем **Экспортировать файл**.

**Примечание:** Если не указать полный путь к экспортируемому файлу LDIF, то файл будет создан в домашнем каталоге, указанном в пользовательском профайле операционной системы.

5. Укажите либо **Экспортировать весь каталог**, либо **Экспортировать выбранный подкаталог**, а также укажите, необходимо ли**Экспортировать операционные атрибуты**. Экспортироваться будут следующие операционные атрибуты creatorsName, createTimestamp, modifiersName и modifyTimestamp.

**Примечания:**

1. При экспорте данных в V5R3 или более ранних серверах каталогов не выбирайте пункт**Экспортировать операционные атрибуты**. В выпуске V5R3 и более ранних эти атрибуты не поддерживаются.
2. Файл LDIF можно также создать с помощью утилиты ldapsearch. Дополнительная информация приведена в разделе “ldapsearch” на стр. 219. Укажите опцию -L, чтобы перенаправить вывод в файл.
3. Для защиты доступа к данным каталога необходимо задать права доступа к созданному файлу LDIF. Для этого щелкните правой кнопкой мыши на имени файла в Навигаторе и выберите пункт **Права доступа**.

## Копирование пользователей из контрольного списка сервера HTTP на сервер каталогов

Если вы работаете сейчас или работали раньше с сервером HTTP, то вы наверняка создавали контрольные списки для хранения пользователей Internet и их паролей. После перехода к WebSphere Application Server, Portal Server или другим приложениям с поддержкой идентификации LDAP вы, возможно, захотите и дальше пользоваться этими списками. Это можно сделать с помощью API ″Копирования контрольных списков в каталог″, или QGLDCPYVL.

QGLDCPYVL читает записи из контрольного списка и создает соответствующие им объекты LDAP на локальном сервере каталогов. Объекты будут скелетными записями inetOrgPerson, атрибут userPassword которых содержит копию информации о пароле из контрольного списка. Время и способ вызова этого API можно настроить. Можно применить этот API в качестве одноразовой операции для контрольного списка, который не будет изменяться, а можно - в качестве запланированного задания для обновления сервера каталогов при изменениях контрольного списка.

Более подробное описание API QGLDCPYVL приведено в разделе API сервера каталогов. Пример использования API можно найти в разделе “Сценарий: Копирование пользователей из контрольного списка сервера HTTP на сервер каталогов”.

### Сценарий: Копирование пользователей из контрольного списка сервера HTTP на сервер каталогов

**Постановка задачи и обзор**

Предположим, у вас есть приложение, работающее на сервере HTTP на основе Apache, при этом пользователи Internet хранятся в контрольном списке MYLIB/HTTPVLDL. Очевидно, вы захотите работать с тем же списком пользователей Internet в WebSphere Application Server (WAS), который поддерживает идентификацию LDAP. Для того чтобы избежать дублирования информации о пользователях (в контрольном списке и в LDAP), следует настроить поддержку идентификации LDAP для приложения, работающего на сервере HTTP.

Для этого выполните следующие действия:

1. Скопируйте существующий контрольный список на локальный сервер каталогов.
2. Настройте на сервере WAS идентификацию LDAP.
3. Измените конфигурацию сервера HTTP так, чтобы вместо контрольных списков использовалась идентификация LDAP.

**Шаг 1: Копирование существующего контрольного списка пользователей на локальный сервер каталогов**

Допустим, что сервер каталогов запущен и настроен с суффиксом ″o=my company″. Пользователи LDAP будут сохраняться в поддереве каталога ″cn=users,o=my company″. DN администратора сервера каталогов - ″cn=administrator″, а пароль - ″secret″.

В командной строке вызовите API:

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL  MYLIB     ' 'cn=administrator' X'00000000' 'secret'
X'00000000' 'cn=users,o=my company' X'00000000' '' X'00000000' X'00000000')
```

После этого на сервере каталогов появятся записи inetorgperson, основанные на записях контрольного списка. Например, пользователь из контрольного списка:

```
User name: jsmith
Description: John Smith
Password: ******
```

будет преобразован в следующую запись каталога:

```
dn: uid=jsmith,cn=users,o=my company
 objectclass: top
      objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
uid: jsmith
sn: jsmith
cn: jsmith
description: John Smith
userpassword: ******
```

Теперь идентификация на сервере каталогов будет выполняться на основе этой записи. Например, при QSH-поиске на сервере LDAP будет считана корневая запись DSE сервера:

```
> ldapsearch -D "uid=jsmith,cn=users,o=my company" -w ****** -s base "(objectclass=*)"
```

Созданные записи каталогов можно изменять и добавлять в них информацию. Например, необходимо изменить значения cn и sn, указав в них полное имя и фамилию пользователя соответственно, или нужно добавить номер телефона и электронный адрес.

**Шаг 2: Настройка идентификации LDAP на сервере WAS**

Для защиты LDAP на сервере WAS необходима настройка поиска записей в каталоге dn ″cn=users,o=my company″ с помощью фильтра поиска, сопоставляющего введенное имя пользователя с записью inetOrgPerson, содержащую заданное значение атрибута uid. Например, идентификация на сервере WAS с именем пользователя jsmith должна вызывать поиск записей, удовлетворяющих фильтру поиска ″(uid=jsmith)″. Дополнительная информация приведена в разделе Настройка фильтров поиска LDAP справочной системы Information Center для Websphere Application Server for iSeries.

**Изменение конфигурации сервера HTTP так, чтобы вместо контрольных списков использовалась идентификация LDAP**

**Примечание:** Ниже описана процедура, иллюстрирующая примеры этого сценария, и приведен подробный обзор настройки идентификации LDAP на сервере HTTP. Дополнительную информацию можно найти в руководстве IBM Реализация и практическое применение LDAP на сервере IBM eServer iSeries, SG24-6193  Раздел 6.3.2 ″Настройка идентификации LDAP для сервера на основе Apache″, а также в разделе Настройка защиты паролей на сервере HTTP на основе Apache.

1. Выберите Средства администрирования HTTP на сервере HTTP, перейдите на вкладку **Конфигурация** и выберите пункт **Простая идентификация**.

2. В разделе **Способ идентификации пользователей** измените значение **Получать пользователей Internet из контрольных списков** на значение **Применять записи о пользователях на сервере LDAP**, затем нажмите **OK**.
3. Вернитесь на вкладку **Конфигурация** и выберите **Управление доступом**. Настройте управление доступом согласно инструкциям вышеуказанного руководства и нажмите **OK**.
4. На вкладке **Конфигурация** выберите **Идентификация LDAP**.
   a. Введите имя хоста и порт для сервера LDAP. Для **DN базы поиска пользователей** укажите `cn=users,o=my company`.
   b. В разделе **Создать уникальное DN LDAP для идентификации пользователей** введите фильтр `(&objectclass=person)(uid=%v1))`.
   c. Введите сведения о группе и нажмите **OK**.
5. Настройте подключение к серверу LDAP согласно инструкциям из вышеуказанного руководства.

## Рекомендуемые способы работы со структурой каталогов

Сервер каталогов часто применяется в качестве хранилища для пользователей и групп. В этом разделе описываются некоторые рекомендуемые приемы настройки структуры, оптимизирующие управление пользователями и группами. Эту структуру и связанную с ней модель защиты можно расширить для других возможностей использования каталога.

Как правило, пользователи хранятся в одном или нескольких местах. Можно использовать в качестве родительской записи для всех пользователей один контейнер cn=users, а можно создать отдельные контейнеры для нескольких наборов пользователей, которые администрируются по отдельности. Например, сотрудники, поставщики и автоматически регистрируемые пользователи Internet могут храниться в объектах cn=employees, cn=vendors и cn=internet users соответственно. Можно попробовать рассортировать сотрудников по организациям, но тогда возникнут некоторые сложности: если сотрудник перейдет из одной организации в другую, то потребуется переместить его запись каталога и в связи с этим обновить еще ряд источников данных (как внутренних, так и внешних для каталога). Отношение пользователей к организации можно зафиксировать в пользовательской записи с помощью атрибутов ″o″ (имя организации), ″ou″ (имя подразделения) и departmentNumber, входящих в стандартную схему для organizationalPerson и inetOrgPerson.

Аналогично, группы обычно размещаются в отдельных контейнерах, например, ″cn=groups″.

Если организовать пользователей и группы таким способом, то настройка списков управления доступом (ACL) понадобится только для нескольких мест.

В зависимости от способа применения сервера каталогов и управления пользователями и группами можно применить один из приведенных ниже шаблонов управления доступом:

- Если каталог используется для приложений типа адресной книги, то, возможно, потребуется предоставить группе cn=anybody права на чтение и поиск ″обычных″ атрибутов в контейнере cn=users и его родительских объектах.
- Как правило, доступ к контейнеру cn=groups необходим только для определенных приложений и для администраторов групп. Вы можете создать группу, которая будет хранить имена DN администраторов группы, и сделать ее владельцем контейнера cn=groups и подчиненных ему объектов. Можно создать также другую группу, в которую будут входить DN, используемые приложением для чтения информации о группах, и дать этой группе права на чтение и поиск в контейнере cn=groups.
- Если пользовательские объекты обновляются непосредственно пользователями, то можно предоставить определенным ИД права на чтение, запись и поиск в объекте cn=this appropriate.
- Если пользователи обновляются из приложений, то как правило эти приложения работают под собственными идентификаторами и имеют исключительные права на обновление пользовательского объекта. Будет удобно собрать эти DN в группу, например, cn=user administrators, и предоставить этой группе необходимые права доступа к объекту cn=users.

При использовании такой структуры и управления доступом ваш каталог первоначально может выглядеть следующим образом:

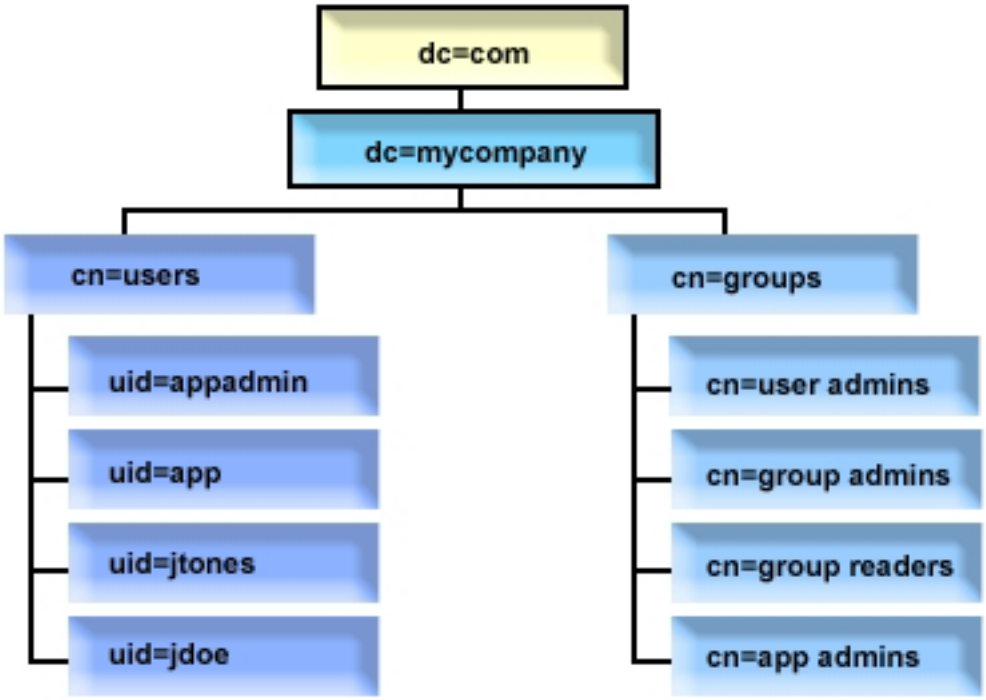



*Рисунок 3. Пример структуры каталога*

- Контейнером c=mycompany, dc=com владеет администратор каталога или другой пользователь или группа с правами на управление верхним уровнем каталога. Дополнительные записи списка ACL предоставляют права на чтение обычных атрибутов группе cn=anybody или cn=authenticated, либо, если требуется более жесткий ACL, какой-либо другой группе.
- Для cn=users в списке ACL есть записи, управляющие доступом для пользователей. В ACL может входить:
  - права на чтение и поиск обычных атрибутов для группы cn=anybody или cn=authenticated
  - права на чтение и поиск обычных и промежуточных атрибутов для администраторов
  - При необходимости - другие записи ACL, возможно, предоставляющие отдельным пользователям права на запись для своей собственной записи каталога.

**Примечание:**

- Для повышения читабельности вместо полных имен DN используются имена RDN. Например, вместо полного DN группы ″администраторы пользователей″ uid=app,cn=users,dc=mycompany,dc=com используется краткое: uid=app.
- Некоторых пользователей и группы можно объединять. Например, если администратор приложения имеет права на управление пользователями, то приложение может работать под DN администратора. Но в этом случае могут появиться ограничения, например, нельзя будет изменить пароль администратора приложения, не изменяя при этом пароль самого приложения.
- Так как выше описаны рекомендуемые приемы работы с каталогами, используемыми только одним приложением, возникает желание выполнять все обновления от имени администратора каталога. Однако этот способ считается неподходящим по вышеуказанным причинам.

## Web-администрирование

С помощью консоли Web-администрирования вы можете управлять одним или несколькими серверами каталогов. Консоль Web-администрирования позволяет выполнять следующие операции:

- Дополнять и изменять список администрируемых серверов каталогов.
- Управлять сервером каталогов с помощью Web-инструмента администрирования.
- Изменять атрибуты консоли Web-администрирования.

Для работы с консолью Web-администрирования выполните следующие действия:

1. Если это первое обращение к средствам Web-администрирования сервера каталогов, то сначала необходимо выполнить настройку (см. раздел “Первоначальная настройка средств Web-администрирования”), а затем перейти к следующему шагу.
2. Войдите в систему Web-администрирования сервера каталогов:
   - В Навигаторе iSeries выберите сервер, разверните **Сеть > Серверы > TCP/IP**, щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Администрирование сервера**.
   - На странице Задачи iSeries (http://*имя_сервера*:2001) выберите **IBM Directory Server**.
3. Для того чтобы начать управление сервером каталогов, выполните следующие действия:
   a. Выберите нужный сервер каталогов в списке **Имя хоста LDAP**.
   b. Введите DN администратора, применяемое для подключения к серверу каталогов.
   c. Введите пароль администратора.
   d. Нажмите кнопку **Вход в систему**. Будет показана страница Web-инструмента администрирования сервера каталогов IBM Directory Server. Дополнительная информация о странице Web-инструмента администрирования IBM Directory Server приведена в разделе “Web-инструмент администрирования” на стр. 107.
4. Для того чтобы дополнить или изменить список администрируемых серверов каталогов, либо изменить атрибуты консоли Web-администрирования, выполните следующие действия:
   a. В поле **Имя хоста LDAP** выберите пункт **Администрирование консоли**.
   b. Укажите ИД администратора консоли.
   c. Укажите пароль администратора консоли.
   d. Нажмите кнопку **Вход в систему**. Будет показана страница Web-инструмента администрирования сервера каталогов IBM Directory Server. Дополнительная информация о странице Web-инструмента администрирования IBM Directory Server приведена в разделе “Web-инструмент администрирования” на стр. 107.
   e. Выберите **Администрирование консоли**, а затем выберите одну из следующих опций:
      - **Изменить имя администратора консоли** - для изменения имени, применяемого администратором консоли для входа в систему.
      - **Изменить пароль администратора консоли** - для изменения пароля, применяемого администратором консоли для входа в систему.
      - **Управление серверами консоли** - для изменения списка серверов каталогов, которыми можно управлять с помощью консоли Web-администрирования.
      - **Управление свойствами консоли** - для изменения свойств консоли Web-администрирования.

## Первоначальная настройка средств Web-администрирования

Для первоначальной настройки Web-инструмента администрирования сервера каталогов выполните следующие действия.

1. Установите IBM WebSphere Application Server - Express 5.1 (5722E51 - базовый компонент и компонент 2), а также другие обязательные программные продукты, если они еще не установлены.
2. На экземпляре сервера ADMIN HTTP включите поддержку системного экземпляра сервера приложений. Дополнительная информация приведена в разделе IBM HTTP Server.

a. Запустите экземпляр сервера ADMIN HTTP, выполнив одно из следующих действий:
   - В Навигаторе iSeries выберите **Сеть -> Серверы -> TCP/IP** и щелкните правой кнопкой мыши на пункте **Администрирование HTTP**. После этого нажмите кнопку **Запустить**.
   - В командной строке введите команду `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

b. Войдите в систему IBM Web-администратора iSeries. Указав пользовательский профайл операционной системы и пароль, откройте страницу Задачи iSeries (http://*имя-сервера*:2001), затем выберите **IBM Web-администратор iSeries**.

c. На странице Администрирование сервера HTTP *имя_сервера* откройте вкладку **Управление** и затем вкладку **Серверы HTTP**.Убедитесь, что в выпадающем списке **Сервер** выбрана опция **ADMIN – Apache**. Также убедитесь, что в списке **Область сервера** выбрана опция **Включить /QIBM/UserData/HTTPA/admin/conf/admin-cust.conf** .

d. В списке опций в левой части страницы выберите **Общая конфигурация сервера**.

   **Примечание:** Возможно, для просмотра опции **Общая конфигурация сервера** вам потребуется развернуть раздел **Свойства сервера**.

e. Укажите **Да** в опции **Запускать экземпляр системного сервера приложений при запуске сервера 'Admin'**.

f. Нажмите кнопку **OK**.

g. Перезапустите экземпляр сервера ADMIN HTTP, нажав кнопку перезапуска (вторая кнопка на вкладке **Серверы HTTP**). Остановить и запустить сервер ADMIN HTTP можно также с помощью Навигатора iSeries или командной строки.

   Остановите экземпляр сервера ADMIN HTTP, выполнив одно из следующих действий:
   - В Навигаторе iSeries выберите опцию **Сеть -> Серверы -> TCP/IP** и щелкните правой кнопкой мыши на пункте **Администрирование HTTP**. После этого нажмите кнопку **Остановить**.
   - В командной строке введите команду `ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

   Запустите экземпляр сервера ADMIN HTTP, выполнив одно из следующих действий:
   - В Навигаторе iSeries выберите опцию **Сеть -> Серверы -> TCP/IP** и щелкните правой кнопкой мыши на пункте **Администрирование HTTP**. После этого нажмите кнопку **Запустить**.
   - В командной строке введите команду `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

   Дополнительная информация приведена в разделе IBM HTTP Server.

3. Откройте Web-инструмент администрирования сервера каталогов.
   a. Перейдите на **страницу входа в систему**, выполнив одно из следующих действий.
      - В Навигаторе iSeries выберите сервер, разверните **Сеть -> Серверы -> TCP/IP**, щелкните правой кнопкой мыши на **IBM Directory Server** и щелкните на **Администрирование сервера**.
      - На странице Задачи iSeries (http://*имя_сервера*:2001) выберите ссылку **IBM Directory Server for iSeries**.

   b. В поле **Имя хоста LDAP** выберите пункт **Администрирование консоли**.

   c. В поле **Имя пользователя** введите значение `superadmin`.

   d. В поле **Пароль** введите значение `secret`.

   e. Нажмите кнопку **Вход в систему**. Будет показана страница Web-инструмента администрирования сервера каталогов IBM Directory Server.

4. Измените имя администратора консоли.
   a. Щелкните на **Администрирование консоли** в левой панели, чтобы развернуть раздел, затем щелкните на **Изменить имя администратора консоли для входа в систему**.

   b. В поле **Имя администратора консоли** введите новое имя для входа в систему.

   c. В поле **Текущий пароль** введите текущий пароль (`secret`).

   d. Нажмите кнопку **OK**.

5. Измените пароль администратора консоли. Выберите опцию **Изменить пароль администратора консоли** в левой панели.

6. Добавьте в список сервер каталогов, которым вы планируете управлять. Выберите опцию **Управление серверами консоли** в левой панели.

   **Примечание:** При добавлении сервера каталогов значение **Порта администрирования** не используется и игнорируется.
7. Если вы хотите изменить свойства консоли, выполните следующие действия. Выберите опцию **Управление свойствами консоли** в левой панели.
8. Нажмите кнопку **Выход из системы**. После появления меню с подтверждением успешного выхода из системы щелкните на ссылке **здесь** для возврата к странице входа в систему Web-инструмента администрирования.

После первоначальной настройки консоли вы можете вернуться к консоли в любой момент для выполнения следующих операций:

- Изменение имени и пароля администратора консоли.
- Изменение списка серверов каталогов, которыми можно управлять с помощью Web-инструмента администрирования.
- Изменение свойств консоли.

## Web-инструмент администрирования

После входа в систему Web-инструмента администрирования будет показано окно приложения, состоящее из следующих пяти частей:

**Область баннера**
Эта область находится в верхней части окна. Она содержит имя приложения и логотип IBM.

**Область навигации**
Область навигации, расположенная в левой части окна, содержит список разворачиваемых категорий, соответствующих различным задачам управления сервером:

**Свойства пользователя**
Эта задача позволяет изменить пароль текущего пользователя.

**Управление схемой**
Эта задача позволяет работать с классами объектов, атрибутами, правилами соответствия и вариантами синтаксисов.

**Управление каталогом**
Эта задача позволяет работать с записями каталога.

**Управление копированием**
Эта задача позволяет работать с идентификационными данными, топологией, расписанием и очередями.

**Области и шаблоны**
Эта задача позволяет работать с областями и шаблонами пользователей.

**Пользователи и группы**
Эта задача позволяет работать с пользователями и группами в определенных областях. Например, если вы хотите создать нового пользователя Web, то задача **Пользователи и группы** позволит воспользоваться одним классом объекта группы, groupOfNames. Настраивать поддержку групп нельзя.

**Администрирование сервера**
Эта задача позволяет изменять конфигурацию сервера и параметры защиты.

**Рабочая область**
В этой области показана информация, связанная с задачами, выбранными в области навигации.

Например, если в области навигации выбрана опция Управление защитой сервера, то в рабочей области будет показана страница Защита сервера со вкладками, предназначенными для выполнения задач настройки защиты сервера.

**Область состояния сервера**

Эта область расположена в нижней части окна. Показанной в левой части области состояния значок позволяет определить текущее состояние сервера. Рядом со значком показано имя сервера, с которым вы работаете. Значок, показанный в правой части этой области, позволяет вызвать электронную справку.

**Область состояния задачи**

Эта область расположена под рабочей областью и содержит сведения о состоянии выполнения текущей задачи.

# Глава 6. Сценарий: Настройка сервера каталогов

**Ситуация**

Вы являетесь администратором информационных систем в своей организации и хотите поместить информацию о сотрудниках организации, например, номера телефонов и адреса электронной почты, в централизованный каталог LDAP.

**Цели**

В этом сценарии компания MyCo, Inc. хочет настроить сервер каталогов и создать базу данных каталога, которая будет содержать информацию о сотрудниках, включающую, например, имена, адреса электронной почты и номера телефонов.

Цели этого сценария:

- Обеспечить доступ к информации о сотрудниках из любой точки сети организации всем клиентам, использующим Lotus Notes или Microsoft Outlook Express.
- Предоставить менеджерам возможность изменять хранящиеся в базе данных каталога сведения о сотрудниках. При этом остальные пользователи не должны иметь такой возможности.
- Предоставить серверу iSeries возможность публикации данных о сотрудниках в базе данных каталога.

**Подробные сведения**

Сервер каталогов будет работать в системе iSeries с именем myiSeries.

Приведен пример информации о сотруднике, которую компания MyCo, Inc. хочет в включить в базу данных каталога:

```
Имя: Jose Alvirez
Отдел: DEPTA
Номер телефона: 999 999 9999
Адрес электронной почты: jalvirez@my_co.com
```

Структуру каталога, реализуемого в данном сценарии, можно представить примерно следующим образом:

```
/
|
+- my_co.com
   |
   +- employees
      |
      +- Jose Alvirez
      |  DEPTA
      |  999-555-1234
      |  jalvirez@my_co.com
      |
      +- John Smith
      |  DEPTA
      |  999-555-1235
      |  jsmith@my_co.com
      |
      +  Managers group
         Jose Alvirez
         myiSeries.my_co.com
.
.
.
```

В дереве каталога хранятся сведения о всех сотрудниках (как менеджерах, так и об обычных сотрудниках). Менеджеры также входят в состав группы managers. Члены этой группы имеют права доступа на изменение сведений о сотрудниках.

У сервера iSeries (myiSeries) также должны быть права доступа на изменение сведений о сотрудниках. В данном сценарии сервер iSeries сервер находится в дереве сотрудников и входит в состав группы менеджеров.

Если вы хотите, чтобы записи сотрудников хранились отдельно от записи сервера iSeries, то можно создать отдельное поддерево каталога (например, computers) и добавить в него запись сервера iSeries. У сервера iSeries должны быть те же права доступа, что и у менеджеров.

**Предварительные требования и предположения**

Web-инструмент администрирования должен быть правильно настроен и работоспособен. Дополнительная информация приведена в разделе “Web-администрирование” на стр. 105.

**Действия по настройке**

Выполните следующие задачи:
1. “Подробные сведения о сценарии: Настройка сервера каталогов”.
2. “Подробные сведения о сценарии: Создание базы данных каталога” на стр. 111.
3. “Подробные сведения о сценарии: Публикация данных iSeries в базе данных каталога” на стр. 113.
4. “Подробные сведения о сценарии: Ввод информации о базе данных каталога” на стр. 114.
5. “Подробные сведения о сценарии: Тестирование базы данных каталога” на стр. 115.

## Подробные сведения о сценарии: Настройка сервера каталогов

**Шаг 1: Настройка сервера каталогов**

**Примечание:** Для настройки сервера необходимы специальные права доступа *ALLOBJ и *IOSYSCFG.

1. В Навигаторе iSeries выберите опции **Сеть—> Серверы—> TCP/IP**.
2. В правой нижней части окна **Задачи настройки сервера** Навигатора iSeries выберите опцию **Настроить систему в качестве сервера каталогов**.
3. Появится окно **Мастера настройки сервера каталогов**.
4. В окне **приветствия мастера настройки IBM Directory Server** выберите опцию **Настроить локальный сервер каталогов LDAP**.
5. В окне **Мастер настройки IBM Directory Server - Приветствие** нажмите кнопку **Далее**.
6. В окне **Мастер настройки IBM Directory Server - Указать параметры** выберите ответ **Нет**. Это позволит вам настроить сервер LDAP, не используя параметры по умолчанию.
7. В окне **Мастер настройки IBM Directory Server - Указать параметры** нажмите кнопку **Далее**.
8. В окне **Мастер настройки IBM Directory Server - Указать DN администратора** отмените выбор опции **Создается системой** и введите следующие значения:

| | |
|---|---|
| **DN администратора** | `cn=administrator` |
| **Пароль** | `secret` |
| **Подтверждение пароля** | `secret` |

**Примечание:** Все указанные в этом сценарии пароли приведены лишь в качестве примера. Во избежание нарушения защиты вашей сети никогда не используйте эти пароли в реальной конфигурации.

9. В окне **Мастер настройки IBM Directory Server - Указать DN администратора** нажмите кнопку **Далее**.

10. В поле **Суффикс** окна **Мастер настройки IBM Directory Server - Указать суффиксы** введите значение `dc=my_co,dc=com`.
11. В окне **Мастер настройки IBM Directory Server - Указать суффиксы** нажмите кнопку **Добавить**.
12. В окне **Мастер настройки IBM Directory Server - Указать суффиксы** нажмите кнопку **Далее**.
13. В окне **Мастер настройки IBM Directory Server - Выбрать IP-адреса** выберите опцию **Да, использовать все IP-адреса**.
14. В окне **Мастер настройки IBM Directory Server - Выбрать IP-адреса** нажмите кнопку **Далее**.
15. В окне **Мастер настройки IBM Directory Server - Указать параметры TCP/IP** выберите ответ **Да** .
16. В окне **Мастер настройки IBM Directory Server - Указать параметры TCP/IP** нажмите кнопку **Далее**.
17. В окне **Мастер настройки IBM Directory Server - Сводка** нажмите кнопку **Готово**.
18. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите опцию **Запустить**.

**Шаг 2: Настройка Web-инструмента администрирования сервера каталогов**

1. Укажите в браузере адрес http://*myiSeries.my_co.com*:9080/IDSWebApp/IDSjsp/Login.jsp, где *myiSeries.my_co.com* - имя сервера iSeries.
2. Появится страница входа в систему. В списке **Имя хоста LDAP** выберите опцию **Администрирование консоли**. В качестве имени пользователя укажите `superadmin`, а в качестве пароля - `secret`.Нажмите кнопку **Вход в систему**.
3. Настройте Web-инструмент администрирования для подключения к серверу LDAP в системе iSeries. В области навигации выберите опцию **Администрирование консоли —> Управление серверами консоли**.
4. Нажмите кнопку **Добавить**.
5. В поле **Добавить сервер** введите `myiSeries.my_co.com`.
6. Нажмите **Ok**. Новый сервер появится в списке **Управление серверами консоли**.
7. Выберите в области навигации опцию **Выход из системы**.
8. На странице входа в систему Web-инструмента администрирования откройте список **Имя хоста LDAP** и выберите только что настроенный сервер (**myiSeries.my_co.com**).
9. В поле **Имя пользователя** введите `cn=administrator`, а в поле **Пароль** - `secret`. Нажмите **Вход в систему**. Будет показана главная страница Web-инструмента администрирования сервера каталогов.

## Подробные сведения о сценарии: Создание базы данных каталога

Перед началом ввода данных необходимо создать хранилище данных.

**Шаг 1: Создание объекта базового DN**

1. В Web-инструменте администрирования выберите опции **Управление каталогом —> Управление записями**. Будет показан список объектов, находящихся на базовом уровне каталога. Поскольку мы имеем дело с новым сервером, то будут показаны только структурные объекты, содержащие информацию о конфигурации.
2. Добавьте новый объект, в котором будут храниться данные MyCo, Inc. Нажмите кнопку **Добавить...** в правой части окна. В следующем окне пролистайте список **Класс объектов**, выберите в нем значение **domain** и нажмите кнопку **Далее**.
3. Если вы не хотите добавлять вспомогательные классы объектов, то еще раз нажмите кнопку **Далее**.
4. В окне **Ввод атрибутов** укажите данные, соответствующие суффиксу, созданному ранее с помощью мастера. В списке **Класс объектов** оставьте выбранным значение **domain**. В поле **Относительное DN** введите значение `dc=my_co`. В поле **Родительское DN** введите `dc=com`. В поле **dc** введите my_co.
5. Нажмите кнопку **Готово** в нижней части окна. Теперь на базовом уровне будет показано новое базовое DN.

**Шаг 2: Создание шаблона пользователя**

Для того чтобы упростить ввод данных о сотрудниках MyCo, Inc., рекомендуется создать шаблон пользователя.

1. В Web-инструменте администрирования выберите опции **Области и шаблоны —> Добавить шаблон пользователя**.
2. В поле **Имя шаблона пользователя** введите значение `Employee`.
3. Нажмите кнопку **Обзор...**, расположенную рядом с полем **Родительское DN**. Выделите базовое DN, созданное на предыдущем шаге (**dc=my_co,dc=com**, и нажмите кнопку **Выбрать** в правой части окна.
4. Нажмите кнопку **Далее**.
5. В списке **Структурный класс объектов** выберите **inetOrgPerson** и нажмите кнопку **Далее**.
6. В списке **Атрибут присвоения имени** выберите **cn**.
7. В списке **Вкладки** выберите **Обязательные** и нажмите кнопку **Редактировать**.
8. В окне **Редактирование вкладки** вы сможете выбрать поля, которые должны быть включены в шаблон пользователя. Обязательными являются поля **sn** и **cn**.
9. В списке **Атрибуты** выберите **departmentNumber** и нажмите кнопку **Добавить >>>**.
10. Выберите **telephoneNumber** и нажмите **Добавить >>>**.
11. Выберите **mail** и нажмите **Добавить >>>**.
12. Выберите **userPassword** и нажмите **Добавить >>>**.
13. Для завершения создания шаблона пользователя нажмите кнопку **OK**, а затем - кнопку **Готово**.

**Шаг 3: Создание области**

1. В Web-инструменте администрирования выберите опции **Области и шаблоны —> Добавить область**.
2. В поле **Имя области** введите значение `employees`.
3. Нажмите кнопку **Обзор...**, показанную справа от поля **Родительское DN**.
4. Выделите созданное DN (**dc=my_co,dc=com**) и нажмите кнопку **Выбрать** в правой части окна.
5. Нажмите кнопку **Далее**.
6. В следующем окне нужно будет только изменить значение в списке **Шаблон пользователя**. Выберите только что созданный шаблон пользователя **cn=employees,dc=my_co,dc=com**.
7. Нажмите кнопку **Готово**.

**Шаг 4: Создание группы менеджеров**

1. Создайте группу менеджеров.
   a. В Web-инструменте администрирования выберите опции **Пользователи и группы —> Добавить группу**.
   b. В поле **Имя группы** введите значение `managers`.
   c. Убедитесь, что в списке **Область** выбрано значение **employees**.
   d. Нажмите кнопку **Готово**.
2. Настройте администратора группы менеджеров для области **employees**.
   a. Выберите опции **Пользователи и шаблоны —> Управление областями**.
   b. Выберите созданную область (**cn=employees,dc=my_co,dc=com** и нажмите кнопку **Редактировать**.
   c. Нажмите кнопку **Обзор...**, показанную справа от поля **Группа администраторов**.
   d. Выберите **dc=my_co,dc=com** и нажмите кнопку **Развернуть**.
   e. Выберите **cn=employees** и нажмите кнопку **Развернуть**.
   f. Выделите запись **cn=managers** и нажмите кнопку **Выбрать**.
   g. В окне **Редактирование области** нажмите кнопку **OK**.
3. Предоставьте группе менеджеров доступ к суффиксу **dc=my_co,dc=com**.
   a. Выберите опции **Управление каталогом —> Управление записями**.
   b. Выберите **dc=my_co,dc=com** и нажмите кнопку **Редактировать ACL...**
   c. В окне **Редактировать ACL...** щелкните на вкладке **Владельцы**.

d. Отметьте опцию **Наследовать владельца**. Все пользователи, входящие в группу менеджеров, будут считаться владельцами поддерева **dc=my_co,dc=com**.

e. В списке **Тип** выберите значение **Группа**.

f. В поле **DN (Отличительное имя)** введите `cn=managers,cn=employees,dc=my_co,dc=com`.

g. Нажмите кнопку **Добавить**.

h. Нажмите **Ok**.

**Шаг 5: Добавление пользователя в качестве менеджера**

1. В Web-инструменте администрирования выберите опции **Пользователи и группы —> Добавить пользователя**.
2. Выберите созданную область **employees** в списке **Область** и нажмите **Далее**.
3. В поле **cn** введите значение `Jose Alvirez`.
4. В поле ***sn** (surname - фамилия) введите `Alvirez`.
5. В поле ***cn** (complete name - полное имя) введите `Jose Alvirez`. cn применяется для создания DN записей. *cn является атрибутом объекта.
6. В поле **telephoneNumber** введите значение `999 555 1234`.
7. В поле **departmentNumber** введите значение `DEPTA`.
8. В поле **mail** введите значение `jalvirez@my_co.com`.
9. В поле **userPassword** введите значение `secret`.
10. Щелкните на вкладке **Группы пользователей**.
11. В списке **Доступные группы** выберите группу **managers** и нажмите кнопку **Добавить—>**.
12. Нажмите кнопку **Готово** в нижней части окна.
13. Выйдите из системы Web-инструмента администрирования, выбрав опцию **Выход из системы** в нижней части окна.

## Подробные сведения о сценарии: Публикация данных iSeries в базе данных каталога

Для того чтобы сервер iSeries мог автоматически добавлять в каталог LDAP информацию о пользователях необходимо настроить публикацию. Информация о пользователях из системного каталога рассылки публикуется в каталоге LDAP.

**Примечание:** Для пользователей, создаваемых с помощью Навигатора iSeries, создается пользовательский профайл и запись системного каталога рассылки. Если вы создаете пользовательский профайл с помощью команд CL, то необходимо сначала создать пользовательский профайл (**CRTUSRPRF**), а затем добавить его в системный каталог рассылки (**WRKDIRE**). Если пользователи существуют в системе только в виде пользовательских профайлов, но вы хотите опубликовать их в каталоге LDAP, то необходимо создать для этих пользователей записи системного каталога рассылки.

**Шаг:1 Создание сервере iSeries в качестве пользователя сервера каталогов**

1. Войдите в Web-инструмент администрирования (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.jsp) под именем администратора.
   a. В списке **Имя хоста LDAP** выберите **myiSeries.my_co.com**.
   b. В поле **Имя пользователя** введите значение `cn=administrator`.
   c. В поле **Пароль** введите значение `secret`.
   d. Нажмите кнопку **Вход в систему**.
2. Выберите опции **Пользователи и группы —> Добавить пользователя**.
3. В списке **Область** выберите **employees**.

4. Нажмите кнопку **Далее**.
5. В поле **cn** введите значение myiSeries.my_co.com.
6. В поле ***sn** укажите значение myiSeries.my_co.com.
7. В поле ***cn** введите значение myiSeries.my_co.com.
8. В поле **userPassword** введите secret.
9. Щелкните на вкладке **Группы пользователей**.
10. Выберите группу **managers**.
11. Нажмите кнопку **Добавить —>**.
12. Нажмите кнопку **Готово**.

**Шаг 2: Настройка публикации данных на сервере iSeries**

1. В Навигаторе iSeries щелкните правой кнопкой мыши на значке сервера iSeries и выберите опцию **Свойства**.
2. В окне диалога **Свойства** выберите вкладку **Сервер каталогов**.
3. Выберите **Пользователи** и нажмите кнопку **Сведения**.
4. Отметьте переключатель **Публиковать информацию о пользователях**.
5. В разделе **Где публиковать** нажмите кнопку **Редактировать**. Появится новое окно.
6. Введите имя myiSeries.my_co.com.
7. В поле **Под DN** введите значение cn=employees,dc=my_co,dc=com.
8. Убедитесь, что в разделе **Подключение к серверу** в поле **Порт** указан номер порта по умолчанию (**389**). В списке **Способ идентификации** выберите опцию **Отличительное имя** и укажите в поле **Отличительное имя** значение cn=myiSeries,cn=employees,dc=my_co,dc=com.
9. Нажмите кнопку **Пароль**.
10. В поле **Пароль** введите secret.
11. В поле **Подтверждение пароля** введите secret.
12. Нажмите кнопку **OK**.
13. Нажмите кнопку **Проверить**. Тем самым вы сможете проверить правильность введенной информации и возможность подключения iSeries к каталогу LDAP.
14. Нажмите кнопку **OK**.
15. Нажмите кнопку **OK**.

## Подробные сведения о сценарии: Ввод информации о базе данных каталога

Менеджер Jose Alvirez должен добавить и обновить сведения о сотрудниках своего отдела. В частности, он должен указать дополнительную информацию о пользователе Jane Doe. Jane Doe является пользователем сервера iSeries и информация о ней опубликована сервером. Кроме того, необходимо добавить информацию о пользователе John Smith. John Smith не является пользователем сервера iSeries. Для решения этой задачи Jose Alvirez должен выполнить следующие действия:

**Шаг 1: Вход в Web-инструмент администрирования**

Войдите в систему Web-инструмента администрирования. (http://**myiSeries.my_co.com**:9080/IDSWebApp/IDSjsp/Login.)

1. В списке **Имя хоста LDAP** выберите **myiSeries.my_co.com**.
2. В поле **Имя пользователя** введите cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com.
3. В поле **Пароль** введите secret.
4. Нажмите кнопку **Вход в систему**.

**Шаг 2: Изменение данных о сотруднике**

1. Выберите опции **Пользователи и группы —> Управление пользователями**.
2. В списке **Область** выберите **employees** и нажмите кнопку **Просмотреть пользователей**.
3. В списке пользователей выберите опцию **Jane Doe** и нажмите кнопку **Редактировать**.
4. В поле **departmentNumber** введите значение DEPTA.
5. Нажмите кнопку **OK**.
6. Нажмите кнопку **Закрыть**.

**Шаг 3: Добавление данных о сотруднике**

1. Выберите опции **Пользователи и группы —> Добавить пользователя**.
2. В списке **Область** выберите **employees** и нажмите кнопку **Далее**.
3. В поле **cn** введите значение John Smith.
4. В поле ***sn** введите значение Smith.
5. В поле ***cn** введите значение John Smith.
6. В поле **telephoneNumber** введите значение 999 555 1235.
7. В поле **departmentNumber** введите значение DEPTA.
8. В поле **mail** введите значение jsmith@my_co.com.
9. Нажмите кнопку **Готово** в нижней части окна.

## Подробные сведения о сценарии: Тестирование базы данных каталога

После ввода в базу данных каталога сведения о сотрудниках необходимо проверить работу базы данных и сервера каталога. Для этого выполните следующие действия:

**Поиск в базе данных каталога с помощью адресной книги электронной почты**

Для поиска хранящейся в каталоге LDAP информации можно применять любые программы с поддержкой LDAP. Например, поиск на серверах каталогов LDAP включен в число функций адресной книги многих клиентов электронной почты. Ниже приведены примеры процедур настройки клиентов Lotus Notes 6 и Microsoft Outlook Express 6. Процедуры настройки большинства других клиентов электронной почты аналогичны описанным.

**Lotus Notes**

1. Откройте адресную книгу.
2. Выберите опции **Действия —> Создать —> Учетная запись**.
3. В поле **Имя учетной записи** введите значение myiSeries.
4. В поле **Имя сервера учетной записи** введите значение myiSeries.my_co.com.
5. В поле **Протокол** выберите значение **LDAP**.
6. Щелкните на вкладке **Конфигурация протокола**.
7. В поле **База для поиска** введите значение dc=my_co,dc=com.
8. Нажмите кнопку **Сохранить и закрыть**.
9. Выберите опции **Создать —> Почта —> Сообщение**.
10. Нажмите кнопку **Адрес...**
11. В поле **Выбрать адресную книгу** выберите опцию myiSeries.
12. В поле **Искать** введите значение Alvirez.
13. Нажмите кнопку **Найти**. Будут показаны сведения о пользователе Jose Alvirez.

**Microsoft Outlook Express**

1. Выберите опции **Сервис —> Учетные записи**.
2. Нажмите кнопку **Добавить —> Служба каталогов**.
3. В поле **Сервер каталогов (LDAP)** введите адрес сервера iSeries (`myiSeries.my_co.com`).
4. Выключите переключатель **Требуется вход на сервер каталогов**.
5. Нажмите кнопку **Далее**.
6. Нажмите кнопку **Далее**.
7. Нажмите кнопку **Готово**.
8. Выберите только что настроенную службу каталогов `myiSeries.my_co.com` и нажмите кнопку **Свойства**.
9. Щелкните на вкладке **Дополнительно**.
10. В поле **Search base** введите значение `dc=my_co,dc=com`.
11. Нажмите **Ok**.
12. Нажмите кнопку **Закрыть**.
13. Для перехода к окну **Поиск людей** нажмите `Ctrl+E`.
14. В списке **Место поиска** выберите `myiSeries.my_co.com`.
15. В поле **Имя** введите значение `Alvirez`.
16. Нажмите кнопку **Найти**. Будут показаны сведения о пользователе Jose Alvirez.

**Поиск в базе данных каталогов с помощью команды ldapsearch**

1. В текстовом интерфейсе введите команду CL **QSH** для запуска сеанса Qshell.
2. Для получения записей базы данных LDAP введите следующую команду:

   ```
   ldapsearch -h myiSeries.my_co.com -b dc=my_co,dc=com objectclass=*
   ```

   где:

   **-h** имя хоста, на котором работает сервер LDAP.

   **-b** базовое DN для поиска.

   **objectclass=***
   возвращает все найденные в каталоге записи.

   Пример вывода команды:

   ```
    dc=my_co,dc=com
    dc=my_co
    objectclass=domain
   objectclass=top

    cn=MyCo employee,dc=my_co,dc=com

   .
   .
   .

   cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com

   sn=Alvirez
   departmentNumber=DEPTA
   mail=jalvirez@my_co.com
   telephoneNumber=999 999 9999
   objectclass=top
   objectclass=inetOrgPerson
   objectclass=organizationalPerson
   objectclass=person
   cn=Jose Alvirez
   ```

.
.
.
Первая строка каждой записи называется отличительным именем (DN). DN записи аналогично полному имени файла. Некоторые записи являются структурными и не содержат данных. Записи со строкой **objectclass=inetOrgPerson** соответствуют созданным вами записям сотрудников. DN пользователя Jose Alvirez: **cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com**.

# Глава 7. Администрирование сервера каталогов

Для администрирования сервера каталогов пользовательский профайл должен иметь следующие права доступа:

- Для настройки сервера и изменения его конфигурации: специальные права доступа ко всем объектам (*ALLOBJ) и специальные права на настройку системы ввода-вывода (*IOSYSCFG)
- Для запуска и остановки сервера: Права доступа на управление заданиями (*JOBCTL) и права доступа к объектам команд Завершить TCP/IP (ENDTCP), Запустить TCP/IP (STRTCP), Запустить сервер TCP/IP (STRTCPSVR) и Завершить работу сервера TCP/IP (ENDTCPSVR)
- Для настройки стратегии контроля сервера каталогов: специальные права доступа на контроль (*AUDIT)
- Для просмотра протокола задания сервера: специальные права доступа на управление буфером (*SPLCTL)

Для работы с объектами каталога (включая списки управления доступом, принадлежность объектов и копии) необходимо подключиться к каталогу, указав DN администратора, либо любое другое DN с соответствующими правами доступа. Если применяется интеграция прав доступа, то роль администратора может исполнять спроецированный пользователь (см. раздел “Спроецированная база данных операционной системы” на стр. 80), имеющий права доступа к ИД администратора сервера каталогов. Также большинство задач администрирования могут выполнять члены группы администраторов (см. раздел “Права доступа администратора” на стр. 59).

**Общие задачи администрирования**



**Задачи защиты**

- “Управление паролями” на стр. 161
- “Включение SSL и TLS на сервере каталогов” на стр. 165
- “Включение идентификации Kerberos на сервере каталогов” на стр. 167
- “Настройка идентификации DIGEST-MD5 на сервере каталогов” на стр. 168

**Задачи управления содержимым каталога**
- “Управление схемой” на стр. 168
- “Управление записями каталога” на стр. 179
- “Управление пользователями и группами” на стр. 186
- “Управление областями и шаблонами пользователей” на стр. 189
- “Управление списками управления доступом (ACL)” на стр. 197

**Задачи публикации**
- “Публикация информации на сервере каталогов” на стр. 98

## Запуск/останов сервера каталогов

**Для запуска сервера каталогов выполните следующие действия:**
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Запустить**.

   Время, необходимое для запуска сервера, зависит от производительности сервера и объема свободной памяти. Оно может составлять несколько минут. Первый запуск сервера может выполняться несколько дольше, чем последующие, так как при первом запуске сервер создает новые файлы. Аналогично, первый запуск сервера каталогов после перехода от более ранней версии может занять больше времени, чем обычно, так как сервер должен преобразовывать файлы. Во время запуска вы можете периодически проверять состояние сервера (см. раздел “Просмотр состояния сервера каталогов” на стр. 121).

Сервер каталогов можно запустить и с помощью текстового интерфейса командой `STRTCPSVR *DIRSRV`. Если сервер каталогов настроен для запуска вместе с TCP/IP, то его можно запустить с помощью команды `STRTCP`.

**Режим только настройки**

Сервер каталогов можно запустить в режиме только настройки. Для этого введите в текстовом интерфейсе команду `TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE)`.

При запуске сервера в режиме только настройки активным является только суффикс cn=configuration и сервер не требует успешной инициализации системы управления базой данных.

Для останова сервера каталогов выполните следующие действия:

Завершение работы сервера каталогов скажется на выполнении всех подключенных к нему приложений. В том числе, завершение работы сервера затрагивает приложения Enterprise Identity Mapping (EIM), применяющие сервер каталогов для выполнения операций EIM. Все приложения отключаются от сервера каталогов, однако они могут попытаться восстановить соединение с сервером.

**Для останова сервера каталогов выполните следующие действия:**
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **IBM Directory Server** и выберите **Остановить**.

Завершение работы сервера каталогов может занять до нескольких минут, в зависимости от производительности системы, количества выполняемых операций сервера и объема свободной памяти. Во время запуска вы можете периодически проверять состояние сервера (см. раздел “Просмотр состояния сервера каталогов”).

**Примечание:** Работу сервера каталогов можно завершить и в сеансе 5250 с помощью команд `ENDTCPSVR *DIRSRV`, `ENDTCPSVR *ALL` и `ENDTCP`. Команды `ENDTCPSVR *ALL` и `ENDTCP` завершают работу всех серверов TCP/IP в системе. Команда `ENDTCP` дополнительно завершает работу TCP/IP.

## Просмотр состояния сервера каталогов

Базовая информация о состоянии находится в Навигаторе iSeries. Более полные и подробные сведения о состоянии можно просмотреть с помощью Web-инструмента администрирования.

Состояние сервера каталогов указывается в столбце **Состояние** на правой панели окна программы Навигатор.

Для просмотра состояния сервера каталогов в Навигаторе iSeries выполните следующие действия:
1. Разверните пункт **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**. В столбце **Состояние** окна программы Навигатор будет указано состояние всех серверов TCP/IP, в том числе сервера каталогов.Для обновления информации о состоянии серверов выберите в меню **Вид** пункт **Обновить**.
4. Для просмотра более подробной информации о состоянии сервера каталогов щелкните правой кнопкой мыши на пункте **IBM Directory Server** и выберите **Состояние**. Будет показано число активных соединений, а также другие сведения, например, текущий уровень активности и уровень активности за истекший период.

   Просмотр информации о состоянии с помощью этой опции позволяет не только получить дополнительные сведения, но и сэкономить время. При обновлении значения состояния сервера каталогов не тратится дополнительное время на получение информации о состоянии остальных серверов TCP/IP.

Для просмотра состояния сервера каталогов с помощью Web-инструмента администрирования выполните следующие действия:

1. В области навигации разверните категорию **Администрирование сервера**.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. Выберите **Состояние сервера**.
3. Информация о состоянии отображается на различных вкладках страницы **Состояния сервера**.

## Проверка заданий сервера каталогов

В некоторых случаях может потребоваться контроль за работой определенных заданий на сервере каталогов. Для просмотра заданий сервера в Навигаторе iSeries выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.

4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите опцию **Задания сервера**.

## Управление соединениями сервера

Администратору часто требуется просмотреть соединения сервера и операции, выполняющиеся этими соединениями. На основе этого администратор планирует управление доступом так, чтобы воспрепятствовать атакам отказа в обслуживании. Для этой цели можно воспользоваться Web-инструментом администрирования.

В области навигации разверните категорию **Администрирование сервера**. Выберите **Управление соединениями сервера**. Будет показана таблица с данными по каждому соединению:

**Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.

**DN** Указывает DN соединения клиента и сервера.

**IP-адрес**
Указывает IP-адрес клиента, подключенного к серверу.

**Время запуска**
Указывает дату и время (местное время для сервера) установки соединения.

**Состояние**
Указывает, активно соединение или не используется. Соединение считается активным, если выполняется хоть одна операция.

**Начато операций**
Указывает количество операций, запрошенных с момента установки соединения.

**Завершено операций**
Указывает количество выполненных операций для каждого соединения.

**Тип** Указывает, защищено ли соединение с помощью SSL или TLS. В противном случае поле остается пустым.

**Примечание:** В этой таблице одновременно может отображаться до 20 соединений.

Выпадающее меню в верхней части страницы позволяет задать сортировку таблицы - по DN либо по IP-адресам. По умолчанию таблица сортируется по DN. Аналогично, можно указать порядок сортировки таблицы - по возрастанию или по убыванию.

Для обновления информации в таблице нажмите кнопку **Обновить**.

Если вы вошли в систему под именем администратора или члена группы администраторов, то вам будут доступны дополнительные опции отключения соединения. Возможность отключения соединения с сервером позволяет прерывать атаки отказа в обслуживании и управлять доступом к серверу. Отключить соединение можно, выбрав DN или IP-адрес соединения и нажав **Отключить**.

Для отключения всех соединений сервера, кроме того, по которому пришел запрос, нажмите кнопку**Отключить все**. Будет показано сообщение подтверждения. Нажмите **OK** для выполнения отключения, или **Cancel** для отмены действия и возврата на страницу **Управление соединениями сервера**.

Дополнительная информация по предотвращению атак отказа в обслуживании приведена в разделе “Управление свойствами соединения”.

## Управление свойствами соединения

Возможность управлять свойствами соединения позволяет предотвратить блокировку сервера клиентами. Кроме того, эта возможность гарантирует администратору постоянный доступ к серверу, даже в случаях, когда базовая программа загружает сервер длительной задачей. Для управления свойствами соединений служит Web-инструмент администрирования.

**Примечание:** Эти опции отображаются только в том случае, если вы вошли в систему под именем администратора или члена группы администраторов, и если эта функция поддерживается на сервере.

Для настройки свойств соединения выполните следующие действия:

1. В области навигации разверните категорию **Администрирование сервера** и выберите **Управление свойствами соединения**.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. Перейдите на вкладку **Общие**.
3. Настройте параметры анонимного соединения. Так как переключатель **Разрешить анонимные соединения** уже включен, то анонимные подключения разрешены. Это значение принято по умолчанию. Выключив этот переключатель, можно отключить функцию **Разрешить анонимные соединения**. В результате сервер будет аннулировать все анонимные подключения.

   **Примечание:** Однако, если анонимные подключения запрещены, некоторые приложения могут работать неправильно.
4. В поле **Порог отключения анонимных соединений** укажите пороговое значение, при котором анонимные соединения будут аннулироваться. Для этого поля допускаются значения от 0 до 65535 .

   **Примечание:** Фактически максимум ограничен количеством файлов, разрешенных для процесса. В системах UNIX можно определить граничные значения с помощью команды **ulimit -a**. В системах Windows это значение зафиксировано.

   По умолчанию принято значение 0. Когда это количество анонимных соединений будет превышено, соединения аннулируются по истечении тайм-аута простоя, указанного в поле **Тайм-аут простоя**.
5. В поле **Порог отключения идентифицированных соединений** укажите пороговое значение, при котором идентифицированные соединения будут аннулироваться. Для этого поля допускаются значения от 0 до 65535 .

   **Примечание:** Фактически максимум ограничен количеством файлов, разрешенных для процесса. В системах UNIX можно определить граничные значения с помощью команды ulimit -a. В системах Windows это значение зафиксировано.

   По умолчанию принято значение 1100. Когда это количество идентифицированных соединений будет превышено, соединения аннулируются по истечении тайм-аута простоя, указанного в поле **Тайм-аут простоя**.

6. В поле **Порог отключения всех соединений** укажите пороговое значение, при котором все соединения будут аннулироваться. Для этого поля допускаются значения от 0 до 65535 .

   **Примечание:** Фактически максимум ограничен количеством файлов, разрешенных для процесса. В системах UNIX можно определить граничные значения с помощью команды ulimit -a. В системах Windows это значение зафиксировано.

   По умолчанию принято значение 1200. Когда это количество соединений будет превышено, соединения аннулируются по истечении тайм-аута простоя, указанного в поле **Тайм-аут простоя**.
7. В поле **Тайм-аут простоя** указывается время в секундах, в течение которого соединение может быть неактивным. По истечении этого времени соединение аннулируется. Для этого поля допускаются значения от 0 до 65535 .

   **Примечание:** Фактически максимум ограничен количеством файлов, разрешенных для процесса. В системах UNIX можно определить граничные значения с помощью команды ulimit -a. В системах Windows это значение зафиксировано.

   По умолчанию принято значение 300. Когда начинается процесс очистки, закрываются все соединения, имеющие отношение к процессу и превысившие тайм-аут.
8. В поле **Итоговый тайм-аут** указывается время в секундах между попытками записи. Для этого поля допускаются значения от 0 до 65535 .По умолчанию принято значение 120. Все соединения, превысившие этот предел, закрываются.

   **Примечание:** Этот параметр относится только к системам Windows. Соединение больше 30 секунд автоматически аннулируется операционной системой. Следовательно, если значение поля **Итоговый тайм-аут** больше 30 секунд, то оно переопределяется системой.
9. Перейдите на вкладку **Аварийная нить**.
10. Настройте параметры аварийной нити. Так как переключатель **Включить аварийную нить** уже включен, то аварийная нить активирована. Это значение принято по умолчанию. Выключив этот переключатель, можно отключить функцию **Включить аварийную нить**. В результате аварийная нить никогда не активируется.
11. В поле **Порог ожидающих запросов** укажите предельное количество рабочих запросов, по достижении которого будет активизирована аварийная нить. Для этого поля допускаются значения от 0 до 65535. Это максимальное число запросов в очереди, после превышения которого активизируется аварийная нить. По умолчанию принято значение 50. Когда указанный предел будет превышен, активизируется аварийная нить.
12. В поле **Пороговое время** указывается время в минутах, которое может пройти с момента удаления из очереди последнего задания. Если в очереди еще есть задания, а пороговое время превышено, то активизируется аварийная нить. Для этого поля допускаются значения от 0 до 240. По умолчанию принять значение 5.
13. В выпадающем списке выберите критерии для активизации аварийной нити. Эти критерии следующие:
    - **Только размер:** Аварийная нить активизируется только в том случае, когда количество ожидающих заданий в очереди достигнет указанного значения.
    - **Только время:** Аварийная нить активизируется только в том случае, когда будет превышено указанное время между удалением заданий.
    - **Размер или время:** Аварийная нить активизируется в случае, когда превышено пороговое значение либо для размера очереди, либо для времени.
    - **Размер и время:** Аварийная нить активизируется в том случае, когда превышаются пороговые значения и для размера очереди, и для времени.

    По умолчанию принято значение Размер и время.
14. Нажмите **OK**

Дополнительная информация приведена в разделе “Управление соединениями сервера” на стр. 122.

## Включение уведомления о событиях

Сервер каталогов поддерживает функцию уведомления о событиях, позволяющую уведомлять клиентов, зарегистрированных на сервере LDAP, о наступлении заданных событий, например о добавлении информации в каталог.

Для включения функции уведомления о событиях на сервере выполните следующие действия:

1. В области навигации Web-инструмента администрирования разверните категорию **Управление свойствами сервера** и перейдите на вкладку **Уведомления о событиях**.
2. Включите переключатель **Разрешить уведомления о событиях**, чтобы разрешить уведомления о событиях. Если функция **Разрешить уведомления о событиях** отключена, то все остальные опции на этой странице будут проигнорированы.
3. Настройте значение **Максимальное количество регистраций для соединения**. Включите переключатель **Регистрации** или **Не ограничено**. Если вы выбрали **Регистрации**, то необходимо указать в соответствующем поле максимальное количество регистраций для соединения. Максимальное количество транзакций может быть 2, 147, 483, 647. По умолчанию принято 100 регистраций.
4. Настройте значение **Общее количество регистраций**. В этом поле указывается, сколько регистраций одновременно допускается на сервере. Включите либо переключатель **Регистраций**, либо **Не ограничено**. Если вы выбрали **Регистраций**, то необходимо указать в соответствующем поле максимальное количество регистраций для соединения. Максимальное количество транзакций может быть 2, 147, 483, 647. По умолчанию для количества регистраций принято значение **Не ограничено**.
5. По окончании настройки нажмите **Применить** для сохранения изменений без выхода, или **OK** для сохранения и закрытия страницы. Если вы не хотите сохранять изменения, нажмите кнопку **Отмена**.
6. Для того чтобы вступило в силу включение уведомлений о событиях, необходимо перезапустить сервер. Если вы изменяли только параметры, то перезапуск не нужен.

**Примечание:** Для отключения уведомления о событиях выключите переключатель **Разрешить уведомления о событиях** и перезапустите сервер.

Дополнительная информация, связанная с функцией уведомления о событиях, приведена в соответствующем разделе справочника IBM Directory Server Version 5.2 Programming Reference.

## Настройка параметров транзакций

Сервер каталогов поддерживают транзакции, объединяющие несколько операций с каталогом LDAP. Дополнительная информация приведена в разделе “Транзакции” на стр. 50.

Для настройки параметров транзакций на сервере выполните следующие действия:

1. В области навигации Web-инструмента администрирования разверните категорию **Управление свойствами сервера** и перейдите на вкладку **Транзакции**.
2. Включите переключатель **Разрешить обработку транзакций** для разрешения обработки транзакций. Если переключатель **Разрешить обработку транзакций** выключен, то все остальные опции на этой странице, в частности, **Максимальное количество операций для транзакции** и **Предельное время ожидания** система проигнорирует.
3. Настройте параметр **Максимальное количество транзакций**. Включите либо переключатель **Транзакций**, либо **Не ограничено**. Если вы выбрали **Транзакций**, то необходимо указать в соответствующем поле максимальное количество транзакций. Максимальное количество транзакций может быть 2, 147, 483, 647. По умолчанию принято значение 20 транзакций.
4. Настройте значение **Максимальное количество операций для транзакции**. Включите переключатель **Операций** или **Не ограничено**. Если вы выбрали **Операций**, то необходимо указать в соответствующем поле максимальное количество операций для транзакции. Максимальное количество операций может быть 2, 147, 483, 647. Чем меньше количество операций, тем выше производительность. По умолчанию принято 5 операций.

5. Настройте значение **Предельное время ожидания**. В этом поле задается максимальное время ожидания для транзакции в секундах. Включите либо переключатель **Секунд**, либо **Не ограничено**. Если вы выбрали **Секунд**, то необходимо указать в соответствующем поле максимальное время в секундах для транзакции. Допустимы значения 2, 147, 483 или 647 секунд. Транзакции, не выполнившиеся в течение этого времени, отменяются (откатываются). По умолчанию принято значение 300 секунд.
6. По окончании настройки нажмите **Применить** для сохранения изменений без выхода, или **OK** для сохранения и закрытия страницы. Если вы не хотите сохранять изменения, нажмите кнопку **Отмена**.
7. Если вы включили поддержку транзакций, то для вступления изменений в силу необходимо перезапустить сервер. Если вы изменяли только параметры, то перезапуск не нужен.

**Примечание:** Для отключения поддержки транзакций выключите переключатель **Разрешить обработку транзакций** и перезапустите сервер.

## Изменение номера порта или IP-адреса

Сервер каталогов по умолчанию использует следующие порты:
- 389 для незащищенных соединений.
- 636 для защищенных соединений (если вы разрешили серверу каталогов применять защищенные порты в диспетчере цифровых сертификатов).

**Примечание:** По умолчанию с сервером связаны все IP-адреса, определенные в системе.

Если эти порты уже применяются другим приложением, выберите другой порт для сервера каталогов, либо, если приложением поддерживает связывание с определенным IP-адресом, задайте различные IP-адреса для двух серверов.

Пример сервера LDAP Domino, конфликтующего с сервером каталогов, приведен в разделе Применение хоста LDAP Domino и сервера каталогов в одной системе iSeries.

Для изменения портов сервера каталогов выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на страницу **Сеть**.
6. Введите необходимые номера портов и нажмите кнопку **OK**.

Для изменения IP-адреса, применяемого для подключения к серверу каталогов, выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на страницу **Сеть**.
6. Нажмите кнопку **IP-адреса...**.
7. Выберите опцию **Применять выбранные IP-адреса** и задайте IP-адреса для подключения к серверу.

## Выбор сервера каталогов для переадресации

Для того чтобы назначить серверы переадресации для сервера каталогов, выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.

5. Выберите страницу свойств **Общие**.
6. В поле **Новая переадресация** укажите URL сервера переадресации.
7. В приглашении введите имя сервера переадресации в формате URL. Ниже приведены примеры допустимых URL LDAP:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   **Примечание:** Если сервер переадресации не применяет порт по умолчанию, укажите в URL необходимый номер порта. Во втором из приведенных выше примеров задан порт 400.
8. Нажмите кнопку **Добавить**.
9. Нажмите кнопку **OK**.

## Добавление и удаление суффиксов сервера каталогов

Добавление суффикса на сервер каталогов позволяет серверу управлять соответствующей частью дерева каталогов.

**Примечание:** Добавление суффикса, являющегося частью другого суффикса на сервере, недопустимо. Например, если `o=ibm, c=us` - суффикс на сервере, то нельзя добавить суффикс `ou=rochester, o=ibm, c=us`.

Для добавления суффикса на сервер каталогов выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на страницу **База данных/Суффиксы**.
6. В поле **Новый суффикс** введите имя нового суффикса.
7. Нажмите кнопку **Добавить**.
8. Нажмите кнопку **OK**.

**Примечание:** Суффикс на сервере указывает на определенный раздел каталога, однако при его добавлении никакие объекты не создаются. Если объект, соответствующий добавленному суффиксу, не существует, его необходимо создать, как любой другой объект.

Для удаления суффикса с сервера каталогов выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на страницу **База данных/Суффиксы**.
6. Щелкните на суффиксе, который необходимо удалить.
7. Нажмите кнопку **Удалить**.

   **Примечание:** Можно указать, чтобы при удалении суффикса не удалялись объекты, находящиеся в структуре каталога под этим суффиксом. Эта информация станет недоступной на сервере каталогов. Однако позже доступ к данным можно восстановить, добавив удаленный суффикс.

## Сохранение и восстановление информации сервера каталогов

Сервер каталогов хранит информацию в следующих объектах:

- В библиотеке базы данных (по умолчанию, QUSRDIRDB), содержащей информацию серверов каталогов.

**Примечание:** Можно посмотреть, какая библиотека активна в данный момент. Она отображается на вкладке **База данных/Суффиксы** страницы свойств IBM Directory Server в Навигаторе iSeries.

- В библиотеке QDIRSRV2, содержащей информацию о публикации.
- В библиотеке QUSRSYS, содержащей различные элементы объектов, начиная с QGLD (для их сохранения необходимо указать QUSRSYS/QGLD*).
- Если на сервере каталогов настроено ведение протокола изменений, то информация также хранится в библиотеке QUSRDIRCL.

Если информация каталога изменяется регулярно, то следует регулярно сохранять библиотеку базы данных и ее объекты. Кроме того, данные конфигурации хранятся в следующем каталоге:

```
/QIBM/UserData/OS400/Dirsrv/
```

Файлы в этом каталоге следует сохранять после изменения конфигурации или применения PTF.

Сведения о сохранении и восстановлении данных приведены в разделе Резервное копирование и восстановление, SH43-0080  .

## Предоставление спроецированным пользователям администраторских прав доступа

Вы можете предоставлять права доступа администратора пользовательским профайлам, у которых есть доступ к ИД функции администратора сервера каталогов (QIBM_DIRSRV_ADMIN).

Например, если у пользовательского профайла JOHNSMITH есть права доступа к ИД функции администратора сервера каталогов, и в окне свойств каталога выбрана опция Предоставить права администратора уполномоченным пользователям, то пользовательскому профайлу JOHNSMITH будут предоставлены права доступа администратора. При подключении к серверу каталогов с помощью этого пользовательского профайла и DN os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com пользователю предоставляются права доступа администратора. Суффиксом системных объектов в этом примере является os400-sys=systemA.acme.com. Дополнительная информация о спроецированных пользователях приведена в разделе “Спроецированная база данных операционной системы” на стр. 80.

Для выбора этой опции выполните следующие действия:

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
4. На странице **Общие** отметьте опцию **Предоставить права администратора уполномоченным пользователям** в категории **Информация об администраторе**.

Для того чтобы предоставить пользовательскому профайлу права доступа к ИД функции администратора сервера каталогов, выполните следующие действия:

1. В Навигаторе щелкните правой кнопкой мыши на имени системы и выберите пункт **Администрирование приложений**.
2. Перейдите на страницу **Приложения хоста**.
3. Откройте **Operating System/400**.
4. Выберите опцию **Администратор сервера каталогов**.
5. Нажмите кнопку **Настроить**.
6. В зависимости от категории пользователя откройте папку **Пользователи**, **Группы** или **Пользователи вне групп**.
7. Выберите пользователя или группу для добавления в список **Доступ разрешен**.
8. Нажмите кнопку **Добавить**.

9. Нажмите кнопку **OK**, чтобы сохранить изменения.
10. Нажмите кнопку **OK** в окне диалога **Администрирование приложений**.

## Работа с группой администраторов

Группа администраторов позволяет получить административные права доступа, не применяя один общий ИД администратора и пароль. У каждого члена группы администраторов есть свой собственный ИД пользователя и пароль. Имена DN членов группы администраторов не должны совпадать друг с другом и не должны совпадать с DN администратора IBM Directory Server. И наоборот, DN администратора IBM Directory Server не должно совпадать ни с одним DN члена группы администраторов.

Это правило также применимо к ИД администратора IBM Directory Server и членов группы администраторов при идентификации Kerberos и Digest-MD5. Эти DN не должны совпадать ни с одним DN сервера-поставщика копирования IBM Directory Server. Также это означает, что DN сервера-поставщика копирования IBM Directory Server не должно совпадать ни с DN какого-либо члена группы администраторов, ни с DN администратора IBM Directory Server.

**Примечание:** Имена DN сервера-поставщика копирования IBM Directory Server могут совпадать друг с другом.

Дополнительная информация приведена в разделе:

- “Активизация группы администраторов”
- “Добавление, изменение и удаление членов группы администраторов” на стр. 130

**Связанная информация**

“Права доступа администратора” на стр. 59

## Активизация группы администраторов

Для этой операции необходимы права доступа администратора IBM Directory Server.

1. В области навигации Web-инструмента администрирования разверните категорию **Администрирование сервера** и выберите **Управление группой администраторов**.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. Для включения или выключения поддержки группы администраторов включите переключатель **Активизировать группу администраторов**. Включенный переключатель означает, что группа администраторов активна.
3. Нажмите кнопку **OK**.

   **Примечание:** Если вы отключаете поддержку группы администраторов, то для всех участников группы, уже вошедших в систему, возможность администрирования сохраняется до конца сеанса.

## Добавление, изменение и удаление членов группы администраторов

**Предварительное требование:** Для этой операции необходимы права доступа администратора IBM Directory Server.

1. В области навигации Web-инструмента администрирования разверните категорию **Администрирование сервера** и выберите **Управление группой администраторов**.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. На странице **Управление группой администраторов** нажмите **Добавить**.
3. На странице **Добавление участника группы администраторов** выполните следующие действия:
   a. Введите администраторское DN участника (согласно соответствующему синтаксису DN).
   b. Введите пароль участника.
   c. Введите пароль еще раз для подтверждения.
   d. Необязательно: Введите ИД участника для Kerberos. ИД для Kerberos следует указывать в формате либо ibm-kn, либо ibm-KerberosName. Значения можно указывать без учета регистра символов. Например, ibm-kn=root@TEST.ROCHESTER.IBM.COM и ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM - это одно и то же.
4. Необязательно: введите **Имя пользователя Digest-MD5** участника.

   **Примечание:** Имя пользователя Digest-MD5 указывается с учетом регистра букв.
5. Нажмите кнопку **OK**.
6. Повторите эту процедуру для каждого участника, добавляемого в группу администраторов.

Администраторское DN участника, имя пользователя Digest-MD5 (если указано) и ИД Kerberos (если указан) отображаются в списке Члены группы администраторов.

Процедура изменения или удаления члена группы администраторов аналогична вышеописанной, с тем лишь отличием, что на странице **Управление группой администраторов** используются кнопки **Изменить** и **Удалить**.

---

## Управление группами ограниченного поиска

Во избежание значительного снижения производительности сервера вследствие того, что пользовательский поиск занимает много ресурсов, на запросы для любого заданного сервера налагаются ограничения поиска. Эти ограничения задаются администратором при настройке сервера и включают размер и продолжительность поиска.

Эти ограничения не распространяются только на самого администратора и членов группы администраторов. Однако при необходимости администратор может создать группу ограниченного поиска. Эта группа имеет более гибкие ограничения поиска, чем обычные пользователи. В этом случае администратор может предоставить группе пользователей особые права доступа.

Дополнительная информация приведена в разделах:

- “Создание группы ограниченного поиска” на стр. 131
- “Изменение группы ограниченного поиска” на стр. 132

| • “Копирование группы ограниченного поиска” на стр. 132
| • “Удаление группы ограниченного поиска” на стр. 132

| Управление группами ограниченного поиска осуществляется с помощью Web-инструмента
| администрирования.

**Связанные концепции**

“Параметры поиска” на стр. 47

## Создание группы ограниченного поиска

Для создания группы ограниченного поиска следует сначала с помощью Web-инструмента администрирования создать запись группы.

1. В области навигации разверните категорию **Управление каталогом** и выберите **Добавить запись**. Или выберите расположение (cn=IBMpolicies или cn=localhost) в категории **Управление записями** и нажмите **Добавить**. Записи в контейнере cn=IBMpolicies копируются, тогда как записи в cn=localhost - нет.
2. В меню **Структурный класс объекта** выберите один из классов объектов группы.
3. Нажмите кнопку **Далее**.
4. В меню **Доступные** выберите вспомогательный класс объектов**ibm-searchLimits** и нажмите **Добавить**. Повторите эти действия для всех добавляемых объектов вспомогательных классов. Вспомогательный класс объектов можно удалить из списка **Выбранные**, выделив его и нажав **Удалить**.
5. Нажмите кнопку **Далее**.
6. В поле **Относительное DN** введите относительное отличительное имя (RDN) добавляемой группы. Например, cn=Search Group1.
7. В поле **Родительское DN** введите отличительное имя выбранной записи дерева. Например, cn=localhost. Вы также можете нажать кнопку **Обзор** и выбрать в списке нужное родительское DN. Выделите запись и нажмите **Выбрать** для указаного родительского DN. По умолчанию в качестве **Родительского DN** применяется выбранная запись.

   **Примечание:** Если вы перешли к этой панели из окна **Управление записями**, то значение в этом поле уже будет указано. Вы выбрали **Родительское DN** перед тем, как нажать кнопку **Добавить**.
8. На вкладке **Обязательные атрибуты** укажите значения обязательных атрибутов.
   - **cn** - это относительное DN, указанное ранее.
   - В поле **ibm-searchSizeLimit** укажите максимальное количество записей, возвращаемых поиском. Это число может быть от 0 до 2 147 483 647. Нулевое значение эквивалентно значению **Не ограничено**.
   - В поле **ibm-searchTimeLimit** укажите время в секундах, ограничивающее продолжительность поиска. Это число может быть от 0 до 2 147 483 647. Нулевое значение эквивалентно значению **Не ограничено**.
   - В зависимости от выбранного класса объектов может отображаться либо поле **Участник**, либо **uniqueMember**. Эти поля указывают членов создаваемой группы. Значение в этих полях указывается в формате DN, например, cn=Bob Garcia,ou=austin,o=ibm,c=us.
9. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке. По окончании добавления значений нажмите **OK**. Значения будут добавлены в разворачиваемое меню данного атрибута.
10. Если на сервере включена поддержка языковых тегов, то выберите **Значение языкового тега** для добавления или удаления описателей языковых тегов.
11. Перейдите на вкладку **Прочие атрибуты**.
12. На вкладке **Прочие атрибуты** настройте необходимые значения для атрибутов. Дополнительная информация приведена в разделе “Изменение двоичных атрибутов” на стр. 185.
13. Для создания записи нажмите **Готово**.

## Изменение группы ограниченного поиска

Для группы ограниченного поиска вы можете изменить атрибуты размера и времени. Также вы можете добавлять и удалять членов группы. Управление группой ограниченного поиска осуществляется с помощью Web-инструмента администрирования.

Информация об изменении группы ограниченного поиска приведена в разделе “Редактирование записи” на стр. 181.

## Копирование группы ограниченного поиска

Если необходимо, чтобы одна и та же группа ограниченного поиска хранилась и в localhost, и в IBMpolicies, то можно воспользоваться возможностью копирования. Кроме этого, если требуется создать новую группу, которая незначительно отличается от уже существующей, то также удобнее будет воспользоваться копированием.

Информация о копировании существующей группы ограниченного поиска приведена в разделе “Копирование записи” на стр. 182.

## Удаление группы ограниченного поиска

Информация по удалению группы ограниченного поиска приведена в разделе “Удаление записи” на стр. 181.

---

## Управление группой Proxy-идентификации

Члены группы Proxy-идентификации могут обращаться к серверу каталогов и выполнять многие задачи от имени разных пользователей, не подключая при этом каждого по отдельности. Члены группы Proxy-идентификации могут выступить от имени любого пользователя, за исключением администратора и членов группы администраторов. Дополнительная информация приведена в разделе “Proxy-идентификация” на стр. 60.

Управление группой Proxy-идентификации осуществляется с помощью Web-инструмента администрирования.

Дополнительная информация приведена в разделах:

- “Создание группы Proxy-идентификации”
- “Изменение группы Proxy-идентификации” на стр. 133
- “Копирование группы Proxy-идентификации” на стр. 133
- “Удаление группы Proxy-идентификации” на стр. 133

## Создание группы Proxy-идентификации

1. В области навигации разверните категорию **Управление каталогом** и выберите **Добавить запись**. Или выберите расположение (cn=ibmPolicies или cn=localhost) в категории **Управление записями** и нажмите **Добавить**.
2. В меню **Структурные классы объектов** выберите классы объектов **группа имен**.
3. Нажмите кнопку **Далее**.
4. В меню **Доступные** выберите вспомогательный класс объектов**ibm-proxyGroup** и нажмите кнопку **Добавить**. Повторите эту операцию для всех добавляемых вспомогательных классов объектов.
5. Нажмите кнопку **Далее**.
6. В поле **Относительное DN** укажите значение `cn=proxyGroup`.
7. В поле **Родительское DN** введите отличительное имя выбранной записи дерева, например, cn=localhost. Вы можете также нажать **Обзор** и выбрать **Родительское DN** в появившемся списке. Сделайте выбор и нажмите кнопку **Выбрать**, чтобы указать Родительское DN. По умолчанию в качестве Родительского DN применяется выбранная запись.

**Примечание:** Если вы перешли к этой панели из окна Управление записями, то значение в этом поле уже будет указано. Родительское DN было выбрано перед нажатием кнопки Добавить.

8. На вкладке **Required attributes** укажите значения обязательных атрибутов.
   - **cn** - это `proxyGroup`.
   - Атрибут **Member** задается в формате DN, например, cn=Bob Garcia,ou=austin,o=ibm,c=us.

   Дополнительная информация о добавлении двоичных значений приведена в разделе “Изменение двоичных атрибутов” на стр. 185.
9. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.

   **Примечание:** Не указывайте нескольких значений в поле cn. Группе Proxy-идентификации должно быть присвоено стандартное имя, proxyGroup.

   По окончании добавления значений нажмите **OK**. Значения будут добавлены в разворачиваемое меню данного атрибута.
10. Если на сервере включена поддержка языковых тегов, то выберите **Значение языкового тега** для добавления или удаления описателей языковых тегов.
11. Перейдите на вкладку **Прочие атрибуты**.
12. На вкладке **Прочие атрибуты** настройте необходимые значения для атрибутов. Дополнительная информация о добавлении двоичных значений приведена в разделе “Изменение двоичных атрибутов” на стр. 185.
13. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.По окончании добавления значений нажмите **OK**. Значения будут добавлены в разворачиваемое меню данного атрибута.
14. Если на сервере включена поддержка языковых тегов, то выберите **Значение языкового тега** для добавления или удаления описателей языковых тегов.
15. Для создания записи нажмите **Готово**.

## Изменение группы Proxy-идентификации

Группу Proxy-идентификации можно изменять: добавлять или удалять участников с помощью Web-инструмента администрирования.

Информация об изменении группы Proxy-идентификации приведена в разделе “Редактирование записи” на стр. 181.

## Копирование группы Proxy-идентификации

Если вы хотите, чтобы одна и та же группа Proxy-идентификации хранилась и в localhost, и в IBMpolicies, то можно воспользоваться возможностью копирования.

Информация о копировании группы Proxy-идентификации приведена в разделе “Копирование записи” на стр. 182.

## Удаление группы Proxy-идентификации

Информация по удалению группы Proxy-идентификации с помощью Web-инструмента администрирования приведена в разделе “Удаление записи” на стр. 181.

---

## Управление уникальными атрибутами

Управление уникальными атрибутами осуществляется посредством категории **Администрирование сервера** Web-инструмента администрирования. Дополнительная информация приведена в следующих разделах:

- “Создание списка уникальных атрибутов” на стр. 134
- “Удаление записи из списка уникальных атрибутов” на стр. 135

**Примечание:** На уровне атрибутов языковые теги являются и уникальные атрибуты являются взаимно исключающими. Если конкретный атрибут планируется сделать уникальным, то с ним нельзя связывать языковые теги.

**Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.

## Создание списка уникальных атрибутов

1. В области навигации разверните категорию **Администрирование сервера**. Выберите опцию **Управление уникальными атрибутами**.
2. В списке **Доступные атрибуты** выберите атрибут, который необходимо сделать уникальным. Список доступных атрибутов содержит те атрибуты, которые можно сделать уникальными; например, sn.
3. Нажмите либо **Добавить в cn=localhost**, либо **Добавить в cn=IBMpolicies**. Различие между этими двумя контейнерами в том, что записи, хранящиеся в cn=IBMpolicies, копируются, а записи в cn=localhost - нет. Атрибут появится в соответствующем списке. Одни и те же атрибуты можно хранить в обоих контейнерах.

   **Примечание:** Если запись создана и в cn=localhost, и в cn=IBMpolicies, то в результате уникальными будут атрибуты обеих записей. Например, если атрибуты cn и employeeNumber настроены уникальными в cn=localhost, а атрибуты cn и telephoneNumber настроены как уникальные в cn=IBMploicies, то сервер будет считать уникальными атрибуты cn, employeeNumber и telephoneNumber.
4. Повторите эту процедуру для каждого атрибута, настраиваемого в качестве уникального.
5. Нажмите **OK**, чтобы сохранить изменения.

Если при добавлении или изменении записи об уникальными атрибутами ограничение уникальности для какого-либо атрибута вызывает ошибку, то запись не создается и в каталог не добавляется. Прежде, чем создавать или изменять запись, следует исправить ситуацию и повторно вызвать команду добавления или изменения. Например, если при добавлении записи уникального атрибута в каталог ограничение уникальности для таблицы вызывает ошибку для какого-либо из атрибутов списка (например, вследствие дублирования значений в базе данных), то запись уникального атрибута не будет добавлена в каталог. Будет выведено сообщение об ошибке.

Если приложение попытается добавить в каталог запись, значение одного из атрибутов которой дублирует значение атрибута существующей в базе записи, будет выведена ошибка сервера LDAP с кодом 20 (LDAP: код ошибки 20 - Атрибут или значение уже существует).

При запуске сервер проверяет список уникальных атрибутов и определяет, связаны ли с каждым из них ограничения DB2. Если с атрибутом не связано ограничение (например, атрибут удален утилитой bulkload или пользователем), то он удаляется из списка уникальных атрибутов, а в протокол ошибок ibmslapd.log заносится сообщение об ошибке. Например, если атрибут cn настроен в качестве уникального в контейнере cn=uniqueattributes,cn=localhost, но с ним не связано ограничений DB2, то в протокол будет занесено следующее сообщение:

```
Значения атрибута CN не являются уникальными.
Атрибут CN был удален из списка уникальных атрибутов
запись: CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

## Удаление записи из списка уникальных атрибутов

Если уникальный атрибут есть и в контейнере cn=uniqueattribute,cn=localhost, и в cn=uniqueattribute,cn=IBMpolicies, и он удаляется только из одной записи, то сервер будет продолжать обрабатывать этот атрибут как уникальный. Атрибут теряет уникальность, если удалить его из обеих записей.

1. В области навигации разверните категорию **Администрирование сервера** и выберите опцию **Управление уникальными атрибутами**.
2. В соответствующем списке атрибутов выберите атрибут, который требуется удалить из числа уникальных.
3. Нажмите кнопку **Удалить**.
4. Повторите эту процедуру для всех удаляемых атрибутов.
5. Нажмите **OK**, чтобы сохранить изменения.

**Примечание:** Если вы удаляете из списка cn=localhost или cn=IBMpolicies последний уникальный атрибут, то автоматически удаляется запись контейнера для этого списка, cn=uniqueattribute,cn=localhost или cn=uniqueattribute,cn=IBMpolicies.

---

## Отслеживание обращений к каталогу LDAP и изменений каталога

У вас есть возможность отслеживать обращения к каталогу LDAP и изменения, вносимые в этот каталог. Для этого служит протокол изменений каталога LDAP. С протоколом изменений связан особый суффикс `cn=changelog`. Протокол хранится в библиотеке QUSRDIRCL.

Для того чтобы включить функцию ведения протокола изменений, выполните следующие действия:

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на вкладку **Протокол изменений**.
6. Выберите опцию **Заносить в протокол сведения об изменении каталога**.
7. Необязательно: В поле **Максимальное количество записей** укажите максимальное количество записей протокола изменений. В поле **Максимальное время хранения** можно указать время хранения записей протокола изменений.

   **Примечание:** Несмотря на то, что эти параметры не являются обязательными, настоятельно рекомендуется указать максимальное число или максимальное время хранения записей. Если не сделать этого, то записи в протоколе изменений будут накапливаться, и его размер может стать очень большим.

Класс объектов `changeLogEntry` представляет изменения, внесенные на сервере каталогов. Набор изменений представляется в виде упорядоченного набора записей объекта change в соответствии с параметром `changeNumber`. Информация из протокола изменений предназначена только для чтения.

Пользователи, указанные в списке управления доступом суффикса `cn=changelog`, могут выполнять поиск записей в протоколе изменений. Для суффикса протокола изменений `cn=changelog` доступна только операция поиска. Не пытайтесь добавлять, изменять или удалять записи в суффиксе протокола изменений, даже при наличии соответствующих прав доступа. Такие действия приведут к непредсказуемым последствиям.

**Пример:**

Ниже приведен пример получения всех записей протокола изменений на сервере с помощью утилиты **ldapsearch**:

```
ldapsearch -h хост-ldap -D cn=admininistrator -w пароль -b cn=changelog  (changetype=*)
```

## Включение контроля объектов для сервера каталогов

Сервер каталогов поддерживает средства контроля из подсистемы защиты i5/OS. Если системное значение QAUDCTL равно *OBJAUD, в программе Навигатор можно включить функцию контроля за объектами.

Для включения функции контроля за объектами для сервера каталогов выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на страницу **Контроль**.
6. Выберите необходимое значение контроля для сервера.
7. Нажмите **OK**

Изменения параметров контроля вступают в силу сразу после нажатия кнопки **OK**. Перезапускать сервер каталогов не нужно. Дополнительная информация приведена в разделе “Защита сервера каталогов” на стр. 51.

## Настройка параметров поиска

С помощью Web-инструмента администрирования можно настраивать параметры, позволяющие управлять функцией поиска пользователей, а также настраивать страницы результатов поиска и задавать параметры сортировки, предельные значения размера и времени, а также параметры учета псевдонимов.

Настройка страниц позволяет клиенту управлять объемом данных, возвращаемых в ответе на запрос. Вместо всех результатов запроса система может вернуть только некоторый набор данных (страницу). Следующий запрос покажет следующую страницу и так далее, пока не будут показаны все результаты или операция не будет отменена.

Сортировка позволяет клиенту получать результаты поиска, отсортированные на основании заданных критериев, задаваемых ключами сортировки. При этом сортировка выполняется не клиентским приложением, а сервером.

Для настройки параметров поиска на сервере каталогов выполните следующие действия:
1. В области навигации разверните категорию **Администрирование сервера** и выберите **Управление свойствами сервера**.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. Перейдите на вкладку **Параметры поиска**.
3. Настройте значение **Максимальный размер поиска**. Включите либо переключатель **Записей**, либо **Не ограничено**. Если вы выбрали **Записей**, то необходимо указать в соответствующем поле максимальное количество записей, которые может возвращать поиск. По умолчанию принято значение 500. Если критериям поиска удовлетворяет большее количество записей, лишние записи возвращаться не будут. Это ограничение не распространяется на администраторов и членов группы администраторов, для которых настроен больший максимальный размер поиска.
4. Укажите значение **Максимальное время поиска**. Включите либо переключатель **Секунд**, либо **Не ограничено**. Если вы выбрали **Секунд**, то необходимо указать в соответствующем поле максимальное

время, которое отводится серверу на обработку запроса на поиск. По умолчанию принято значение 900. Это ограничение не распространяется на администраторов и членов группы администраторов, для которых настроено большее максимальное время поиска.

5. Поиск можно настроить так, чтобы сортировать результаты могли только администраторы. Для этого можно включить переключатель **Разрешить сортировку только администраторам**.
6. Функцию поиска можно настроить так, чтобы постраничный поиск могли выполнять только администраторы. Для этого можно включить переключатель **Разрешить постраничный поиск только администраторам**.
7. Откройте контекстное меню для опции **Учет псевдонимов** и выберите одно из следующих свойств. По умолчанию принято значение **Всегда**.

   **Никогда**
   Псевдонимы не учитываются.

   **Нахождение**
   Псевдонимы учитываются при нахождении исходной точки поиска, но не учитываются при поиске начиная с этой начальной записи.

   **Поиск** Псевдонимы учитываются при поиске записей начиная с исходной точки поиска, но не учитываются при нахождении начальной записи.

   **Всегда** Псевдонимы учитываются всегда, как при нахождении исходной точки поиска, так и при поиске записей начиная с исходной точки. Это значение принято по умолчанию.

Дополнительная информация приведена в разделах “Параметры поиска” на стр. 47 и “Поиск записей каталога” на стр. 183.

## Настройка параметров производительности

Для повышения производительности сервера каталогов можно настраивать следующие параметры:
- Размер кэша ACL, размер кэша записей, максимальное число операций поиска, хранящихся в кэше фильтра, а также максимальный размер операции поиска, сохраняемой в кэше фильтра.
- Число соединений с базой данных и число нитей сервера.
- Параметры кэша атрибутов
- Параметры транзакций сервера

Дополнительная информация приведена в разделах:
- “Настройка соединений базы данных и параметров кэша”
- “Настройка кэша атрибутов” на стр. 138
- “Настройка параметров транзакций” на стр. 140

## Настройка соединений базы данных и параметров кэша

Для настройки соединений базы данных и параметров кэша выполните следующие действия:

1. В области навигации Web-инструмента администрирования разверните категорию **Управление свойствами сервера**, затем перейдите на вкладку **Параметры производительности** с правой стороны.
2. Укажите **Количество соединений базы данных**. Этот параметр задает количество соединений DB2 для сервера. По минимуму может быть 4 соединения. По умолчанию принято значение 15. Если сервер LDAP получает много клиентских запросов, или клиенты часто получают сообщения об ошибке ″отказ в соединении″, то можно улучшить ситуацию, увеличив количество соединений DB2 для сервера. Максимальное количество соединений зависит от настройки базы данных DB2. Так как на количество ваших соединений серверные ограничения не распространяются, каждое соединение потребляет ресурсы.
3. Укажите **Количество соединений базы данных для копирования**. Этот параметр задает количество соединений DB2, которые сервер будет использовать для копирования. Минимальное допустимое значение равно 1. По умолчанию принято значение 4.

**Примечание:** Общее количество соединений для базы данных, в том числе соединения для копирования, не может превышать количество соединений, указанное в параметрах базы данных DB2.

4. Выберите опцию **Кэшировать информацию ACL**, позволяющую настраивать следующие параметры кэша ACL.
5. Укажите **Максимальное количество элементов в кэше ACL**. По умолчанию принято значение 25000.
6. Укажите **Максимальное количество элементов записи кэша**. По умолчанию принято значение 25000.
7. Укажите **Максимальное количество элементов в кэше фильтров поиска**. По умолчанию принято значение 25000. В кэше фильтра поиска хранятся действительные запросы фильтров атрибутов и ИД соответствующих им записей. При обновлении все записи кэша фильтров становятся недействительными.
8. Укажите **Максимальное количество элементов отдельного поиска, добавляемого в кэш фильтров поиска**. Если вы выбираете **Элементов**, то следует указать число. По умолчанию принято значение 100. В противном случае выбирайте вариант **Не ограничено**. Записи о поиске, соответствующие большему, чем указанное, количеству записей, не добавляются в кэш фильтров.
9. После завершения ввода нажмите **OK**.
10. После настройки количества соединений базы данных необходимо перезапустить сервер. Если вы изменяли только параметры кэша, то перезапуск не нужен.

## Настройка кэша атрибутов

Параметры кэша атрибутов можно настраивать как с помощью Web-инструмента администрирования, так и с помощью Навигатора iSeries.

Для того чтобы настроить кэш атрибутов вручную, с помощью Web-инструмента администрирования, выполните следующие действия.

1. В области навигации Web-инструмента администрирования разверните категорию **Администрирование сервера** и перейдите на вкладку **Кэш атрибутов** с правой стороны.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. Настройте объем памяти для кэша каталога (в килобайтах). По умолчанию принято значение 16384 кб (16 Мб).
3. Настройте объем памяти для кэша протокола изменений (в килобайтах). По умолчанию принято значение 16384 кб (16 Мб).

   **Примечание:** Если протокол изменений не настроен, то этот параметр будет недоступным. Если вам редко необходим поиск в протоколе изменений, то для кэширования протокола изменений следует указывать значение 0 и не настраивать никаких атрибутов, поскольку этот поиск влияет на быстродействие.
4. В списке **Доступные атрибуты** выберите атрибуты, которые требуется сохранять в кэше. В списке отображаются только атрибуты, допускающие кэширование, например, sn.

   **Примечание:** В списке доступных атрибутов представлены только те атрибуты, которые помещены в оба контейнера: cn=directory и cn=changelog.
5. Нажмите либо **Добавить в cn=directory**, либо **Добавить в cn=changelog**. Атрибут появится в соответствующем списке. Одни и те же атрибуты можно хранить в обоих контейнерах.

**Примечание:** Если протокол изменений не настроен, то опция **Добавить в cn=changelog** будет недоступной. Если вам редко необходим поиск в протоколе изменений, то для кэширования протокола изменений следует указывать значение 0 и не настраивать никаких атрибутов, поскольку этот поиск влияет на быстродействие.

6. Повторите эту процедуру для всех атрибутов, добавляемых в кэш атрибутов.
7. После завершения ввода нажмите **OK**.

Для включения автоматического кэширования атрибутов в Навигаторе iSeries выполните следующие действия:

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на страницу **Производительность**.
6. Выберите опцию **Разрешить автоматическое кэширование атрибутов** либо для **Базы данных**, либо для **Протокола изменений**, либо для обоих сразу. Если вам редко необходим поиск в протоколе изменений, то автоматическое кэширование атрибутов протокола изменений разрешать не следует, поскольку этот поиск влияет на быстродействие.
7. Укажите **Время начала** (местное время для сервера) и **Интервал** для каждого выбранного типа кэширования. Например, если вы включили кэширование базы данных, указали время начала 6:00 с шестичасовым интервалом, то кэширование будет автоматически выполняться в 6 часов, 12, 18 и в полночь независимо от времени запуска сервера и времени настройки автоматической регулировки.

**Примечание:** Автоматическое кэширование атрибутов будет накапливать кэш до тех пор, пока не будет достигнут максимальный объем памяти, указанный с помощью Web-инструмента администрирования.

*Таблица 4. Взаимодействие параметров кэша атрибутов*

| Операция | Что произойдет |
|---|---|
| Запуск сервера | Если автоматическое кэширование атрибутов включено в данный момент и было включено во время последнего останова сервера, то атрибуты, кэшированные при останове, будут повторно созданы при перезапуске. Если для кэширования атрибутов еще доступна дополнительная память, то также будут сохранены и те атрибуты, которые были настроены вручную. Если автоматическое кэширование в данный момент включено, но в момент последнего останова сервера было отключено, то будут кэшироваться атрибуты, вручную настроенные для кэширования. Так или иначе, сервер затем автоматически выровняет кэши атрибутов, основываясь на указанном времени начала и интервале. Если автоматическое кэширование не включено, то в силу вступают параметры ручного кэширования. |
| Включение автоматического кэширования атрибутов после запуска сервера | После запуска сервера будет выполнено автоматическое кэширование атрибутов. Все вручную настроенные атрибуты, которые не укладываются в заданный объем кэша, будут удалены. |
| Отключение автоматического кэширования атрибутов после запуска сервера | Кэшироваться будут только атрибуты, настроенные вручную. |
| Изменение атрибутов, настроенных вручную, после запуска сервера при включенном автоматическом кэшировании | Ничего не произойдет. Настройка вручную имеет силу только при отключенном автоматическом кэшировании. |
| Изменение максимального объема кэша после запуска сервера | Если автоматическое кэширование включено, то сервер сразу же перестроит кэш на основе нового размера. Если автоматическое кэширование отключено, то сервер применит новый размер для кэширования атрибутов, настроенных вручную. |

*Таблица 4. Взаимодействие параметров кэша атрибутов (продолжение)*

| Операция | Что произойдет |
|---|---|
| Изменение времени начала или интервала после запуска сервера | Если автоматическое кэширование включено, то новые параметры вступят в силу сразу же. Если отключено, то параметры будут сохранены и вступят в силу при включении автоматического кэширования. |

## Настройка параметров транзакций

Для настройки параметров транзакций выполните следующие действия:

1. В области навигации Web-инструмента администрирования разверните категорию **Управление свойствами сервера**, затем перейдите на вкладку **Транзакции**.
2. Включите переключатель **Разрешить обработку транзакций** для разрешения обработки транзакций. Если переключатель **Разрешить обработку транзакций** выключен, то все остальные опции на этой странице система проигнорирует.
3. Настройте параметр **Максимальное количество транзакций**. Включите либо переключатель **Транзакций**, либо **Не ограничено**. Если вы выбрали **Транзакций**, то необходимо указать количество транзакций. Максимальное количество транзакций может составлять 2 147 483 647. По умолчанию принято значение 20 транзакций.
4. Настройте значение **Максимальное количество операций для транзакции**. Включите переключатель **Операций** или **Не ограничено**. Если вы выбрали **Операций**, то необходимо указать максимальное количество операций для транзакции. Максимальное количество операций может составлять 2 147 483 647. Чем меньше количество операций, тем выше производительность. По умолчанию принято 5 операций.
5. Настройте значение **Предельное время ожидания**. В этом поле задается максимальное время ожидания для транзакции в секундах. Включите либо переключатель **Секунд**, либо **Не ограничено**. Если вы выбрали **Секунд**, то необходимо указать максимальное время транзакции в секундах. Максимальное время может составлять 2 147 483 647 секунд. Транзакции, не выполнившиеся в течение этого времени, отменяются (откатываются). По умолчанию принято значение 300 секунд.
6. После завершения ввода нажмите **OK**.
7. Если вы включили поддержку транзакций, то для вступления изменений в силу перезапустите сервер. Если вы изменяли только параметры, то перезапуск не нужен.

## Управление копированием

Для управления копированием разверните в Web-инструменте администрирования категорию **Управление копированием**. Дополнительная информация о принципах работы функции копирования приведена в разделе “Копирование” на стр. 39.

Дополнительная информация приведена в следующих разделах:


- “Создание топологии с главными серверами и серверами-копиями” на стр. 141
- “Создание топологии с главным сервером, сервером пересылки и сервером-копией” на стр. 147
- “Обзор процедуры создания сложной топологии копирования” на стр. 148
- “Создание сложной топологии с копированием на равноправные серверы” на стр. 149
- “Настройка топологии шлюза” на стр. 152
- “Управление топологиями” на стр. 153
- “Изменение свойств копирования” на стр. 156
- “Создание расписания копирования” на стр. 158
- “Управление очередями” на стр. 159
- “Настройка копирования по защищенному соединению” на стр. 160

## Создание топологии с главными серверами и серверами-копиями

Для определения базовой топологии с главными серверами и серверами-копиями выполните следующие действия:

1. Создайте главный сервер и определите его содержимое. Выберите поддерево для копирования и укажите сервер в качестве главного. Обратитесь к разделу “Создание главного сервера (копируемое поддерево)”.
2. Создайте идентификационные данные, которые будут применяться сервером-поставщиком. См. раздел “Создание идентификационных данных” на стр. 142.
3. Создайте сервер-копию. См. раздел “Создание сервера-копии” на стр. 144.
4. Экспортируйте топологию с главного сервера на сервер-копию. См. раздел “Копирование данных на сервер-копию” на стр. 145.
5. Измените конфигурацию сервера-копии, указав, кто может копировать на этот сервер изменения, а также добавьте переадресацию на главный сервер. См. раздел “Добавление на сервер-копию информации о поставщике” на стр. 146.

**Примечание:**

Если запись, находящаяся в корне копируемого поддерева, не является суффиксом сервера, то для применения функции **Добавить поддерево** необходимо убедиться, что ее ACL определены следующим образом:

**ACL без фильтров:**

```
ownersource: <совпадает с DN записи>
ownerpropagate: TRUE

aclsource: <совпадает с DN записи>
aclpropagate: TRUE
```

**ACL с фильтрами:**

```
ibm-filteraclinherit: FALSE
```

Для приведения записи, не являющейся суффиксом сервера, в соответствие с требованиями ACL, отредактируйте ACL этой записи с помощью панели **Управление записями**. Выберите запись и нажмите кнопку **Редактировать ACL**. Если вы хотите добавить ACL без фильтров, то выберите вкладку и отметьте для ACL и владельцев переключатель, указывающий, применяются ли явные значения. Обязательно отметьте переключатели **Наследовать ACL** и **Наследовать владельца**.Если вы хотите добавить ACL с фильтрами, то выберите вкладку и добавьте для ACL и владельцев запись **cn=this** С ролью **access-id**. Переключатель **Накапливать ACL с фильтрами** должен быть не выбран, а переключатель **Наследовать владельца** - выбран. Подробная информация приведена в разделе “Управление списками управления доступом (ACL)” на стр. 197.

Первоначально создаваемый этим процессом объект **ibm-replicagroup** наследует ACL корневой записи копируемого поддерева. Такие ACL могут не отвечать требованиям средств управления доступом к хранящейся в каталоге информации о копировании.

## Создание главного сервера (копируемое поддерево)

**Примечание:** Для выполнения этой задачи сервер должен быть запущен.

Эта задача обозначает запись как корень независимо копируемого поддерева и создает атрибут **ibm-replicasubentry**, идентифицирующий данный сервер как единственный главный сервер для этого поддерева. Для создания копируемого поддерева необходимо обозначить поддерево, которое сервер должен копировать.

Разверните в области навигации категорию управления копированием и выберите опцию **Управление топологией**.

1. Нажмите кнопку **Добавить поддерево**.
2. Укажите DN корневой записи поддерева для копирования, либо нажмите кнопку **Обзор** и выберите корневую запись нужного поддерева.
3. URL переадресации главного сервера задается в формате URL LDAP, например:
   `ldap://<сервер>.<имя>.<организация>.com`

   **Примечание:** URL переадресации главного сервера можно не указывать. Он применяется только в следующих случаях:
   - Если сервер содержит (или будет содержать) какие-либо поддеревья, предназначенные только для чтения.
   - Если необходимо определить URL переадресации, возвращаемый для обновления какого либо поддерева, предназначенного только для чтения.
4. Нажмите кнопку **OK**.
5. Новый сервер будет показан в списке управления топологией под заголовком **Копируемые поддеревья**.

## Создание идентификационных данных

В области навигации Web-инструмента администрирования разверните категорию управления копированием и выберите опцию **Управление идентификационными данными**.

1. Выберите в списке поддеревьев расположение. Web-инструмент администрирования позволяет определять идентификационные данные в следующих расположениях:
   - В ветви **cn=replication,cn=localhost**. В этом случае идентификационные данные хранятся только на текущем сервере.

     **Примечание:** В большинстве случаев предпочитаемым является размещение идентификационных данных именно в ветви cn=replication,cn=localhost, поскольку при этом достигается более высокая степень защиты, чем при размещении в других поддеревьях. Однако, существует ряд ситуаций, в которых идентификационные данные, хранящиеся в cn=replication,cn=localhost, оказываются недоступными.

     Если вы пытаетесь добавить для сервера сервер-копию, например, serverA, и при этом подключены с помощью Web-инструмента администрирования к другому серверу (serverB), то в поле **Выбрать идентификационные данные** не будет показан вариант **cn=replication,cn=localhost**. Это связано с невозможностью чтения или обновления информации в ветви **cn=localhost** сервера serverA в то время, как вы подключены к серверу serverB.

     Опция cn=replication,cn=localhost доступна только в том случае, если сервер, на котором вы пытаетесь добавить копию, является тем же сервером, к которому вы подключены с помощью Web-инструмента администрирования.
   - В копируемом поддереве. В этом случае идентификационные данные копируются вместе с поддеревом. Идентификационные данные, размещенные в копируемом поддереве, помещаются в ветви **ibm-replicagroup=default** этого поддерева.

     **Примечание:** Если поддеревья отсутствуют, то для создания копируемого поддерева обратитесь к инструкциям из раздела “Создание главного сервера (копируемое поддерево)” на стр. 141.
2. Нажмите кнопку **Добавить**.
3. Введите имя создаваемого объекта идентификационных данных, например, **mycreds**; строка cn= будет заранее указана в поле ввода.
4. Выберите тип идентификации и нажмите кнопку **Далее**.
   - Если выбрана простая идентификация:
     a. Введите DN, которое сервер будет применять для подключения к копии, например, cn=any

b. Введите пароль, который сервер будет применять для подключения к копии, например, `secret`

c. Введите пароль еще раз для подтверждения.

d. Введите необязательное краткое описание идентификационных данных.

e. Нажмите кнопку **Готово**.

**Примечание:** Рекомендуется записать указанные в идентификационных данных DN и пароль. Этот пароль потребуется при создании соглашения о копировании.

- Если выбрана идентификация Kerberos:

  a. Введите DN подключения Kerberos.

  b. Введите имя таблицы ключей.

  c. Введите необязательное краткое описание идентификационных данных. Больше никакую информацию вводить не нужно. Дополнительная информация приведена в разделе “Включение идентификации Kerberos на сервере каталогов” на стр. 167.

  d. Нажмите кнопку **Готово**.

  На странице **Добавить разрешения Kerberos** содержатся необязательное DN подключения в форме `ibm-kn=пользователь@область` и необязательное имя файла таблицы ключей (обычно называемой файл ключей). Если указано DN подключения, то сервер будет идентифицировать сервер приемника на основе указанного имени субъекта. В противном случае будет использоваться имя службы сервера Kerberos (ldap/хост-имя@область). Если применяется файл ключей, то сервер получает разрешения для указанного субъекта с помощью этого файла. Если файл ключей не указан, то сервер использует файл ключей, указанный в конфигурации Kerberos. Если существует несколько поставщиков, то необходимо указать имя субъекта и файл ключей, применяемые всеми поставщиками.

  **На сервере, на котором вы создали идентификационные данные:**

  a. Разверните категорию **Управление каталогом** и выберите **Управление записями**.

  b. Выберите поддерево, в котором хранятся идентификационные данные, например, **cn=localhost**, и нажмите кнопку **Развернуть**.

  c. Выберите **cn=replication** и нажмите кнопку **Развернуть**.

  d. Выберите идентификационные данные kerberos (ibm-replicationCredentialsKerberos) и нажмите кнопку **Редактировать атрибуты**.

  e. Щелкните на вкладке **Прочие атрибуты**.

  f. Введите **replicaBindDN**, например, **ibm-kn=myprincipal@SOME.REALM**.

  g. Введите **replicaCredentials**. Это имя файла таблицы ключей для **myprincipal**.

  **Примечание:** Этот субъект и пароль должны совпадать с применяемыми при запуске **kinit** из командной строки.

  **На сервере-копии**

  a. В области навигации выберите опцию **Управление свойствами копирования**.

  b. В списке **Информация о поставщике** выберите поставщика или введите имя копируемого поддерева, для которого необходимо настроить идентификационные данные поставщика.

  c. Нажмите кнопку **Редактировать**.

  d. Введите bindDN для копирования. В нашем примере это **ibm-kn=myprincipal@SOME.REALM**.

  e. Введите и подтвердите **Пароль подключения для копирования**. Это пароль KDC, применяемый для **myprincipal**.

- Если вы выбрали идентификацию SSL с сертификатом, то в случае применения сертификата сервера указывать какую-либо дополнительную информацию не нужно. Если вы решили применять сертификат, отличный от сертификата сервера, то выполните следующие действия:

  a. Введите имя файла ключей.

  b. Введите пароль файла ключей.

c. Введите пароль файла ключей еще раз для подтверждения

d. Введите метку ключа.

e. Введите необязательное краткое описание.

f. Нажмите кнопку **Готово**.

Дополнительная информация приведена в разделе “Включение SSL и TLS на сервере каталогов” на стр. 165.

5. На сервере, на котором вы создали идентификационные данные, установите системное значение Разрешить сохранение информации защиты (QRETSVRSEC) равным 1 (сохранять данные). Поскольку идентификационные данные для копирования хранятся в контрольном списке, то при подключении к серверу-копии сервер сможет получать эти идентификационные данные из контрольного списка.

## Создание сервера-копии

**Примечание:** Для выполнения этой задачи сервер должен быть запущен.

Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление топологией**.

1. Выберите поддерево для копирования и нажмите кнопку **Показать топологию**.
2. Разверните список серверов-поставщиков, щелкнув на стрелке рядом с опцией **Топология копирования**.
3. Выберите сервер-поставщик и нажмите кнопку **Добавить копию**.

На вкладке **Сервер** в окне **Добавить копию** выполните следующие действия:

- Введите имя хоста и номер порта для создаваемой копии. По умолчанию для обычных соединений применяется порт 389, а для соединений SSL - порт 636. Это обязательные поля.
- Укажите, нужно ли применять соединения SSL.
- Введите имя копии или оставьте это поле пустым, чтобы применялось имя хоста.
- Введите ИД копии. Если сервер, на котором создается копия, работает, то для автоматического заполнения этого поля можно нажать кнопку **Получить ИД копии**. Если добавляемый сервер будет равноправным сервером или сервером пересылки, то это обязательное поле. Рекомендуется, чтобы все серверы были одного выпуска.
- Введите описание сервера-копии.

На вкладке **Дополнительно**:

1. Укажите идентификационные данные, применяемые сервером-копией для взаимодействия с главным сервером.

   **Примечание:** Web-инструмент администрирования позволяет определять идентификационные данные в следующих расположениях:

   - В ветви **cn=replication,cn=localhost**. В этом случае идентификационные данные хранятся только на том сервере, на котором они применяются.
   - В копируемом поддереве. В этом случае идентификационные данные копируются вместе с поддеревом. Идентификационные данные, размещенные в копируемом поддереве, помещаются в ветви **ibm-replicagroup=default** этого поддерева.

   Размещение идентификационных данных в cn=replication,cn=localhost считается более безопасным.

   a. Нажмите кнопку **Выбрать**.

   b. Выберите расположение идентификационных данных, которые должны применяться. Рекомендуется выбрать cn=replication,cn=localhost.

   c. Выберите опцию **Показать идентификационные данные**.

d. Разверните список идентификационных данных и выберите те из них, которые вы планируете применять.

e. Нажмите кнопку **OK**.

Дополнительная информация об идентификационных данных для соглашения о копировании приведена в разделе “Создание идентификационных данных” на стр. 142.

2. Выберите в списке расписание копирования или нажмите кнопку **Добавить** для создания нового расписания. См. раздел “Создание расписания копирования” на стр. 158.
3. В списке возможностей поставщика можно отменить выбор тех возможностей, которые не должны копироваться на сервер-потребитель.

   Если в вашей сети установлены серверы разных выпусков, то возможности, поддерживаемые серверами последних выпусков, будут недоступны на серверах более ранних выпусков. Некоторые возможности, например, ACL с фильтрами и стратегия управления паролями, используют операционные атрибуты, которые копируются вместе с другими изменениями. В большинстве случаев, если такие функции применяются, то они должны поддерживаться всеми серверами. Если какая-либо возможность поддерживается не всеми серверами, то применять ее не рекомендуется. Например, не следует применять на каждом сервере собственные ACL. Однако, в ряде случаев вы можете применять какую-либо возможность на тех серверах, на которых она поддерживается, и не копировать связанные с этой возможностью изменения на те серверы, на которых она не поддерживается. В таком случае вы можете пометить в списке те возможности, которые не должны копироваться.
4. Для создания сервера-копии нажмите кнопку **OK**.
5. Будет показано сообщение о необходимости выполнить дополнительные действия. Нажмите кнопку **OK**.

**Примечание:** Если вы добавляете новые серверы в качестве дополнительных серверов-копий или создаете сложную топологию, то не выполняйте инструкции из разделов “Копирование данных на сервер-копию” и “Добавление на сервер-копию информации о поставщике” на стр. 146 до тех пор, пока вы не закончите определение топологии на главном сервере. Если вы создали *masterfile.ldif* после создания топологии, то он будет содержать записи каталога главного сервера, а также полную копию соглашений топологии. После загрузки этого файла на все серверы каждый из серверов будет содержать ту же информацию.

## Копирование данных на сервер-копию

После создания сервера-копии необходимо экспортировать на него сведения о топологии с главного сервера.

1. Создайте на главном сервере файл LDIF для данных. Для копирования всех данных, хранящихся на главном сервере, выполните следующие действия:
   a. В Навигаторе откройте **Сеть**.
   b. Откройте **Серверы**.
   c. Выберите **TCP/IP**.
   d. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Сервис**, а затем **Экспортировать файл**.
   e. Укажите имя файла вывода LDIF (например, `masterfile.ldif`), при желании укажите экспортируемое поддерево (например, `subtreeDN`) и нажмите **OK**.
2. В системе, в которой вы создаете сервер-копию, выполните следующие действия:
   a. Убедитесь, что копируемые суффиксы определены в конфигурации сервера-копии.
   b. Остановите сервер-копию.
   c. Скопируйте файл LDIF на сервер-копию и выполните следующие действия:
      1) В Навигаторе откройте **Сеть**.
      2) Откройте **Серверы**.
      3) Выберите **TCP/IP**.
      4) Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Сервис**, а затем **Импортировать файл**.
      5) Укажите имя исходного файла LDIF (например, `masterfile.ldif`), при необходимости укажите на необходимость копирования данных, и нажмите **OK**.

На сервер-копию будут загружены соглашения о копировании, расписания, идентификационные данные (если они хранились в копируемом поддереве), а также данные записей.

d. Запустите сервер.

## Добавление на сервер-копию информации о поставщике

Теперь необходимо изменить конфигурацию сервера-копии, указав, кто может копировать на этот сервер изменения, а также добавьте переадресацию на главный сервер.

В системе, в которой вы создаете сервер-копию, выполните следующие действия:

1. В области навигации разверните категорию **Управление копированием** и выберите опцию **Управление свойствами копирования**.

   **Примечание:** Для изменения параметров на странице **Управление свойствами копирования** вы должны войти в систему Web-инструмента администрирования как спроецированный пользователь OS/400 с правами доступа *ALLOBJ и *IOSYSCFG.

2. Нажмите кнопку **Добавить**.
3. В списке **Скопированное поддерево** выберите поставщика или введите имя копируемого поддерева, для которого необходимо настроить идентификационные данные поставщика. При изменении идентификационных данных поставщика это поле изменять нельзя.
4. Введите bindDN для копирования. В нашем примере это cn=any.

   **Примечание:** В зависимости от ситуации, вы можете воспользоваться любым из следующих вариантов.

   - Настройте DN подключения (и пароль) для копирования, а также адрес переадресации для всех копируемых на сервер поддеревьев с помощью опции 'идентификационные данные и адрес переадресации по умолчанию'. Такой вариант можно использовать в том случае, если все поддеревья копируются с одного поставщика.
   - Независимо укажите для каждого копируемого поддерева собственное значение DN и пароля. Для этого необходимо добавить для каждого поддерева информацию о поставщике. Этот вариант можно использовать в том случае, если каждому поддереву соответствует свой поставщик (т.е. для каждого поддерева существует собственный главный сервер).

5. В зависимости от типа идентификационных данных, введите и подтвердите пароль. (Вы записали его ранее.)
   - **Простое подключение** - Укажите DN и пароль.
   - **Kerberos** - Если в идентификационных данных на поставщике не указан субъект и пароль, т.е. должен применяться служебный субъект сервера, то укажите DN подключения ibm-kn=ldap/<*сервер@область*>. Если же задано имя субъекта, например<*myprincipal@myrealm*>, то используйте в качестве DN это значение. В обоих случаях пароль не требуется.
   - **Внешнее подключение SSL** - Укажите DN субъекта для сертификата. Пароль не требуется.

   См. раздел "Создание идентификационных данных" на стр. 142.

6. Нажмите кнопку **OK**.
7. Для того чтобы изменения вступили в силу, перезапустите сервер-копию.

Дополнительная информация приведена в разделе "Изменение свойств копирования" на стр. 156.

Сервер-копия находится в приостановленном состоянии и копирование не выполняется. После завершения настройки топологии копирования выберите опцию **Управление очередями**, затем выберите сервер-копию и запустите копирование с помощью команды **Приостановить/Возобновить**. Подробная информация приведена в разделе "Управление очередями" на стр. 159. Теперь сервер-копия будет получать обновления с главного сервера.

# Создание топологии с главным сервером, сервером пересылки и сервером-копией

Для определения топологии с главным сервером, сервером пересылки и сервером-копией выполните следующие действия:

1. Создайте главный сервер и сервер-копию. См. раздел “Создание топологии с главными серверами и серверами-копиями” на стр. 141.
2. Создайте новый сервер-копию для исходной копии. См. раздел “Создание нового сервера-копии”.
3. Скопируйте данные на серверы-копии. См. раздел “Копирование данных на сервер-копию” на стр. 145.

## Создание нового сервера-копии

Если вы настроили топологию копирования (см. раздел “Создание главного сервера (копируемое поддерево)” на стр. 141) с главным сервером (server1) и сервером-копией (server2), то вы можете изменить роль сервера server2, сделав его сервером пересылки. Для этого необходимо создать новый сервер-копию (server3), который будет подчинен серверу server2.

1. Подключитесь к Web-инструменту администрирования главного сервера (server1).
2. Разверните в области навигации категорию управления копированием и выберите опцию **Управление топологией**.
3. Выберите поддерево для копирования и нажмите кнопку **Показать топологию**.
4. Разверните список серверов-поставщиков, щелкнув на стрелке рядом с опцией **Топология копирования**.
5. Разверните список серверов, щелкнув на стрелке рядом с опцией **server1**.
6. Выберите server2 и нажмите кнопку **Добавить копию**.
7. На вкладке **Сервер** в окне **Добавить копию** выполните следующие действия:
   - Введите имя хоста и номер порта для создаваемой копии (server3). По умолчанию для обычных соединений применяется порт 389, а для соединений SSL - порт 636. Это обязательные поля.
   - Укажите, нужно ли применять соединения SSL.
   - Введите имя копии или оставьте это поле пустым, чтобы применялось имя хоста.
   - Введите ИД копии. Если сервер, на котором создается копия, работает, то для автоматического заполнения этого поля можно нажать кнопку **Получить ИД копии**. Если добавляемый сервер будет равноправным сервером или сервером пересылки, то это обязательное поле. Рекомендуется, чтобы все серверы были одного выпуска.
   - Введите описание сервера-копии.

   На вкладке **Дополнительно**:

   a. Укажите идентификационные данные, применяемые сервером-копией для взаимодействия с главным сервером.

      **Примечание:** Web-инструмент администрирования позволяет определять идентификационные данные в следующих двух расположениях:
      - В ветви **cn=replication,cn=localhost**. В этом случае идентификационные данные хранятся только на том сервере, на котором они применяются.
      - В копируемом поддереве. В этом случае идентификационные данные копируются вместе с поддеревом.

      Размещение идентификационных данных в cn=replication,cn=localhost считается более безопасным. Идентификационные данные, размещенные в копируемом поддереве, помещаются в ветви **ibm-replicagroup=default** этого поддерева.

      1) Нажмите кнопку **Выбрать**.
      2) Выберите расположение идентификационных данных, которые должны применяться. Рекомендуется выбрать cn=replication,cn=localhost.
      3) Выберите опцию **Показать идентификационные данные**.

4) Разверните список идентификационных данных и выберите те из них, которые вы планируете применять.

5) Нажмите кнопку **OK**.

Дополнительная информация об идентификационных данных для соглашения о копировании приведена в разделе “Создание идентификационных данных” на стр. 142.

b. Выберите в списке расписание копирования или нажмите кнопку **Добавить** для создания нового расписания. См. раздел “Создание расписания копирования” на стр. 158.

c. В списке возможностей поставщика можно отменить выбор тех возможностей, которые не должны копироваться на сервер-потребитель.

Если в вашей сети установлены серверы разных выпусков, то возможности, поддерживаемые серверами последних выпусков, будут недоступны на серверах более ранних выпусков. Некоторые возможности, например, ACL с фильтрами и стратегия управления паролями, используют операционные атрибуты, которые копируются вместе с другими изменениями. В большинстве случаев, если такие функции применяются, то они должны поддерживаться всеми серверами. Если какая-либо возможность поддерживается не всеми серверами, то применять ее не рекомендуется. Например, не следует применять на каждом сервере собственные ACL. Однако, в ряде случаев вы можете применять какую-либо возможность на тех серверах, на которых она поддерживается, и не копировать связанные с этой возможностью изменения на те серверы, на которых она не поддерживается. В таком случае вы можете пометить в списке те возможности, которые не должны копироваться.

d. Для создания сервера-копии нажмите кнопку **OK**.

8. Скопируйте данные с сервера server2 на новый сервер-копию server3. Необходимые инструкции приведены в разделе “Копирование данных на сервер-копию” на стр. 145.
9. Добавьте на server3 соглашение поставщика, которое делает server2 поставщиком для server3, а сервер server3 - потребителем для server2. Необходимые инструкции приведены в разделе “Добавление на сервер-копию информации о поставщике” на стр. 146.

Роли серверов обозначены значками в Web-инструменте администрирования. В итоге вы создали следующую топологию:

- server1 (главный сервер)
  - server2 (сервер пересылки)
    - server3 (сервер-копия)

## Обзор процедуры создания сложной топологии копирования

Этот обзор поможет вам настроить среду со сложной топологией копирования.

1. Запустите все равноправные серверы или серверы, которые будут применяться в качестве копий. Это необходимо для того, чтобы Web-инструмент администрирования мог собрать информацию о всех серверах.
2. Запустите ’первый’ главный сервер и настройте его в качестве главного сервера контекста.
3. Загрузите на ’первый’ главный сервер данные копируемого поддерева, если они еще не загружены.
4. Выберите поддерево для копирования.
5. Добавьте все серверы, которые будут применяться в качестве равноправных главных серверов, в качестве копий ’первого’ главного сервера.
6. Добавьте все остальные серверы-копии.
7. Сделайте остальные серверы равноправными главными серверами.
8. Добавьте на каждый из равноправных главных серверов соглашения о копировании для их серверов-копий.

**Примечание:** Если идентификационные данные будут храниться в **cn=replication,cn=localhost**, то после перезапуска необходимо создать идентификационные данные на каждом сервере. Равноправные серверы смогут выполнять копирование только после создания объектов идентификационных данных.

9. Добавьте на каждый из равноправных главных серверов соглашения о копировании для других равноправных главных серверов. На 'первом' главном сервере эта информация уже есть.
10. Стабилизируйте копируемое поддерево. Тем самым вы запретите внесение обновлений в данные на то время, пока они будут копироваться на другие серверы.
11. С помощью средств управления очередями выберите для каждой очереди опцию пропуска всех.
12. На 'первом' главном сервере экспортируйте данные копируемого поддерева.
13. Отключите стабилизацию поддерева.
14. Остановите серверы-копии и импортируйте на каждый сервер-копию и на каждый равноправный сервер данные копируемого поддерева. Перезапустите серверы.
15. С помощью свойств управления копированием задайте на каждом сервере-копии и на каждом равноправном сервере идентификационные данные, которые должны применяться поставщиками.

## Создание сложной топологии с копированием на равноправные серверы

Топология с копированием на равноправные серверы - это топология, в которой применяется несколько главных серверов. Однако, в отличие от обычной среды с несколькими главными серверами, между равноправными серверами не выполняется устранение конфликтов. Серверы LDAP принимают обновления от равноправных серверов и обновляют свои копии данных. При этом не учитывается порядок получения обновлений и не предусмотрены никакие средства предотвращения многократного применения обновлений.

Для создания дополнительных равноправных серверов необходимо сначала добавить сервер в качестве предназначенного только для чтения сервера-копии уже существующих главных серверов (см. раздел "Создание сервера-копии" на стр. 144), инициализировать данные каталога, а затем сделать этот сервер главным сервером (см. раздел "Перемещение сервера или изменение его роли" на стр. 154).

Первоначально создаваемый этим процессом объект **ibm-replicagroup** наследует ACL корневой записи копируемого поддерева. Такие ACL могут не отвечать требованиям средств управления доступом к хранящейся в каталоге информации о копировании.

Для успешного добавления поддерева DN добавляемой записи должен иметь правильно настроенные ACL (если он не является суффиксом сервера).

**ACL без фильтров:**

- ownersource : <*DN записи*>
- ownerpropagate : TRUE
- aclsource : <*DN записи*>
- aclpropagate: TRUE

**ACL с фильтрами:**

- ownersource : <*DN записи*>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <*любое значение*>

Для того чтобы задать ACL для информации о копировании, связанной с только что созданным копируемым поддеревом (см. раздел "Редактирование списков управления доступом" на стр. 156), воспользуйтесь функцией **Редактировать ACL** в Web-инструменте администрирования.

Сервер-копия находится в приостановленном состоянии и копирование не выполняется. После завершения настройки топологии копирования выберите опцию **Управление очередями**, затем выберите сервер-копию и запустите копирование с помощью команды **Приостановить/Возобновить**. Подробная информация приведена в разделе “Управление очередями” на стр. 159. Теперь сервер-копия будет получать обновления с главного сервера.

Среда копирования с равноправными серверами может применяться только в том случае, если заранее известно, как именно будет обновляться каталог. Обновления отдельных объектов каталога должны выполняться только на одном сервере. Это необходимо для того, чтобы избежать ситуации, когда один сервер удаляет объект, а затем другой сервер пытается изменить этот объект. В этом случае равноправный сервер может получить команду удаления, за которой будет следовать команда изменения, что приведет к возникновению конфликта.

Для определения топологии с двумя равноправными серверами, двумя серверами пересылки и четырьмя серверами-копиями выполните следующие действия:

1. Создайте главный сервер и сервер-копию. См. раздел “Создание топологии с главными серверами и серверами-копиями” на стр. 141.
2. Создайте для главного сервера два дополнительных сервера-копии. См. раздел “Создание сервера-копии” на стр. 144.
3. Для каждого из только что созданных серверов-копий создайте еще по две копии.
4. Сделайте первоначальные серверы-копии главными серверами. См. раздел “Изменение роли сервера на равноправный”.

   **Примечание:** Сервер, который вы делаете главным сервером, должен быть конечной копией, не имеющей подчиненных копий.
5. Скопируйте данные с главного сервера на новый главный сервер и на серверы-копии. См. раздел “Копирование данных на сервер-копию” на стр. 145.

## Изменение роли сервера на равноправный

В топологии с серверами пересылки, описанной в разделе “Создание топологии с главным сервером, сервером пересылки и сервером-копией” на стр. 147, вы можете сделать сервер равноправным. В этом примере вы должны сделать сервер-копию (server3) сервером, равноправным с главным сервером (server1).

1. Подключитесь к Web-инструменту администрирования главного сервера (server1).
2. Разверните в области навигации категорию управления копированием и выберите опцию **Управление топологией**.
3. Выберите поддерево для копирования и нажмите кнопку **Показать топологию**.
4. Разверните список серверов, щелкнув на стрелке рядом с опцией **Топология копирования**.
5. Разверните список серверов, щелкнув на стрелке рядом с опцией **server1**.
6. Разверните список серверов, щелкнув на стрелке рядом с опцией **server2**.
7. Выберите **server1** и нажмите кнопку **Добавить копию**. Создайте server4. См. раздел “Создание сервера-копии” на стр. 144. С помощью аналогичной процедуры создайте server5. Роли серверов обозначены значками в Web-инструменте администрирования. В итоге вы создали следующую топологию:
   - server1 (главный сервер)
     - server2 (сервер пересылки)
       - server3 (сервер-копия)
     - server4 (сервер-копия)
     - server5 (сервер-копия)
8. Выберите **server2** и нажмите кнопку **Добавить копию**, чтобы добавить сервер server6.
9. Выберите **server4** и нажмите кнопку **Добавить копию**, чтобы добавить сервер server7. С помощью аналогичной процедуры создайте server8. В итоге вы создали следующую топологию:

- server1 (главный сервер)
  - server2 (сервер пересылки)
    - server3 (сервер-копия)
    - server6 (сервер-копия)
  - server4 (сервер пересылки)
    - server7 (сервер-копия)
    - server8 (сервер-копия)
  - server5 (сервер-копия)

10. Выберите **server5** и нажмите кнопку **Переместить**.

    **Примечание:** Перемещаемый сервер должен быть конечной копией, не имеющей подчиненных копий.

11. Для того чтобы сделать сервер-копию главным сервером, выберите опцию **Топология копирования**. Нажмите кнопку **Переместить**.
12. Появится окно **Создать дополнительные соглашения поставщиков**. Для копирования на равноправные серверы необходимо, чтобы каждый главный сервер был поставщиком и потребителем всех остальных главных серверов топологии, а также для всех копий первого уровня, т.е. server2 и server4. Server5 уже является потребителем server1. Теперь его необходимо сделать поставщиком серверов server1, server2 и server4. Убедитесь, что отмечены переключатели соглашений поставщиков для следующих серверов:

*Таблица 5.*

| | Поставщик | Потребитель |
|---|---|---|
| ✓ | server5 | server1 |
| ✓ | server5 | server2 |
| ✓ | server5 | server4 |

Нажмите кнопку **Продолжить**.

**Примечание:** В некоторых случаях появляется окно с запросом идентификационных данных, которые находятся в поддереве, отличном от cn=replication,cn=localhost. В этом случае необходимо указать соответствующий объект, находящийся в поддереве, отличном от cn=replication,cn=localhost. Выберите идентификационные данные из существующих наборов или создайте новые идентификационные данные. См. раздел “Создание идентификационных данных” на стр. 142.

.

13. Нажмите кнопку **OK**. В итоге вы создали следующую топологию:
    - server1 (главный сервер)
      - server2 (сервер пересылки)
        - server3 (сервер-копия)
        - server6 (сервер-копия)
      - server4 (сервер пересылки)
        - server7 (сервер-копия)
        - server8 (сервер-копия)
      - server5 (главный сервер)
    - server5 (главный сервер)
      - server1 (главный сервер)
      - server2 (сервер пересылки)
      - server4 (сервер пересылки)
14. Скопируйте данные с сервера server1 на все остальные серверы. Необходимые инструкции приведены в разделе “Копирование данных на сервер-копию” на стр. 145.

## Настройка топологии шлюза

Прежде, чем начинать настройку топологии копирования, создайте резервную копию файла ibmslapd.conf. Эта копия может пригодиться для восстановления первоначальной конфигурации в случае неполадок с копированием.

Для настройки шлюза посредством составной топологии с копированием равноправного сервера с помощью процедуры, описанной в разделе “Изменение роли сервера на равноправный” на стр. 150 выполните следующие действия:

- Для создания узла копирования 1 преобразуйте существующий равноправный сервер (peer 1) в сервер-шлюз.
- Создайте новый сервер-шлюз для узла копирования 2 и соглашений с равноправным сервером 1.
- Создайте топологию для узла копирования 2 (в данном примере не рассматривается).
- Скопируйте данные с главного сервера во все системы топологии.

**Преобразование существующего равноправного сервера в шлюз**

1. С помощью Web-инструмента администрирования подключитесь к главному серверу (server1).
2. Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление топологией**.
3. Выберите поддерево для копирования и нажмите кнопку **Показать топологию**.
4. Разверните список серверов, щелкнув на стрелке рядом с опцией **Топология копирования**.
5. Для преобразования существующего сервера в шлюз выберите **server1** или равноправный для него **server5**. В данном примере используется **server1**.
6. Нажмите **Изменить сервер**.
7. Сейчас включен переключатель **Главный сервер**. Выберите **Сервер-шлюз**.
8. Нажмите кнопку **OK**.

**Примечание:** Если сервер, который вы преобразовываете в шлюз, не является главным сервером, он должен быть конечным сервером-копией, то есть таким, у которого нет подчиненных объектов. Тогда этот сервер можно будет преобразовать в главный, а затем - в шлюз.

**Создание сервера-шлюза и копирование данных с главного сервера во все системы топологии**

1. Выберите **server1** и нажмите **Добавить сервер-копию**.
2. Создайте новый сервер-копию **server9**. Дополнительная информация о создании серверов-копий, добавлении разрешений, а также о серверах-поставщиках приведена в разделе “Создание сервера-копии” на стр. 144.
3. Выберите **server9** и нажмите **Переместить**.
4. Для того чтобы сделать сервер-копию главным сервером, выберите опцию **Топология копирования**. Нажмите кнопку **Переместить**.
5. Появится окно **Создать дополнительные соглашения поставщиков**. Убедитесь, что в этом окне включены переключатели соглашений поставщиков только для сервера server1.

| | Поставщик | Потребитель |
|---|---|---|
| ✓ | server9 | server1 |
| | server9 | server2 |
| | server9 | server4 |
| | server9 | server5 |

Нажмите кнопку **Продолжить**.

**Примечание:** В некоторых случаях появляется окно **Выбрать разрешение** с запросом идентификационных данных, которые находятся в объекте, отличном от cn=replication,cn=localhost. В этом случае необходимо указать соответствующий объект, находящийся в поддереве, отличном от cn=replication,cn=localhost. Выберите идентификационные данные из существующих наборов или создайте новые идентификационные данные. См. раздел “Создание идентификационных данных” на стр. 142.

6. Нажмите кнопку **OK**.
7. Выберите **server9** и нажмите **Изменить сервер**.
8. Сейчас включен переключатель **Главный сервер**. Выберите **Сервер-шлюз**.
9. Нажмите кнопку **OK**. Роли серверов обозначены значками в Web-инструменте администрирования. В итоге вы создали следующую топологию:
   - server1 (главный шлюз для узла копирования 1)
     - server2 (сервер пересылки)
       - server3 (сервер-копия)
       - server6 (сервер-копия)
     - server4 (сервер пересылки)
       - server7 (сервер-копия)
       - server8 (сервер-копия)
     - server5 (главный сервер)
     - server9 (главный шлюз для узла копирования 2)
   - server5 (главный сервер)
     - server1 (главный сервер)
     - server2 (сервер пересылки)
     - server4 (сервер пересылки)
   - server9 (главный шлюз)
     - server1 (главный шлюз)
10. Добавьте серверы-копии к **server9** для создания топологии для узла копирования 2.
11. Повторите эту процедуру для создания дополнительных узлов копирования. Помните, что на один узел копирования должен приходиться только один сервер-шлюз.
12. По окончании создания топологии скопируйте данные с сервера server1 на все новые серверы всех узлов копирования и добавьте на все новые серверы информацию о поставщиках. Дополнительные сведения приведены в разделах “Копирование данных на сервер-копию” на стр. 145 и “Добавление на сервер-копию информации о поставщике” на стр. 146.

## Управление топологиями

Варианты топологии зависят от копируемых поддеревьев.

## Просмотр топологии

**Примечание:** Для выполнения этой задачи сервер должен быть запущен.

Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление топологией**.

1. Выберите поддерево для просмотра и нажмите кнопку **Показать топологию**.

В списке Топология копирования будет представлена текущая топология. Для развертывания элемента топологии щелкните на синем треугольнике. С помощью этого списка вы можете выполнить следующие операции:

- Добавить копию
- Изменить информацию о существующей копии
- Переключить копию на другого поставщика или сделать сервер-копию главным сервером
- Удаление копии

## Добавление копии

См. раздел “Создание сервера-копии” на стр. 144.

## Редактирование соглашения

Вы можете изменить следующую информацию о сервере-копии:

На вкладке **Сервер** можно изменить только следующие значения

- Имя хоста
- Порт
- Поддержка SSL
- Описание

На вкладке **Дополнительно** можно изменить следующие значения:

- Идентификационные данные - см. раздел “Создание идентификационных данных” на стр. 142.
- Расписание копирования - см. раздел “Создание расписания копирования” на стр. 158.
- Список возможностей, копируемых на сервер-потребитель. В списке возможностей поставщика можно отменить выбор тех возможностей, которые не должны копироваться на сервер-потребитель.
- После завершения ввода нажмите **OK**.

## Перемещение сервера или изменение его роли

1. Выберите требуемый сервер и нажмите кнопку **Переместить**.
2. Выберите сервер, на который вы хотите переместить копию, либо выберите опцию **Управление топологией**, позволяющую сделать сервер-копию главным сервером. Нажмите кнопку **Переместить**.
3. В некоторых случаях появляется окно с запросом идентификационных данных, которые находятся в поддереве, отличном от cn=replication,cn=localhost. В этом случае необходимо указать соответствующий объект, находящийся в поддереве, отличном от cn=replication,cn=localhost. Выберите идентификационные данные из существующих наборов или создайте новые идентификационные данные. См. раздел “Создание идентификационных данных” на стр. 142.
4. Появится окно **Создать дополнительные соглашения поставщиков**. Выберите соглашения поставщиков, соответствующие роли сервера. Например, если вы хотите сделать сервер-копию равноправным сервером, то необходимо создать соглашения поставщиков для связи со всеми остальными равноправными серверами, а также с их копиями первого уровня. Эти соглашения позволят новому равноправному серверу выполнять функции поставщика для других серверов и их копий. Существующие соглашения поставщиков для копирования данных с других сервер на сервер с измененной ролью по-прежнему будут действовать и создавать их заново не нужно.
5. Нажмите кнопку **OK**.

Перемещение сервера будет отражено в дереве топологии.

Дополнительная информация приведена в разделе “Создание сложной топологии с копированием на равноправные серверы” на стр. 149.

## Изменение роли главного сервера на сервер-копию

Для того чтобы сделать главный сервер сервером-копией, выполните следующие действия:

1. Подключитесь к Web-инструменту администрирования того сервера, роль которого необходимо изменить.
2. Выберите опцию **Управление топологией**.
3. Выберите поддерево и нажмите кнопку **Показать топологию**.
4. Удалите все соглашения для перемещаемого сервера.
5. Выберите сервер и нажмите кнопку **Переместить**.
6. Выберите сервер, которому будет подчинен перемещаемый сервер, и нажмите кнопку **Переместить**.
7. Как и при создании нового сервера-копии, создайте новые соглашения поставщиков для копирования данных между сервером-копией и его поставщиком. Инструкции по выполнению этой задачи приведены в разделе “Создание сервера-копии” на стр. 144.

## Копирование поддерева

**Примечание:** Для выполнения этой задачи сервер должен быть запущен.

Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление топологией**.

- Нажмите кнопку **Добавить поддерево**.
- Укажите DN поддерева для копирования, либо нажмите кнопку **Обзор** и выберите корневую запись нужного поддерева.
- Введите URL переадресации для главного сервера. URL должен быть задан в формате LDAP, например:
  `ldap://<сервер>.<имя>.<организация>.com`
- Нажмите кнопку **OK**.
- Новый сервер будет показан в списке управления топологией под заголовком **Копируемые поддеревья**.

## Редактирование поддерева

Эта опция позволяет изменить URL главного сервера, которому передает сведения об обновлениях данное поддерево и все его копии. Это необходимо сделать, например, в случае изменения номера порта или имени хоста главного сервера.

1. Выберите поддерево для редактирования.
2. Нажмите кнопку **Редактировать поддерево**.
3. Введите URL переадресации для главного сервера. URL должен быть задан в формате LDAP, например:
   `ldap://<новый-сервер>.<имя>.<организация>.com`

В зависимости от роли сервера по отношению к данному поддереву (главный сервер, сервер-копия или сервер пересылки), будут показаны разные наборы кнопок и меток.

- Если сервер выполняет для поддерева роль копии, то будет показано сообщение о том, что сервер выполняет функции сервера-копии или сервера пересылки. Кроме того появится кнопка **Сделать сервер главным**.Если нажать эту кнопку, то сервер, к которому подключен Web-инструмент администрирования, станет главным сервером.
- Если поддерево настроено для копирования только путем добавления вспомогательного класса (группа по умолчанию и подзапись отсутствуют), то появится сообщение **Это поддерево не копируется** и кнопка **Скопировать поддерево**. Если нажать эту кнопку, то на сервер, к которому подключен Web-инструмент администрирования, будет добавлена группа по умолчанию и подзапись, а сам сервер станет главным сервером.

- Если подзаписи главного сервера не найдены, то будет показано сообщение **Главный сервер для этого поддерева не определен** и кнопка **Сделать сервер главным**. Если нажать эту кнопку, то на сервер, к которому подключен Web-инструмент администрирования, будет добавлена отсутствующая подзапись, а сам сервер станет главным сервером.

### Удаление поддерева

1. Выберите поддерево для удаления.
2. Нажмите кнопку **Удалить поддерево**.
3. При появлении просьбы подтвердить операцию нажмите **OK**.

Поддерево будет удалено из списка **Копируемое поддерево**.

**Примечание:** Эта операция будет успешно выполнена лишь в том случае, если запись ibm-replicaGroup=default пуста.

### Стабилизация поддерева

Эта функция полезна при обслуживании и изменении топологии. Она позволяет минимизировать число выполняемых на сервере обновлений. Стабилизированный сервер не принимает запросы клиентов. Он принимает только запросы администратора, отправляемые с помощью инструмента управления.

Это булевская функция.

1. Для стабилизации поддерева нажмите кнопку **Стабилизировать/Отменить стабилизацию**.
2. При появлении просьбы подтвердить операцию нажмите **OK**.
3. Для отмены стабилизации поддерева нажмите кнопку **Стабилизировать/Отменить стабилизацию**.
4. При появлении просьбы подтвердить операцию нажмите **OK**.

### Редактирование списков управления доступом

Информация о копировании (подзаписи копий, соглашения о копировании, расписания, а также, в ряде случаев, идентификационные данные) хранится в особом объекте **ibm-replicagroup=default**. Объект ibm-replicagroup находится непосредственно под корневой записью копируемого поддерева. По умолчанию это поддерево наследует ACL корневой записи поддерева. ACL может не отвечать требованиям, предъявляемым к настройке средств управления доступом к копируемой информации.

Необходимые права доступа:

- Управление копированием - у вас должны быть права доступа на запись к объекту ibm-replicagroup=default (либо вы должны быть администратором или владельцем этого объекта.
- Управление каскадным копированием - у вас должны быть права доступа на запись к объекту ibm-replicagroup=default (либо вы должны быть администратором или владельцем этого объекта.
- Управление очередью - у вас должны быть права доступа на запись соглашения о копировании.

Для просмотра свойств ACL с помощью Web-инструмента администрирования и работы с ACL ознакомьтесь с разделом “Управление списками управления доступом (ACL)” на стр. 197.

Дополнительная информация приведена в разделе “Списки управления доступом” на стр. 60.

## Изменение свойств копирования

Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление свойствами копирования**. Для изменения параметров на странице **Управление свойствами копирования** вы должны войти в систему Web-инструмента администрирования как спроецированный пользователь с правами доступа *ALLOBJ и *IOSYSCFG.

Вы можете выполнять следующие операции:

- Изменять максимальное число ожидающих изменений, возвращаемых очередями состояния копирования. Значение по умолчанию - 200.
- Добавлять, изменять и удалять информацию о поставщиках.

**Примечание:** DN поставщика может представлять собой DN спроецированного пользовательского профайла i5/OS. У спроецированного профайла i5/OS не должно быть прав доступа администратора LDAP. Пользователь не должен иметь специальных прав доступа *ALLOBJ и *IOSYSCFG и не должен иметь прав доступа администратора каталога, предоставленных с помощью ИД приложения администратора сервера каталогов.

Дополнительная информация приведена в следующих разделах:

- “Добавление информации о поставщике”
- “Редактирование информации о поставщике”
- “Удаление информации о поставщике” на стр. 158

## Добавление информации о поставщике

1. Нажмите кнопку **Добавить**.
2. В списке выберите поставщика или введите имя копируемого поддерева, которое необходимо добавить в качестве поставщика.
3. Введите DN подключения для копирования.

   **Примечание:** В зависимости от ситуации, вы можете воспользоваться любым из следующих вариантов.
   - Настройте DN подключения (и пароль) для копирования, а также адрес переадресации для всех копируемых на сервер поддеревьев с помощью опции ’идентификационные данные и адрес переадресации по умолчанию’. Такой вариант можно использовать в том случае, если все поддеревья копируются с одного поставщика.
   - Независимо укажите для каждого копируемого поддерева собственное значение DN и пароля. Для этого необходимо добавить для каждого поддерева информацию о поставщике. Этот вариант можно использовать в том случае, если каждому поддереву соответствует свой поставщик (т.е. для каждого поддерева существует собственный главный сервер).
4. В зависимости от типа идентификационных данных, введите и подтвердите пароль. (Вы записали его ранее.)
   - **Простое подключение** - Укажите DN и пароль.
   - **Kerberos** - укажите псевдо DN в формате ’ibm-kn=служебное-имя-LDAP@область’ без пароля.
   - **Внешнее подключение SSL** - Укажите DN субъекта для сертификата. Пароль не требуется.

   См. раздел “Создание идентификационных данных” на стр. 142.
5. Нажмите кнопку **OK**.

Поддерево поставщика будет добавлено в список.

## Редактирование информации о поставщике

1. Выберите поддерево поставщика для редактирования.
2. Нажмите кнопку **Редактировать**.
3. Если вы редактируете **Адрес пересылки и идентификационные данные по умолчанию**, применяемые для создания записи cn=Master Server в cn=configuration, то в поле **URL LDAP поставщика по умолчанию** укажите URL сервера, с которого клиент должен получать обновления. Это должен быть допустимый URL LDAP (начинающийся с символов ldap://). В противном случае перейдите к шагу 4.
4. Укажите DN для подключения.
5. Введите и подтвердите пароль.
6. Нажмите кнопку **OK**.

### Удаление информации о поставщике

1. Выберите поддерево поставщика для удаления.
2. Нажмите кнопку **Удалить**.
3. При появлении просьбы подтвердить операцию нажмите **OK**.

Поддерево будет удалено из списка информации о поставщиках.

## Создание расписания копирования

При необходимости вы можете определить расписание копирования, позволяющее запланировать копирование на определенные интервалы времени, либо запрещающее копирование в указанные интервалы времени. Если расписание не применяется, то сервер будет планировать копирование по мере внесения изменений. Это эквивалентно указанию расписания с немедленным копированием с 00:00 каждый день.

Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление расписанием**.

На вкладке **Еженедельные расписания** выберите поддерево, для которого необходимо создать расписание, а затем нажмите кнопку **Показать расписания**. Если существуют какие-либо расписания, то они будут показаны в окне **Еженедельные расписания**. Для создания или добавления нового расписания:

1. Нажмите кнопку **Добавить**.
2. Введите имя расписания. Например, **schedule1**.
3. Для каждого дня с понедельника по воскресенье ежедневное расписание определено как **Нет**. Это значит, что события копирования не запланированы. Последнее событие копирования, если оно определено, по-прежнему действует. Поскольку это новая копия, то предыдущих событий копирования нет и по умолчанию применяется немедленное копирование.
4. Вы можете выбрать день и нажать кнопку **Добавить ежедневное расписание** для планирования копирования на этот день. После создания ежедневного расписания это расписание становится расписанием по умолчанию для всех дней недели. Вы можете:
   - Сохранить ежедневное расписание по умолчанию для каждого дня или выбрать любой день и снова указать для него опцию планирования копирования Нет. При этом необходимо помнить, что последнее событие копирования продолжает действовать для дня, на который не запланированы никакие события копирования.
   - Изменить ежедневное расписание копирования, выбрав день и нажав кнопку **Изменить ежедневное расписание**. Помните, что изменения, внесенные в ежедневное расписание, влияют на все дни, использующие данное расписание, а не только на выбранный день.
   - Создать другое ежедневное расписание, выбрав день и нажав кнопку **Добавить ежедневное расписание**. После создания расписание добавляется в список **Ежедневное расписание**. Необходимо выбрать расписание для каждого дня, когда оно должно применяться.

   Дополнительная информация о настройке ежедневных расписаний приведена в разделе “Создание ежедневного расписания”.
5. После завершения ввода нажмите **OK**.

### Создание ежедневного расписания

Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление расписанием**.

На вкладке **Ежедневное расписание** выберите поддерево, для которого необходимо создать расписание, а затем нажмите кнопку **Показать расписания**. Если существуют какие-либо расписания, то они будут показаны в окне **Ежедневные расписания**.Для создания или добавления нового расписания:

1. Нажмите кнопку **Добавить**.
2. Введите имя расписания. Например, **monday1**.
3. Выберите опцию часового пояса (UTC или локальное время).

4. Выберите в списке тип копирования:

   **Немедленно**
   Копирует все ожидающие обновления записей с момента последнего события копирования, а затем непрерывно обновляет записи до достижения следующего запланированного события обновления.

   **Однократно**
   Копирует все ожидающие обновления вплоть до времени запуска. Все обновления, внесенные после времени запуска будут ожидать следующего запланированного события копирования.
5. Выберите начальное время (местное время для сервера) события копирования.
6. Нажмите кнопку **Добавить**. Будет показан тип события копирования и время.
7. Для завершения настройки расписания добавьте или удалите события. События упорядочены в списке в хронологическом порядке.
8. После завершения ввода нажмите **OK**.

Например:

*Таблица 6.*

| **Тип копирования** | **Время запуска** |
|---|---|
| Немедленно | 00:00 |
| Однократно | 10:00 |
| Однократно | 2:00 |
| Немедленно | 16:00 |
| Однократно | 20:00 |

В этом расписании первое событие копирования происходит в полночь. При этом применяются все накопившиеся к этому моменту ожидающие обновления. Дальнейшие обновления копируются по мере внесения до 10:00. Обновления, внесенные с 10:00 до 14:00 ожидают копирования до 14:00. Все обновления, внесенные между 14:00 и 16:00 ожидают следующего события копирования, запланированного на 16:00, а затем копирование обновлений продолжается вплоть до следующего события, запланированного на 20:00. Все обновления, внесенные после 20:00, будут ожидать следующего запланированного события.

**Примечание:** Если события копирования запланированы с недостаточным интервалом, то в том случае, когда предыдущая операция копирования обновлений к запланированному моменту еще не завершилась, очередное событие копирования может быть пропущено.

## Управление очередями

Эта задача позволяет отслеживать состояние процесса копирования для каждого используемого сервером соглашения о копировании (т.е. для каждой очереди).

Разверните в области навигации категорию **Управление копированием** и выберите опцию **Управление очередями**.

Выберите копию, для которой вы хотите управлять очередями.

- В зависимости от состояния копии вы можете выбрать опцию **Приостановить/возобновить** для остановки или запуска копирования.
- Для копирования всех ожидающих изменений независимо от момента, на который запланировано следующее копирование, нажмите кнопку **Принудительное копирование**.
- Для просмотра подробной информации об очереди выбранной копии нажмите кнопку **Сведения об очереди**. Показанное окно также позволяет управлять очередью.
- Для обновления сведений об очередях и очистки сообщений сервера нажмите кнопку **Обновить**.

**Сведения об очереди**

При нажатии кнопки **Сведения об очереди** появляется окно с тремя вкладками:

- Состояние
- Сведения о последней попытке
- Ожидающие изменения

На вкладке **Состояние** показано имя копии, ее поддерево, состояние, а также число операций копирования. С помощью этой панели вы можете приостановить или возобновить копирование, выбрав опцию **Возобновить**. Для обновления сведений об очередях нажмите кнопку **Обновить**.

На вкладке **Сведения о последней попытке** приведена информация о последней попытке обновления. Если загрузить запись невозможно, то нажмите кнопку **Пропустить блокирующую запись** для перехода к копированию следующей ожидающей записи. Для обновления сведений об очередях нажмите кнопку **Обновить**.

На вкладке **Ожидающие изменения** перечислены все изменения, ожидающие копирования. Если копирование блокировано, вы можете удалить все ожидающие изменения с помощью опции **Пропустить все**. Для обновления списка ожидающих изменений с учетом всех вновь внесенных и уже обработанных обновлений нажмите кнопку **Обновить**.

**Примечание:** Если вы решили пропустить блокирующие изменения, то необходимо обеспечить обновление сервера-потребителя другими средствами. Дополнительная информация приведена в разделе “ldapdiff” на стр. 230.

## Настройка копирования по защищенному соединению

Для того чтобы можно было проверить ход процесса, при загрузке следует настроить копирование по SSL.

Прежде, чем настраивать копирование по защищенному соединению, необходимо выполнить следующие задачи (в любом порядке):

- Настройка копирования по незащищенному соединению.
- Настройка сервера-потребителя для принятия защищенных соединений по защищенному порту. Убедитесь, что система клиента поддерживает защищенные соединения с сервером-потребителем. Это можно сделать с помощью утилиты ldapsearch. Если требуется, чтобы на сервере-поставщике применялась идентификация по сертификатам, например, внешнее подключение SASL по SSL, то сначала настройте идентификацию сервера, а затем клиента и сервера. Сервер в данном случае - это сервер-потребитель, а клиент - это сервер-поставщик.

  **Примечание:** Как только на сервере будет настроена идентификация клиента и сервера, для всех клиентов с поддержкой SSL потребуются клиентские сертификаты.
- Настройте на сервере-поставщике поддержку доверенной CA, выпускающей сертификат для приемника.

1. В Web-инструменте администрирования войдите в категорию **Управление копированием** и выберите опцию**Управление топологией**.
2. Выберите из имеющихся соглашений то, которое требуется сделать защищенным.
3. Выберите **Изменить соглашение...** и укажите SSL, при этом убедившись, что стоит правильный номер порта. Стандартный номер защищенного порта - 636.
4. Проверьте правильность работы функции копирования с учетом соглашения.

Если вы пытаетесь только настроить копирование для идентификации с помощью DN и пароля по защищенному соединению, то это уже сделано. Для идентификации по клиентским сертификатам требуется, чтобы в соглашении сервера-поставщика использовались разные объекты разрешений. Также необходимо, чтобы сервер-приемник принимал эти сертификаты в роли сервера-поставщика.

# Управление свойствами защиты

Сервер каталогов предоставляет ряд возможностей для защиты данных. В их число входит управление паролями, шифрование с помощью SSL и TLS, идентификация Kerberos и DIGEST-MD5. Информация о способах защиты приведена в разделе “Защита сервера каталогов” на стр. 51.

Дополнительная информация приведена в следующих разделах:

- “Управление паролями”
- “Включение SSL и TLS на сервере каталогов” на стр. 165
- “Включение идентификации Kerberos на сервере каталогов” на стр. 167
- “Настройка идентификации DIGEST-MD5 на сервере каталогов” на стр. 168

# Управление паролями

Для управления паролями разверните в области навигации Web-инструмента администрирования категорию **Управление свойствами защиты** и перейдите на вкладку **Стратегия управления паролями**.

Дополнительная информация приведена в следующих разделах:

- “Настройка свойств пароля”
- “Советы по стратегии управления паролями” на стр. 163

## Настройка свойств пароля

Для того чтобы доступ к каталогу был только у пользователей с соответствующими правами доступа, на сервере каталогов предусмотрено множество опций для управления паролями. Эти опции объединяются в стратегию управления паролями, блокировку и проверку пароля.

**Стратегия управления паролями**

Для настройки стратегии управления паролями выполните следующие действия:

1. В области навигации Web-инструмента администрирования разверните категорию **Управление свойствами защиты** и перейдите на вкладку **Стратегия управления паролями**.На этой странице отображаются неизменяемое поле **Атрибут пароля**, содержащее имя атрибута, используемого стратегией.
2. В выпадающем списке выберите тип шифрования пароля:

   **Нет** Без шифрования. Пароли хранятся в формате обычного текста.

   **crypt** Перед сохранением в каталоге пароли кодируются с помощью алгоритма кодирования UNIX crypt.

   **SHA-1** Перед сохранением в каталоге пароли кодируются с помощью алгоритма кодирования SHA-1.
3. Для активизации стратегии управления паролями включите переключатель **Разрешить стратегию управления паролями**.

   **Примечание:** Если стратегия не включена, то ни одна из этих и других панелей, связанных с паролями, не будет доступной. По умолчанию стратегия управления паролями отключена.
4. Укажите, может ли пользователь менять свой пароль, с помощью переключателя **Пользователю разрешено изменять пароль**.
5. Укажите, должен ли пользователь изменить пароль после входа в систему со сброшенным паролем. Для этого служит переключатель**Пользователь должен изменить пароль после сброса**.
6. Укажите, должен ли пользователь после первого входа в систему указать пароль повторно для получения возможности изменения. Для этого служит переключатель **Пользователь должен указать пароль при изменении**.

7. Настройте максимальный срок действия пароля. Переключатель **Срок действия пароля не ограничен** позволяет не изменять пароль в течение указанного периода времени, а переключатель **Дней** и указанный период времени в днях позволяет задать ограниченный срок действия пароля.
8. Укажите, должно ли выводиться предупреждение системы перед окончанием срока действия пароля.

   Переключатель **Не выводить предупреждение** обозначает, что система не будет предупреждать пользователя об окончании срока действия. При устаревании пароля пользователь теряет доступ к каталогу до тех пор, пока администратор не создаст ему новый пароль.

   Если вы включите переключатель **Дней до окончания срока действия** и укажете количество дней (n), то начиная с n дней до окончания срока действия пароля пользователь будет получать предупреждение с приглашением изменить пароль всякий раз при входе в систему. Пока пароль не устареет, у пользователя сохранится доступ к каталогу.
9. Укажите, сколько раз пользователь сможет войти в систему после окончания срока действия пароля. Этот переключатель позволит пользователю обращаться к каталогу с устаревшим паролем.
10. Нажмите кнопку **OK**.

**Примечание:** Для настройки стратегии управления паролями можно также воспользоваться утилитой ldapmodify (см. раздел “ldapmodify и ldapadd” на стр. 203).

Дополнительная информация о стратегии управления паролями приведена в разделе “Стратегия управления паролями” на стр. 73.

**Блокировка пароля**

1. В области навигации Web-инструмента администрирования разверните категорию **Управление свойствами защиты** и перейдите на вкладку **Блокировка пароля**.

   **Примечание:** Функции на этой вкладке не будут иметь силы, если на сервере не активирована стратегия управления паролями.
2. Укажите время в секундах, минутах, часах или днях, которое должно пройти до того, как пароль можно будет изменить.
3. Укажите, будет ли пароль заблокирован при неудачных попытках входа в систему.
   - Если вы разрешите неограниченное количество попыток входа в систему, то включите переключатель **Пароль никогда не будет блокирован**. Эта опция позволяет отключить функцию блокирования пароля.
   - Для разрешения нескольких попыток входа в систему до того, как пароль будет заблокирован, включите переключатель Попыток и укажите количество попыток входа в систему. Этот переключатель активизирует функцию блокирования паролей.
4. Укажите длительность блокирования. Для того чтобы указать, что пароль должен сбрасываться системным администратором, включите переключатель**Срок действия блокировки не ограничен**. Переключатель **Секунд** и указание времени в секундах позволяет задать срок действия блокировки, по истечении которого можно возобновить попытки входа в систему.
5. Укажите время истечения срока действия для неудачных попыток входа в систему. Переключатель **Неудачные попытки входа в систему очищаются только при правильном вводе пароля** позволяет указать, что неудачные попытки входа в систему будут удалены из памяти только при введении правильного пароля. Переключатель **Секунд** и заданное время в секундах позволяет настроить удаление из памяти неудачных попыток входа в систему через определенное время.

   **Примечание:** Эта опция работает только для незаблокированного пароля.
6. По окончании настройки нажмите **Применить** для сохранения изменений без выхода, или **OK** для сохранения и закрытия страницы. Если вы не хотите сохранять изменения, нажмите кнопку **Отмена**.

**Проверка пароля**

1. В области навигации Web-инструмента администрирования разверните категорию **Управление свойствами защиты** и перейдите на вкладку **Проверка пароля**.

**Примечание:** Функции на этой вкладке не будут иметь силы, если на сервере не активирована стратегия управления паролями.

2. Укажите, сколько паролей должно смениться прежде, чем указанный пароль можно будет использовать повторно. Введите число от 0 до 30. Нулевое значение обозначает, что пароль может использоваться неограниченно.
3. В выпадающем списке выберите, должен ли проверяться синтаксис пароля, определенный в следующих полях записи. Вы можете выбрать:

   **Не проверять синтаксис**
   Синтаксис проверяться не будет.

   **Проверять синтаксис (за исключением шифрования)**
   Будет проверяться синтаксис всех незашифрованных паролей.

   **Проверять синтаксис**
   Будет проверяться синтаксис всех паролей.
4. Укажите минимальную длину пароля. При нулевом значении не будет выполняться проверка синтаксиса.
   - Укажите минимальное количество буквенных символов в пароле.
   - Укажите минимальное количество цифр и специальных символов в пароле.

   **Примечание:** Сумма минимального количества букв, цифр и специальных символов должна быть меньшей или равной указанной минимальной длине пароля.
5. Укажите максимальное количество повторяющихся символов в пароле. Этот параметр ограничивает количество повторений какого-либо символа в пароле. При нулевом значении количество повторяющихся символов не проверяется.
6. Укажите минимальное количество символов, на которое пароль должен отличаться от предыдущего пароля. В поле **Минимальное количество паролей до повторного использования** укажите количество предыдущих паролей. При нулевом значении количество отличающихся символов не проверяется.
7. По окончании настройки нажмите **Применить** для сохранения изменений без выхода, или **OK** для сохранения и закрытия страницы. Если вы не хотите сохранять изменения, нажмите кнопку **Отмена**.

## Советы по стратегии управления паролями

**Запросы стратегии управления паролями**

Для просмотра состояния записи каталога и для запроса записей, удовлетворяющих заданным критериям, можно воспользоваться операционными атрибутами стратегии управления паролями. Операционные атрибуты возвращаются запросом на поиск только в том случае, если они специально запрошены клиентом. Для применения этих атрибутов в операциях поиска необходимо иметь права доступа к атрибутам класса critical или права доступа для применения специальных атрибутов.

Для просмотра всех атрибутов стратегии управления паролями для заданной записи выполните следующие команды:

```
> ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
 pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
 pwdFailureTime pwdGraceUseTime pwdReset
```

Для запроса записей с устаревающими паролями служит атрибут pwdChangedTime. Например, чтобы найти пароли, срок действия которых истечет 26 августа 2004 года, со стратегией истечения срока действия пароля 186 дней, запросите записи, для которых пароль был изменен минимум 186 дней назад (22 февраля 2004 года):

```
> ldapsearch -b "cn=users,o=ibm" -s sub
 "(!(pwdChangedTime>20040222000000Z))" 1.1
```

где the фильтр соответствует pwdChangedTime в полночь 22 февраля 2004 года.

Для запроса заблокированных учетных записей служит атрибут pwdAccountLockedTime:

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
```

где ″1.1″ обозначает возвращение только имен отличительных имен.

Для запроса учетных записей, пароль которых должен быть изменен вследствие сброса, служит атрибут pwdReset:

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
```

**Переопределение стратегии управления паролями**

Администратор каталога может переопределить обычную стратегию управления паролями для некоторых записей. Это можно сделать с помощью изменения операционных атрибутов или с помощью средств управления администрированием сервера (опция -k для утилит командной строки LDAP).

Вы можете предотвратить устаревание пароля для какой-либо учетной записи, настроив в атрибуте pwdChangedTime дату, отстоящую далеко вперед от даты установки атрибута userPassword. В следующем примере настраивается дата 1 января 2200 года, полночь.

```
> ldapmodify -D cn=root -w ? -k
dn: uid=wasadmin,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 220001010000000Z
```

Удалив атрибуты pwdAccountLockedTime и pwdFailureTime, можно разблокировать учетную запись, заблокированную из-за сбоев входа в систему:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdAccountLockedTime
-
delete: pwdFailureTime
```

Путем изменения атрибута pwdChangedTime и очистки атрибутов pwdExpirationWarned и pwdGraceUseTime можно разблокировать устаревшую учетную запись:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 200408260000000Z
-
delete: pwdExpirationWarned
-
delete: pwdGraceUseTime
```

Путем настройки атрибута pwdReset можно очистить или установить состояние ″пароль должен быть изменен″:

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdReset

> ldapmodify -D cn=root -w ? -k
dn: uid=user2,cn=users,o=ibm
changetype: modify
replace: pwdReset
pwdReset: TRUE
```

Установив значение TRUE для атрибута ibm-pwdAccountLocked, можно принудительно заблокировать учетную запись. Разблокирование этой записи делается путем установки для этого атрибута значения

FALSE. Такой способ разблокирования учетной записи не влияет на состояние учетной записи, заблокированной вследствие ошибок пароля или его устаревания.

Для настройки этих атрибутов пользователь должен иметь права на запись атрибута ibm-pwdAccountLocked, относящегося к классу доступа CRITICAL.

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: TRUE
```

Разблокирование учетной записи:

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: FALSE
```

**Прочие советы по стратегии управления паролями**

Есть две ситуации, в которых стратегия управления паролями может вести себя непредсказуемо:

1. Если для записи был настроен атрибут pwdReset, то клиент может подключаться со сброшенным паролем и DN записи неограниченное количество раз. При наличии управляющего элемента запроса функции управления паролями подключение будет успешным, но клиент получит предупреждение в управляющем элементе ответа. Если же управляющий элемент запроса не указан, то такой ″неосведомленный″ клиент увидит успешное подключение, но не получит предупреждения о необходимости изменения пароля. В то же время последующие операции под этим DN будут по-прежнему вызывать ошибку ″unwilling to perform″. Первоначальная успешность подключения может ввести в заблуждение. Если целью подключения была только идентификация, то эта ситуация может стать проблемой, как например в web-приложении использующем каталог для идентификации.
2. Стратегии pwdSafeModify и pwdMustChange могут вести себя непредсказуемо с приложениями, которые изменяют пароли, находясь под именем, отличным от DN записи, для которой изменяется пароль. В этом случае безопасное изменение пароля, выполняемое, например, под именем администратора, приведет к установке атрибута pwdReset. Приложение, изменяющее пароль, может с помощью учетной записи администратора удалить атрибут pwdReset, как описано выше.

## Включение SSL и TLS на сервере каталогов

**Поддержка SSL**

Если в системе установлен компонент Диспетчер цифровых сертификатов, то для защиты данных сервера каталогов можно настроить протокол Secure Sockets Layer (SSL). Прежде, чем настраивать SSL на сервере каталогов рекомендуется ознакомиться с разделом “Поддержка протоколов SSL и TLS на сервере каталогов” на стр. 51.

Для настройки SSL на сервере LDAP выполните следующие действия:

1. **Связывание сертификата с сервером каталогов**
   a. Если вы хотите управлять сервером каталогов через соединение SSL с Навигатором iSeries, то обратитесь к книге Руководство пользователя iSeries Access for Windows (ее можно установить на PC при установке Навигатора iSeries). Если вы планируете разрешить подключение к серверу каталогов как с помощью SSL, так и без SSL, то этот шаг можно пропустить.
   b. Запустите диспетчер цифровых сертификатов IBM. Дополнительная информация приведена в разделе Запуск диспетчера цифровых сертификатов.

c. Если необходимо получить или создать сертификат, а также настроить или изменить применяемые сертификаты, то сделайте это сейчас. Информация о настройке сертификатов приведена в разделе диспетчер цифровых сертификатов. С сервером каталогов связано два приложения серверов и одно приложение клиента. Это следующие приложения:

**Приложение сервера каталогов**
Это собственно сервер каталогов.

**Приложение публикации сервера каталогов**
Это приложение идентифицирует сертификаты, применяемые при публикации.

**Приложение клиента сервера каталогов**
Это приложение идентифицирует сертификат по умолчанию, применяемый приложениями, использующими API ILE клиента LDAP.

d. Нажмите кнопку **Выбрать хранилище сертификатов**.

e. Выберите ***SYSTEM**. Нажмите кнопку **Продолжить**.

f. Введите пароль хранилища сертификатов *SYSTEM. Нажмите кнопку **Продолжить**.

g. После перезагрузки меню навигации разверните категорию **Управление приложениями**.

h. Нажмите кнопку **Обновить присвоение сертификатов**.

i. В следующем окне выберите приложение **Сервер**. Нажмите кнопку **Продолжить**.

j. Выберите **Сервер каталогов**.

k. Выберите опцию **Обновить присвоение сертификата** для присвоения серверу каталогов сертификата, применяемого для его идентификации во время подключения к клиентам iSeries Access for Windows.

**Примечание:** Если вы решили воспользоваться сертификатом CA, сертификат которой отсутствует в базе данных ключей клиента iSeries Access for Windows, то для применения SSL нужно будет добавить сертификат этой CA с базу данных ключей клиента. Перед тем, как сделать это, закончите выполнение данной процедуры.

l. Выберите в списке сертификат, который необходимо присвоить серверу.

m. Нажмите кнопку **Присвоить новый сертификат**.

n. DCM покажет страницу **Обновление присвоения сертификата** с подтверждающим сообщением. После завершения настройки сертификатов для сервера каталогов нажмите кнопку **Готово**.

2. **Связывание сертификата с приложением публикации сервера каталогов**. (Необязательно.) Если вы хотите также включить публикацию на сервере каталогов с помощью соединения SSL, то может также потребоваться связать сертификат с приложением публикации сервера каталогов. Тем самым вы укажете сертификат по умолчанию и доверенные CA для приложений, которые применяют API ILE LDAP и не имеют собственного ИД приложения или альтернативной базы данных ключей.

a. Запустите Диспетчер цифровых сертификатов IBM.

b. Нажмите кнопку **Выбрать хранилище сертификатов**.

c. Выберите ***SYSTEM**. Нажмите кнопку **Продолжить**.

d. Введите пароль хранилища сертификатов *SYSTEM. Нажмите кнопку **Продолжить**.

e. После перезагрузки меню навигации разверните категорию **Управление приложениями**.

f. Нажмите кнопку **Обновить присвоение сертификатов**.

g. В следующем окне выберите приложение **Клиент**. Нажмите кнопку **Продолжить**.

h. Выберите **Публикация сервера каталогов**.

i. Выберите опцию **Обновить присвоение сертификата** для присвоения приложению публикации сервера каталогов сертификата, применяемого для его идентификации.

j. Выберите в списке сертификат, который необходимо присвоить серверу.

k. Нажмите кнопку **Присвоить новый сертификат**.

l. DCM покажет страницу **Обновление присвоения сертификата** с подтверждающим сообщением.

**Примечание:** В этих инструкциях предполагается, что вы уже публикуете информацию на сервере каталогов без применения соединений SSL. Полная информация о настройке публикации приведена в разделе “Публикация информации на сервере каталогов” на стр. 98.

3. **Связывание сертификата с приложением клиента сервера каталогов**. (Необязательно.) Если у вас есть другие приложения, которые подключаются к серверу каталогов с помощью SSL, то необходимо также связать сертификат с клиентом сервера каталогов.
   a. Запустите Диспетчер цифровых сертификатов IBM.
   b. Нажмите кнопку **Выбрать хранилище сертификатов**.
   c. Выберите ***SYSTEM**. Нажмите кнопку **Продолжить**.
   d. Введите пароль хранилища сертификатов *SYSTEM. Нажмите кнопку **Продолжить**.
   e. После перезагрузки меню навигации разверните категорию **Управление приложениями**.
   f. Нажмите кнопку **Обновить присвоение сертификатов**.
   g. В следующем окне выберите приложение **Клиент**. Нажмите кнопку **Продолжить**.
   h. Выберите **Клиент сервера каталогов**.
   i. Выберите опцию **Обновить присвоение сертификата** для присвоения клиенту сервера каталогов сертификата, применяемого для его идентификации.
   j. Выберите в списке сертификат, который необходимо присвоить серверу.
   k. Нажмите кнопку **Присвоить новый сертификат**.
   l. DCM покажет страницу **Обновление присвоения сертификата** с подтверждающим сообщением.

После настройки SSL можно изменить порт, применяемый сервером каталогов для защищенных соединений.

**Поддержка TLS**

Для того чтобы применять SSL или TLS, следует разрешить эти протоколы в Навигаторе iSeries.

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
4. На вкладке **Сеть** включите переключатель **Защита**.

Кроме этого можно указать номер порта, который требуется защитить. Включение переключателя **Защита** означает, что приложение может открывать соединения SSL или TLS по защищенному порту. Также приложение может вызывать операцию StartTLS для разрешения соединений TLS по незащищенному порту. TLS можно вызвать и другим способом: с помощью опции -Y утилиты командной строки системы клиента. При работе в командной строке для атрибута ibm-slapdSecurity должно быть указано значение TLS или SSLTLS.

Дополнительные сведения по SSL и TLS приведены в разделе “Поддержка протоколов SSL и TLS на сервере каталогов” на стр. 51.

## Включение идентификации Kerberos на сервере каталогов

Если в системе настроена Служба сетевой идентификации, то на сервере каталогов можно настроить функцию идентификации Kerberos. Идентификация Kerberos применяется как по отношению к пользователям, так и по отношению к администраторам. Перед настройкой Kerberos на сервере каталогов рекомендуется ознакомиться с обзором применения Kerberos с сервером каталогов.

Для включения функции идентификации Kerberos выполните следующие действия:

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.

4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Свойства**.
5. Перейдите на страницу **Kerberos**.
6. Отметьте опцию **Разрешить применение идентификации Kerberos**.
7. Настройте другие параметры на странице **Kerberos**. Информация о полях, расположенных на этой странице, приведена в электронной справке.

## Настройка идентификации DIGEST-MD5 на сервере каталогов

DIGEST-MD5 - это механизм идентификации SASL. Если клиент применяет механизм DIGEST-MD5, то пароль передается не в виде обычного текста, препятствуя атакам воспроизведения. Настройка DIGEST-MD5 осуществляется с помощью Web-инструмента администрирования.

1. В области навигации, в разделе **Администрирование сервера** разверните категорию **Управление свойствами защиты** и перейдите на вкладку **DIGEST-MD5**.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. В разделе **Область сервера** либо оставьте значение **По умолчанию**, которое представляет собой полное имя хоста сервера, либо щелкните на **Область** и введите имя области, которую требуется настроить в качестве сервера. По этому имени клиент будет определять, какие идентификационные данные (имя пользователя и пароль) применять. При использовании копирования необходимо, чтобы на всех серверах была настроена одна область.
3. Для атрибута **Имя пользователя** либо оставьте значение **По умолчанию**, которое представляет собой ИД пользователя, либо выберите **Атрибут** и введите имя атрибута, по которому сервер будет уникально идентифицировать пользовательскую запись при подключении посредством SASL DIGEST-MD5.
4. Если вы вошли в систему как администратор каталога, то в поле **Имя администратора** введите имя администратора. Члены группы администраторов не могут изменять это поле. Если имя пользователя, указанное при подключении по SASL DIGEST-MD5, соответствует этой строке, значит, пользователь является администратором.

   **Примечание:** Имя администратора указывается с учетом регистра букв.
5. После завершения ввода нажмите **OK**.

---

## Управление схемой

Дополнительная информация о схеме приведена в разделе “Схема” на стр. 18.

Схемой можно управлять с помощью Web-инструмента администрирования или с помощью приложения LDAP, например, ldapmodify, в сочетании с файлами LDIF. При первом определении новых классов объектов или атрибутов удобнее всего воспользоваться Web-инструментом администрирования. Если необходимо скопировать схему на другие серверы (например, в ходе развертывания продукта или инструмента), то более удобной может оказаться утилита ldapmodify. Дополнительная информация приведена в разделе “Копирование схемы на другие серверы” на стр. 178.

Дополнительная информация приведена в следующих разделах:

- “Просмотр классов объектов” на стр. 169
- “Добавление класса объектов” на стр. 169
- “Редактирование класса объектов” на стр. 171

## Просмотр классов объектов

Просматривать классы объектов схемы можно с помощью Web-инструмента администрирования (это предпочитаемый способ) или с помощью командной строки.

**Web-администрирование**

В области навигации разверните категорию **Управление схемой** и выберите опцию **Управление классами объектов**. Будет показана предназначенная только для чтения панель, позволяющая просматривать классы объектов схемы и их характеристики. Классы объектов расположены в алфавитном порядке. Для перемещения по страницам воспользуйтесь кнопками Назад и Вперед. Рядом с кнопками указаны номера просматриваемых в настоящий момент страниц. Кроме того, вы можете перейти к нужной странице, выбрав ее в списке. Рядом с первым классом объектов в списке показан показан номер соответствующей страницы. Например, если вам нужен класс объектов **person**, то найдите в выпадающем списке записи **Страница 14 из 16 nsLiServer** и **Страница 15 из 16 printerLPR**. Поскольку слово person расположено по алфавиту между nsLiServer и printerLPR, выберите Стр. 14 и нажмите **Перейти**.

Классы объектов можно также упорядочить по типу. Выберите **Тип** и нажмите **Сортировка**. Классы будут упорядочены по типу, Абстрактный, Вспомогательный и Структурированный. Вы можете изменить направление сортировки, выбрав опцию **По убыванию**, и нажав кнопку **Сортировка**.

Найдя требуемый класс объектов, вы можете просмотреть его тип, наследование, обязательные и дополнительные атрибуты. Для просмотра всех значений разверните выпадающие списки, в которых показан тип, наследование, обязательные и дополнительные атрибуты.

На панели инструментов справа можно выбрать операцию над объектом:

- Добавление
- Изменение
- Копирование
- Удаление

После завершения нажмите **Закрыть** для возврата к окну **Приветствие** IBM Directory Server.

**Командная строка**

Для просмотра содержащихся в схеме классов объектов введите следующую команду:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

## Добавление класса объектов

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление классами объектов**. Для создания нового класса объектов:

1. Нажмите кнопку **Добавить**.

**Примечание:** К этой панели можно также перейти, развернув в области навигации категорию **Управление схемой** и выбрав опцию **Добавить класс объектов**.

2. На вкладке **Общие свойства**:
   - Введите **Имя класса объектов**. Это обязательное значение; имя класса должно описывать его функцию. Например, класс **tempEmployee** может применяться для объектов, связанных со временными служащими.
   - Введите **Описание** класса объектов, например, **Класс объектов для временных служащих**.
   - Введите **OID** класса объектов. Это обязательное поле. См. раздел “Идентификатор объекта (OID)” на стр. 29. Если вы не можете выбрать OID, то укажите **Имя класса объектов** и добавьте к нему символы **-oid**. Например, для класса объектов **tempEmployee** следует указать OID **tempEmployee-oid**. Это значение можно изменить.
   - Выберите в списке **Родительский класс объектов**. Он определяет, от какого класса будут наследоваться атрибуты данного класса. Обычно в качестве **Родительского класса объектов** применяется **top**, однако это может быть и любой другой класс объектов. Например, родительским классом для **tempEmployee** может быть **ePerson**.
   - Выберите **Тип класса объектов**. Дополнительная информация о типах классов объектов приведена в разделе “Классы объектов” на стр. 21.
   - Перейдите на вкладку Атрибуты, на которой указываются обязательные и дополнительные атрибуты, а также отображаются унаследованные атрибуты; нажмите **OK** для добавления нового класса объектов или нажмите кнопку **Отмена** для возврата к окну **Управление классами объектов** без внесения изменений.
3. На вкладке **Атрибуты**:
   - Выберите атрибут в списке **Доступные атрибуты** и нажмите кнопку **Добавить в обязательные**, чтобы сделать его обязательным, либо кнопку **Добавить в дополнительные**, чтобы сделать атрибут класса объектов необязательным. Атрибут будет показан в соответствующем списке.
   - Повторите операцию для всех выбранных атрибутов.
   - Вы можете перемещать атрибуты из одного списка в другой, а также удалять их из списков. Для этого необходимо выделить атрибут и нажать кнопку **Переместить в** или **Удалить**.
   - Вы можете просматривать списки унаследованных обязательных и дополнительных атрибутов. Список унаследованных атрибутов зависит от **Родительского класса объектов**, выбранного на вкладке **Общие**. Изменить унаследованные атрибуты нельзя. Однако, если вы измените **Родительский класс объектов** на вкладке **Общие**, то будет показан другой набор унаследованных атрибутов.
4. Нажмите **OK** для добавления нового класса объектов, или **Отмена** для возврата к окну **Управление классами объектов** без внесения изменений.

**Примечание:** Если вы нажмете кнопку **OK** на вкладке **Общие** без добавления каких-либо атрибутов, то сможете добавить их потом, изменив новый класс объектов.

**Командная строка**

Для добавления класса объектов с помощью командной строки введите следующую команду:

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i <имя-файла>
```

где <*имя-файла*> задает файл со следующим содержимым:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<An object class
                 I defined for my LDAP application>' SUP '<objectclassinheritance>'
                 <objectclasstype> MAY (<attribute1> $ <attribute2>))
```

## Редактирование класса объектов

Не все изменения схемы являются разрешенными. Сведения об ограничениях приведены в разделе “Запрещенные изменения схемы” на стр. 31.

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление классами объектов**. Для изменения класса объектов:

1. Выберите радиокнопку, соответствующую изменяемому классу объектов.
2. Нажмите кнопку **Редактировать**.
3. Выберите вкладку:
   - Вкладка **Общие** позволяет выполнять следующие операции:
     - Изменение **Описания**.
     - Изменение **Родительского класса объектов**. Выберите в списке родительский класс объектов. Он определяет, от какого класса будут наследоваться атрибуты данного класса. Обычно в качестве **Родительского класса объектов** применяется **top**, однако это может быть и любой другой класс объектов. Например, родительским классом для **tempEmployee** может быть **ePerson**.
     - Изменение **Типа класса объектов**. Выберите тип класса объектов. Дополнительная информация о типах классов объектов приведена в разделе “Классы объектов” на стр. 21.
     - Перейдите на вкладку Атрибуты для изменения обязательных и дополнительных атрибутов или просмотра унаследованных атрибутов; нажмите **OK** для применения внесенных изменений или **Отмена** для возврата к окну **Управление классами объектов** без внесения изменений.
   - Вкладка **Атрибуты** позволяет выполнять следующие операции:

     Выберите атрибут в списке **Доступные атрибуты** и нажмите кнопку **Добавить в обязательные**, чтобы сделать его обязательным, либо кнопку **Добавить в дополнительные**, чтобы сделать атрибут класса объектов необязательным. Атрибут будет показан в соответствующем списке.

     Повторите операцию для всех выбранных атрибутов.

     Вы можете перемещать атрибуты из одного списка в другой, а также удалять их из списков. Для этого необходимо выделить атрибут и нажать кнопку **Переместить в** или **Удалить**.

     Вы можете просматривать списки унаследованных обязательных и дополнительных атрибутов. Список унаследованных атрибутов зависит от **Родительского класса объектов**, выбранного на вкладке **Общие**. Изменить унаследованные атрибуты нельзя. Однако, если вы измените **Родительский класс объектов** на вкладке **Общие**, то будет показан другой набор унаследованных атрибутов.
4. Нажмите **OK** для сохранения изменений или **Отмена** для возврата к панели **Управление классами объектов** без сохранения изменений.

**Командная строка**

Для просмотра содержащихся в схеме классов объектов введите следующую команду:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Для изменения класса объектов с помощью командной строки введите следующую команду:

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i <имя-файла>
```

где <*имя-файла*> задает файл со следующим содержимым:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<An object class
                I defined for my LDAP application>' SUP '<newsuperiorclassobject>'
                <newobjectclasstype> MAY (attribute1> $ <attribute2>
                 $ <newattribute3>) )
```

## Копирование класса объектов

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление классами объектов**. Для копирования класса объектов:

1. Выберите радиокнопку, соответствующую копируемому классу объектов.
2. Нажмите кнопку **Скопировать**.
3. Выберите вкладку:
   - Вкладка **Общие** позволяет выполнять следующие операции:
     - Изменение **имени класса объектов**. Имя по умолчанию представляет собой имя исходного класса, после которого добавлено слово COPY. Например: **tempPerson** по умолчанию копируется под именем **tempPersonCOPY**.
     - Изменение **Описания**.
     - Изменение **OID**. OID по умолчанию представляет собой OID исходного класса, после которого добавлено слово COPY. Например: **tempPerson-oid** по умолчанию копируется с OID **tempPerson-oidCOPY**.
     - Изменение **Родительского класса объектов**. Выберите в списке родительский класс объектов. Он определяет, от какого класса будут наследоваться атрибуты данного класса. Обычно в качестве **Родительского класса объектов** применяется **top**, однако это может быть и любой другой класс объектов. Например, родительским классом для **tempEmployeeCOPY** может быть **ePerson**.
     - Изменение **Типа класса объектов**. Выберите тип класса объектов. Дополнительная информация о типах классов объектов приведена в разделе “Классы объектов” на стр. 21.
     - Щелкните на вкладке **Атрибуты** для изменения обязательных и дополнительных атрибутов класса объектов и просмотра унаследованных атрибутов; нажмите кнопку **OK** для добавления нового класса объектов, либо нажмите кнопку **Отмена** для возврата к окну **Управление классами объектов** без внесения изменений.
   - Вкладка **Атрибуты** позволяет выполнять следующие операции:

     Выберите атрибут в списке **Доступные атрибуты** и нажмите кнопку **Добавить в обязательные**, чтобы сделать его обязательным, либо кнопку **Добавить в дополнительные**, чтобы сделать атрибут класса объектов необязательным. Атрибут будет показан в соответствующем списке.

     Повторите операцию для всех выбранных атрибутов.

     Вы можете перемещать атрибуты из одного списка в другой, а также удалять их из списков. Для этого необходимо выделить атрибут и нажать кнопку **Переместить в** или **Удалить**.

     Вы можете просматривать списки унаследованных обязательных и дополнительных атрибутов. Список унаследованных атрибутов зависит от **Родительского класса объектов**, выбранного на вкладке **Общие**. Изменить унаследованные атрибуты нельзя. Однако, если вы измените **Родительский класс объектов** на вкладке **Общие**, то будет показан другой набор унаследованных атрибутов.
4. Нажмите **OK** для сохранения изменений или **Отмена** для возврата к панели **Управление классами объектов** без сохранения изменений.

**Командная строка**

Для просмотра содержащихся в схеме классов объектов введите следующую команду:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Выберите класс объектов для копирования. С помощью редактора измените информацию и сохраните изменения в файле <*имя-файла*>. Введите следующую команду:

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i <имя-файла>
```

где <*имя-файла*> задает файл со следующим содержимым:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <mynewobjectClass-oid> NAME '<mynewObjectClass>'
                 DESC '<A new object class
                   I copied for my LDAP application>'
                SUP '<superiorclassobject>'<objectclasstype> MAY (attribute1>
$ <attribute2> $ <attribute3>) )
```

## Удаление класса объектов

Не все изменения схемы являются разрешенными. Сведения об ограничениях приведены в разделе “Запрещенные изменения схемы” на стр. 31.

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление классами объектов**. Для удаления класса объектов:

1. Выберите радиокнопку, соответствующую удаляемому классу объектов.
2. Нажмите кнопку **Удалить**.
3. Вам будет предложено подтвердить удаление класса объектов. Нажмите кнопку **OK** для удаления класса объектов или **Отмена** для возврата к окну **Управление классами объектов** без внесения изменений.

**Командная строка**

Для просмотра содержащихся в схеме классов объектов введите следующую команду:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Выберите класс объектов для удаления и введите следующую команду:

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i <имя-файла>
```

где <*имя-файла*> задает файл со следующим содержимым:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

## Просмотр атрибутов

Просматривать атрибуты схемы можно с помощью Web-инструмента администрирования (это предпочитаемый способ) или с помощью командной строки.

**Web-администрирование**

В области навигации разверните категорию **Управление схемой** и выберите опцию **Управление атрибутами**. Будет показана предназначенная только для чтения панель, позволяющая просматривать атрибуты схемы и их характеристики. Атрибуты перечисляются в алфавитном порядке. Для перемещения по страницам воспользуйтесь кнопками Назад и Вперед. Рядом с кнопками указаны номера просматриваемых в настоящий момент страниц. Кроме того, вы можете перейти к нужной странице, выбрав ее в списке. Рядом с первым классом объектов в списке показан показан номер соответствующей страницы. Например, если вам нужно найти атрибут **authenticationUserID**, то вы найдете в выпадающем списке **Страница 3 из 62 applSystemHint** и **Страница 4 из 62 authorityRevocatonList**. Поскольку authenticationUserID находится между applSystemHint и authorityRevocatonList, следует выбрать страницу 3 и нажать кнопку **Перейти**.

Вы также можете просматривать список атрибутов, упорядоченный по синтаксису. Выберите **Синтаксис** и нажмите кнопку **Отсортировать**. Атрибуты будут упорядочены в алфавитном порядке по суффиксу. Список типов синтаксиса приведен в разделе “Синтаксис атрибута” на стр. 27. Вы можете изменить направление сортировки, выбрав опцию **По убыванию**, и нажав кнопку **Сортировка**.

После того, как вы найдете нужный атрибут, вы можете просмотреть его синтаксис, определить, является ли он многозначным, а также выяснить, к каким классам объектов он относится. Классы объектов атрибута перечислены в списке.

После завершения нажмите **Закрыть** для возврата к окну **Приветствие** IBM Directory Server.

**Командная строка**

Для просмотра содержащихся в схеме атрибутов введите следующую команду:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

## Добавление атрибута

Создать новый атрибут можно с помощью любого из следующих методов. Рекомендуется использовать Web-инструмент администрирования.

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление атрибутами**. Для создания нового атрибута:

1. Нажмите кнопку **Добавить**.

   **Примечание:** К этой панели можно также перейти, развернув в области навигации категорию **Управление схемой** и выбрав опцию **Добавить атрибут**.
2. Введите **Имя атрибута**, например, **tempId**. Это обязательное поле. Имя атрибута должно начинаться с буквы.
3. Введите **Описание** атрибута, например, **ИД временного служащего**.
4. Введите **OID** атрибута. Это обязательное поле. См. раздел “Идентификатор объекта (OID)” на стр. 29. Если вы не можете выбрать OID, то укажите имя атрибута и добавьте к нему символы -oid. Например, если имя атрибута **tempID**, то OID по умолчанию будет **tempID-oid**.Это значение можно изменить.
5. Выберите в списке **Родительский атрибут**. Текущий атрибут унаследует свойства родительского.
6. Выберите в списке **Синтаксис**. Дополнительная информация о синтаксисе приведена в разделе “Синтаксис атрибута” на стр. 27.
7. Укажите значение **Длины атрибута**, задающей максимальную длину значения атрибута. Длина указывается в байтах.
8. Для того чтобы у атрибута могло быть несколько значений, отметьте переключатель **Разрешить многозначные атрибуты**.
9. Выберите в списках правила соответствия для равенства, упорядочения и подстрок. Полный список правил соответствия приведен в разделе “Правила соответствия” на стр. 25.
10. Перейдите на вкладку **Расширения IBM** для указания дополнительных расширений для атрибута, нажмите **OK** для добавления нового атрибута или **Отмена** для возврата к окну **Управление атрибутами** без внесения изменений.
11. На вкладке **Расширения IBM** можно сделать следующее:
    - Изменить **Имя таблицы DB2**. Если это поле оставить пустым, то сервер создаст имя таблицы DB2 автоматически. Если вы указали имя таблицы DB2, то необходимо также указать имя столбца DB2.
    - Изменить **Имя столбца DB2**. Если это поле оставить пустым, то сервер создаст имя столбца DB2 автоматически. Если вы указали имя столбца DB2, то необходимо также указать имя таблицы DB2.
    - Задать **Класс защиты**, выбрав в списке значение **normal**, **sensitive** или **critical**.
    - Выбрать одно или несколько **Правил индексации**. Дополнительная информация о правилах индексации приведена в разделе “Правила индексации” на стр. 26.

      **Примечание:** Для всех атрибутов, которые могут применяться в фильтрах поиска, рекомендуется указывать как минимум индексацию с учетом равенства.

12. Нажмите **OK** для добавления нового атрибута или **Отмена** для возврата к панели **Управление атрибутами** без сохранения изменений.

**Примечание:** Если вы нажмете кнопку OK на вкладке Общие без добавления каких-либо расширений, то сможете добавить их потом, изменив новый атрибут.

**Командная строка**

Следующий пример иллюстрирует добавление определения типа атрибута ″myAttribute″ с синтаксисом Directory String (см. “Синтаксис атрибута” на стр. 27) и правилом соответствия равенства без учета регистра (см. “Правила соответствия” на стр. 25). А разделе определения, относящемся к расширениям IBM, указано, что данные атрибута хранятся в столбце ″myAttrColumn″ таблицы ″myAttrTable″. Если эти имена не указаны, то по умолчанию в качестве имени таблицы и имени столбца будет применяться ″myAttribute″. Атрибут относится к классу доступа ″normal″, а максимальная длина значений составляет 200 байт.

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i myschema.ldif
```

где файл **myschema.ldif** содержит следующую информацию:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                 DESC 'An attribute I defined for my LDAP application'
                 EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Подробная информация об этой команде приведена в разделе “ldapmodify и ldapadd” на стр. 203.

## Редактирование атрибута

Не все изменения схемы являются разрешенными. Сведения об ограничениях приведены в разделе “Запрещенные изменения схемы” на стр. 31.

Перед добавлением записей, использующих атрибут, можно изменить любую часть определения атрибута. Изменить атрибут можно с помощью любого из следующих методов. Рекомендуется использовать Web-инструмент администрирования.

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление атрибутами**. Для изменения атрибута:

1. Выберите радиокнопку, соответствующую изменяемому атрибуту.
2. Нажмите кнопку **Редактировать**.
3. Выберите вкладку:
   - Вкладка **Общие** позволяет выполнять следующие операции:
     – Выберите вкладку:
       - Вкладка **Общие** позволяет выполнять следующие операции:
         - Изменение **Описания**
         - Изменение **Синтаксиса**.
         - Установка **Длины атрибута**.
         - Изменение опции **Нескольких значений**.
         - Выбор **Правила соответствия**.

- Изменение **Родительского атрибута**.

- Перейдите на вкладку **Расширения IBM** для изменения расширений для атрибута, нажмите **OK** для применения внесенных изменений или **Отмена** для возврата к окну **Управление атрибутами** без внесения изменений.
- Если вы работаете с IBM Directory Server, то вкладка **Расширения IBM** позволяет выполнить следующее:
  - Изменение **Класса защиты**.
  - Изменение **Правил индексации**.

– Нажмите **OK** для сохранения изменений или **Отмена** для возврата к панели **Управление атрибутами** без сохранения изменений.

4. Нажмите **OK** для сохранения изменений или **Отмена** для возврата к панели **Управление атрибутами** без сохранения изменений.

**Командная строка**

В этом примере для ускорения поиска по атрибуту к этому атрибуту добавляется индекс. Для изменения определения используйте команду ldapmodify и файл LDIF:

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i myschemachange.ldif
```

где файл **myschemachange.ldif** содержит следующую информацию:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'An attribute
                 I defined for my LDAP application' EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                  ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

**Примечание:** В операцию изменения должны быть включены обе части определения (**attributetypes** и **ibmattributetypes**), несмотря на то, что изменяется только часть **ibmattributetypes**. Единственным изменением является добавление в конец определения строки ″EQUALITY SUBSTR″, указывающей на необходимость создания индексов для сравнения по равенству и по подстроке.

Подробная информация об этой команде приведена в разделе “ldapmodify и ldapadd” на стр. 203.

## Копирование атрибута

Скопировать атрибут можно с помощью любого из следующих методов. Рекомендуется использовать Web-инструмент администрирования.

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление атрибутами**. Для копирования атрибута:

1. Выберите радиокнопку, соответствующую копируемому атрибуту.
2. Нажмите кнопку **Скопировать**.
3. Измените **Имя атрибута**. Имя по умолчанию представляет собой имя исходного атрибута, после которого добавлено слово COPY. Например: **tempID** по умолчанию копируется с именем **tempIDCOPY**.
4. Измените **Описание** атрибута, например, **ИД временного служащего**.
5. Измените **OID**. OID по умолчанию представляет собой OID исходного атрибута, после которого добавлено слово COPYOID. Например: **tempID-oid** по умолчанию копируется с OID **tempID-oidCOPYOID**.

6. Выберите в списке **Родительский атрибут**. Текущий атрибут унаследует свойства родительского.
7. Выберите в списке **Синтаксис**. Дополнительная информация о синтаксисе приведена в разделе “Синтаксис атрибута” на стр. 27.
8. Укажите значение **Длины атрибута**, задающей максимальную длину значения атрибута. Длина указывается в байтах.
9. Для того чтобы у атрибута могло быть несколько значений, отметьте переключатель **Разрешить многозначные атрибуты**.
10. Выберите в списках правила соответствия для равенства, упорядочения и подстрок. Полный список правил соответствия приведен в разделе “Правила соответствия” на стр. 25.
11. Перейдите на вкладку **Расширения IBM** для изменения дополнительных расширений атрибута, нажмите **OK** для применения внесенных изменений или **Отмена** для возврата к окну **Управление атрибутами** без внесения изменений.
12. На вкладке **Расширения IBM** можно сделать следующее:
    - Изменить **Имя таблицы DB2**. Если это поле оставить пустым, то сервер создаст имя таблицы DB2 автоматически. Если вы указали имя таблицы DB2, то необходимо также указать имя столбца DB2.
    - Изменить **Имя столбца DB2**. Если это поле оставить пустым, то сервер создаст имя столбца DB2 автоматически. Если вы указали имя столбца DB2, то необходимо также указать имя таблицы DB2.
    - Изменить **Класс защиты**, выбрав в списке значение **normal**, **sensitive** или **critical**.
    - Выбрать одно или несколько **Правил индексации**. Дополнительная информация о правилах индексации приведена в разделе “Правила индексации” на стр. 26.

    **Примечание:** Для всех атрибутов, которые могут применяться в фильтрах поиска, рекомендуется указывать как минимум индексацию с учетом равенства.
13. Нажмите **OK** для сохранения изменений или **Отмена** для возврата к панели **Управление атрибутами** без сохранения изменений.

**Примечание:** Если вы нажимаете кнопку **OK** на вкладке **Общие** без добавления каких-либо расширений, то вы сможете добавить или изменить их потом, при редактировании нового атрибута.

**Командная строка**

Для просмотра содержащихся в схеме атрибутов введите следующую команду:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Выберите атрибут для копирования. С помощью редактора измените информацию и сохраните изменения в файле <*имя-файла*>. Затем введите следующую команду:

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i <имя-файла>
```

где <*имя-файла*> задает файл со следующим содержимым:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME '<mynewAttribute>' DESC '<A new
                 attribute I copied for my LDAP application> EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                   ACCESS-CLASS normal LENGTH 200 )
```

## Удаление атрибута

Не все изменения схемы являются разрешенными. Сведения об ограничениях приведены в разделе “Запрещенные изменения схемы” на стр. 31.

Удалить атрибут можно с помощью любого из следующих методов. Рекомендуется использовать Web-инструмент администрирования.

**Web-администрирование**

Если вы еще не сделали этого, то разверните в области навигации категорию **Управление схемой** и выберите опцию **Управление атрибутами**. Для удаления атрибута:

1. Выберите радиокнопку, соответствующую удаляемому атрибуту.
2. Нажмите кнопку **Удалить**.
3. Вам будет предложено подтвердить удаление атрибута. Нажмите **OK** для удаления атрибута или **Отмена** для возврата к панели **Управление атрибутами** без сохранения изменений.

**Командная строка**

```
ldapmodify -D <DN-администратора> -w <пароль-администратора> -i myschemadelete.ldif
```

где файл **myschemadelete.ldif** содержит следующую информацию:

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: (<myAttribute-oid>)
```

Подробная информация об этой команде приведена в разделе “ldapmodify и ldapadd” на стр. 203.

## Копирование схемы на другие серверы

Для копирования схемы на другие серверы выполните следующие действия:

1. С помощью утилиты ldapsearch скопируйте схему в файл:

   ```
   ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
   ```

2. Файл схемы будет содержать все классы объектов и атрибуты. Отредактируйте файл LDIF, включив в него только требуемые элементы схемы, либо отфильтруйте вывод команды ldapsearch с помощью какой-либо утилиты типа grep. Помните, что атрибуты должны находиться перед ссылающимися на них классами объектов. В результате может получиться, например следующий файл (обратите внимание, что в конце каждой продолжающейся строки находится один пробел, а в начале каждой продолжающей строки находится не менее одного пробела).

   ```
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Some piece of
     information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
     ACCESS-CLASS normal LENGTH 500 )
   attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Some piece of
     information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
     ACCESS-CLASS normal LENGTH 500 )
   objectclasses: ( myobject-oid NAME 'myobject' DESC 'Represents
     something.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
   ```

3. Перед каждой строкой objectclasses и attributetype вставьте строки с директивами LDIF, добавляющими эти значения в запись cn=schema. Каждый класс объектов и каждый атрибут должен добавляться с помощью отдельной операции.

   ```
   dn: cn=schema
   changetype: modify
   add: attributetypes ibmattributetypes
   attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Some piece of
     information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
     ACCESS-CLASS normal LENGTH 500 )
   ```

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Some piece of
  information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
  USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
  ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Represents
  something.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Загрузите схему на другой сервер с помощью утилиты ldapmodify:

```
ldapmodify -D cn=administrator -w <пароль> -f schema.ldif
```

## Управление записями каталога

Для управления записями каталога разверните в области навигации Web-инструмента администрирования категорию **Управление каталогами**.

Дополнительная информация приведена в следующих разделах:



## Просмотр дерева

Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом** и выберите опцию **Управление записями**.Вы можете разворачивать ветки поддерева и выбирать записи для работы. Выберите на панели инструментов операцию, которую необходимо выполнить.

## Добавление записи

Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом**.

1. Нажмите кнопку **Добавить запись**.
2. Выберите в списке **Структурный класс объектов**.
3. Нажмите кнопку **Далее**.
4. Выберите в списке **Доступные** нужные **Вспомогательные классы объектов** и нажмите кнопку **Добавить**. Повторите эту операцию для всех добавляемых вспомогательных классов. Вы также можете удалить вспомогательный класс объектов из списка **Выбранные**, выделив его имя и нажав кнопку **Удалить**.
5. Нажмите кнопку **Далее**.

6. В поле **Относительное DN** укажите относительное отличительное имя (RDN) добавляемой записи; например, cn=John Doe.
7. В поле **Родительское DN** укажите отличительное имя выбранной записи дерева, например, ou=Austin, o=IBM. Вы также можете нажать кнопку **Обзор** и выбрать в списке нужное родительское DN. Вы также можете развернуть выбранную ветвь и выбрать запись, находящуюся на более низком уровне иерархии. Сделайте выбор и нажмите кнопку **Выбрать**, чтобы указать родительское DN. По умолчанию в качестве **Родительского DN** применяется выбранная запись.

   **Примечание:** Если вы перешли к этой панели из окна **Управление записями**, то значение в этом поле уже будет указано.
8. На вкладке **Обязательные атрибуты** укажите значения обязательных атрибутов. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.
9. Выберите **Дополнительные атрибуты**.
10. На вкладке **Дополнительные атрибуты** введите значения необязательных атрибутов. Информация о добавлении двоичных значений приведена в разделе “Изменение двоичных атрибутов” на стр. 185. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.
11. Для создания записи нажмите OK.
12. Для изменения списка управления доступом для записи нажмите кнопку **ACL**. Информация об ACL приведена в разделе “Списки управления доступом” на стр. 60.
13. После заполнения всех обязательных полей нажмите кнопку **Добавить** для добавления новой записи или кнопку **Отмена** для возврата к окну **Просмотр дерева каталогов** без внесения изменений.

## Добавление записи, содержащей языковые теги

Для того чтобы клиенты могли осуществлять в каталоге поиск значений на нескольких языках, можно связать с записями в каталоге языковые коды. Языковой тег входит в состав определения атрибута. Дополнительная информация о языковых тегах приведена в разделе “Языковые теги” на стр. 48.

Для включения поддержки языковых тегов выполните следующие действия (по умолчанию языковые теги отключены):

1. В области навигации разверните категорию **Администрирование сервера** и выберите **Управление свойствами сервера**.

   **Примечание:** Для изменения параметров конфигурации сервера с помощью задач категории Администрирование сервера Web-инструмента администрирования следует войти на сервер с профайлом пользователя i5/OS, в котором указаны специальные права *ALLOBJ и IOSYSCFG. Для этого можно идентифицироваться в качестве спроецированного пользователя с паролем для этого профайла. Для подключения в качестве спроецированного пользователя из Web-инструмента администрирования введите имя пользователя формы `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, подставив вместо MYUSERNAME и MYSYSTEM.COM имя вашего пользовательского профайла и настроенный суффикс защиты системы соответственно.
2. По умолчанию активна вкладка Общие. Включите переключатель **Разрешить поддержку языковых тегов**.

   **Примечание:** После включения поддержки языковых тегов, если с атрибутами записи будут связаны языковые теги, то сервер будет возвращать записи с этими тегами. Такое поведение сохранится даже если вы позже отключите поддержку языковых тегов. Так как сервер может повести себя не так, как ожидает приложение, то во избежание возможных неполадок не отключайте компонент языковых тегов после того как он был включен.

Для создания записи, содержащей атрибуты с языковыми тегами, выполните следующие действия:

1. В области навигации разверните категорию **Управление каталогом** и выберите **Управление записями**.

2. Нажмите **Изменить атрибуты**.
3. Выберите атрибут, для которого требуется создать языковой тег.
4. Нажмите **Значение языкового тега**. Появится окно **Значения языковых тегов**.
5. В поле **Языковой тег** введите имя создаваемого тега. Оно должно начинаться с суффикса lang-.
6. В поле **Value** введите значение тега.
7. Нажмите кнопку **Добавить**.Языковой тег и его значение появится в соответствующем списке.
8. Повторите шаги 3, 4 и 5 для создания дополнительных тегов или изменения существующих. По окончании создания необходимых языковых тегов нажмите **OK**.
9. Выберите языковой тег в меню **Отображать с языковым тегом**. Нажмите **Изменить вид**, и в списке отобразятся значения атрибутов для этого языкового тега. Значения, которые вы добавляете или изменяете в этом окне, будут применены только для выбранного тега.
10. По окончании нажмите **OK**.

## Удаление записи

Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом** и выберите опцию **Управление записями**.Вы можете разворачивать ветки поддерева и выбирать записи для работы. Нажмите кнопку **Удалить** на панели инструментов справа.

- Операцию удаления необходимо подтвердить. Нажмите кнопку **OK**.
- Запись будет удалена из каталога, после чего появится список записей.

## Редактирование записи

Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом** и выберите опцию **Управление записями**.Вы можете разворачивать ветки поддерева и выбирать записи для работы. Нажмите кнопку **Редактировать атрибуты** на панели инструментов справа.

1. На вкладке **Обязательные атрибуты** укажите значения обязательных атрибутов. Информация о добавлении двоичных значений приведена в разделе “Изменение двоичных атрибутов” на стр. 185. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.
2. Выберите **Дополнительные атрибуты**.
3. На вкладке **Дополнительные атрибуты** введите значения необязательных атрибутов. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.
4. Нажмите кнопку **Группы**.
5. Если вы создали группы, то на вкладке **Группы** выполните следующие действия:
   - Выберите группу в списке **Доступные группы** и нажмите **Добавить**, чтобы включить запись в состав выбранной **Статистической группы**.
   - Выберите группу в списке **Статических групп** и нажмите кнопку **Удалить** для исключения записи из выбранной группы.
6. Если запись соответствует группе, то будет показана вкладка **Элементы**. На вкладке **Элементы** перечислены элементы выбранной группы. Вы можете добавлять и удалять членов группы.
   - Для добавления элемента в группу:
     a. Щелкните на значке **Нескольких значений** рядом со вкладкой **Элементы**, либо на вкладке **Элементы** выберите опцию **Элементы**.
     b. В поле Элемент укажите DN элемента, добавляемого в группу.
     c. Нажмите кнопку **Добавить**.
     d. Нажмите кнопку **OK**.
   - Для удаления элемента из группы:
     a. Щелкните на значке **Несколько значений** рядом со вкладкой **Элементы**, либо выберите опцию **Элементы** на вкладке **Элементы**.

b. Выберите запись для удаления.
c. Нажмите кнопку **Удалить**.
d. Нажмите кнопку **OK**.

- Для обновления списка элементов группы нажмите кнопку **Обновить**.

7. Для изменения записи нажмите **OK**.

## Копирование записи

Эта функция полезна при создании похожих записей. При копировании наследуются все атрибуты оригинала. Вам необходимо лишь изменить имя новой записи.

Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом** и выберите опцию **Управление записями**.Он позволяет разворачивать ветки поддерева и выбирать записи для работы, например, вы можете выбрать запись John Doe. Нажмите кнопку **Скопировать** на панели инструментов справа.

- Измените RDN записи в поле DN. Например, измените cn=John Doe на cn=Jim Smith.
- На вкладке обязательных атрибутов измените cn записи в соответствии с новом RDN. В нашем примере это Jim Smith.
- Измените остальные обязательные атрибуты. В данном примере следует изменить атрибут sn с Doe на Smith.
- После внесения всех требуемых изменений нажмите **OK** для создания новой записи.
- В нижнюю часть списка записей будет добавлена новая запись Jim Smith.

**Примечание:** Эта процедура копирует только атрибуты записи. Сведения о членстве исходной записи в группах не копируются. Для включения записи в состав групп нажмите кнопку Редактировать атрибуты.

## Редактирование списков управления доступом

Для просмотра свойств ACL с помощью Web-инструмента администрирования и работы с ACL ознакомьтесь с разделом “Управление списками управления доступом (ACL)” на стр. 197.

Дополнительная информация приведена в разделе “Списки управления доступом” на стр. 60.

## Добавление вспомогательного класса объектов

Для добавления к существующей записи каталога вспомогательного класса нажмите кнопку панели инструментов **Добавить вспомогательный класс**. Вспомогательный класс содержит дополнительные атрибуты записи, к которой он добавляется.

Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом** и выберите опцию **Управление записями**.Он позволяет разворачивать ветки поддерева и выбирать записи для работы, например, вы можете выбрать запись John Doe. Нажмите кнопку **Добавить вспомогательный класс** на панели инструментов справа.

1. Выберите в списке **Доступные** нужные **Вспомогательные классы объектов** и нажмите кнопку **Добавить**. Повторите эту операцию для всех добавляемых вспомогательных классов. Вы также можете удалить вспомогательный класс объектов из списка **Выбранные**, выделив его имя и нажав кнопку **Удалить**.
2. На вкладке **Обязательные атрибуты** укажите значения обязательных атрибутов. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.
3. Выберите **Дополнительные атрибуты**.
4. На вкладке **Дополнительные атрибуты** введите значения необязательных атрибутов. Если необходимо добавить несколько значений атрибута, то щелкните на значке **Многозначный атрибут** и перечислите значения по одному в строке.

5. Нажмите кнопку **Группы**.
6. Если вы создали группы, то на вкладке **Группы** выполните следующие действия:
   - Выберите группу в списке **Доступные группы** и нажмите **Добавить**, чтобы включить запись в состав выбранной **Статистической группы**.
   - Выберите группу в списке **Статических групп** и нажмите кнопку **Удалить** для исключения записи из выбранной группы.
7. Для изменения записи нажмите **OK**.

## Удаление вспомогательного класса

Несмотря на то, что удалить вспомогательный класс можно с помощью процедуры добавления вспомогательного класса, для удаления из записи отдельного вспомогательного класса проще будет воспользоваться функцией удаления вспомогательного класса. Однако, если вы хотите удалить из записи несколько вспомогательных классов, то удобней будет воспользоваться процедурой добавления вспомогательного класса.

1. Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом** и выберите опцию **Управление записями**.Он позволяет разворачивать ветки поддерева и выбирать записи для работы, например, вы можете выбрать запись John Doe. Нажмите кнопку **Удалить вспомогательный класс** на панели инструментов справа.
2. В списке вспомогательных классов выберите класс для удаления и нажмите кнопку **OK**.
3. При появлении просьбы подтвердить удаление нажмите **OK**.
4. Вспомогательный класс будет удален и появится список записей.

Повторите эту операцию для каждого удаляемого вспомогательного класса.

## Изменение членства в группах

Если вы еще не сделали этого, разверните в области навигации категорию **Управление каталогом**.

1. Выберите опцию **Управление записями**.
2. Выберите пользователя в дереве каталогов и нажмите на панели инструментов кнопку **Изменить атрибуты**.
3. Перейдите на вкладку **Группы**.
4. Теперь вы можете изменить список групп, в состав которых входит пользователь. В окне **Изменить членство в группах** показан список **Доступных групп**, в которые можно добавить пользователя, и список **Статических групп**, состав которых входит выбранная запись.
   - Выберите группу в списке **Доступные группы** и нажмите **Добавить**, чтобы включить запись в состав выбранной группы.
   - Выберите группу в списке **Статические группы** и нажмите кнопку **Удалить** для исключения записи из выбранной группы.
5. Нажмите **OK** для сохранения внесенных изменений или **Отмена** для возврата к предыдущему окну без сохранения изменений.

## Поиск записей каталога

Существует три способа поиска информации в дереве каталога:

- Простой поиск с помощью заранее определенного набора условий
- Расширенный поиск с помощью пользовательского набора условий
- Поиск вручную

Для работы с опциями поиска разверните в области навигации категорию **Управление каталогом** и выберите опцию **Поиск записей**. Выберите вкладку **Фильтры поиска** или **Опции**.

**Примечание:** Поиск по двоичным значениям, например, по паролям, невозможен.

**Фильтры поиска**

Выберите один из следующих типов поиска:

**Простой поиск**

При простом поиске применяются условия поиска по умолчанию:

- Основной DN - **Все суффиксы**
- Область поиска - **Поддерево**
- Объем поиска **Не ограничен**
- Ограничение времени - **Не ограничено**
- Учет псевдонимов - **Нет**
- Переадресация - Выключена

Для выполнения простого поиска:

1. На вкладке **Фильтр поиска** выберите опцию **Простой поиск**.
2. Выберите в списке класс объектов.
3. Выберите атрибут типа записи. Если нужно найти записи с заданным атрибутом, то выберите его в выпадающем списке и введите значение в поле **равен**. Если атрибут не указан, то будут найдены все записи заданного типа.

**Расширенный поиск**

Расширенный поиск позволяет указать ограничения и воспользоваться фильтрами поиска. Для применения условий поиска по умолчанию воспользуйтесь простым поиском.

- Для выполнения расширенного поиска:
  1. На вкладке **Фильтр поиска** выберите опцию **Расширенный поиск**.
  2. Выберите в списке **Атрибут**.
  3. Выберите оператор **Сравнения**.
     - = Атрибут равен указанному значению.
     - ! Атрибут не равен указанному значению.
     - < Атрибут меньше или равен указанному значению.
     - > Атрибут больше или равен указанному значению.
     - ~ Атрибут примерно равен указанному значению.
  4. Введите **Значение** для сравнения.
  5. Для задания сложных запросов воспользуйтесь кнопками операторов.
     - Если вы уже указали первый фильтр поиска, то укажите дополнительный критерий и нажмите **И**. Предикат **И** возвращает записи, удовлетворяющие всем заданным условиям.
     - Если вы уже указали фильтр поиска, то укажите дополнительный критерий и нажмите **ИЛИ**. Предикат **ИЛИ** возвращает записи, удовлетворяющие хотя бы одному из указанных критериев.
  6.
     - Нажмите **Добавить** для добавления фильтра поиска.
     - Нажмите **Удалить** для удаления фильтра поиска.
     - Нажмите **Сбросить** для очистки фильтров поиска.

**Поиск вручную**

Поиск вручную позволяет задать фильтр поиска. Например, для поиска по фамилии укажите `sn=*`. При поиске по нескольким атрибутам следует применять синтаксис фильтра поиска. Например, для поиска по фамилии сотрудников из определенного отдела введите:

`(&(sn=*)(dept=<отдел>))`

**Опции**

На вкладке **Опции**:

- **Базовое DN для поиска** - Для поиска только в пределах одного суффикса выберите в списке нужный суффикс.

  **Примечание:** Если вы перешли к этой панели из окна **Управление записями**, то значение в этом поле уже будет указано. Вы выбрали **Родительское DN** перед нажатием кнопки **Добавить**.

  Для поиска во всем дереве вы можете также выбрать опцию **Все суффиксы**.

  **Примечание:** Поиск в поддереве с параметром **Все суффиксы** не возвращает ни информацию о схеме, ни данные протокола изменений, ни сведения от спроецированной базы данных системы.
- **Область поиска**
  - Для поиска только в пределах одного объекта выберите **Объект**.
  - Для поиска только среди непосредственных потомков определенного объекта выберите **Один уровень**.
  - Для поиска среди всех потомков определенной записи выберите **Поддерево**.
- **Ограничение объема поиска** - Введите максимальное число записей или укажите **Не ограничено**.
- **Ограничение времени поиска** - Введите максимальное время поиска (в секундах) или укажите **Не ограничено**.
- Выберите в списке способ **Учета псевдонимов**.
  - **Никогда** - Если выбранная запись - псевдоним, то она не будет учитываться при поиске, то есть ссылка на псевдоним будет проигнорирована.
  - **Найти** - Если выбранная запись - псевдоним, то она будет учтена при поиске, и поиск будет продолжен в поддереве псевдонима.
  - **Просмотреть** - Выбранная запись не будет учитываться, но поиск будет продолжен в поддереве.
  - **Всегда** - Будут учитываться все псевдонимы.
- Отметьте переключатель **Переадресация**, если при поиске следует переходить по ссылкам на другие серверы. При переходе по ссылке на другой сервер применяются текущие права доступа. Если вы вошли в систему как Anonymous, то вам может потребоваться повторно подключиться к серверу, указав DN с достаточными правами доступа.

Дополнительная информация о поиске приведена в разделе “Настройка параметров поиска” на стр. 136.

## Изменение двоичных атрибутов

Если атрибут должен содержать двоичные данные, то рядом с полем будет показана кнопка **Двоичные данные**. Если атрибут не содержит данные, то поле будет пустым. Поскольку показать данные двоичного атрибута невозможно, то при наличии таких данных будет показана строка **Двоичные данные - 1**. Если атрибут содержит несколько значений, то будет показан список.

Для работы с двоичными атрибутами щелкните на значке **Двоичные данные**.

Вы можете импортировать, экспортировать и удалять двоичные данные.

Для добавления к атрибуту двоичных данных:

1. Нажмите кнопку **Двоичные данные**.
2. Нажмите кнопку **Импортировать**.

3. Вы можете указать полное имя файла или нажать кнопку **Обзор** и найти требуемый двоичный файл.
4. Нажмите кнопку **Передать файл**. Будет показано сообщение `Файл загружен`.
5. Нажмите кнопку **Закрыть**. В разделе **Записи двоичных данных** будет показана строка **Двоичные данные - 1**.
6. Повторите импорт для требуемого числа двоичных файлов. Последующие записи будут показаны как **Двоичные данные - 2**, **Двоичные данные -3** и т.д.
7. После того как вы завершите добавление данных, нажмите кнопку **OK**.

Для экспорта двоичных данных:

1. Нажмите кнопку **Двоичные данные**.
2. Нажмите кнопку **Экспортировать**.
3. Выберите ссылку **Двоичные данные для загрузки**.
4. Выполните инструкции мастера для просмотра двоичного файла или его сохранения на локальном диске.
5. Нажмите кнопку **Закрыть**.
6. Повторите экспорт для требуемого числа двоичных файлов.
7. После того как вы завершите экспорт данных, нажмите кнопку **OK**.

Для удаления двоичных данных:

1. Нажмите кнопку **Двоичные данные**.
2. Выберите файл с двоичными данными для удаления. Можно выбрать сразу несколько файлов.
3. Нажмите кнопку **Удалить**.
4. При появлении просьбы подтвердить операцию нажмите **OK**. Выбранные двоичные данные будут удалены из списка.
5. После того как вы завершите удаление данных, нажмите кнопку **OK**.

**Примечание:** Поиск по двоичным атрибутам возможен только при их наличии.

---

# Управление пользователями и группами

Для управления пользователями и группами разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

Дополнительная информация приведена в следующих разделах:

- “Управление пользователями”
- “Управление группами” на стр. 188

# Управление пользователями

После настройки областей и шаблонов вы можете начать создавать пользователей каталога. Подробные сведения можно найти в следующих разделах:

- “Добавление пользователей”
- “Поиск пользователей в области” на стр. 187
- “Редактирование информации о пользователе” на стр. 187
- “Копирование пользователя” на стр. 187
- “Удаление пользователя” на стр. 187

## Добавление пользователей

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Добавить пользователя** или перейдите в раздел **Управление пользователями** и нажмите кнопку **Добавить**.
2. Выберите в списке область, в которую вы хотите добавить пользователя.

3. Нажмите кнопку **Далее**. Будет показан связанный с выбранной областью шаблон. Заполните обязательные поля, обозначенные звездочкой (*), а также другие поля, которые сочтете нужными. Если вы уже создали в области какие-либо группы, то вы можете также добавить пользователя в одну или несколько групп.
4. После завершения ввода нажмите кнопку **Готово**.

## Поиск пользователей в области

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Найти пользователя** или перейдите в раздел **Управление пользователями** и нажмите кнопку **Найти**.
2. В списке **Выберите область** укажите область, в которой необходимо выполнить поиск.
3. В поле **Атрибут присвоения имен** задайте строку поиска. Поддерживаются символы подстановки, т.е. при вводе строки ***smith** будут найдены все записи, в которых атрибут присвоения имен заканчивается символами smith.
4. Над выбранным пользователем можно выполнить следующие операции:
   - **Редактирование** - см. раздел “Редактирование информации о пользователе”.
   - **Копирование** - см. раздел “Копирование пользователя”.
   - **Удаление** - см. раздел “Удаление пользователя”.
5. После завершения ввода нажмите **OK**.

## Редактирование информации о пользователе

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Управление пользователями**.
2. Выберите в списке область. Если пользователи не показаны в списке **Пользователи**, выберите опцию **Показать пользователей**.
3. Выберите пользователя для редактирования и нажмите кнопку **Редактировать**.
4. Измените показанную на вкладках информацию и сведения о членстве в группах.
5. После завершения ввода нажмите **OK**.

## Копирование пользователя

Если вам нужно создать большое количество пользователей с почти одинаковыми характеристиками, то для создания новых пользователей вы можете копировать уже имеющегося пользователя и изменять информацию о нем.

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Управление пользователями**.
2. Выберите в списке область. Если пользователи не показаны в списке **Пользователи**, выберите опцию **Показать пользователей**.
3. Выберите пользователя для копирования и нажмите кнопку **Скопировать**.
4. Измените информацию о новом пользователе, в частности, обязательную информацию, идентифицирующую каждого пользователя, например, sn или cn. Информацию, одинаковую для обоих пользователей, изменять не нужно.
5. После завершения ввода нажмите **OK**.

## Удаление пользователя

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Управление пользователями**.
2. Выберите в списке область. Если пользователи не показаны в списке **Пользователи**, выберите опцию **Показать пользователей**.
3. Выберите пользователя для удаления и нажмите кнопку **Удалить**.
4. При появлении просьбы подтвердить операцию нажмите **OK**.

5. Пользователь будет удален из списка.

# Управление группами

После настройки областей и шаблонов вы можете начать создавать группы. Подробные сведения можно найти в следующих разделах:

- “Добавление групп”
- “Поиск групп в области”
- “Редактирование информации о группе”
- “Копирование группы”
- “Удаление группы” на стр. 189

## Добавление групп

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Добавить группу** или перейдите в раздел **Управление группами** и нажмите кнопку **Добавить**.
2. В поле Имя группы ограничения поиска введите имя создаваемой группы.
3. Выберите в списке область, в которую вы хотите добавить группу.
4. Для создания группы нажмите кнопку **Готово**. Если в группе уже есть пользователи, то вы можете нажать кнопку **Далее** и выбрать пользователей для добавления в новую группу. После этого нажмите кнопку **Готово**.

Дополнительная информация приведена в разделе “Группы и роли” на стр. 53.

## Поиск групп в области

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Найти группу** или перейдите в раздел **Управление группами** и нажмите кнопку **Найти**.
2. В списке **Выберите область** укажите область, в которой необходимо выполнить поиск.
3. В поле **Атрибут присвоения имен** задайте строку поиска. Поддерживаются символы подстановки, т.е. при вводе строки ***club** будут найдены все записи, в которых атрибут присвоения имен заканчивается символами club, например, ’book club’, ’chess club’, ’garden club’ и т.д.
4. Над выбранной группой можно выполнить следующие операции:
   - **Редактирование** - см. раздел “Редактирование информации о группе”.
   - **Копирование** - см. раздел “Копирование группы”.
   - **Удаление** - см. раздел “Удаление группы” на стр. 189.
5. После завершения работы нажмите кнопку **Закрыть**.

## Редактирование информации о группе

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Управление группами**.
2. Выберите в списке область. Если группы не показаны в списке **Группы**, выберите опцию **Показать группы**.
3. Выберите группу для редактирования и нажмите кнопку **Редактировать**.
4. Нажав кнопку **Фильтр**, вы можете ограничить количество пользователей, показанных в списке **Доступные пользователи**. Например, если ввести *smith в поле фамилии, то будут показаны только те пользователи, фамилия которых заканчивается символами smith, например, Ann Smith, Bob Smith, Joe Goldsmith и т.д.
5. Вы можете добавлять и удалять членов группы.
6. После завершения ввода нажмите **OK**.

## Копирование группы

Если вам нужно создать большое количество групп с почти одинаковым составом, то для создания новых групп вы можете копировать уже существующую группу и изменять информацию о ней.

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Управление группами**.
2. Выберите в списке область. Если группы не показаны в списке **Группы**, выберите опцию **Показать группы**.
3. Выберите группу для копирования и нажмите кнопку **Скопировать**.
4. Измените имя группы, показанное в поле **Имя группы**. В состав новой группы будут входить те же элементы, что и в состав исходной группы.
5. Вы можете изменять элементы группы.
6. После завершения ввода нажмите **OK**. Будет создана новая группа, которая будет содержать все элементы исходной группы, а также будет учитывать все изменения, внесенные во время копирования.

### Удаление группы

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Выберите опцию **Управление группами**.
2. Выберите в списке область. Если группы не показаны в списке **Группы**, выберите опцию **Показать группы**.
3. Выберите группу для удаления и нажмите кнопку **Удалить**.
4. При появлении просьбы подтвердить операцию нажмите **OK**.
5. Группа будет удалена из списка.

## Управление областями и шаблонами пользователей

Для управления областями и шаблонами пользователей разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**. Области и шаблоны пользователей упрощают ввод данных в каталог. Дополнительная информация об областях и группах приведена в разделе “Области и шаблоны пользователей” на стр. 46.

Дополнительная информация приведена в следующих разделах:

- “Создание области”
- “Создание администратора области” на стр. 190
- “Создание шаблона” на стр. 191
- “Добавление шаблона в область” на стр. 192
- “Создание групп” на стр. 192
- “Добавление пользователя в область” на стр. 193
- “Управление областями” на стр. 193
- “Управление шаблонами” на стр. 194

## Создание области

Дополнительная информация об областях и группах приведена в разделе “Области и шаблоны пользователей” на стр. 46.

Для создания области выполните следующие действия:

1. Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.
2. Нажмите кнопку **Добавить область**.
   - Введите имя области. Например: **realm1**.
   - Введите родительский DN, идентифицирующий расположение области. Это должна быть запись в формате суффикса, например, o=ibm,c=us. Эта запись может быть суффиксом или произвольной записью каталога. Вы также можете нажать кнопку **Обзор** и выбрать в списке нужное расположение.
3. Нажмите кнопку **Далее** для продолжения или кнопку **Готово** для выполнения операции.
4. Если вы нажали кнопку **Далее**, то просмотрите показанную информацию. Область еще не создана, поэтому значения **Шаблона пользователей** и **Фильтра поиска пользователей** можно проигнорировать.

5. Для создания области нажмите кнопку **Готово**.

## Создание администратора области

Для создания администратора области необходимо сначала создать для области группу администраторов:

1. Создайте группу администраторов области.
   a. Разверните в области навигации Web-инструмента администрирования категорию **Управление каталогом**.
   b. Выберите опцию **Управление записями**.
   c. Разверните дерево и выберите только что созданную область **cn=realm1,o=ibm,c=us**.
   d. Нажмите кнопку **Редактировать ACL**.
   e. Перейдите на вкладку **Владельцы**.
   f. Обязательно отметьте переключатель **Наследовать владельца**.
   g. Введите DN области **cn=realm1,o=ibm,c=us**.
   h. В качестве **Типа** укажите значение Группа.
   i. Нажмите кнопку **Добавить**.
2. Создайте запись администратора. Если вы еще не создали запись администратора, то создайте ее сейчас.
   a. Разверните в области навигации Web-инструмента администрирования категорию **Управление каталогом**.
   b. Выберите опцию **Управление записями**.
   c. Разверните дерево до той ветви, где должна находиться запись администратора.

      **Примечание:** Размещение записи администратора вне области позволяет избежать ситуации, в которой администратор может случайно удалить себя. В данном примере можно выбрать, например, ветвь **o=ibm,c=us**.
   d. Нажмите кнопку **Добавить**.
   e. Выберите **Структурный класс объектов**, например, **inetOrgPerson**.
   f. Нажмите кнопку **Далее**.
   g. Выберите вспомогательный класс объектов, который необходимо добавить.
   h. Нажмите кнопку **Далее**.
   i. Введите обязательные атрибуты записи. Например:
      - **RDN** cn=JohnDoe
      - **DN** o=ibm,c=us
      - **cn** John Doe
      - **sn** Doe
   j. На вкладке **Прочие атрибуты** обязательно укажите пароль.
   k. После завершения ввода нажмите кнопку **Готово**.
3. Добавьте администратора в группу администраторов.
   a. Разверните в области навигации Web-инструмента администрирования категорию **Управление каталогом**.
   b. Выберите опцию **Управление записями**.
   c. Разверните дерево и выберите только что созданную область **cn=realm1,o=ibm,c=us**.
   d. Нажмите кнопку **Изменить атрибуты**.
   e. Щелкните на вкладке **Элементы**.
   f. Выберите опцию **Элементы**.
   g. В поле **Элементы** введите DN администратора. В нашем примере это **cn=John Doe,o=ibm,c=us**.
   h. Нажмите кнопку **Добавить**. DN будет показано в списке **Элементы**.

i. Нажмите кнопку **OK**.

j. Нажмите кнопку **Обновить**. DN будет показано в списке **Текущие элементы**.

k. Нажмите кнопку **OK**.

4. Вы создали администратора, который сможет управлять записями этой области.

## Создание шаблона

Следующим шагом после создания области является создание шаблона пользователя. Шаблон позволяет упорядочить информацию, которую необходимо вводить. Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

1. Нажмите кнопку **Добавить шаблон пользователя**.
   - Укажите имя шаблона, например, **template1**.
   - Укажите расположение, в котором должен находиться шаблон. Для копирования поместите шаблон в то же поддерево области, в котором этот шаблон будет применяться. В нашем примере создана область **cn=realm1,o=ibm,c=us**. Вы также можете нажать кнопку **Обзор** и выбрать в списке нужное расположение шаблона.
2. Нажмите кнопку **Далее**. Для создания пустого шаблона можно нажать кнопку **Готово**. В дальнейшем вы сможете добавить информацию в шаблон. См. раздел “Редактирование шаблона” на стр. 196.
3. Если вы нажали кнопку **Далее**, то выберите для шаблона структурный класс объектов, например, **inetOrgPerson**. Вы также можете добавить любые вспомогательные классы объектов.
4. Нажмите кнопку **Далее**.
5. Для шаблона будет создана вкладка **Обязательные**. Вы можете изменить показанную на этой вкладке информацию.
   a. Выберите в меню вкладки пункт **Обязательные** и нажмите кнопку **Редактировать**.Будет показана панель **Редактировать вкладку**. Будет показано имя вкладки **Обязательные** и выбранные атрибуты, которые являются обязательными для класса объектов **inetOrgPerson**:
      - *sn - фамилия
      - *cn - общее имя

      **Примечание:** Звездочка (*) означает обязательную информацию.
   b. Если вы хотите добавить на эту вкладку дополнительную информацию, то выберите в меню **Атрибуты** нужный атрибут. Например, выберите **departmentNumber** и нажмите кнопку **Добавить**.Выберите **employeeNumber** и нажмите кнопку **Добавить**. Выберите **title** и нажмите кнопку **Добавить**. Теперь список **Выбранные атрибуты** будет выглядеть следующим образом:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Вы можете изменить расположение полей шаблона. Для этого выберите атрибут и нажмите кнопку **Вверх** или **Вниз**. При этом положение атрибута будет изменено на единицу. Повторите процедуру нужное число раз, разместив все атрибуты в требуемом порядке. Например:
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Вы можете также изменить каждый выделенный атрибут.
      1) Выделите атрибут в списке **Выбранные атрибуты** и нажмите кнопку **Редактировать**.

2) Вы можете изменить отображаемое в шаблоне имя атрибута. Например, если вы хотите, чтобы для атрибута **departmentNumber** была показана строка **Номер отдела**, то укажите эту строку в поле **Отображаемое имя**.
3) Вы можете также указать значение по умолчанию, которое будет указываться в поле атрибута в шаблоне. Например, если большинство пользователей, информацию о которых вы будете вводить, относятся к отделу 789, то в качестве значения по умолчанию можно указать 789. В поле шаблона для атрибута будет заранее указываться значение 789. Это значение можно изменить при вводе фактической информации о пользователе.
4) Нажмите кнопку **OK**.

e. Нажмите кнопку **OK**.

6. Для создания еще одной категории вкладки с дополнительной информацией нажмите кнопку **Добавить**.
   - Введите имя вкладки. Например: Адрес.
   - В меню **Атрибуты** выберите атрибуты для этой вкладки. Например, выберите **homePostalAddress** и нажмите кнопку **Добавить**. Выберите **postOfficeBox** и нажмите кнопку **Добавить**. Выберите **telephoneNumber** и нажмите кнопку **Добавить**.Выберите **homePhone** и нажмите кнопку **Добавить**. Выберите **facsimileTelephoneNumber** и нажмите кнопку **Добавить**. Теперь список **Выбранные атрибуты** будет выглядеть следующим образом:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Вы можете изменить расположение полей шаблона. Для этого выберите атрибут и нажмите кнопку **Вверх** или **Вниз**. При этом положение атрибута будет изменено на единицу. Повторите процедуру нужное число раз, разместив все атрибуты в требуемом порядке. Например:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber
     – homePhone
   - Нажмите кнопку **OK**.
7. Повторите процесс, чтобы добавить все необходимые вкладки. После завершения ввода нажмите кнопку **Готово** для создания шаблона.

## Добавление шаблона в область

После создания области и шаблона необходимо добавить шаблон в область. Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

1. Выберите опцию **Управление областями**.
2. Выберите область для добавления шаблона, например, **cn=realm1,o=ibm,c=us**, и нажмите кнопку **Редактировать**.
3. Пролистайте меню до пункта **Шаблон пользователей** и разверните меню.
4. Выберите шаблон, например, **cn=template1,cn=realm1,o=ibm,c=us**.
5. Нажмите кнопку **OK**.
6. Нажмите кнопку **Закрыть**.

## Создание групп

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Нажмите кнопку **Добавить группу**.

2. В поле Имя группы ограничения поиска введите имя создаваемой группы. Например, **group1**.
3. Выберите в списке область, в которую вы хотите добавить пользователя. В нашем примере это **realm1**.
4. Для создания группы нажмите кнопку **Готово**. Если в области уже есть пользователи, то вы можете нажать кнопку **Далее** и выбрать пользователей для добавления в группу group1. После этого нажмите кнопку **Готово**.

Дополнительная информация приведена в разделе “Группы и роли” на стр. 53.

## Добавление пользователя в область

Разверните в области навигации Web-инструмента администрирования категорию **Пользователи и группы**.

1. Нажмите кнопку **Добавить пользователя**.
2. Выберите в списке область, в которую вы хотите добавить пользователя. В нашем примере это **realm1**.
3. Нажмите кнопку **Далее**. Будет показан только что созданный шаблон template1. Заполните обязательные поля, обозначенные звездочкой (*), а также другие поля, которые сочтете нужными. Если вы уже создали в области какие-либо группы, то вы можете также добавить пользователя в одну или несколько групп.
4. После завершения ввода нажмите кнопку **Готово**.

## Управление областями

После настройки и заполнения области вы можете добавить новые области или изменить уже существующие.

Разверните в области навигации категорию **Области и шаблоны** и выберите опцию **Управление областями**. Будет показан список существующих областей. С помощью этой панели вы можете добавить, изменить или удалить область, а также изменить список управления доступом (ACL) для области. Дополнительная информация приведена в следующих разделах:

- “Добавление области”
- “Редактирование области”
- “Удаление области” на стр. 194
- “Редактирование ACL области” на стр. 194

### Добавление области

Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

1. Нажмите кнопку **Добавить область**.
   - Введите имя области. Например: **realm2**.
   - Если вы уже создали какие-либо области, например, **realm1**, то для копирования параметров существующей области в новую вы можете выбрать одну из уже созданных областей.
   - Введите родительский DN, идентифицирующий расположение области. Это должна быть запись в формате суффикса, например, **o=ibm,c=us**. Вы также можете нажать кнопку **Обзор** и выбрать в списке нужное расположение.
2. Нажмите кнопку **Далее** для продолжения или кнопку **Готово** для выполнения операции.
3. Если вы нажали кнопку **Далее**, то просмотрите показанную информацию.
4. Выберите в списке **Шаблон пользователя**. Если вы скопировали параметры существующей области, то в этом поле будет указан ее шаблон.
5. Введите **Фильтр поиска пользователей**.
6. Для создания области нажмите кнопку **Готово**.

### Редактирование области

Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

- Выберите опцию **Управление областями**.
- Выберите в списке область для редактирования.

- Нажмите кнопку **Редактировать**.
  - С помощью кнопок **Обзор** вы можете изменить следующие значения:
    - Группа администраторов
    - Контейнер групп
    - Контейнер пользователей
  - Вы можете выбрать в списке другой шаблон.
  - Для изменения **Фильтра поиска пользователей** нажмите **Изменить**.
- После внесения изменений нажмите кнопку **OK**.

### Удаление области

Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

1. Выберите опцию **Управление областями**.
2. Выберите область для удаления.
3. Нажмите кнопку **Удалить**.
4. При появлении просьбы подтвердить операцию нажмите **OK**.
5. Область будет удалена из списка.

### Редактирование ACL области

Для просмотра свойств ACL с помощью Web-инструмента администрирования и работы с ACL ознакомьтесь с разделом “Управление списками управления доступом (ACL)” на стр. 197.

Дополнительная информация приведена в разделе “Списки управления доступом” на стр. 60.

## Управление шаблонами

После создания первого шаблона вы можете создавать новые и изменять уже существующие шаблоны.

Разверните в области навигации категорию **Области и шаблоны** и выберите опцию **Управление шаблонами пользователей**. Будет показан список существующих шаблонов. С помощью этой панели вы можете добавить, изменить или удалить шаблон пользователя а также изменить список управления доступом (ACL) для шаблона. Дополнительная информация приведена в следующих разделах:

- “Добавление шаблона пользователя”
- “Редактирование шаблона” на стр. 196
- “Удаление шаблона” на стр. 196
- “Редактирование ACL шаблона” на стр. 196

### Добавление шаблона пользователя

Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

1. Нажмите кнопку **Добавить шаблон пользователя** или выберите опцию **Управление шаблонами пользователей** и нажмите кнопку **Добавить**.
   - Введите имя шаблона. Например, **template2**.
   - Если вы уже создали какие-либо шаблоны, например, **template1**, то для копирования параметров существующего шаблона в новый вы можете выбрать один из уже созданных шаблонов.
   - Введите родительский DN, идентифицирующий расположение шаблона. Значение должно быть указано в формате DN, например, **cn=realm1,o=ibm,c=us**. Вы также можете нажать кнопку **Обзор** и выбрать в списке нужное расположение.
2. Нажмите кнопку **Далее**. Для создания пустого шаблона можно нажать кнопку **Готово**. В дальнейшем вы сможете добавить информацию в шаблон. См. раздел “Редактирование шаблона” на стр. 196.
3. Если вы нажали кнопку **Далее**, то выберите для шаблона структурный класс объектов, например, **inetOrgPerson**. Вы также можете добавить любые вспомогательные классы объектов.
4. Нажмите кнопку **Далее**.

5. Для шаблона будет создана вкладка **Обязательные**. Информация, показанная на этой вкладке, доступна для изменения.
   a. Выберите в меню вкладки пункт **Обязательные** и нажмите кнопку **Редактировать**.Будет показана панель **Редактировать вкладку**. Будет показано имя вкладки **Обязательные** и выбранные атрибуты, которые являются обязательными для класса объектов **inetOrgPerson**:
      - *sn - фамилия
      - *cn - общее имя

      **Примечание:** Звездочка (*) означает обязательную информацию.
   b. Если вы хотите добавить на эту вкладку дополнительную информацию, то выберите в меню **Атрибуты** нужный атрибут. Например, выберите **departmentNumber** и нажмите кнопку **Добавить**.Выберите **employeeNumber** и нажмите кнопку **Добавить**. Выберите **title** и нажмите кнопку **Добавить**. Теперь список **Выбранные атрибуты** будет выглядеть следующим образом:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Вы можете изменить расположение полей шаблона. Для этого выберите атрибут и нажмите кнопку **Вверх** или **Вниз**. При этом положение атрибута будет изменено на единицу. Повторите процедуру нужное число раз, разместив все атрибуты в требуемом порядке. Например:
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Вы можете также изменить каждый выделенный атрибут.
      1) Выделите атрибут в списке **Выбранные атрибуты** и нажмите кнопку **Редактировать**.
      2) Вы можете изменить отображаемое в шаблоне имя атрибута. Например, если вы хотите, чтобы для атрибута **departmentNumber** была показана строка **Номер отдела**, то укажите эту строку в поле **Отображаемое имя**.
      3) Вы можете также указать значение по умолчанию, которое будет указываться в поле атрибута в шаблоне. Например, если большинство пользователей, информацию о которых вы будете вводить, относятся к отделу 789, то в качестве значения по умолчанию можно указать 789. В поле шаблона для атрибута будет заранее указываться значение 789. Это значение можно изменить при вводе фактической информации о пользователе.
      4) Нажмите кнопку **OK**.
   e. Нажмите кнопку **OK**.
6. Для создания еще одной категории вкладки с дополнительной информацией нажмите кнопку **Добавить**.
   - Введите имя вкладки. Например: Адрес.
   - В меню **Атрибуты** выберите атрибуты для этой вкладки. Например, выберите **homePostalAddress** и нажмите кнопку **Добавить**. Выберите **postOfficeBox** и нажмите кнопку **Добавить**. Выберите **telephoneNumber** и нажмите кнопку **Добавить**.Выберите **homePhone** и нажмите кнопку **Добавить**. Выберите **facsimileTelephoneNumber** и нажмите кнопку **Добавить**. Теперь список **Выбранные атрибуты** будет выглядеть следующим образом:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone

- facsimileTelephoneNumber

- Вы можете изменить расположение полей шаблона. Для этого выберите атрибут и нажмите кнопку **Вверх** или **Вниз**. При этом положение атрибута будет изменено на единицу. Повторите процедуру нужное число раз, разместив все атрибуты в требуемом порядке. Например:
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - facsimileTelephoneNumber
  - homePhone
- Нажмите кнопку **OK**.

7. Повторите процесс, чтобы добавить все необходимые вкладки. После завершения ввода нажмите кнопку **Готово** для создания шаблона.

## Редактирование шаблона

Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

- Нажмите кнопку **Управление шаблонами пользователей**.
- Выберите в списке область для редактирования.
- Нажмите кнопку **Редактировать**.
- Если вы уже создали какие-либо шаблоны, например, **template1**, то для копирования параметров существующего шаблона в редактируемый шаблон вы можете выбрать один из уже созданных шаблонов.
- Нажмите кнопку **Далее**.
  - С помощью списка вы можете изменить структурный класс объектов шаблона.
  - Вы можете добавлять и удалять вспомогательные классы объектов.
- Нажмите кнопку **Далее**.
- Вы можете изменять вкладки и атрибуты шаблона. Дополнительная информация об изменении вкладок приведена в разделе 5 на стр. 195.
- После завершения ввода нажмите кнопку **Готово**.

## Удаление шаблона

Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

1. Нажмите кнопку **Управление шаблонами пользователей**.
2. Выберите шаблон для удаления.
3. Нажмите кнопку **Удалить**.
4. При появлении просьбы подтвердить операцию нажмите **OK**.
5. Шаблон будет удален из списка.

## Редактирование ACL шаблона

Разверните в области навигации Web-инструмента администрирования категорию **Области и шаблоны**.

1. Нажмите кнопку **Управление шаблонами пользователей**.
2. Выберите шаблон, для которого необходимо изменить ACL.
3. Нажмите кнопку **Редактировать ACL**.

Для просмотра свойств ACL с помощью Web-инструмента администрирования и работы с ACL ознакомьтесь с разделом “Управление списками управления доступом (ACL)” на стр. 197.

Дополнительная информация приведена в разделе “Списки управления доступом” на стр. 60.

## Управление списками управления доступом (ACL)

Дополнительная информация о списках управления доступом приведена в разделе “Списки управления доступом” на стр. 60.

Для просмотра свойств ACL с помощью Web-инструмента администрирования и работы с ACL ознакомьтесь выполните следующие действия:

1. Выберите запись каталога. Например: cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Нажмите кнопку **Редактировать ACL**. Будет показано окно Редактировать ACL с выбранной вкладкой **Действующие ACL**.

На этой панели расположено пять вкладок:

- “Действующие ACL”
- “Действующие владельцы” на стр. 198
- “ACL без фильтров” на стр. 198
- “ACL с фильтрами” на стр. 199
- “Владельцы” на стр. 201

Вкладки **Действующие ACL** и **Действующие владельцы** содержат информацию об ACL, предназначенную только для чтения.

## Действующие ACL

Действующие ACL - это все явно заданные и унаследованные ACL выбранной записи. Для просмотра прав доступа, заданных действующим ACL, необходимо выбрать его и нажать кнопку **Показать**. Будет показана панель **Показать права доступа**.

**Просмотр прав доступа**

- В разделе **Права доступа** указаны права на добавление и удаление, предоставленные объекту.
  - **Добавление потомка** - предоставляет или аннулирует права объекта на добавление записи о каталоге, расположенной ниже выбранной записи.
  - **Удаление записи** - предоставляет или аннулирует права объекта на удаление выбранной записи.
- В разделе **Класс защиты** указываются права доступа для классов защиты. Атрибуты объединяются в следующие классы защиты:
  - **Обычный** - К этому классу относятся атрибуты, для которых требуется минимальная защита, например, атрибут commonName.
  - **Промежуточный** - К этому классу относятся атрибуты, для которых требуется средний уровень защиты, например, атрибут homePhone.
  - **Полный** - К этому классу относятся атрибуты, для которых должна быть установлена максимальная защита, например, userpassword.
  - **Системный** - К этому классу относятся атрибуты, для которых требуются права только на чтение и которые управляются сервером.
  - **Ограниченный** - К этому классу относятся ограниченные атрибуты, служащие для определения прав доступа.

  С каждым классом защиты связаны права доступа.
  - **Чтение** - права на чтение атрибутов.
  - **Запись** - права на изменение атрибутов.
  - **Поиск** - права на поиск в атрибутах.
  - **Сравнение** - права на сравнение атрибутов.

Для возврата к вкладке Действующие ACL нажмите кнопку **OK**.

Для возврата к панели Редактировать ACL нажмите кнопку **Отмена**.

## Действующие владельцы

Действующие владельцы - это все явно заданные и унаследованные владельцы выбранной записи.

## ACL без фильтров

Вы можете добавить к записи новые ACL без фильтров или изменить уже существующие.

Действие ACL без фильтров можно расширять. Это значит, что информацию об управлении доступом, определенная для одной записи, можно применять ко всем подчиненным ей записям. Источник ACL - это источник текущего ACL выбранной записи. Если для записи не создан ACL, она наследует ACL родительского объекта.

На вкладке **ACL без фильтров** введите следующую информацию:

- Наследовать ACL - Выбор переключателя **Наследовать ACL** позволяет дочерним записям без явно заданного ACL наследовать ACL этой записи. Если этот переключатель выбран, то потомки будут наследовать ACL этой записи до тех пор, пока для очередной дочерней записи не будет явно определен собственный ACL, который в этом случае заменит собой унаследованный ACL. Если переключатель не отмечен, дочерние записи без собственного ACL унаследуют ACL той родительской записи, для которой разрешено наследование.
- DN (Отличительное имя) - Введите **Отличительное имя (DN)** записи, запрашивающей доступ на выполнение операций над выбранной записью, например, cn=Marketing Group.
- Тип - Введите **Тип** DN. Например, если DN соответствует пользователю, то выберите access-id.

**Добавление и редактирование прав доступа**

Нажмите кнопку **Добавить** для добавления в список ACL DN, указанного в поле DN (отличительное имя), или кнопку Изменить для изменения ACL существующего DN.

Панели **Добавить права доступа** и **Редактировать права доступа** позволяют задать права доступа для нового или существующего списка управления доступом (ACL). В поле **Тип** по умолчанию указан тип, выбранный вами в панели **Изменить ACL**. При добавлении ACL во всех остальных полях будут указаны пробелы. При изменении ACL во всех полях будут указаны значения, заданные при последнем изменении ACL.

Вы можете:

- Изменить тип ACL
- Добавить или аннулировать отдельные права доступа
- Задать права доступа для классов защиты

Для того чтобы задать права доступа:

1. Выберите **Тип** записи ACL. Например, если DN соответствует пользователю, то выберите access-id.
2. В разделе **Права доступа** указаны права на добавление и удаление, предоставленные объекту.
   - **Добавление потомка** - предоставляет или аннулирует права объекта на добавление записи о каталоге, расположенной ниже выбранной записи.
   - **Удаление записи** - предоставляет или аннулирует права объекта на удаление выбранной записи.
3. В разделе **Класс защиты** указываются права доступа для классов атрибута. Атрибуты объединяются в следующие классы защиты:
   - **Обычный** - К этому классу относятся атрибуты, для которых требуется минимальная защита, например, атрибут commonName.
   - **Промежуточный** - К этому классу относятся атрибуты, для которых требуется средний уровень защиты, например, атрибут homePhone.

- **Полный** - К этому классу относятся атрибуты, для которых должна быть установлена максимальная защита, например, userpassword.
- **Системный** - К этому классу относятся атрибуты, для которых требуются права только на чтение и которые управляются сервером.
- **Ограниченный** - К этому классу относятся ограниченные атрибуты, служащие для определения прав доступа.

С каждым классом защиты связаны права доступа.

- Чтение - права на чтение атрибутов.
- Запись - права на изменение атрибутов.
- Поиск - права на поиск в атрибутах.
- Сравнение - права на сравнение атрибутов.

Для любого атрибута можно задать права доступа, которые переопределяют права доступа, установленные для класса защиты этого атрибута. Раздел атрибутов находится ниже строки, соответствующей **полному классу защиты**.

- Выберите атрибут в списке **Определить атрибут**.
- Нажмите кнопку **Определить**. Атрибут будет показан в таблице прав доступа.
- Укажите, права доступа к атрибуту (разрешить или запретить) для каждого из четырех классов защиты.
- Вы можете повторить эту процедуру для нескольких атрибутов.
- Для удаления атрибута просто выберите его и нажмите кнопку **Удалить**.
- После завершения нажмите **OK**.

**Удаление ACL**

Удалить ACL можно двумя способами:

- Выберите радиокнопку, расположенную рядом с именем удаляемого ACL. Нажмите кнопку **Удалить**.
- Для удаления из списка всех DN нажмите кнопку **Удалить все**.

## ACL с фильтрами

Вы можете добавить к записи новые или изменить уже существующие ACL с фильтрами.

В ACL с фильтрами для определения объектов, к которым должны применяться права доступа, используется сравнение на основе фильтра объектов.

По умолчанию ACL с фильтрами накапливают права доступа от включенной записи наименьшего уровня вверх по цепочке предков, до включенной записи наивысшего уровня в дереве информации о каталоге (DIT). Действующие права доступа вычисляются как объединение разрешений или запретов для всех записей, отвечающих условиям фильтра. Однако в этом алгоритме есть одно исключение. Для совместимости с функцией копирования поддерева, а также для обеспечения более надежного контроля со стороны администратора накопление прав доступа ограничивается сверху атрибутом ceiling.

На вкладке ACL с фильтрами введите следующую информацию:

- Накапливать ACL с фильтрами -
  - Для удаления из выбранной записи атрибута ibm-filterACLInherit выберите радиокнопку **Не задано**.
  - Выберите радиокнопку **Да**, чтобы разрешить выбранной записи накапливать ACL вверх по цепочке предков, вплоть до самого верхнего ACL, соответствующего фильтру и включающего данную запись в DIT.
  - Для того чтобы запретить накопление ACL с фильтрами для выбранной записи, выберите радиокнопку **Нет**.

- DN (Отличительное имя) - Введите **Отличительное имя (DN)** записи, запрашивающей доступ на выполнение операций над выбранной записью, например, cn=Marketing Group.
- Тип - Введите **Тип** DN. Например, если DN соответствует пользователю, то выберите access-id.

**Добавление и редактирование прав доступа**

Нажмите кнопку **Добавить** для добавления в список ACL DN, указанного в поле DN (отличительное имя), или кнопку Изменить для изменения ACL существующего DN.

Панели **Добавить права доступа** и **Редактировать права доступа** позволяют задать права доступа для нового или существующего списка управления доступом (ACL). В поле Тип по умолчанию указан тип, выбранный вами в панели Изменить ACL. При добавлении ACL во всех остальных полях будут указаны пробелы. При изменении ACL во всех полях будут указаны значения, заданные при последнем изменении ACL.

Вы можете:
- Изменить тип ACL
- Добавить или аннулировать отдельные права доступа
- Задать фильтр объектов для ACL с фильтрами
- Задать права доступа для классов защиты

Для того чтобы задать права доступа:
1. Выберите **Тип** записи ACL. Например, если DN соответствует пользователю, то выберите access-id.
2. В разделе **Права доступа** указаны права на добавление и удаление, предоставленные объекту.
   - **Добавление потомка** - предоставляет или аннулирует права объекта на добавление записи о каталоге, расположенной ниже выбранной записи.
   - **Удаление записи** - предоставляет или аннулирует права объекта на удаление выбранной записи.
3. Задать фильтр объектов на основе сравнения. В поле **Фильтр объектов** укажите фильтр для выбранного ACL. Для задания строки фильтра нажмите кнопку **Редактировать фильтр**. Текущий ACL с фильтром будет применяться ко всем дочерним записям, а также ко всем объектам поддерева, соответствующим заданному фильтру.
4. В разделе **Класс защиты** указываются права доступа для классов атрибута. Атрибуты объединяются в следующие классы защиты:
   - **Обычный** - К этому классу относятся атрибуты, для которых требуется минимальная защита, например, атрибут commonName.
   - **Промежуточный** - К этому классу относятся атрибуты, для которых требуется средний уровень защиты, например, атрибут homePhone.
   - **Полный** - К этому классу относятся атрибуты, для которых должна быть установлена максимальная защита, например, userpassword.
   - **Системный** - К этому классу относятся атрибуты, для которых требуются права только на чтение и которые управляются сервером.
   - **Ограниченный** - К этому классу относятся ограниченные атрибуты, служащие для определения прав доступа.

   С каждым классом защиты связаны права доступа.
   - Чтение - права на чтение атрибутов.
   - Запись - права на изменение атрибутов.
   - Поиск - права на поиск в атрибутах.
   - Сравнение - права на сравнение атрибутов.

   Для любого атрибута можно задать права доступа, которые переопределяют права доступа, установленные для класса защиты этого атрибута. Раздел атрибутов находится ниже строки, соответствующей **полному классу защиты**.

- Выберите атрибут в списке **Определить атрибут**.
- Нажмите кнопку **Определить**. Атрибут будет показан в таблице прав доступа.
- Укажите, права доступа к атрибуту (разрешить или запретить) для каждого из четырех классов защиты.
- Вы можете повторить эту процедуру для нескольких атрибутов.
- Для удаления атрибута просто выберите его и нажмите кнопку **Удалить**.
- После завершения нажмите **OK**.

**Удаление ACL**

Удалить ACL можно двумя способами:

- Выберите радиокнопку, расположенную рядом с именем удаляемого ACL. Нажмите кнопку **Удалить**.
- Для удаления из списка всех DN нажмите кнопку **Удалить все**.

## Владельцы

У владельцев записи есть полный набор прав доступа к объекту, разрешающий выполнять над объектом любые операции. Владельцы записи могут быть заданы явно или унаследованы.

На вкладке **Владельцы** укажите следующую информацию:

- Выбор переключателя **Расширить владельцев** позволяет дочерним записям без явно заданного владельца наследовать владельца этой записи. Если переключатель не отмечен, то дочерние записи без собственного владельца унаследуют владельца той родительской записи, в которой наследование разрешено.
- DN (Отличительное имя) - Введите **Отличительное имя (DN)** записи, запрашивающей доступ на выполнение операций над выбранной записью, например, `cn=Marketing Group`.

  С помощью `cn=this` и объектов, наследующих владельца, легко создать поддерево каталога, каждый объект которого принадлежит самому себе.
- Тип - Введите **Тип** DN. Например, если DN соответствует пользователю, то выберите access-id.

**Добавление владельца**

Для добавления в список DN (отличительного имени), указанного в поле **DN (отличительное имя)**, нажмите кнопку **Добавить**.

**Удаление владельца**

Удалить владельца можно двумя способами:

- Выберите радиокнопку, соответствующую удаляемому владельцу. Нажмите кнопку **Удалить**.
- Для удаления из списка всех DN владельце в нажмите кнопку **Удалить все**.

# Глава 8. Справочник

В следующих разделах приведена дополнительная справочная информация.



## Утилиты командной строки

В этом разделе описаны утилиты, которые можно выполнять в командной строке Qshell i5/OS. Дополнительная информация приведена в описании следующих команд:



Обратите внимание, что для правильной обработки в командной строке Qshell некоторые строки должны быть заключены в кавычки. Это правило относится, с частности к DN, фильтрам поиска и спискам атрибутов, которые должны возвращаться утилитой ldapsearch. Примеры таких строк:

- Строки, содержащие пробелы: `"cn=John Smith,cn=users"`
- Строки, содержащие символы подстановки: `"*"`
- Строки, содержащие скобки: `"(objectclass=person)"`

Дополнительная информация о среде Qshell приведена в разделе “Qshell”.

## ldapmodify и ldapadd

Утилиты изменения и добавления записей LDAP

**Формат**

```
ldapmodify [-a] [-b] [-c] [-C набор-символов] [-d уровень-отладки][-D dn-подключения][-g]
[-f файл][-F][-g][-G область] [-h хост-ldap] [-i файл] [-k] [-K файл ключей]
[-m механизм] [-M][-n][-N сертификат] [-O макс.-число] [-p порт-ldap]
[-P пароль-файла-ключей] [-r] [-R][-U имя-пользователя] [-v] [-V] [-w пароль | ?] [-y dn-proxy]
[-Y] [-Z]


ldapadd [-a] [-b] [-c] [-C набор-символов] [-d уровень-отладки][-D dn-подключения][-g]
[-f файл][-F][-g][-G область] [-h хост-ldap] [-i файл] [-k] [-K файл ключей]
[-m механизм] [-M][-n][-N сертификат] [-O макс.-число] [-p порт-ldap]
[-P пароль-файла-ключей] [-r] [-R][-U имя-пользователя] [-v] [-V] [-w пароль | ?] [-y dn-proxy]
[-Y] [-Z]
```

**Описание**

**ldapmodify** - это интерфейс командной строки к API ldap_modify, ldap_add, ldap_delete b ldap_modrdn. **ldapadd** представляет собой переименованную версию ldapmodify. При вызове в виде ldapadd автоматически включается флаг **-a** (добавить новую запись).

**ldapmodify** открывает соединение с сервером LDAP и подключается к этому серверу. С помощью утилиты **ldapmodify** можно изменять и добавлять записи. Информация о записи считывается из стандартного потока ввода или из файла, указанного в опции **-i**.

Для просмотра справки по синтаксису вызова команды **ldapmodify** или **ldapadd** введите

```
ldapmodify -?
```

или

```
ldapadd -?
```

**Опции**

**-a** Добавляет новые записи. По умолчанию **ldapmodify** изменяет существующие записи. При вызове в качестве **ldapadd** этот флаг устанавливается автоматически.

**-b** Все значения, начинающиеся с символа `/', интерпретируются как двоичные. При этом считается, что фактическое значение находится в файле, путь ко которому задан вместо значения.

**-c** Режим непрерывной работы. Работа **ldapmodify** продолжается несмотря на выдачу сообщений об ошибках. По умолчанию программа после выдачи сообщения об ошибке прекращает работу.

**-C** *набор-символов*
Указывает, что входные данные для утилиты **ldapmodify** или **ldapadd** заданы в локальном наборе символов (набор-символов) и их необходимо преобразовать в UTF-8. Опцию **-C** *набор-символов* следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Список поддерживаемых значений кодовых страниц приведен в описании API ldap_set_iconv_local_charset().

**-d** *уровень-отладки*
Устанавливает указанный уровень отладки LDAP.

**-D** *dn-подключения*
***DN-подключения*** применяется для подключения к каталогу LDAP. ***DN-подключения*** задается в виде строки. При использовании с -m DIGEST-MD5 оно задает ИД предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с ″u:″ или ″dn:″.

**-f** *файл*
Считывает информацию об изменении записей из файла LDIF вместо стандартного ввода. Если файл LDIF не указан, обновленные записи в формате LDIF должны быть заданы в стандартном вводе.

**-F** Принудительно применяются все изменения, независимо от содержимого входных строк, начинающихся с replica: (по умолчанию строки replica: сравниваются с именем хоста и портом сервера LDAP и на основе этого сравнения определяется, должна ли на самом деле применяться запись протокола копирования).

**-g** Не обрезать конечные пробелы в значениях атрибутов.

**–G** Задает область. Этот параметр необязателен. При использовании с -m DIGEST-MD5 значение передается серверу при подключении.

**-h** *хост*
Задает альтернативный хост, на котором работает сервер LDAP.

**-i** *файл* Считывает информацию об изменении записей из файла LDIF вместо стандартного ввода. Если файл LDIF не указан, обновленные записи в формате LDIF должны быть заданы в стандартном вводе.

**-k** Указывает, что необходимо применять средства управления администрированием сервера.

**-K** *файл-ключей*

Укажите имя файла базы данных ключей SSL с расширением по умолчанию **kdb**. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла. Если имя файла базы данных ключей не указано, то утилита сначала проверит наличие переменной среды SSL_KEYRING, в которой может быть задано имя файла. Если переменная среды SSL_KEYRING не определена, то будет применяться системный файл ключей (если он существует).

Этот параметр включает опцию **-Z**. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-m** *механизм*

Параметр ***механизм*** указывает механизм SASL, применяемый для подключения к серверу. Применяется API ldap_sasl_bind_s(). Если указано **-V 2**, то параметр **-m** игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации. Допустимые механизмы:

- CRAM-MD5 - защищает передаваемый серверу пароль.
- EXTERNAL - использует сертификат SSL. Требует указания ключа -Z.
- GSSAPI - использует разрешения Kerberos.
- Для DIGEST-MD5 необходимо, чтобы клиент отправлял на сервер имя пользователя. Требует указания ключа -U. Параметр -D (обычно это DN подключения) служит для указания ID предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с u: или dn:.
- OS400_PRFTKN - идентификация на локальном сервере LDAP в качестве текущего пользователя i5/OS посредством DN пользователя в спроецированной базе данных системы. Параметры -D (DN подключения) и -w (пароль) указывать не нужно.

**-M** Считает объекты переадресации обычными записями.

**-n** Показывает результаты выполнения операции, но не вносит изменения в записи. Вместе с параметром -v применяется для отладки.

**-N** *сертификат*

Задает метку, связанную с сертификатом клиента в файле базы данных ключей. Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то может потребоваться сертификат клиента. ***сертификат*** не нужен в том случае, если пара сертификат/личный ключ выбрана в файле базы данных ключей в качестве пары по умолчанию. Кроме того, параметр ***сертификат*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ.Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-O** *макс.-число*

Параметр ***максимальное-число*** позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.

**-p** *порт*

Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если опция **-p** не указана, и указана опция **-Z**, то по умолчанию применяется порт SSL LDAP 636.

**-P** *пароль-файла-ключей*

Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, включая или несколько личных ключей. Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-P** указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

**-r** Заменять существующие значения по умолчанию.

**-R** Отключает автоматический переход по ссылкам.

**–U** Задает имя пользователя. Необходим при использовании -m DIGEST-MD5 и игнорируется для других механизмов.

**-v** Подробный вывод, при котором создается множество диагностических сообщений.

**-V** *версия*
Задает версию LDAP, которая должна применяться утилитой **ldapmodify** при подключении к серверу LDAP. По умолчанию устанавливается соединение LDAP V3. Для явного выбора LDAP V3 укажите **-V 3**. Для работы в режиме приложения LDAP V2 укажите **-V 2**.

**-w** *пароль* **| ?**
***Пароль*** для идентификации. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?.

**-y** *dn-proxy*
Задает ИД сервера proxy для идентификации.

**-Y** Используется защищенное соединение LDAP (TLS).

**-Z** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**Формат ввода**

Содержимое файла (или стандартного потока ввода, если флаг **-i** не указан) должно соответствовать формату LDIF. Дополнительная информация о формате LDIF приведена в разделе “Формат обмена данными LDAP (LDIF)” на стр. 234.

**Примеры**

Допустим, что существует файл /tmp/entrymods, содержащий следующую информацию:

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: modme@student.of.life.edu
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto: /tmp/modme.jpeg
-
delete: description
-
```

В этом случае команда

```
ldapmodify -b -r -i /tmp/entrymods
```

удалит содержимое атрибута mail записи Modify Me на значение modme@student.of.life.edu, добавит заголовок Grand Poobah, загрузит содержимое файла /tmp/modme.jpeg в качестве значения атрибута jpegPhoto, а также полностью удалит атрибут description. Эти же изменения можно выполнить с помощью старого исходного формата ldapmodify:

```
cn=Modify Me, o=University of Higher Learning, c=US
mail=modme@student.of.life.edu
+title=Grand Poobah
+jpegPhoto=/tmp/modme.jpeg
-description
```

и команды

```
ldapmodify -b -r -i /tmp/entrymods
```

Допустим, что существует файл /tmp/newentry, содержащий следующую информацию:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
      sn: Doe
title: the world's most famous mythical person
mail: johndoe@student.of.life.edu
uid: jdoe
```

В этом случае команда

```
 ldapadd -i /tmp/entrymods
```

добавит новую запись John Doe, применяя значения из файла /tmp/newentry.

**Примечания**

Если информация о записи не указана в файле с помощью опции **-i**, то команда **ldapmodify** будет ожидать получения записей из стандартного потока ввода.

**Диагностика**

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

## ldapdelete

Утилита удаления записи LDAP

**Формат**

```
ldapdelete [-c] [-C набор-символов] [-d уровень-отладки][-D dn-подключения] [-f файл]
[-G область] [-h хост-ldap] [-i файл] [-k] [-K файл-ключей] [-m механизм]
[-M] [-n] [-N сертификат] [-O макс.-число] [-p порт-ldap]
[-P пароль-файла-ключей] [-R] [-s][-U имя-пользователя} [-v] [-V версия]
[-w пароль | ?] [-y dn-proxy][-Y] [-Z] [dn]......
```

**Описание**

**ldapdelete** - это интерфейс командной строки к API ldap_delete.

**ldapdelete** открывает соединение с сервером LDAP, подключается к нему и удаляет одну или несколько записей. Если в качестве аргументов указано одно или несколько отличительных имен (DN), то удаляются записи с такими DN. DN задаются в строковом представлении. Если аргументы DN не указаны, то список DN считывается из стандартного потока ввода или из файла, заданного флагом **-i**.

Для просмотра справки по синтаксису вызова команды **ldapdelete** введите

```
ldapdelete -?
```

**Опции**

**-c** Режим непрерывной работы. Работе **ldapdelete** продолжается несмотря на сообщения об ошибках. По умолчанию программа после выдачи сообщения об ошибке прекращает работу.

**-C** *набор-символов*
Указывает, что DN в исходных данных утилиты **ldapdelete** заданы в локальном наборе символов. Опцию **-C** *набор-символов* следует применять в том случае, если кодовая страница входных данных

отличается от кодовой страницы задания. Список поддерживаемых значений кодовых страниц приведен в описании API ldap_set_iconv_local_charset().

**-d** *уровень-отладки*
Устанавливает указанный уровень отладки LDAP.

**-D** *dn-подключения*
***DN-подключения*** применяется для подключения к каталогу LDAP. ***DN-подключения*** задается в виде строки. При использовании с -m DIGEST-MD5 оно задает ИД предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с ″u:″ или ″dn:″.

**-f** *файл*
Утилита считывает последовательность строк из файла, выполняя функцию удаления LDAP для каждой строки. В каждой строке файла должно содержаться одно отличительное имя (DN).

**-G** *область*
Задает область. Этот параметр необязателен. При использовании с -m DIGEST-MD5 значение передается серверу при подключении.

**-h** *хост*
Укажите альтернативный хост, на котором работает сервер LDAP.

**-i** *файл* Утилита считывает последовательность строк из файла, выполняя функцию удаления LDAP для каждой строки. Каждая строка в файле должна содержать одно отличительное имя (DN).

**-k** Указывает, что необходимо применять средства управления администрированием сервера.

**-K** *файл-ключей*
Задает имя файла базы данных ключей SSL. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла.

Если утилите не удается обнаружить базу данных ключей, то применяется набор надежных базовых сертификатов сертификатных компаний, заданный по умолчанию. Файл базы данных ключей, как правило, содержит один или несколько сертификатов сертификатных компаний (CA), сертификаты которых принимает клиент. Сертификаты X.509 этого типа известны также как надежные базовые сертификаты.

Этот параметр включает опцию **-Z**. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-m** *механизм*
Параметр ***механизм*** указывает механизм SASL, применяемый для подключения к серверу. Применяется API ldap_sasl_bind_s(). Если указано **-V 2**, то параметр **-m** игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации. Допустимые механизмы:

- CRAM-MD5 - защищает передаваемый серверу пароль.
- EXTERNAL - использует сертификат SSL. Требует указания ключа -Z.
- GSSAPI - использует разрешения Kerberos.
- Для DIGEST-MD5 необходимо, чтобы клиент отправлял на сервер имя пользователя. Требует указания ключа -U. Параметр -D (обычно это DN подключения) служит для указания ID предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с u: или dn:.
- OS400_PRFTKN - идентификация на локальном сервере LDAP в качестве текущего пользователя i5/OS посредством DN пользователя в спроецированной базе данных системы. Параметры -D (DN подключения) и -w (пароль) указывать не нужно.

**-M** Считает объекты переадресации обычными записями.

**-n** Показывает результаты выполнения операции, но не вносит изменения в записи. Применяется для отладки вместе с параметром **-v**.

**-N** *сертификат*

Задает метку, связанную с сертификатом клиента в файле базы данных ключей. Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то может потребоваться сертификат клиента. Параметр ***имя-сертификата*** не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр ***сертификат*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-O** *макс.-число*

Параметр ***максимальное-число*** позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.

**-p** *порт*

Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если опция **-p** не указана, и указана опция **-Z**, то по умолчанию применяется порт SSL LDAP 636.

**-P** *пароль-файла-ключей*

Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, включая или несколько личных ключей. Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-P** указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

**-R** Отключает автоматический переход по ссылкам.

**-s** Эта опция применяется для удаления поддерева, начинающегося с указанной записи.

**–U** *имя-пользователя*

Задает имя пользователя. Необходим при использовании -m DIGEST-MD5 и игнорируется для других механизмов.

**-v** Подробный вывод, при котором создается множество диагностических сообщений.

**-V** *версия*

Задает версию LDAP, которая должна применяться утилитой **ldapdelete** при подключении к серверу LDAP. По умолчанию устанавливается соединение LDAP V3. Для явного выбора LDAP V3 укажите **-V 3**. Для работы в режиме приложения LDAP V2 укажите **-V 2**.

**-w** *пароль* **| ?**

***Пароль*** для идентификации. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?.

**-y dn-proxy**

Задает ИД сервера proxy для идентификации.

**–Y** Используется защищенное соединение LDAP (TLS).

**-Z** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**dn** Задает один или несколько аргументов DN. DN задаются в строковом представлении.

**Примеры**

Команда

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

пытается удалить запись с атрибутом commonName ″Delete Me″, являющуюся дочерней записью организации University of Life.

**Примечания**

Если аргументы DN не указаны, то команда **ldapdelete** будет ожидать указания DN в стандартном потоке ввода.

**Диагностика**

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

# ldapexop

Утилита выполнения расширенных операций LDAP.

**Формат**

```
ldapexop [-C набор-символов] [-d уровень-отладки][-D dn-подключения][-e] [-G область]
[-h хост-ldap][-help][-K файл-ключей] [-m механизм] [-N сертификат]
[-p порт-ldap] [-P пароль-файла-ключей] [-?] [-U] [-v] [-w пароль | ?] [-Y] [-Z]
-op {cascrepl | controlqueue | controlrepl | getAttributes |
getusertype | quiesce | readconfig | uniqueattr}
```

**Описание**

Утилита **ldapexop** позволяет подключиться к серверу каталогов и выполнить единую расширенную операцию, включающую в себя все необходимые данные.

Утилита **ldapexop** поддерживает стандартные опции хоста, порта, SSL и опции идентификации, применяемые всеми клиентскими утилитами LDAP. Кроме того, определен набор опций, задающих выполняемую операцию, а также аргументы для каждой расширенной операции.

Для просмотра справки по синтаксису вызова команды **ldapexop** введите

```
ldapexop -?
```

или

```
ldapexop -help
```

**Опции**

Опции команды ldapexop можно разделить на две категории.

1. Общие опции, описывающие подключение к серверу. Эти опции следует указывать перед опциями конкретной операции.
2. Опции расширенной операции, описывающие требуемую расширенную операцию.

**Общие опции**

Эти опции описывают способы подключения к серверу. Они должны быть указаны перед опцией **-op**.

**-C** *набор-символов*
: Указывает, что DN в исходных данных утилиты **ldapexop** заданы в локальном наборе символов. Опцию **-C** *набор-символов* следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Список поддерживаемых значений кодовых страниц приведен в описании API ldap_set_iconv_local_charset().

**-d** *уровень-отладки*
Устанавливает указанный уровень отладки LDAP.

**-D** *dn-подключения*
***DN-подключения*** применяется для подключения к каталогу LDAP. ***DN-подключения*** задается в виде строки. При использовании с -m DIGEST-MD5 оно задает ИД предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с ″u:″ или ″dn:″.

**-e** Показывает информацию о версии библиотеки LDAP и завершает работу.

**-G** Задает область. Этот параметр необязателен. При использовании с -m DIGEST-MD5 значение передается серверу при подключении.

**-h** *хост*
Укажите альтернативный хост, на котором работает сервер LDAP.

**-help** Показывает информацию о синтаксисе вызова команды.

**-K** *файл-ключей*
Задает имя файла базы данных ключей SSL. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла.

Если утилите не удается обнаружить базу данных ключей, то применяется системная база данных ключей. Файл базы данных ключей, как правило, содержит один или несколько сертификатов сертификатных компаний (CA), сертификаты которых принимает клиент. Сертификаты X.509 этого типа известны также как надежные базовые сертификаты.

Этот параметр включает опцию **-Z**. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-m** *механизм*
Параметр ***механизм*** указывает механизм SASL, применяемый для подключения к серверу. Применяется API ldap_sasl_bind_s(). Если указано **-V 2**, то параметр **-m** игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации. Допустимые механизмы:

- CRAM-MD5 - защищает передаваемый серверу пароль.
- EXTERNAL - использует сертификат SSL. Требует указания ключа -Z.
- GSSAPI - использует разрешения Kerberos.
- Для DIGEST-MD5 необходимо, чтобы клиент отправлял на сервер имя пользователя. Требует указания ключа -U. Параметр -D (обычно это DN подключения) служит для указания ID предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с u: или dn:.
- OS400_PRFTKN - идентификация на локальном сервере LDAP в качестве текущего пользователя i5/OS посредством DN пользователя в спроецированной базе данных системы. Параметры -D (DN подключения) и -w (пароль) указывать не нужно.

**-N** *сертификат*
Задает метку, связанную с сертификатом клиента в файле базы данных ключей. Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то может потребоваться сертификат клиента. Параметр ***имя-сертификата*** не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр ***сертификат*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-p** *порт*

Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если опция **-p** не указана, и указана опция **-Z**, то по умолчанию применяется порт SSL LDAP 636.

**-P** *пароль-файла-ключей*

Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, включая или несколько личных ключей. Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-P** указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

**-?** Показывает информацию о синтаксисе вызова команды.

**–U** Задает имя пользователя. Необходим при использовании -m DIGEST-MD5 и игнорируется для других механизмов.

**-v** Подробный вывод, при котором создается множество диагностических сообщений.

**-w** *пароль* **| ?**

***Пароль*** для идентификации. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?.

**–Y** Используется защищенное соединение LDAP (TLS).

**-Z** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**Опция расширенной операции**

Опция **-op** указывает требуемую расширенную операцию. В качестве расширенной операции может быть указано одно из следующих значений:

- **cascrepl**: расширенная операция управления каскадным копированием. Запрошенное действие применяется к указанному серверу и передается всем серверам-копиям выбранного поддерева. Если какой-либо из этих серверов является сервером пересылки, то он передает расширенную операцию своим копиям. Операция каскадным образом передается по всей топологии копирования.

  **-action quiesce | unquiesce | replnow | wait**

  Обязательный атрибут, задающий выполняемое действие.

  **quiesce**

  Дальнейшие обновления (вносимые не с помощью функции копирования) запрещены.

  **unquiesce**

  Возобновление обычной работы, прием передаваемых клиентами запросов на обновление.

  **replnow**

  Немедленное копирование всех находящихся в очереди изменений на все серверы-копии независимо от расписания.

  **wait** Ожидание копирования всех изменений на все серверы-копии.

  **-rc** *Dn-контекста*

  Обязательный атрибут, задающий корень поддерева.

  **-timeout** *секунды*

  Необязательный атрибут, задающий интервал тайм-аута в секундах. Если атрибут не указан или равен 0, то время ожидания будет неограниченным.

  **Пример:**

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **controlqueue**: расширенная операция управления очередью копирования. Эта опция позволяет удалить из очереди ожидающие изменения, которые еще не были обработаны из-за сбоя копирования. Эта возможность полезна в том случае, если данные на сервере-копии были исправлены вручную. После этого с помощью данной операции можно пропустить обработку ожидающих запросов, при обработке которых произошли ошибки.

  **-skip all | change-id**
  Это обязательный атрибут.
  - **-skip all** указывает, что необходимо пропустить все ожидающие изменения, связанные с данным соглашением.
  - **change-id** указывает отдельное изменение, которое необходимо пропустить. Если сервер в настоящее время не копирует изменение, то запрос выполнен не будет.

  **-ra** *Dn-соглашения*
  Это обязательный атрибут, указывающий DN соглашения о копировании.

  **Примеры:**:

```
ldapexop -op controlqueue -skip all -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"

ldapexop -op controlqueue -skip 2185 -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **controlrepl**: управление расширенной операцией копирования

  **-action suspend | resume | replnow**
  Обязательный атрибут, задающий выполняемое действие.

  **-rc** *Dn-контекста* **| -ra** *Dn-соглашения*
  Опция **-rc** *Dn-контекста* задает DN контекста копирования. Действие выполняется для всех соглашений этого контекста. Опция **-ra** *Dn-соглашения* задает DN соглашения о копировании. В этом случае действие выполняется для указанного соглашения.

  **Пример**:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **getattributes -attrType**<*type*> **-matches bool**<*value*>

  **-attrType {operational | language_tag | attribute_cache | unique | configuration}**
  Это обязательный атрибут, задающий тип запрашиваемого атрибута.

  **-matches bool {true | false}**
  Указывает, должен ли возвращаемый список атрибутов соответствовать типу атрибута, указанному в параметре -attrType<.

  **Пример**

```
ldapexop -op getattributes -attrType unique -matches bool true
```

  Возвращает список всех атрибутов, настроенных уникальными.

```
ldapexop -op getattributes -attrType unique -matches bool false
```

  Возвращает список всех атрибутов, не настроенных как уникальные.

- **getusertype:** расширенная операция запроса типа пользователя

  Эта операция возвращает тип пользователя на основе DN подключения.

  **Пример:**

```
ldapexop - D <AdminDN> -w <Adminpw> -op getusertype
```

  возвращает:

```
User : root_administrator
Role(s) : server_config_administrator directory_administrator
```

- **quiesce**: расширенная операция стабилизация или отмены стабилизации поддерева

  **-rc** *Dn-контекста*
  Это обязательный атрибут, указывающий DN контекста копирования (поддерева) для стабилизации или отмены стабилизации.

  **-end** Это необязательный атрибут, указывающий, что необходимо отменить стабилизацию поддерева. Если этот атрибут не указан, то по умолчанию поддерево стабилизируется.

  **Примеры:**:

```
ldapexop -op quiesce -rc "o=acme,c=us"

ldapexop -op quiesce -end -rc "o=ibm,c=us"
```

- **readconfig**: расширенная операция повторного считывания файла конфигурации

  **-scope entire | single<***DN-записи***><***атрибут***>**
  Это обязательный атрибут.
  - **entire** - указывает, что необходимо считать весь файл конфигурации.
  - **single** - указывает, что необходимо считать только отдельную запись и атрибут.

  **Примеры:**:

```
ldapexop -op readconfig -scope entire

ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
```

  **Примечание:** Ниже применяются следующие обозначения:
  - [1] применяется сразу же после чтения конфигурации
  - [2] - будет применяться для новых операций.
  - [3] - начнет применяться сразу после изменения пароля (readconfig не требуется)
  - [4] поддерживается утилитой командной строки i5/OS, но не поддерживается сервером каталогов в i5/OS

```
cn=Configuration
ibm-slapdadmindn[2]
ibm-slapdadminpw[2, 3]
ibm-slapderrorlog[1, 4]
ibm-slapdpwencryption[1]
ibm-slapdsizelimit[1]
ibm-slapdsysloglevel[1, 4]
ibm-slapdtimelimit[1]

cn=Front End, cn=Configuration
ibm-slapdaclcache[1]
ibm-slapdaclcachesize[1]
ibm-slapdentrycachesize[1]
ibm-slapdfiltercachebypasslimit[1]
ibm-slapdfiltercachesize[1]
ibm-slapdidletimeout[1]

cn=Event Notification, cn=Configuration ibm-slapdmaxeventsperconnection[2]
ibm-slapdmaxeventstotal[2]

cn=Transaction, cn=Configuration
ibm-slapdmaxnumoftransactions[2]
ibm-slapdmaxoppertransaction[2]
ibm-slapdmaxtimelimitoftransactions[2]


cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
```

```
ibm-slapdreadonly[2]

cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdbulkloaderrors[1, 4]
ibm-slapdclierrors[1, 4]
ibm-slapdpagedresallownonadmin[2]
ibm-slapdpagedreslmt[2]
ibm-slapdpagesizelmt[2]
ibm-slapdreadonly[2]
ibm-slapdsortkeylimit[2]
ibm-slapdsortsrchallownonadmin[2]
ibm-slapdsuffix[2]
```

- **unbind** {**-dn**<*указанное-DN*>| **-ip**<*исходный-IP-адрес*> | **-dn**<*указанное-DN*> **-ip**<*исходный-IP-адрес*> | **all**}:

  отключает соединения на основе DN, IP, DN/IP, либо отключает все соединения. Сразу же закрываются все соединения, как без операций, так и с операциями в рабочей очереди. Если в этот момент по соединению работает обработчик, то соединение закроется сразу же после окончания выполняемой операции обработчика.

  **-dn**<*указанное-DN*>
  Вызывает запрос на отключение соединения только по DN. В результате вычищаются все соединения с этим DN.

  **-ip**<*исходный-IP-адрес*>
  Вызывает запрос на отключение соединения только по IP-адресу. В результате вычищаются все соединения от этого исходного IP-адреса.

  **-dn**<*указанное-DN*> **-ip**<*исходный-IP-адрес*>
  Вызывает запрос на закрытие соединения по DN и IP-адресу. В результате вычищаются все соединения с указанным DN от заданного исходного IP-адреса.

  **-all** Вызывает запрос на закрытие всех соединений. В результате вычищаются все соединения кроме инициатора запроса. Этот атрибут нельзя использовать вместе с -D или -IP. атрибуты

  **Примеры:**

  ```
  ldapexop -op unbind -dn cn=john
  ldapexop -op unbind -ip 9.182.173.43
  ldapexop -op unbind -dn cn=john -ip 9.182.173.43
  ldapexop -op unbind -all
  ```

- **uniqueattr -a** <*Тип-атрибута*>**:** обозначает все не уникальные значения для атрибута.

  **-a** <*атрибут*>
  Задает атрибут, содержащий конфликтующие значения.

  **Примечание:** Не отображаются дублирующиеся значения для двоичных, операционных атрибутов, атрибутов конфигурации и атрибутов классов объектов. Эти атрибуты не поддерживают расширенные операции для уникальных атрибутов.

  **Пример:**

  ```
  ldapexop -op uniqueattr -a "uid"
  ```

  Для этой расширенной операции в запись ″cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration″ добавляется следующая строка:

  ```
  ibm-slapdPlugin:extendedop /bin/libback-rdbm.dll initUniqueAttr
  ```

**Диагностика**

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

# ldapmodrdn

Утилита изменения RDN LDAP.

**Формат**

```
ldapmodrdn [-c] [-C набор-символов] [-d уровень-отладки][-D dn-подключения]
[-f файл][-G область] [-h хост-ldap] [-i файл] [-k] [-K файл-ключей]
[-m механизм] [-M] [-n] [-N сертификат] [-O макс.-число]
[-p порт-ldap] [-P пароль-файла-ключей] [-r] [-R] [-U имя-пользователя] [-v] [-V версия]
[-w пароль | ?] [-y dn-proxy] [-Y] [-Z] [dn новое-rdn | [-i файл]]
```

**Описание**

**ldapmodrdn** - это интерфейс командной строки к API ldap_modrdn.

**ldapmodrdn** открывает соединение с сервером LDAP, подключается к нему и изменяет RDN записей. Информация о записи считывается из потока ввода, из файла указанного с помощью опции **- f**, либо из указанных в командной строке значений dn и rdn.

Информация об RDN (относительных отличительных именах) и DN (отличительных именах) приведена в разделе “Отличительные имена (DN)” на стр. 13.

Для просмотра справки по синтаксису вызова команды **ldapmodrdn** введите

```
ldapmodrdn -?
```

**Опции**

**-c** Режим непрерывной работы. Работа **ldapmodrdn** продолжается несмотря на выдачу сообщений об ошибках. По умолчанию программа после выдачи сообщения об ошибке прекращает работу.

**-C** *набор-символов*
Указывает, что строки, указанные в исходных данных утилиты **ldapmodrdn**, заданы в локальном наборе символов. Опцию **-C** *набор-символов* следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Поддерживаемые значения наборов символов перечислены в описании API ldap_set_iconv_local_charset(). Обратите внимание, что поддерживаемые значения наборов символов совпадают со значениями, поддерживаемыми необязательным тегом charset, определенным в файлах LDIF версии 1.

**-d** *уровень-отладки*
Устанавливает указанный уровень отладки LDAP.

**-D** *dn-подключения*
***DN-подключения*** применяется для подключения к каталогу LDAP. ***dn-подключения*** задается в виде строки. При использовании с -m DIGEST-MD5 оно задает ИД предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с ″u:″ или ″dn:″.

**-f** *файл*
Считывает информацию об изменении записей из файла LDIF, а не из стандартного потока ввода и не из командной строки (с помощью значений dn и новое-rdn). Стандартный поток ввода можно также получить из файла (< файл).

**-G** *область*
Задает область. Этот параметр необязателен. При использовании с -m DIGEST-MD5 значение передается серверу при подключении.

**-h** *хост*
Задает альтернативный хост, на котором работает сервер LDAP.

**-i** *файл* Считывает информацию об изменении записей из файла, а не из стандартного потока ввода и не из командной строки (с помощью значений rdn и новое-rdn). В стандартный поток ввода также можно направить информацию из файла (″< file″).

**-k** Указывает, что необходимо применять средства управления администрированием сервера.

**-K** *файл-ключей*
Задает имя файла базы данных ключей SSL. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла.

Если утилите не удается обнаружить базу данных ключей, то применяется набор надежных базовых сертификатов сертификатных компаний, заданный по умолчанию. Файл базы данных ключей, как правило, содержит один или несколько сертификатов сертификатных компаний (CA), сертификаты которых принимает клиент. Сертификаты X.509 этого типа известны также как надежные базовые сертификаты.

Этот параметр включает опцию **-Z**. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-m** *механизм*
Параметр ***механизм*** указывает механизм SASL, применяемый для подключения к серверу. Применяется API ldap_sasl_bind_s(). Если указано **-V 2**, то параметр **-m** игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации. Допустимые механизмы:

- CRAM-MD5 - защищает передаваемый серверу пароль.
- EXTERNAL - использует сертификат SSL. Требует указания ключа -Z.
- GSSAPI - использует разрешения Kerberos.
- Для DIGEST-MD5 необходимо, чтобы клиент отправлял на сервер имя пользователя. Требует указания ключа -U. Параметр -D (обычно это DN подключения) служит для указания ID предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с u: или dn:.
- OS400_PRFTKN - идентификация на локальном сервере LDAP в качестве текущего пользователя i5/OS посредством DN пользователя в спроецированной базе данных системы. Параметры -D (DN подключения) и -w (пароль) указывать не нужно.

**-M** Считает объекты переадресации обычными записями.

**-n** Показывает результаты выполнения операции, но не вносит изменения в записи. Применяется для отладки вместе с параметром **-v**.

**-N** *сертификат*
Задает метку, связанную с сертификатом клиента в файле базы данных ключей. Если сервер LDAP выполняет только идентификацию сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то может потребоваться сертификат клиента. Параметр ***имя-сертификата*** не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр ***сертификат*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-O** *макс.-число*
Параметр ***максимальное-число*** позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.

**-p** *порт*
Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если номер порта не задан, и указан параметр **-Z**, то применяется номер порта LDAP SSL по умолчанию, равный 636.

**-P** *пароль-файла-ключей*
Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, который может содержать один или несколько личных

ключей. Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-P** указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

**-r** Удаляет старые значения RDN записи По умолчанию старые значения сохраняются.

**-R** Отключает автоматический переход по ссылкам.

**–U** *имя-пользователя*
Задает имя пользователя. Необходим при использовании -m DIGEST-MD5 и игнорируется для других механизмов.

**-v** Подробный вывод, при котором создается множество диагностических сообщений.

**-V** *версия*
Задает версию LDAP, которая должна применяться утилитой **ldapmodrdn** при подключении к серверу LDAP. По умолчанию устанавливается соединение LDAP V3. Для явного выбора LDAP V3 укажите **-V 3**. Для работы в режиме приложения LDAP V2 укажите **-V 2**. Для таких приложений, как **ldapmodrdn**, предпочитаемым протоколом является LDAP V3. Вместо ldap_open в них применяется ldap_init.

**-w** *пароль* | **?**
***Пароль*** для идентификации. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?.

**-y dn-proxy**
Задает ИД сервера proxy для идентификации.

**–Y** Задает использование защищенного соединение LDAP (TLS).

**-Z** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**dn новое-rdn**
Дополнительная информация приведена в следующем разделе, “Формат ввода значений dn -новое-rdn”.

**Формат ввода значений dn -новое-rdn**

Если заданы аргументы командной строки *dn* и *новое-rdn*, то *новое-rdn* заменит собой RDN записи, DN которой задан значением *dn*. В противном случае файл (или стандартный поток ввода, если не задан флаг **- i**) должен содержать одну или несколько следующих записей:

```
Отличительное имя (DN)

Относительное отличительное имя (RDN)
```

Пары DN + RDN должны разделяться одной или несколькими пустыми строками.

**Примеры**

Допустим, что существует файл /tmp/entrymods, содержащий следующую информацию:

```
cn=Modify Me, o=University of Life, c=US
cn=The New Me
```

В этом случае команда

```
ldapmodrdn -r -i /tmp/entrymods
```

изменит RDN записи `Modify Me` с `Modify Me` на `The New Me` и старое `cn=Modify Me` будет удалено.

**Примечания**

Если информация о записи не указана в файле с помощью опции **-i** (или в командной строке с помощью значений *dn* и *rdn*), то команда **ldapmodrdn** будет ожидать ввода записей из стандартного потока ввода.

**Диагностика**

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

## ldapsearch

Утилита поиска записей LDAP

**Формат**

```
ldapsearch [-a преобразование] [-A] [-b база-поиска] [-B] [-C набор-символов] [-d уровень-отладки]
[-D dn-подключения] [-e] [-f файл] [-F разделитель] [-G область] [-h хост-ldap] [-i файл] [-K файл-ключей]
[-l предельное-время] [-L] [-m механизм] [-M] [-n] [-N сертификат]
[-o тип-атрибута] [-O макс.-число] [-p порт-ldap] [-P пароль-файла-ключей] [-q размер-страницы]
[-R] [-s область] [-t] [-T секунд] [-U имя-пользователя] [-v] [-V версия]
[-w пароль | ?] [-z предельный-размер] [-y dn-proxy] [-Y] [-Z]
filter [-9 p] [-9 s] [attrs...]
```

**Описание**

**ldapsearch** - это интерфейс командной строки к API ldap_search.

**ldapsearch** открывает соединение с сервером LDAP, подключается к нему и выполняет поиск с помощью фильтра. Фильтр должен быть указан в строковом формате фильтров LDAP (дополнительная информация о фильтрах приведена в описании API ldap_search в разделе API сервера каталогов).

Если утилита **ldapsearch** найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если атрибуты не указаны, то возвращаются все атрибуты.

Для просмотра справки по синтаксису вызова команды **ldapsearch** введите

**Опции**

**-a преобразование**
: Задает способ преобразования псевдонимов. Параметр Преобразование может принимать значения never, always, search и find, указывающие, соответственно, что псевдонимы не преобразуются, преобразуются всегда, преобразуются при поиске, либо преобразуются только при определении базового объекта для поиска. По умолчанию псевдонимы не преобразуются.

**-A**
: Получить только атрибуты (без значений). Эта опция применяется в случае, если нужно проверить наличие атрибутов в записи.

**-b база-поиска**
: База-поиска позволяет переопределить заданную по умолчанию начальную точку поиска. Если опция **-b** не указана, то утилита получает определение базы поиска из переменной среды LDAP_BASEDN. Если и это значение не задано, то применяется база по умолчанию ″″.

**-B**
: Не подавлять вывод значений, отличных от ASCII. Эта опция применяется при работе со значениями, использующими другие наборы символов, например, ISO-8859.1. Эта опция неявно задается, если указана опция **-L**.

**-C набор-символов**
: Указывает, что входные данные для утилиты ldapsearch заданы в локальном наборе символов. Входные данные включают в себя фильтр, DN-подключения и базовое DN. Аналогичным образом утилита **ldapsearch** преобразует полученные от сервера LDAP данные в указанный набор символов.

Опцию **-C** *набор-символов* следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Список поддерживаемых значений кодовых страниц приведен в описании API ldap_set_iconv_local_charset(). Кроме того, если указаны опции **-C** и **-L**, то считается, что входные данные заданы в указанном наборе символов, но при наличии в выводе непечатаемых символов вывод утилиты **ldapsearch** должен быть сохранен в кодировке UTF-8 или base-64. Поддержка такого требования связана с тем фактом, что стандартные файлы LDIF содержат только строковые данные в формате UTF-8 (или UTF-8 с кодировкой base-64 64). Обратите внимание, что поддерживаемые значения наборов символов совпадают со значениями, поддерживаемыми необязательным тегом charset, определенным в файлах LDIF версии 1.

**-d уровень-отладки**
Устанавливает указанный уровень отладки LDAP.

**-D dn-подключения**
DN-подключения применяется для подключения к каталогу LDAP. ***dn-подключения*** задается в виде строки (см. раздел Отличительные имена LDAP). При использовании с -m DIGEST-MD5 оно задает ИД предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с ″u:″ или ″dn:″.

**-e** Вывод информации о версии библиотеки LDAP и выход.

**-F разделитель**
Имена атрибутов отделяются от значений с помощью указанного разделителя. По умолчанию применяется разделитель `=’. Если указан флаг **-L**, то эта опция игнорируется.

**-G** *область*
Задает область. Этот параметр необязателен. При использовании с -m DIGEST-MD5 значение передается серверу при подключении.

**-h хост**
Задает альтернативный хост, на котором работает сервер LDAP.

**-i файл** Утилита считывает последовательность строк из файла, выполняя функцию поиска LDAP для каждой строки. В этом случае фильтр, заданный в командной строке, воспринимается как шаблон, в котором первое вхождение % заменяется на строку из файла. Если файл представляет собой отдельный символ ″-″, то строки считываются из стандартного ввода.

**-K файл-ключей**
Задает имя файла базы данных ключей SSL. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла.

Если утилите не удается обнаружить базу данных ключей, то применяется набор надежных базовых сертификатов сертификатных компаний, заданный по умолчанию. Файл базы данных ключей, как правило, содержит один или несколько сертификатов сертификатных компаний (CA), сертификаты которых принимает клиент. Сертификаты X.509 этого типа известны также как надежные базовые сертификаты.

Этот параметр включает опцию **-Z**. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-l ограничение-времени**
Ограничение на время поиска (в секундах).

**-L** Вывести результаты поиска в формате LDIF. Если указана эта опция, то применяется и опция **-B**, а опция **-F** игнорируется.

**-m** *механизм*
Параметр ***механизм*** указывает механизм SASL, применяемый для подключения к серверу. Применяется API ldap_sasl_bind_s(). Если указано **-V 2**, то параметр **-m** игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации. Допустимые механизмы:

- CRAM-MD5 - защищает передаваемый серверу пароль.

- EXTERNAL - использует сертификат SSL. Требует указания ключа -Z.
- GSSAPI - использует разрешения Kerberos.
- Для DIGEST-MD5 необходимо, чтобы клиент отправлял на сервер имя пользователя. Требует указания ключа -U. Параметр -D (обычно это DN подключения) служит для указания ID предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с u: или dn:.
- OS400_PRFTKN - идентификация на локальном сервере LDAP в качестве текущего пользователя i5/OS посредством DN пользователя в спроецированной базе данных системы. Параметры -D (DN подключения) и -w (пароль) указывать не нужно.

**-M** Считает объекты переадресации обычными записями.

**-n** Показывает результаты выполнения операции, но не вносит изменения в записи. Применяется для отладки вместе с параметром **-v**.

**-N сертификат**
Задает метку, связанную с сертификатом клиента в файле базы данных ключей.

**Примечание:** Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то может потребоваться сертификат клиента. Параметр *сертификат* указывать не нужно, если по умолчанию применяется сертификат и личный ключ. Кроме того, параметр *сертификат* не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-o** *тип-атрибута*
Параметр -o позволяет задать атрибут, применяемый для сортировки результатов поиска. Для более точного определения порядка сортировки можно указать несколько параметров -o. В следующем примере результаты поиска сначала сортируются по фамилии (sn), затем по имени (givenname), причем сортировка по имени выполняется в обратном порядке (по убыванию), на что указывает символ минус (-) перед этим атрибутом:

```
-o sn -o -givenname
```

Таким образом, используется следующий синтаксис параметров сортировки:

```
[-]<имя-атрибута>[:<OID-правила-соответствия>]
```

где

- `имя-атрибута` - имя атрибута, по которому должна выполняться сортировка.
- `OID-правила-соответствия` - необязательный OID правила соответствия, которое должно применяться при сортировке. Атрибут OID правила соответствия не поддерживается сервером каталогов, однако другие серверы LDAP могут поддерживать его.
- Знак минус (-) указывает, что результаты должны быть упорядочены в обратном порядке.
- Значение критичности всегда равно critical.

По умолчанию операция ldapsearch не сортирует результаты.

**-O макс.-число**
Позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.

**-p порт**
Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если номер порта не задан, и указан параметр **-Z**, то применяется номер порта LDAP SSL по умолчанию, равный 636.

**-P пароль-файла-ключей**

Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, который может содержать один или несколько личных ключей. Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-P** указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

**-q** *размер-страницы*

Существует два параметра, позволяющих настроить разбиение результатов поиска на страницы: -q (размер страницы запроса) и -T (время в секундах между операциями поиска). В следующем примере за один раз возвращается страница результатов, содержащая 25 записей. Результаты выдаются каждые 15 секунд до тех пор, пока не будут возвращены все полученные результаты поиска. Клиент ldapsearch поддерживает соединение с сервером для каждой возвращаемой страницы на всем протяжении операции поиска.

Эти параметры полезны, например, при наличии у клиента ограниченного объема ресурсов, либо при подключении через медленное соединение. В целом они позволяют управлять скоростью возврата данных сервером в ответе на запрос. Вместо получения всех результатов сразу, вы можете получать их небольшими блоками (страницами). Кроме того, вы можете задавать продолжительность задержки между запросами страниц, предоставляя тем самым клиенту время для обработки результатов.

```
-q 25  -T 15
```

Если указан параметр -v (подробный вывод), то ldapsearch после каждой страницы указывает количество возвращенных на данный момент записей, например, **всего возвращено 30 записей**

Поддерживается указание нескольких параметров -q, что позволяет указать различные размеры страниц для разных этапов одной и той же операции поиска. В следующем примере первая страница содержит 15 записей, вторая - 20, а третья завершает операцию поиска с постраничной выдачей результатов:

```
-q 15 -q 20 -q 0
```

В следующем примере первая страница содержит 15 записей, а вторая и все последующие, вплоть до завершения операции - по 20 записей.

```
-q 15 -q 20
```

По умолчанию операция ldapsearch возвращает в ответе на запрос все записи. Разбиение на страницы по умолчанию не выполняется.

**-R** Отключает автоматический переход по ссылкам.

**-s область**

Задает область поиска. Область может принимать значения base, one и sub, обозначающие базовый объект, поиск на одном уровне и в поддереве, соответственно. Значение по умолчанию - sub.

**-t** Запись полученных значений в набор временных файлов. Эта опция применяется для работы с двоичными значениями, такими как jpegPhoto и audio.

**-T** *секунды*

Время между операциями поиска (в секундах), Опция **-T** поддерживается только при указании опции **-q**.

**–U** *имя-пользователя*

Задает имя пользователя. Необходим при использовании -m DIGEST-MD5 и игнорируется для других механизмов.

**-v** Подробный вывод, при котором создается множество диагностических сообщений.

**-V** Задает версию LDAP, которая должна применяться утилитой ldapmodify при подключении к серверу LDAP. По умолчанию устанавливается соединение LDAP V3. Для явного выбора LDAP V3 укажите

″-V 3″. Значение ″-V 2″ указывает, что приложение должно работать в режиме LDAP V2. Для таких приложений, как ldapmodify, предпочитаемым протоколом является LDAP V3. Вместо ldap_open в них применяется ldap_init.

**-w** *пароль* **| ?**
***Пароль*** для идентификации. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?. .

**-y dn-proxy**
Задает ИД сервера proxy для идентификации.

**–Y** Задает использование защищенного соединение LDAP (TLS).

**-z ограничение-размера**
Число записей, возвращаемых в результате поиска, не должно превышать указанного значения. С его помощью можно задать максимальное число записей, возвращаемых в результате поиска.

**-Z** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**фильтр**
Задает строковое представление фильтра, применяемого при поиске. Простые фильтры можно указать в виде тип-атрибута=значение-атрибута. Более сложные фильтры задаются с помощью префиксной записи в соответствии со следующей диаграммой BNF:

```
<фильтр> ::='('<filtercomp>')'
<filtercomp> ::= <и>|<или>|<не>|<простой-фильтр>
<и> ::= '&' <список-фильтров>
<или> ::= '|' <список-фильтров>
<не> ::= '!' <фильтр>
<список-фильтров> ::= <фильтр>|<фильтр><список-фильтров>
<простой-фильтр> ::= <тип-атрибута><тип-фильтра>
<значение-атрибута>
<тип-фильтра> ::= '='|'~='|'<='|'>='
```

Конструкция ’~=’ позволяет обозначить приблизительное соответствие. Параметры <*тип-атрибута*> и <*значение-атрибута*> задаются согласно спецификации ″RFC 2252, LDAP V3 Attribute Syntax Definitions″ . Кроме того, если указан тип фильтра ’=’, то <*значение-атрибута*> может быть равно *, что означает проверку наличия атрибута, либо может содержать текст и звездочку (*), что означает проверку наличия заданной подстроки.

Например, фильтр ″mail=*″ позволяет найти все записи, содержащие атрибут mail. Фильтр ″mail=*@student.of.life.edu″ найдет все записи, в которых атрибут mail заканчивается указанной строкой. Для применения в фильтре скобок перед символами скобок необходимо указывать обратную косую черту (\).

**Примечание:** Фильтр `"cn=Bob *"`, где между строкой Bob и звездочкой (*) есть пробел, позволяет найти в каталоге IBM строку ″Bob Carter″, но не позволит найти строку ″Bobby Carter″. Пробел между символами ″Bob″ и символом подстановки (*) влияет на результат применения фильтров.

Более полное описание допустимых фильтров приведено в документе ″RFC 2254, A String Representation of LDAP Search Filters″ .

**Формат вывода**

Если найдена одна или несколько записей, то каждая запись передается в поток вывода в следующем формате:

```
Отличительное имя (DN)
имя-атрибута=значение
имя-атрибута=значение
имя-атрибута=значение
...
```

Записи разделяются пустыми строками. Если с помощью опции **-F** задан символ-разделитель, то он будет применяться вместо символа `=’. Если указана опция **-t**, то вместо фактического значения применяется имя временного файла.Если задана опция **-A**, то возвращается только часть, соответствующая значению ″имя-атрибута″.

**Примеры**

Команда:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

выполняет поиск в поддереве записей, у которых атрибут commonName равен ″john doe″ (применяется база поиска по умолчанию). В стандартный вывод передаются значения commonName и telephoneNumber. При обнаружении двух записей вывод может выглядеть, например, следующим образом:

```
  cn=John E Doe, ou="College of Literature, Science, and the Arts",
ou=Students, ou=People, o=University of Higher Learning, c=US
  cn=John Doe
  cn=John Edward Doe
  cn=John E Doe 1
  cn=John E Doe
  telephoneNumber=+1 313 555-5432

  cn=John B Doe, ou=Information Technology Division,
ou=Faculty and Staff, ou=People, o=University of Higher Learning, c=US
  cn=John Doe
  cn=John B Doe 1
  cn=John B Doe
  telephoneNumber=+1 313 555-1111
```

Команда:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

выполняет поиск в поддереве записей, в которых uid равен ″jed″. При этом применяется база поиска по умолчанию. Для найденных записей извлекаются и помещаются во временные файлы значения jpegPhoto и audio. При обнаружении одной записи, содержащей по одному значению каждого запрошенного атрибута вывод может выглядеть, например, следующим образом:

```
cn=John E Doe, ou=Information Technology Division,
  ou=Faculty and Staff,
```

```
ou=People, o=University of Higher Learning, c=US

audio=/tmp/ldapsearch-audio-a19924

jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

Команда:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

выполняет поиск на уровне c=US всех организаций, атрибут organizationName которых начинается со строки university. Результаты поиска отображаются в формате LDIF (см. описание формата обмена данными LDAP). В стандартный поток вывода передаются значения атрибутов organizationName и description. Вывод может выглядеть, например, следующим образом:

```
dn: o=University of Alaska Fairbanks, c=US

o: University of Alaska Fairbanks

description: Preparing Alaska for a brave new tomorrow

description: leaf node only


dn: o=University of Colorado at Boulder, c=US

o: University of Colorado at Boulder

description: No personnel information

description: Institution of education and research


dn: o=University of Colorado at Denver, c=US

o: University of Colorado at Denver

o: UCD

o: CU/Denver

o: CU-Denver

description: Institute for Higher Learning and Research


dn: o=University of Florida, c=US

o: University of Florida

o: UFl

description: Shaper of young minds


...
```

Команда:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

выполняет в поддереве c=US поиск всех записей класса persons. Специальный атрибут ibm-slapdDN, применяемый при поиске с сортировкой, позволяет упорядочить результаты поиска по строковому представлению отличительного имени (DN). Вывод может выглядеть, например, следующим образом:

```
cn=Al Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Al Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

Команда:

```
ldapsearch -h hostname -o sn -b "o=ibm,c=us" "title=engineer"
```

вернет все записи каталога сотрудников IBM, занимающих должность ″engineer″. Результаты будут упорядочены по фамилии (sn).

Команда:

```
ldapsearch -h hostname -o -sn -o cn -b "o=ibm,c=us" "title=engineer"
```

вернет все записи каталога сотрудников IBM, название должности которых (title) начинается со строки ″engineer″. Результаты будут упорядочены по убыванию фамилии (sn), а затем по возрастанию по общему имени (cn).

Команда:

```
ldapsearch -h hostname -q 5 -T 3 -b o=ibm,c=us "title=engineer"
```

будет возвращать по пять записей на странице с задержкой между страницами 3 секунды. Будут возвращены все записи каталога сотрудников IBM, название должности равно ″engineer″.

В этом примере продемонстрирован поиск с применением объекта переадресации. Как уже говорилось в разделе “Переадресация в каталоге LDAP” на стр. 50, каталоги LDAP сервера каталогов могут содержать объекты переадресации только со следующими элементами:

- Отличительное имя (`dn`).
- Атрибут objectClass (`objectClass`).
- Атрибут переадресации (`ref`).

Допустим, что в системе ’System_A’ есть следующая запись переадресации:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
ref: ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US objectclass: referral
```

Все атрибуты, связанные с этой записью, должны находиться в системе ’System_B’.

Система System_B содержит следующую запись:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
cn: Barb Jensen
objectclass: organizationalPerson
sn: Jensen
telephonenumber: (800) 555 1212
```

Когда клиент отправляет запрос системе 'System_A', сервер LDAP в системе System_A возвращает клиенту следующий URL:

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US
```

С помощью этой информации клиент отправляет запрос в систему System_B. Если запись в системе System_A содержит какие-либо еще атрибуты, помимо `dn`, `objectclass` и `ref`, то сервер игнорирует их (если не указан флаг **-R**, означающий игнорирование переадресации).

Получив от сервера в ответ на запрос ссылку, клиент отправляет новый запрос на сервер с указанным адресом. Новый запрос имеет ту же область, что и исходный. Результаты этого поиска зависят от указанного значения области поиска (**-b**).

Если указано значение `-s base`, как показано ниже:

```
ldapsearch -h System_A -b 'ou=Rochester, o=Big Company, c=US'
     -s base 'sn=Jensen'
```

то операция поиска возвращает все атрибуты всех записей с 'sn=Jensen', находящихся в системах System_A и System_B в `'ou=Rochester, o=Big Company, c=US'`.

Если указано значение `-s sub`, как показано ниже:

```
ldapsearch -s sub "cn=John"
```

то сервер будет искать все суффиксы и вернет все записи, для которых ″cn=John″. Такая операция называется поиском с пустой базой в поддереве. Вместо того, чтобы запускать несколько поисков с различными суффиксами в базе, поиск ведется по всему каталогу с помощью всего одного оператора. Поиск такого типа требует больше времени и ресурсов системы, поскольку в поиск вовлекается весь каталог (все суффиксы).

**Примечание:** Поиск в поддереве с пустой базой не возвращает ни информацию о схеме, ни данные протокола изменений, ни сведения от спроецированной базы данных в системе.

Если указано значение `-s sub`, как показано ниже:

```
ldapsearch -h System_A -b 'ou=Rochester, o=Big Company, c=US'
     -s sub 'sn=Jensen'
```

то операция поиска возвращает все атрибуты всех записей с 'sn=Jensen', находящихся в системах System_A и System_B на одном уровне с `'ou=Rochester, o=Big Company, c=US'` или на более глубоких уровнях.

Если указано значение `-s one`, как показано ниже:

```
ldapsearch -h System_A -b 'ou=Rochester, o=Big Company, c=US'
     -s one 'sn=Jensen'
```

то ни в одной системе значения не будут найдены. Вместо этого сервер возвратит клиенту ссылку на сервер:

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US
```

В этом случае клиент отправит следующий запрос:

```
ldapsearch -h System_B -b 'ou=Rochester, o=Big Company, c=US'
    -s one 'sn=Jensen'
```

В этом случае результаты поиска также будут отсутствовать, поскольку запись

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

находится в

```
ou=Rochester, o=Big Company, c=US
```

Опция `-s one` указывает, что следует искать записи на уровне, непосредственно следующем за

```
ou=Rochester, o=Big Company, c=US
```

**Диагностика**

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

## ldapchangepwd

Утилита изменения пароля LDAP.

**Формат**

```
ldapchangepwd -D dn-подключения -w пароль | ? -n новый-пароль| ?
[-C набор-символов] [-d уровень-отладки][-G область][-h хост-ldap]
[-K файл-ключей] [-m механизм] [-M] [-N сертификат]
[-O макс.-число] [-p порт-ldap] [-P пароль-файла-ключей] [-R]
[-U имя-пользователя] [-v] [-V версия] [-y dn-proxy] [-Y] [-Z] [-?]
```

**Описание**

Отправляет на сервер LDAP запрос на изменение пароля. Позволяет изменить пароль записи каталога.

**Опции**

**-C** *набор-символов*
: Указывает, что DN в исходных данных утилиты **ldapdelete** заданы в локальном наборе символов. Опцию **-C** *набор-символов* следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Список поддерживаемых значений кодовых страниц приведен в описании API ldap_set_iconv_local_charset().

**-d** *уровень-отладки*
: Устанавливает указанный уровень отладки LDAP.

**-D** *dn-подключения*
: ***DN-подключения*** применяется для подключения к каталогу LDAP. ***DN-подключения*** задается в виде строки. При использовании с -m DIGEST-MD5 оно задает ИД предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с ″u:″ или ″dn:″.

**–G** *область*
: Задает область. Этот параметр необязателен. При использовании с -m DIGEST-MD5 значение передается серверу при подключении.

**-h** *хост*
: Задает альтернативный хост, на котором работает сервер LDAP.

**-K** *файл-ключей*
: Задает имя файла базы данных ключей SSL. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла.

Если утилите не удается обнаружить базу данных ключей, то применяется набор надежных базовых сертификатов сертификатных компаний, заданный по умолчанию. Файл базы данных ключей, как правило, содержит один или несколько сертификатов сертификатных компаний (CA), сертификаты которых принимает клиент. Сертификаты X.509 этого типа известны также как надежные базовые сертификаты.

Этот параметр включает опцию **-Z**. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-m** *механизм*

Параметр ***механизм*** указывает механизм SASL, применяемый для подключения к серверу. Применяется API ldap_sasl_bind_s(). Если указано **-V 2**, то параметр **-m** игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации. Допустимые механизмы:

- CRAM-MD5 - защищает передаваемый серверу пароль.
- EXTERNAL - использует сертификат SSL. Требует указания ключа -Z.
- GSSAPI - использует разрешения Kerberos.
- Для DIGEST-MD5 необходимо, чтобы клиент отправлял на сервер имя пользователя. Требует указания ключа -U. Параметр -D (обычно это DN подключения) служит для указания ID предоставления прав доступа. Это может быть либо DN, либо строка authzId, начинающаяся с u: или dn:.

**-M** Считает объекты переадресации обычными записями.

**-n** *новый-пароль* **| ?**

Задает новый пароль. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?.

**-N** *сертификат*

Задает метку, связанную с сертификатом клиента в файле базы данных ключей. Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то может потребоваться сертификат клиента. Параметр ***имя-сертификата*** не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр ***сертификат*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-O** *макс.-число*

Параметр ***максимальное-число*** позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.

**-p** *порт*

Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если опция **-p** не указана, и указана опция **-Z**, то по умолчанию применяется порт SSL LDAP 636.

**-P** *пароль-файла-ключей*

Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, включая или несколько личных ключей. Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-P** указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

**-R** Отключает автоматический переход по ссылкам.

**-U** *имя-пользователя*

Задает имя пользователя. Необходим при использовании -m DIGEST-MD5 и игнорируется для других механизмов.

**-v** Подробный вывод, при котором создается множество диагностических сообщений.

**-V** *версия*
Задает версию LDAP, которая должна применяться утилитой **ldapdchangepwd** при подключении к серверу LDAP. По умолчанию устанавливается соединение LDAP V3. Для явного выбора LDAP V3 укажите **-V 3**. Для работы в режиме приложения LDAP V2 укажите **-V 2**. Для таких приложений, как **ldapdchangepwd**, предпочитаемым протоколом является LDAP V3. Вместо ldap_open в них применяется ldap_init.

**-w** *пароль* **| ?**
***Пароль*** для идентификации. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?.

**-y dn-proxy**
Задает ИД сервера proxy для идентификации.

**–Y** Задает использование защищенного соединение LDAP (TLS).

**-Z** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL. В случае работы с сервером каталогов в i5/OS указание опции -Z без опции -K и -N позволяет воспользоваться сертификатом, связанным с ИД приложения клиента сервера каталогов.

**-?** Показывает информацию о синтаксисе вызова команды ldapchangepwd.

**Примеры**

Команда

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

изменяет пароль записи с commonName ″John Doe″ со значения a1b2c3d4 на wxyz9876

**Диагностика**

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

## ldapdiff

Утилита синхронизации серверов-копий LDAP.

**Примечание:** Выполнение этой команды может потребовать очень много времени, в зависимости от числа копируемых записей (и числа атрибутов у каждой записи).

**Формат**

(Сравнивает и синхронизирует записи каталогов на двух серверах в среде копирования).

```
ldapdiff -b базовое-DN -sh хост -ch хост [-a] [-C число]
 [-cD dn] [-cK хранилище-ключей] [-cw пароль] -[cN метка-ключа]
 [-cp порт] [-cP пароль-хранилища-ключей]  [-cZ] [-F] [-L файл] [-sD dn] [-sK хранилище-ключей]
 [-sw пароль] -[sN метка-ключа] [-sp порт] [-sP пароль-хранилища-ключей]
 [-sZ] [-v]
```

или

(Сравнивает схемы двух серверов.)

```
 ldapdiff -S -sh хост -ch хост [-a] [-C число][-cD dn]
 [-cK хранилище-ключей] [-cw пароль] -[cN метка-ключа] [-cp порт]
 [-cP пароль-хранилища-ключей] [-cZ] [-L файл] [-sD dn]
 [-sK хранилище-ключей] [-sw пароль] [-sN метка-ключа] [-sp порт]
 [-sP пароль-хранилища-ключей] [-sZ] [-v]
```

**Описание**

Данный инструмент синхронизирует сервер-копию с главным сервером. Для просмотра справки по синтаксису вызова команды **ldapdiff** введите

```
ldapdiff -?
```

**Опции**

В команде **ldapdiff** применяются следующие опции. Все опции делятся на две подгруппы, одна из которых относится к серверу-поставщику, а вторая - к серверу-потребителю.

**-a** Указывает, что необходимо применять средства управления администрированием сервера для записи на сервер-копию, предназначенный только для чтения.

**-b** *базовое-DN*
База-поиска позволяет переопределить заданную по умолчанию начальную точку поиска. Если опция **-b** не указана, то утилита получает определение базы поиска из переменной среды LDAP_BASEDN.

**-C** *число*
Число обновляемых записей. Если будет найдено большее количество несовпадений, то операция выполнена не будет.

**-F** Опция исправления. Если она указана, то данные на сервере-потребителе будут изменены в соответствии с данными на сервере-поставщике. Если указана также опция **-S**, то сделать это нельзя.

**-L** Если опция **-F** не указана, то воспользуйтесь этой опцией для создания файла вывода LDIF. С помощью файла LDIF можно обновить сервер-поставщик и устранить различия.

**-S** Указывает на необходимость сравнения схем на серверах.

**-v** Подробный вывод, при котором создается множество диагностических сообщений.

**Опции сервера-поставщика**

Следующие опции относятся к серверу-потребителю. Первым символом в именах таких опция является символ ’s’.

**-sD** *dn* Для подключения к каталогу LDAP будет применяться указанное ***dn***. ***DN*** задается в виде строки.

**-sh** *хост*
Задает имя хоста

**-sK** *хранилище-ключей*
Укажите имя файла базы данных ключей SSL с расширением по умолчанию **kdb**. Если этот параметр не указан или в нем задана пустая строка (-sK″″), то применяется системное хранилище ключей. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла.

**-sN** *метка-ключа*
Задает метку, связанную с сертификатом клиента в файле базы данных ключей. Если метка указана без указания хранилища ключей, значит метка является идентификатором приложения в диспетчере цифровых сертификатов (DCM). Метка по умолчанию (ИД приложения) - QIBM_GLD_DIRSRV_CLIENT. Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то необходим сертификат клиента. ***метка-ключа*** не требуется, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр ***метка-ключа*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-sZ** и **-sK**, то этот параметр игнорируется.

**-sp** *порт*

Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если опция **-sp** не указана, и указана опция **-sZ**, то по умолчанию применяется порт SSL LDAP 636.

**-sP** *пароль-хранилища-ключей*

Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, включая или несколько личных ключей. Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-sP** указывать не нужно. Если не указаны параметры **-sZ** и **-sK**, то этот параметр игнорируется.Если используется файл сохранения паролей хранилища ключей, то пароль не применяется.

**-st** *тип-хранилища*

Укажите метку, связанную с сертификатом клиента в файле базы данных. Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если на сервере LDAP настроена идентификация клиента и сервера, то может потребоваться сертификат клиента. Параметр ***тип-хранилища*** не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр ***тип-хранилища*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-sZ** и **-sT**, то этот параметр игнорируется.

**-sZ** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL.

**Опции сервера-потребителя**

Следующие опции относятся к серверу-потребителю. Первым символом в именах таких опция является символ 'c'. Для удобства пользователей, если опция -cZ указана без указания значений -cK, -cN или -cP, то в этих опциях применяются те же значения SSL, что и для поставщика. Для переопределения опций поставщика и применения значений по умолчанию укажите -cK ″″ -cN ″″ -cP ″″.

**-cD** *dn* Для подключения к каталогу LDAP будет применяться указанное ***dn***. ***DN*** задается в виде строки.

**-ch** *хост*

Задает имя хоста

**-cK** *хранилище-ключей*

Задает имя файла базы данных ключей SSL с расширением по умолчанию kdb. Если в этом параметре задана пустая строка (-sK″″), то применяется системное хранилище ключей. Если файл базы данных ключей находится не в текущем каталоге, то следует указать полное имя файла.

**-cN** *метка-ключа*

Задает метку, связанную с сертификатом клиента в файле базы данных ключей. Если на сервере LDAP настроена только идентификация сервера, то сертификат клиента не нужен. Если метка указана без указания хранилища ключей, значит метка является идентификатором приложения в диспетчере цифровых сертификатов (DCM). Метка по умолчанию (ИД приложения) - QIBM_GLD_DIRSRV_CLIENT. Если на сервере LDAP настроена идентификация клиента и сервера, то необходим сертификат клиента. ***метка-ключа*** не требуется, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр ***метка-ключа*** не нужно указывать, если файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-cZ** и **-cK**, то этот параметр игнорируется.

**-cp** *порт*

Задает порт TCP, с помощью которого сервер LDAP принимает запросы. По умолчанию номер порта LDAP равен 389. Если опция **-cp** не указана, и указана опция **-cZ**, то по умолчанию применяется порт SSL LDAP 636.

**-cP** *пароль-хранилища-ключей*

Задает пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей, включая или несколько личных ключей. Если с файлом

базы данных ключей связан файл пароля, пароль считывается из файла, и параметр **-cP** указывать не нужно. Если не указаны параметры **-cZ** и **-cK**, то этот параметр игнорируется.

**-cw** *пароль* **| ?**
***Пароль*** для идентификации. Для того чтобы было показано приглашение для ввода пароля, укажите значение ?.

**-cZ** Указывает, что для обмена данными с сервером LDAP должно применяться защищенное соединение SSL.

**Примеры**

```
ldapdiff -b <базовое-DN> -sh <хост-поставщика> -ch <хост-приемника> [опции]
```

или

```
ldapdiff -S  -sh <хост-поставщика> -ch <хост-приемника> [опции]
```

**Диагностика**

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

## Применение SSL в утилитах командной строки LDAP

Раздел “Поддержка протоколов SSL и TLS на сервере каталогов” на стр. 51 содержит информацию о применении SSL на сервере каталогов. В том числе, в этом разделе приведены сведения о создании и управлении уполномоченными сертификатными компаниями с помощью Диспетчера цифровых сертификатов.

Некоторые серверы LDAP, с которыми работают клиенты, применяют только идентификацию сервера. Для этих серверов достаточно определить в хранилище сертификатов один или два надежных базовых сертификата. Идентификация сервера позволяет клиентам убедиться в том, что сертификат целевого сервера LDAP был выдан одной из уполномоченных сертификатных компаний (CA). Все данные LDAP передаются по соединению SSL в зашифрованном виде. В том числе, зашифровываются и одноразовое разрешение LDAP, которое указывается в интерфейсах прикладных программ (API), применяемых для подключения к серверу каталогов. Например, если сервер LDAP применяет надежный сертификат Verisign, то необходимо выполнить следующие действия:
1. Получить сертификат сертификатной компании Verisign.
2. Импортировать этот сертификат с помощью DCM в хранилище сертификатов.
3. С помощью DCM назначить этот сертификат надежным базовым сертификатом.

Если сертификат сервера LDAP был выдан локальной сертификатной компанией, администратор сервера должен предоставить вам копию файла запроса на получение сертификата сервера. Импортируйте файл запроса на получение сертификата в хранилище сертификатов и назначьте его надежным базовым сертификатом.

Если утилиты оболочки применяются для работы с сервером LDAP, поддерживающим идентификацию клиента и сервера, необходимо выполнить следующие действия:

- Определить один или несколько надежных базовых сертификатов в хранилище сертификатов. Это позволит клиенту убедиться в том, что сертификат целевого сервера LDAP был выдан одной из уполномоченных сертификатных компаний. Все данные LDAP передаются по соединению SSL в зашифрованном виде. В том числе, зашифровываются и одноразовое разрешение LDAP, которое указывается в интерфейсах прикладных программ (API), применяемых для подключения к серверу каталогов.
- Создайте пару ключей и отправьте запрос на получение сертификата клиента в сертификатную компанию. Получив подписанный сертификат от сертификатной компании, поместите его в файл ключей на клиенте.

# Формат обмена данными LDAP (LDIF)

В этом разделе описан формат обмена данными LDAP (LDIF), применяемый утилитами ldapmodify, ldapsearch и ldapadd. Описанный здесь формат LDIF поддерживается также утилитами сервера, входящими в состав сервера каталогов IBM Directory.

Формат LDIF предназначен для текстового представления записей LDAP. Запись LDIF задается в следующем формате:

```
dn: <отличительное-имя>
<тип-атрибута> : <значение-атрибута>
<тип-атрибута> : <значение-атрибута>
...
```

Строку можно продолжить на следующей строке, указав в начале следующей строки одиночный символ пробела или табуляции, например:

```
dn: cn=John E Doe, o=University of Higher
 Learning, c=US
```

Если атрибут имеет несколько значений, то каждое значение указывается на отдельной строке, например:

```
      cn: John E Doe
cn: John Doe
```

Если <*значение-атрибута*> содержит символы, не входящие в набор US-ASCII, либо начинается с пробела или двоеточия ':', то после <*типа-атрибута*> указывается двойное двоеточие и значение задается в формате base-64. Например, значение ″ begins with a space″ записывается следующим образом:

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Несколько записей, находящихся в одном файле LDIF, разделяются пустой строкой. Несколько пустых строк подряд считаются логическим символом конца файла.

Дополнительная информация приведена в следующих разделах:

- "Пример: LDIF"
- "Поддержка LDIF версии 1" на стр. 235
- "Примеры: LDIF версии 1" на стр. 235

## Пример: LDIF

Ниже приведен пример файла LDIF с тремя записями.

```
dn: cn=John E Doe, o=University of High
 er Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: person
sn: Doe

dn: cn=Bjorn L Doe, o=University of High
 er Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: person
sn: Doe

dn: cn=Jennifer K. Doe, o=University of High
 er Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: person
sn: Doe
```

```
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
 A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
 ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

Фотография (jpegPhoto) для записи Jennifer Jensen закодирована в формате base-64. Значения текстовых атрибутов также можно задавать в формате base-64. Однако в этом случае кодировка base-64 должна соответствовать формату передачи протокола (т.е. IA5 для LDAP V2 и UTF-8 для LDAP V3).

## Поддержка LDIF версии 1

Клиентские утилиты (ldapmodify и ldapadd) теперь распознают последнюю версию LDIF, обозначаемую тегом ″version: 1″ в начале файла. В отличие от исходной версии LDIF, в новой версии поддерживаются значения атрибутов в кодировке UTF-8 (в отличие от старого и крайне ограниченного набора символов US-ASCII).

Однако создание файлов LDIF со значениями UTF-8 вручную может оказаться очень непростой задачей. Для того чтобы упростить этот процесс, была добавлена поддержка расширения набора символов для формата LDIF. В этом расширении разрешается указывать имя набора символов IANA в заголовке файла LDIF (рядом с номером версии). Поддерживаются не все наборы символов IANA.

Версия 1 формата LDIF поддерживает также URL файлов. Тем самым обеспечивается более гибкий подход к указанию определений файлов. URL файлов имеют следующий вид:

```
      атрибут:< file:///путь (где синтаксис пути
определяется платформой)
```

Например, следующая строка является допустимым адресом файла Web:

```
      jpegphoto:< file:///d:\temp\photos\myphoto.jpg    (путь в формате DOS/Windows)
      jpegphoto:< file:///etc/temp/photos/myphoto.jpg   (путь в формате Unix)
```

**Примечание:** Утилиты сервера IBM Directory независимо от версии поддерживают как новую спецификацию URL файлов, так и старый формат (″jpegphoto: /etc/temp/myphoto″). Другими словами, новый формат URL файлов может применяться без добавления в файлы LDIF тега версии.

## Примеры: LDIF версии 1

Для того чтобы утилиты автоматически преобразовывали набор символов в UTF-8, этот набор символов нужно указать в теге charset, например:

```
 version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:> file:///usr/local/photos/jgriego.jpg
```

В этом примере все значения, указанные после имени атрибута и одного двоеточия, преобразуются из ISO-8859-1 в UTF-8. Значения после имени атрибута и двоеточия (например, description:: V2hhdCBhIGNhcm...) должны быть заданы в кодировке Base-64. Ожидается, что они будут представлять собой двоичные значения или символьные строки UTF-8. Значения, прочитанные из файла (такие как атрибут jpegPhoto, заданный выше в адресе Web), должны быть в том же формате. Эти значения не преобразуются из указанной кодировки в UTF-8.

В данном примере файла LDIF, не содержащего тега charset, предполагается, что файл содержит данные в UTF-8, UTF-8 в кодировке base-64 или двоичные данные в кодировке base-64:

```
# Пример файла LDIF IBM Directory
 #
 # Перед загрузкой этих данных нужно определить суффикс "o=IBM, c=US"
 #

 version: 1

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Этот же файл можно использовать без тега version: 1, как в предыдущих выпусках of the IBM Directory:

```
 # Пример файла LDIF IBM Directory
 #
 # Перед загрузкой этих данных нужно определить суффикс "o=IBM, c=US"
 #

 dn: o=IBM, c=US
 objectclass: top
 objectclass: organization
 o: IBM

 dn: ou=Austin, o=IBM, c=US
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

**Примечание:** Значения текстовых атрибутов можно задавать в формате base-64.

---

## Схема конфигурации сервера каталогов

В этом разделе описано дерево информации каталога (DIT) и атрибуты, которые задаются в файле конфигурации ibmslapd.conf. В предыдущих выпусках параметры конфигурации каталога хранились в файле конфигурации в особом формате. Теперь параметры каталога хранятся в файле конфигурации в формате LDIF.

Файл конфигурации называется ibmslapd.conf. Кроме того, в этом выпуске доступна схема, применяемая файлом конфигурации. Типы атрибутов определены в файле v3.config.at, а классы объектов определены в файле v3.config.oc. Атрибуты можно изменить с помощью команды ldapmodify. Дополнительная информация о команде ldapmodify приведена в разделе “ldapmodify и ldapadd” на стр. 203.

- “Дерево информации каталога”
- “Атрибуты” на стр. 246

## Дерево информации каталога

cn=Configuration

- cn=Admin
- cn=Event Notification
- cn=Front End
- cn=Kerberos
- cn=Master Server
- cn=Referral
- cn=Schema

  - cn=IBM Directory
    - cn=Config Backends
      - cn=ConfigDB
    - cn=RDBM Backends
      - cn=Directory
      - cn=ChangeLog
    - cn=LDCF Backends
      - cn=SchemaDB
- cn=SSL
  - cn=CRL
- cn=Transaction

**cn=Configuration**

**DN** cn=Configuration

**Описание**

Это запись верхнего уровня в DIT конфигурации. Она содержит общую и, часто, дополнительную информацию. Атрибуты в этой записи получены из первого (глобального) раздела файла ibmslapd.conf.

**Количество**

1 (обязательно)

**Класс объектов**

ibm-slapdTop

**Обязательные атрибуты**

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

**Дополнительные атрибуты**

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

**cn=Admin**

**DN** cn=Admin, cn=Configuration

**Описание**
Глобальные параметры демона администрирования IBM.

**Количество**
1 (обязательно)

**Класс объектов**
ibm-slapdAdmin

**Обязательные атрибуты**

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

**Дополнительные атрибуты**

- ibm-slapdSecurePort

### cn=Event Notification

**DN** cn=Event Notification, cn=Configuration

**Описание**
Глобальные параметры уведомления о событии для сервера каталогов.

**Количество**
0 или 1 (необязательный; применяется только в случае уведомления о событиях)

**Класс объектов**
ibm-slapdEventNotification

**Обязательные атрибуты**

- cn
- ibm-slapdEnableEventNotification
- objectClass

**Дополнительные атрибуты**

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

### cn=Front End

**DN** cn=Front End, cn=Configuration

**Описание**
Глобальные параметры среды, которые устанавливаются сервером во время запуска.

**Количество**
0 или 1 (необязательно)

**Класс объектов**
ibm-slapdFrontEnd

**Обязательные атрибуты**

- cn
- objectClass

**Дополнительные атрибуты**

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP

- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

**cn=Kerberos**

**DN** cn=Kerberos, cn=Configuration

**Описание**
Глобальные параметры идентификации Kerberos для сервера каталогов.

**Количество**
0 или 1 (необязательно)

**Класс объектов**
ibm-slapdKerberos

**Обязательные атрибуты**

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

**Дополнительные атрибуты**

- Нет

**cn=Master Server**

**DN** cn=Master Server, cn=Configuration

**Описание**
При настройке копии в этой записи находятся параметры подключения и URL главного сервера.

**Количество**
0 или 1 (необязательно)

**Класс объектов**
ibm-slapdReplication

**Обязательные атрибуты**

- cn
- ibm-slapdMasterPW (обязательный, если не применяется идентификация Kerberos.)

**Дополнительные атрибуты**

- ibm-slapdMasterDN
- ibm-slapdMasterPW (необязательный, если применяется идентификация Kerberos.)
- ibm-slapdMasterReferral
- objectClass

**cn=Referral**

**DN** cn=Referral, cn=Configuration

**Описание**

Эта запись содержит все адреса для переадресации, указанные в первом (глобальном) разделе файла ibmslapd.conf. Если ни один адрес не задан (как, например, в конфигурации по умолчанию), то эта запись является необязательной.

**Количество**

0 или 1 (необязательно)

**Класс объектов**

ibm-slapdReferral

**Обязательные атрибуты**

- cn
- ibm-slapdReferral
- objectClass

**Дополнительные атрибуты**

- Нет

### cn=Schemas

**DN** cn=Schemas, cn=Configuration

**Описание**

Эта запись содержит информацию о схемах. Она не является обязательной, так как все схемы можно задать с помощью класса объектов ibm-slapdSchema. Однако она позволяет упростить структуру DIT.

В настоящий момент допустима только одна запись схемы: cn=IBM Directory.

**Количество**

1 (обязательно)

**Класс объектов**

Container

**Обязательные атрибуты**

- cn
- objectClass

**Дополнительные атрибуты**

- Нет

### cn=IBM Directory

**DN** cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**

Эта запись содержит всю информацию о конфигурации схемы, указанную в первом (глобальном) разделе файла ibmslapd.conf. Кроме того, она содержит сведения о базах данных, использующих данную схему. В данном продукте в настоящее время поддерживается только одна схема. Если бы поддерживалось несколько схем, то для каждой из них нужно было бы указать одну запись ibm-slapdSchema. Предполагается, что различные схемы несовместимы между собой. Следовательно, с базой данных может быть связана только одна схема.

**Количество**

1 (обязательно)

**Класс объектов**

ibm-slapdSchema

**Обязательные атрибуты**

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

**Дополнительные атрибуты**

- ibm-slapdSchemaAdditions

### cn=Config Backends

**DN** cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**

Эта запись содержит информацию о базах данных конфигурации.

**Количество**

1 (обязательно)

**Класс объектов**

Container

**Обязательные атрибуты**

- cn
- objectClass

**Дополнительные атрибуты**

Нет

### cn=ConfigDB

**DN** cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**

Базовое хранилище данных конфигурации сервера IBM Directory Server

**Количество**

0 - n (необязательно)

**Класс объектов**

ibm-slapdConfigBackend

**Обязательные атрибуты**

- ibm-slapdSuffix
- ibm-slapdPlugin

**Дополнительные атрибуты**

- ibm-slapdReadOnly

### cn=RDBM Backends

**DN** cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**

Эта запись содержит информацию о базах данных RDBM. Она применяется вместо строки database rdbm из файла ibmslapd.conf. Все вложенные в нее записи описывают базы данных DB2. Эта запись не является обязательной, так как базы данных RDBM можно задать с помощью класса объектов ibm-slapdRdbmBackend. Однако она позволяет упростить структуру DIT.

**Количество**

0 или 1 (необязательно)

**Класс объектов**
Container

**Обязательные атрибуты**

- cn
- objectClass

**Дополнительные атрибуты**

- Нет

### cn=Directory

**DN** cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**
Эта запись содержит все параметры конфигурации RDBM по умолчанию.

Хотя можно создать несколько баз данных с различными именами, программа администрирования сервера предполагает, что каталог основной базы данных - это ″cn=Directory″, а каталог необязательного протокола изменений - это ″cn=ChangeLog″. С помощью интерфейса Администрирование сервера можно настраивать только те суффиксы, которые содержатся в ″cn=Directory″ (а также суффикс change, которые настраивается при включении функции ведения протокола изменений).

**Количество**
0 - n (необязательно)

**Класс объектов**
ibm-slapdRdbmBackend

**Обязательные атрибуты**

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

**Дополнительные атрибуты**

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix

- ibm-slapdUseProcessIdPw

**Примечание:** Если применяется атрибут **ibm-slapdUseProcessIdPw**, то необходимо изменить схему таким образом, чтобы атрибут **ibm-slapdDbUserPW** стал необязательным.

**cn=Change Log**

**DN** cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**
Эта запись содержит все параметры конфигурации базы данных протокола изменений.

**Количество**
0 - n (необязательно)

**Класс объектов**
ibm-slapdRdbmBackend

**Обязательные атрибуты**

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

**Дополнительные атрибуты**

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

**Примечание:** Если применяется атрибут **ibm-slapdUseProcessIdPw**, то необходимо изменить схему таким образом, чтобы атрибут **ibm-slapdDbUserPW** стал необязательным.

**cn=LDCF Backends**

**DN** cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**

Эта запись содержит информацию о базах данных LDCF. Она заменяет строку database ldcf из файла ibmslapd.conf. Все вложенные в нее записи описывают базы данных LDCF. Эта запись не является обязательной, так как базы данных LDCF можно задать с помощью класса объектов ibm-slapdLdcfBackend. Однако она позволяет упростить структуру DIT.

**Количество**

1 (обязательно)

**Класс объектов**

Container

**Обязательные атрибуты**

- cn
- objectClass

**Дополнительные атрибуты**

- ibm-slapdPlugin

### cn=SchemaDB

**DN** cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**Описание**

Эта запись содержит всю информацию о конфигурации базы данных из раздела с описанием базы данных ldcf файла ibmslapd.conf.

**Количество**

1 (обязательно)

**Класс объектов**

ibm-slapdLdcfBackend

**Обязательные атрибуты**

- cn
- objectClass

**Дополнительные атрибуты**

- ibm-slapdPlugin
- ibm-slapdSuffix

### cn=SSL

**DN** cn=SSL, cn=Configuration

**Описание**

Глобальные параметры соединений SSL для сервера каталогов.

**Количество**

0 или 1 (необязательно)

**Класс объектов**

ibm-slapdSSL

**Обязательные атрибуты**

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

**Дополнительные атрибуты**

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  **Примечание:** **ibm-slapdSslCipherSpecs** теперь не применяется. Вместо него используется атрибут **ibm-slapdSslCipherSpec**. Если вы укажете атрибут **ibm-slapdSslCipherSpecs**, он будет преобразован сервером в поддерживаемый атрибут.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

### cn=CRL

**DN** cn=CRL, cn=SSL, cn=Configuration

**Описание**

Эта запись содержит информацию о списке аннулированных сертификатов из первого (глобального) раздела файла ibmslapd.conf. Эта запись необходима только в том случае, если в записи cn=SSL задан атрибут ″ibm-slapdSslAuth = serverclientauth″, и клиентам были выданы сертификаты для проверки CRL.

**Количество**

0 или 1 (необязательно)

**Класс объектов**

ibm-slapdCRL

**Обязательные атрибуты**

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

**Дополнительные атрибуты**

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

### cn=Transaction

**DN** cn = Transaction, cn = Configuration

**Описание**

Задает глобальные параметры транзакций. Поддержка транзакций обеспечивается следующим встраиваемым модулем:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Сервер (**slapd**) автоматически загружает этот встраиваемый модуль во время запуска, если указан атрибут **ibm-slapdTransactionEnable = TRUE**. Встраиваемый модуль не нужно явно добавлять в файл **ibmslapd.conf**.

**Количество**

0 или 1 (необязательный; применяется только в случае использования транзакций.)

**Класс объектов**

ibm-slapdTransaction

**Обязательные атрибуты**

- cn

- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

**Дополнительные атрибуты**

- Нет

## Атрибуты

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeAutoAdjust
- ibm-slapdCachedAttributeAutoAdjustTime
- ibm-slapdCachedAttributeAutoAdjustTimeInterval
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog

- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit

- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

**cn**

**Описание**
Атрибут X.500, хранящий имя объекта.

**Синтаксис**
Directory string

**Максимальная длина**
256

**Значение**
Список значений

**ibm-slapdACIMechanism**

**Описание**
Задает модель ACL, применяемую сервером. (Поддерживается только в моделях i5/OS и OS/400, начиная с выпуска v3.2, в других платформах игнорируется.)

- 1.3.18.0.2.26.1 = Модель ACL IBM SecureWay v3.1
- 1.3.18.0.2.26.2 = Модель ACL IBM SecureWay v3.2

**По умолчанию**
1.3.18.0.2.26.2 = Модель ACL IBM SecureWay v3.2

**Синтаксис**
Directory string

**Максимальная длина**
256

**Значение**
Список значений.

**ibm-slapdACLAccess**

**Описание**
Указывает, разрешен ли доступ к ACL. Если значение равно TRUE, то доступ к ACL разрешен. Если значение равно FALSE, доступ к ACL запрещен.

**По умолчанию**
TRUE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

### ibm-slapdACLCache

**Описание**
Указывает, заносит ли сервер в кэш информацию ACL.

- Если значение равно TRUE, то сервер заносит в кэш информацию ACL.
- Если значение равно FALSE, то сервер не заносит в кэш информацию ACL.

**По умолчанию**
TRUE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

### ibm-slapdACLCacheSize

**Описание**
Максимальное число записей в кэше ACL.

**По умолчанию**
25000

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdAdminDN

**Описание**
DN администратора для подключения к серверу каталогов.

**По умолчанию**
cn=root

**Синтаксис**
DN

**Максимальная длина**
Не ограничена

**Значение**
Одно значение

**ibm-slapdAdminGroupEnabled**

**Описание**
Указывает, разрешена ли в данный момент группа администраторов. Значение TRUE этого атрибута обозначает, что члены группы администраторов могут входить на сервер.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Максимальная длина**
128

**Значение**
Одно значение

**ibm-slapdAdminPW**

**Описание**
Пароль администратора для подключения к серверу каталогов.

**По умолчанию**
secret

**Синтаксис**
Binary

**Максимальная длина**
128

**Значение**
Одно значение

**ibm-slapdAllowAnon**

**Описание**
Указывает, разрешены ли анонимные подключения.

**По умолчанию**
True

**Синтаксис**
Boolean

**Максимальная длина**
128

**Значение**
Одно значение

**ibm-slapdAllReapingThreshold**

**Описание**
Задает количество соединений, обрабатываемых на сервере до активизации управления соединениями.

**По умолчанию**
1200

**Синтаксис**
Строка каталога с точным соответствием.

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdAnonReapingThreshold**

**Описание**
Задает количество соединений, обрабатываемых на сервере до активизации управления анонимными соединениями.

**По умолчанию**
0

**Синтаксис**
Directory string with case-exact matching.

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdBoundReapingThreshold**

**Описание**
Задает количество соединений, обрабатываемых на сервере до активизации управления анонимными соединениями и подключениями.

**По умолчанию**
1100

**Синтаксис**
Directory string with case-exact matching.

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdBulkloadErrors**

**Описание**
Файл или устройство хоста ibmslapd, на которое будут отправляться сообщения об ошибках утилиты bulkload.

**По умолчанию**
/var/bulkload.log

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdCachedAttribute**

**Описание**
Содержит имена атрибутов, сохраненных в кэше атрибутов. Каждое значение представляет собой одно имя.

**По умолчанию**
Нет

**Синтаксис**
Directory string

**Максимальная длина**
256

**Значение**
Список значений

### ibm-slapdCachedAttributeAutoAdjust

**Описание**
Указывает, должен ли сервер автоматически запускать кэширование атрибутов в указанный период времени. Период определяется атрибутами ibm-slapdCachedAttributeAutoAdjustTime и ibm-slapdCachedAttributeAutoAdjustTimeInterval.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

### ibm-slapdCachedAttributeAutoAdjustTime

**Описание**
Если значение атрибута ibm-slapdCachedAttributeAutoAdjust равно TRUE, то этот атрибут указывает время, когда на сервере начнется процесс автоматического кэширования атрибутов.

```
Минимум = T000000
Максимум = T235959
```

**По умолчанию**
T000000

**Синтаксис**
Формат Military time

**Максимальная длина**
7

**Значение**
Одно значение

### ibm-slapdCachedAttributeAutoAdjustTimeInterval

**Описание**
Если значение атрибута ibm-slapdCachedAttributeAutoAdjust равно TRUE, то этот атрибут управляет интервалом между процессами автоматического кэширования атрибутов.

```
Минимум = 1
Максимум = 24
```

**По умолчанию**
2

**Синтаксис**
Integer

**Максимальная длина**
2

**Значение**
Одно значение

**ibm-slapdCachedAttributeSize**

**Описание**
Объем памяти для кэша атрибутов (в байтах). Нулевое значение указывает, что кэш атрибутов не используется.

**По умолчанию**
0

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение.

**ibm-slapdChangeLogMaxEntries**

**Описание**
Этот атрибут применяется функцией ведения протокола изменений. Он задает максимальное число записей в базе данных RDBM протокола изменений. Для каждого протокола изменений задается собственный атрибут changeLogMaxEntries.

```
Минимум = 0 (не ограничено). Максимум = 2 147 483 647 (32-разрядное целое число
со знаком)
```

**По умолчанию**
0

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

**ibm-slapdCLIErrors**

**Описание**
Файл или устройство хоста ibmslapd, на которое будут записываться сообщения об ошибках CLI.

**По умолчанию**
/var/db2cli.log

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdConcurrentRW

**Описание**
Если атрибут равен TRUE, то операции поиска и обновления могут выполняться одновременно. Это значение разрешает ″черновое чтение″, возвращающее результат, который может не совпадать с зафиксированным состоянием базы данных.

**Внимание:** Это устаревший атрибут.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

### ibm-slapdDB2CP

**Описание**
Задает кодовую страницу базы данных каталога. Для баз данных UTF-8 применяется кодовая страница 1208.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdDBAlias

**Описание**
Псевдоним базы данных DB2.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
8

**Значение**
Одно значение

### ibm-slapdDbConnections

**Описание**
Задает число соединений, которое сервер выделяет для работы с базой данных DB2. Допустимы значения от 5 до 50 (включительно).

**Примечание:** Значение этого атрибута переопределяется значением переменной среды ODBCCONS.

Если указано значение ibm-slapdDbConnections (или ODBCCONS) меньше 5 или больше 50, то сервер будет применять значения 5 и 50, соответственно. Одно дополнительное соединение создается для копирования данных (даже если не определен ни один сервер-копия). Два дополнительных соединения создаются для протокола изменений (если опция ведения протокола изменений включена).

**По умолчанию**
15

**Синтаксис**
Integer

**Максимальная длина**
50

**Значение**
Одно значение

### ibm-slapdDbInstance

**Описание**
Указывает применяемый экземпляр базы данных DB2.

**По умолчанию**
ldapdb2

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
8

**Значение**
Одно значение

**Примечание:** Все объекты ibm-slapdRdbmBackend должны применять одинаковые ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW и набор символов DB2.

### ibm-slapdDbLocation

**Описание**
Путь к базе данных в файловой системе.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdDbName

**Описание**
Указывает имя применяемой базы данных DB2.

**По умолчанию**
ldapdb2

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
8

**Значение**
Одно значение

**ibm-slapdDbUserID**

**Описание**
Задает имя пользователя для подключения к применяемой базе данных DB2.

**По умолчанию**
ldapdb2

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
8

**Значение**
Одно значение

**Примечание:** Все объекты ibm-slapdRdbmBackend должны применять одинаковые ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW и набор символов DB2.

**ibm-slapdDerefAliases**

**Описание**
Задает максимальный уровень учета псевдонимов в запросах на поиск, независимо от значений derefAliases, заданных в клиентских запросах. Допустимые значения: **never**, **find**, **search** и **always**.

**По умолчанию**
always

**Синтаксис**
Directory string

**Максимальная длина**
6

**Значение**
Одно значение

**ibm-slapdDbUserPW**

**Описание**
Задает пароль пользователя для подключения к применяемой базе данных DB2. Пароль может быть указан прямым текстом или зашифрован с помощью imask.

**По умолчанию**
ldapdb2

**Синтаксис**
Binary

**Максимальная длина**
128

**Значение**
Одно значение

**Примечание:** Все объекты ibm-slapdRdbmBackend должны применять одинаковые ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW и набор символов DB2.

**ibm-slapdDigestAdminUser**

**Описание**
Задает имя администратора или члена группы администраторов LDAP для идентификации Digest MD5. Используется для идентификации администратора, если применяется механизм Digest MD5.

**По умолчанию**
Нет

**Синтаксис**
Directory string

**Максимальная длина**
512

**Значение**
Одно значение

**ibm-slapdDigestAttr**

**Описание**
Переопределяет стандартное значение атрибута имени пользователя DIGEST-MD5. Задает имя атрибута для поиска подключенного по SASL DIGEST-MD5 имени пользователя. Если значение не указано, то сервер будет применять ИД пользователя.

**По умолчанию**
Если значение не указано, то сервер будет применять ИД пользователя.

**Синтаксис**
Directory string.

**Максимальная длина**
64

**Значение**
Одно значение

**ibm-slapdDigestRealm**

**Описание**
Переопределяет область по умолчанию для DIGEST-MD5. Если пользователь работает на разных серверах под разными именами, то эта строка позволяет определить, какое имя и пароль использовать. В сущности, это имя коллекции учетных записей, в которую могут входить и учетные записи пользователя. В этой строке должно содержаться хотя бы имя хоста, выполняющего идентификацию, и при необходимости набор пользователей, которым разрешен доступ. Например: `зарегистрированный-пользователь@gotham.news.example.com`. Если атрибут не указан, то будет применяться полное имя сервера.

**По умолчанию**
Полное имя сервера

**Синтаксис**
Directory string.

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdEnableEventNotification

**Описание**
Указывает, должна ли быть включена функция уведомления о событиях. Допустимы значения TRUE и FALSE.

Если задано значение FALSE, то сервер в ответ на все запросы клиентов на регистрацию уведомления о событиях отправляет сообщение LDAP_UNWILLING_TO_PERFORM.

**По умолчанию**
TRUE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

### ibm-slapdEntryCacheSize

**Описание**
Максимальное число записей в кэше.

**По умолчанию**
25000

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdErrorLog

**Описание**
Задает файл или устройство системы сервера каталогов, на которое записываются сообщения об ошибках.

**По умолчанию**
/var/ibmslapd.log

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdESizeThreshold

**Описание**
Задает количество заданий в рабочей очереди, по достижении которого активируется аварийная нить.

**По умолчанию**
50

**Синтаксис**
Integer

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdEThreadActivate

**Описание**
Задает условия, при которых активизируется аварийная нить. Атрибуту должно быть присвоено одно из следующих значений:

**S** Только размер

**T** Только время

**SOT** Размер или время

**SAT** Размер и время

**По умолчанию**
SAT

**Синтаксис**
Строка

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdEThreadEnable

**Описание**
Указывает, активна ли аварийная нить.

**По умолчанию**
True

**Синтаксис**
Boolean

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdETimeThreshold

**Описание**
Указывает интервал (в минутах) между удалением заданий из рабочей очереди и активизацией аварийной нити.

**По умолчанию**
5

**Синтаксис**
Integer

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdFilterCacheBypassLimit**

**Описание**
Фильтры поиска, которым соответствует большее количество записей, не будут добавляться в кэш фильтров поиска. Поскольку в кэш записывается список ИД записей, соответствующих фильтру, данный параметр позволяет ограничить объем используемой памяти. 0 означает, что число записей не ограничено.

**По умолчанию**
100

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

**ibm-slapdFilterCacheSize**

**Описание**
Задает максимальное число записей в кэше фильтров поиска.

**По умолчанию**
25000

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

**ibm-slapdIdleTimeOut**

**Описание**
Максимальное время простоя соединения LDAP, по истечении которого оно будет закрыто. Время простоя соединения LDAP - это время в секундах, прошедшее с момента выполнения последней операции по соединению вплоть до текущего момента. Если время простоя превысит значение, указанное в этом атрибуте, то сервер LDAP очистит и закроет соединение LDAP, после чего оно может применяться для выполнения других запросов.

**По умолчанию**
300

**Синтаксис**
Integer

**Длина** 11

**Значение**
Одно значение

**Применение**
Операция

**Изменяется пользователем**
Да

**Класс доступа**
Critical

**Обязательный**
Нет

### ibm-slapdIncludeSchema

**Описание**
Задает полное имя файла на компьютере сервера каталогов, содержащего определения схемы.

**По умолчанию**

/etc/V3.system.at
/etc/V3.system.oc
/etc/V3.config.at
/etc/V3.config.oc
/etc/V3.ibm.at
/etc/V3.ibm.oc
/etc/V3.user.at
/etc/V3.user.oc
/etc/V3.ldapsyntaxes
/etc/V3.matchingrules

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Список значений

### ibm-slapdKrbAdminDN

**Описание**
Задает ИД Kerberos, связанный с администратором LDAP (например, ibm-kn=admin1@realm1). Это значение применяется в том случае, если при входе в программу Администрирование сервера для идентификации администратора применяется Kerberos. Может быть задан вместо значений adminDN и adminPW или в дополнение к ним.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
128

**Значение**
Одно значение

**ibm-slapdKrbEnable**

**Описание**
Указывает, поддерживает ли сервер Kerberos. Допустимы значения TRUE и FALSE.

**По умолчанию**
TRUE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdKrbIdentityMap**

**Описание**
Указывает, следует ли преобразовывать ИД Kerberos. Допустимы значения TRUE и FALSE. Если вы измените его на TRUE, то после идентификации клиента сервер будет предоставлять всем локальным пользователям с тем же ИД Kerberos права на подключения для данного соединения. Это позволяет применять ACL, основанные на DN пользователей LDAP, вместе с Kerberos.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdKrbKeyTab**

**Описание**
Задает файл ключей Kerberos сервера LDAP. Этот файл содержит личный ключ сервера LDAP, связанный с его учетной записью Kerberos. Этот файл должен быть защищен от несанкционированного доступа (как и файл базы данных ключей SSL).

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdKrbRealm**

**Описание**
Указывает область Kerberos для сервера LDAP. Это значение применяется для копирования

атрибута ldapservicename в корневой DSE. Обратите внимание, что сервер LDAP может хранить учетные записи нескольких KDC (и областей), однако сам сервер LDAP с поддержкой Kerberos может при этом входить только в одну область.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Directory string with case-insensitive matching

**Максимальная длина**
256

**Значение**
Одно значение

**ibm-slapdLanguageTagsEnabled**

**Описание**
Указывает, должен ли сервер поддерживать языковые теги. В файле ibmslapd.conf значение этого атрибута равно FALSE, но его можно изменить на TRUE.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdLdapCrlHost**

**Описание**
Указывает имя хоста сервера LDAP, содержащего списки аннулированных сертификатов (CRL) для проверки сертификатов клиентов x.509v3. Этот параметр необходимо указывать только в том случае, когда задано значение ibm-slapdSslAuth=serverclientauth, и клиентам выданы сертификаты для проверки с помощью CRL.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Directory string with case-insensitive matching

**Максимальная длина**
256

**Значение**
Одно значение

**ibm-slapdLdapCrlPassword**

**Описание**
Указывает пароль сервера для установления соединения SSL с сервером LDAP, содержащим списки аннулированных сертификатов (CRL) для проверки сертификатов клиентов x.509v3. Этот параметр требуется только в том случае, когда задано значение ibm-slapdSslAuth=serverclientauth и клиентам выданы сертификаты для проверки с помощью CRL.

**Примечание:** Если на сервере LDAP, хранящем CRL, разрешен анонимный доступ к CRL, то значение ibm-slapdLdapCrlPassword можно не указывать .

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Binary

**Максимальная длина**
128

**Значение**
Одно значение

### ibm-slapdLdapCrlPort

**Описание**
Задает порт, применяемый для подключения к серверу LDAP, хранящему Список аннулированных сертификатов (CRLs), для проверки сертификатов клиентов x.509v3. Этот параметр необходимо указывать только в том случае, когда задано значение ibm-slapdSslAuth=serverclientauth, и клиентам выданы сертификаты для проверки с помощью CRL. (Порт IP - это 16-разрядное целое число без знака из диапазона 1 - 65535)

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdLdapCrlUser

**Описание**
Задает DN сервера для установления соединения SSL с сервером LDAP, на котором хранятся списки аннулирования сертификатов (CRL) для проверки сертификатов клиентов x.509v3. Этот параметр требуется только в том случае, когда задано значение ibm-slapdSslAuth=serverclientauth и клиентам выданы сертификаты для проверки с помощью CRL.

**Примечание:** Если на сервере LDAP, хранящем CRL, разрешен анонимный доступ к CRL, то значение ibm-slapdLdapCrlUser можно не указывать.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
DN

**Максимальная длина**
1000

**Значение**
Одно значение

### ibm-slapdMasterDN

**Описание**
Указывает DN подключения к главному серверу. Это значение должно совпадать со значением

replicaBindDN, заданным в объекте replicaObject главного сервера. Если для идентификации на сервере-копии применяется протокол Kerberos, то в ibm-slapdMasterDN должен быть задан DN, связанный с ИД Kerberos (например, ibm-kn=freddy@realm1). Если применяется протокол Kerberos, параметр MasterServerPW игнорируется.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
DN

**Максимальная длина**
1000

**Значение**
Одно значение

### ibm-slapdMasterPW

**Описание**
Задает пароль подключения к главному серверу. Это значение должно совпадать со значением replicaBindDN, заданным в объекте replicaObject главного сервера. Если для идентификации на сервере-копии применяется протокол Kerberos, то в ibm-slapdMasterDN должен быть задан DN, связанный с ИД Kerberos (например, ibm-kn=freddy@realm1). Если применяется протокол Kerberos, параметр MasterServerPW игнорируется.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Binary

**Максимальная длина**
128

**Значение**
Одно значение

### ibm-slapdMasterReferral

**Описание**
Задает адрес главного сервера. Например:

```
ldap://master.us.ibm.com
```

В случае применения только соединений SSL:

```
ldaps://master.us.ibm.com:636
```

В случае отключенной защиты при использовании нестандартного порта:

```
ldap://master.us.ibm.com:1389
```

**По умолчанию**
none

**Синтаксис**
Directory string with case-insensitive matching

**Максимальная длина**
256

**Значение**
Одно значение

**ibm-slapdMaxEventsPerConnection**

**Описание**

Задает максимальное число уведомлений о событиях, которое может быть зарегистрировано для одного соединения.

Минимум = 0 (не ограничено). Максимум = 2 147 483 647.

**По умолчанию**

100

**Синтаксис**

Integer

**Максимальная длина**

11

**Значение**

Одно значение

**ibm-slapdMaxEventsTotal**

**Описание**

Указывает, сколько уведомлений о событиях может быть зарегистрировано для всех соединений.

Минимум = 0 (не ограничено). Максимум = 2 147 483 647.

**По умолчанию**

0

**Синтаксис**

Integer

**Максимальная длина**

11

**Значение**

Одно значение

**ibm-slapdMaxNumOfTransactions**

**Описание**

Задает максимальное число транзакций на один сервер.

Минимум = 0 (не ограничено). Максимум = 2 147 483 647.

**По умолчанию**

20

**Синтаксис**

Integer

**Максимальная длина**

11

**Значение**

Одно значение

**ibm-slapdMaxOpPerTransaction**

**Описание**

Задает максимальное число операций в транзакции.

Минимум = 0 (не ограничено). Максимум = 2 147 483 647.

**По умолчанию**
5

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdMaxPendingChangesDisplayed

**Описание**
Максимальное число ожидаемых изменений, выводимых на экране.

**По умолчанию**
200

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdMaxTimeLimitOfTransactions

**Описание**
Задает максимальное время выполнения транзакции в секундах.

```
Минимум = 0 (не ограничено). Максимум = 2 147 483 647.
```

**По умолчанию**
300

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdPagedResAllowNonAdmin

**Описание**
Указывает, должен ли сервер обрабатывать запросы пользователей, отличных от администратора, на получение результатов поиска страниц. Если в файле ibmslapd.conf задано значение FALSE, то сервер будет обрабатывать запросы только тех пользователей, у которых есть права администратора. Если у пользователя, запросившего результаты поиска страниц, нет прав администратора, и в файле ibmslapd.conf этому атрибуту присвоено значение FALSE, сервер отправит клиенту код возврата insufficientAccessRights. Операции поиска и загрузки страниц выполнены не будут.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Длина** 5

**Значение**
Одно значение

**Применение**
directoryOperation

**Изменяется пользователем**
Да

**Класс доступа**
critical

**Objectclass**
ibm-slapdRdbmBackend

**Обязательный**
Нет

### ibm-slapdPagedResLmt

**Описание**
Максимальное число запросов на получение результатов поиска страниц, которые могут обрабатываться одновременно. Допустимы значения, большие либо равные нулю. Если сервер уже обрабатывает максимальное число запросов на получение результатов поиска страниц, то при получении очередного запроса от клиента ему будет отправлен код возврата, свидетельствующий о занятости сервера. Операции поиска и загрузки страниц выполнены не будут.

**По умолчанию**
3

**Синтаксис**
Integer

**Длина** 11

**Значение**
Одно значение

**Применение**
directoryOperation

**Изменяется пользователем**
Да

**Класс доступа**
critical

**Обязательный**
Нет

**Objectclass**
ibm-slapdRdbmBackend

### ibm-slapdPageSizeLmt

**Описание**
Максимальное число записей, возвращаемых в результатах поиска отдельной страницы, если задано ограничение на число активных запросов на поиск страниц. Это значение применяется даже в том случае, если в запросе на поиск клиент указал размер страницы. Допустимы

значения, большие либо равные нулю. Если клиент указал в запросе размер страницы, то применяется минимальное из двух значений: значения, указанного клиентом, и значения, заданного в файле ibmslapd.conf.

**По умолчанию**
50

**Синтаксис**
Integer

**Длина** 11

**Значение**
Одно значение

**Применение**
directoryOperation

**Изменяется пользователем**
Да

**Класс доступа**
critical

**Обязательный**
Нет

**Objectclass**
ibm-slapdRdbmBackend

### ibm-slapdPlugin

**Описание**

Встраиваемый модуль - это динамически загружаемая библиотека, расширяющая возможности сервера. Атрибут ibm-slapdPlugin указывает, каким образом должна загружаться и инициализироваться библиотека встраиваемого модуля. Синтаксис:

*имя-файла-ключей* `init_function [`*`args`*`...]`

Особенности синтаксиса в каждой операционной системе определяются соглашениями о присвоении имен библиотекам.

Большинство встраиваемых модулей устанавливать не обязательно, однако встраиваемый модуль базы данных RDBM необходим для всех баз данных RDBM.

**По умолчанию**
*база данных* /bin/libback-rdbm.dll rdbm_backend_init

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
2000

**Значение**
Список значений

### ibm-slapdPort

**Описание**

Задает порт TCP/IP, который применяется для незащищенных соединений. Значение этого атрибута не должно совпадать со значением ibm-slapdSecurePort. (Порт IP - это 16-разрядное целое число без знака из диапазона 1 - 65535.)

**По умолчанию**
389

**Синтаксис**
Integer

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdPWEncryption**

**Описание**
Указывает, каким образом зашифрованы пароли пользователей в каталоге. Допустимы значения none, imask, crypt и sha (ключевое слово **sha** применяется в случае использования кодировки SHA-1). Для успешного подключения SASL cram-md5 необходимо задать значение none.

**По умолчанию**
none

**Синтаксис**
Directory string with case-insensitive matching

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdReadOnly**

**Описание**
Обычно этот атрибут влияет на работу с базой данных каталога. Он указывает, можно ли изменять базу данных. Допустимы значения TRUE и FALSE. Значение по умолчанию равно FALSE. Если атрибут равен TRUE, то в ответ на любой запрос клиента об изменении базы данных, доступной только для чтения, сервер будет возвращать сообщение LDAP_UNWILLING_TO_PERFORM (0x35).

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdReferral**

**Описание**
Указывает адрес сервера LDAP, которому будут переадресовываться запрос, когда нужный суффикс не найден. Здесь должен быть указан адрес сервера, расположенного выше в иерархии (то есть, ему переадресуется запрос, когда суффикс отсутствует в контексте имен сервера).

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
32700

**Значение**
Список значений

### ibm-slapdReplDbConns

**Описание**
Максимальное число соединений с базой данных, применяемых для копирования.

**По умолчанию**
4

**Синтаксис**
Integer

**Максимальная длина**
11

**Значение**
Одно значение

### ibm-slapdReplicaSubtree

**Описание**
Указывает DN копируемого поддерева

**Синтаксис**
DN

**Максимальная длина**
1000

**Значение**
Одно значение

### ibm-slapdSchemaAdditions

**Описание**
Атрибут ibm-slapdSchemaAdditions позволяет явно указать файл, содержащий новые записи схемы. По умолчанию задано значение /etc/V3.modifiedschema. Если этот атрибут не указан, сервер применяет последний файл ibm-slapdIncludeSchema, как и в предыдущем выпуске.

До версии 3.2 при получении от клиента запроса на добавление данных сервер добавлял новые записи схемы в файл, указанный в последней записи includeSchema файла **slapd.conf**. Обычно в последней записи includeSchema указан файл V3.modifiedschema, который не содержит данных и предназначен специально для добавления записей.

**Примечание:** Слово modified в имени файла может ввести в заблуждение, так как этот файл применяется только для хранения новых записей. Изменения в существующих схемах вносятся исходные файлах схем.

**По умолчанию**
/etc/V3.modifiedschema

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdSchemaCheck**

**Описание**
Задает способ проверки схемы, выполняемой после изменения данных. Допустимы значения V2, V3 или V3_lenient.

- V2 - Соответствует проверке v2 и v2.1. Это значение рекомендуется установить на время перехода к другой версии.
- V3 - Соответствует проверке v3.
- V3_lenient - Требуются не все родительские классы объектов. При добавлении записей нужен только класс, связанный напрямую.

**По умолчанию**
V3_lenient

**Синтаксис**
Directory string with case-insensitive matching

**Максимальная длина**
10

**Значение**
Одно значение

**ibm-slapdSecurePort**

**Описание**
Задает порт TCP/IP, который применяется для соединений SSL. Значение этого атрибута не должно совпадать со значением ibm-slapdPort. (Порт IP - это 16-разрядное целое число без знака из диапазона 1 - 65535.)

**По умолчанию**
636

**Синтаксис**
Integer

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdSecurity**

**Описание**
Разрешает устанавливать соединения SSL и TLS. Допустимы значения none, SSL, SSLOnly, TLS и SSLTLS.

- none - сервер поддерживает только незащищенные порты.
- SSL - сервер поддерживает как защищенные, так и незащищенные порты. Защищенный порт означает всего лишь использование защищенного соединения.
- SSLOnly - сервер поддерживает только защищенные порты.
- TLS - сервер поддерживает только незащищенные порты. Расширенная операция StartTLS означает всего лишь использование защищенного соединения.
- SSLTLS - сервер поддерживает как защищенные, так и незащищенные порты. С помощью расширенной операции StartTLS можно установить защищенное соединение по

| стандартному порту, или клиент может работать напрямую с защищенным портом. При
| отправке StartTLS по защищенному порту будет выведено сообщение
| LDAP_OPERATIONS_ERROR.

**По умолчанию**
none

**Синтаксис**
Directory string with case-insensitive matching

**Максимальная длина**
7

**Значение**
Одно значение

### ibm-slapdServerId

**Описание**
Задает сервер, применяемый для копирования.

**Синтаксис**
IA5 String with case-sensitive matching

**Максимальная длина**
240

**Значение**
Одно значение

### ibm-slapdSetenv

**Описание**
При запуске сервер выполняет функцию **putenv()** для всех значений ibm-slapdSetenv, чтобы изменить среду выполнения. Переменные оболочки (такие как %PATH% и $LANG) не разворачиваются.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
2000

**Значение**
Список значений

### ibm-slapdSizeLimit

**Описание**
Максимальное число результатов поиска, не зависящее от того, какое ограничение задано в поисковом запросе клиента (допустимы значения больше нуля). Если в запросе клиента указано ограничение, то будет применяться наименьшее из двух значений: значения, переданного клиентом, и значения, заданного в файле **ibmslapd.conf**. Если в запросе клиента не указано ограничение, и подключение к базе данных установлено от имени администратора, то предполагается, что ограничение не установлено. Если в запросе клиента не указано ограничение, и подключение к базе данных установлено от имени обычного пользователя, то применяется ограничение, заданное в файле **ibmslapd.conf**. Значение 0 означает ″не ограничено″.

**По умолчанию**
500

**Синтаксис**
Integer

**Максимальная длина**
12

**Значение**
Одно значение

### ibm-slapdSortKeyLimit

**Описание**
Максимальное число условий (ключей) сортировки в запросе на поиск. Допустимы значения, большие либо равные нулю. Если в запросе клиента превышено ограничение на число ключей сортировки, а в параметре важности параметров поиска с сортировкой задано значение FALSE, то сервер будет применять значение из файла ibmslapd.conf и проигнорирует ключи сортировки, указанные сверх указанного ограничения. Операции поиска и сортировки будут выполнены. Если при превышении числа ключей в параметре важности параметров поиска указано значение TRUE, то клиент получит от сервера код возврата **adminLimitExceeded**. Операции поиска и сортировки выполнены не будут.

**По умолчанию**
3

**Синтаксис**
cis

**Длина** 11

**Значение**
Одно значение

**Применение**
directoryOperation

**Изменяется пользователем**
Да

**Класс доступа**
critical

**Objectclass**
ibm-slapdRdbmBackend

**Обязательный**
Нет

### ibm-slapdSortSrchAllowNonAdmin

**Описание**
Указывает, должен ли сервер обрабатывать запросы пользователей, отличных от администратора, на сортировку результатов поиска. Если в файле ibmslapd.conf задано значение FALSE, то сервер будет обрабатывать запросы только тех пользователей, у которых есть права администратора. Если у пользователя, запросившего сортировку результатов поиска, нет прав администратора, и в файле ibmslapd.conf этому атрибуту присвоено значение FALSE, то сервер отправит клиенту код возврата insufficientAccessRights. Операции поиска и сортировки выполнены не будут.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Длина** 5

**Значение**
Одно значение

**Применение**
directoryOperation

**Изменяется пользователем**
Да

**Класс доступа**
critical

**Objectclass**
ibm-slapdRdbmBackend

**Обязательный**
Нет

### ibm-slapdSslAuth

**Описание**
Задает тип идентификации для соединений ssl. Допустимы значения serverauth и serverclientauth.

- serverauth - поддерживает идентификацию сервера на клиенте. Это значение принято по умолчанию.
- serverclientauth - поддерживает идентификацию сервера и клиента.

**По умолчанию**
serverauth

**Синтаксис**
Directory string with case-insensitive matching

**Максимальная длина**
16

**Значение**
Одно значение

### ibm-slapdSslCertificate

**Описание**
Задает метку личного ключа сервера в файле базы данных ключей. Эта метка задается в том случае, если личный ключ и сертификат созданы с помощью приложения **gsk4ikm**. Если значение ibm-slapdSslCertificate не задано, то для установления соединений SSL сервером LDAP применяется личный ключ по умолчанию, определенный в файле базы данных ключей.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
128

**Значение**
Одно значение

### ibm-slapdSslCipherSpec

Задает метод шифрования SSL для клиентов сервера. Должно быть присвоено одно из следующих значений:

*Таблица 7. Методы шифрования SSL*

| Атрибут | Уровень шифрования |
|---|---|
| TripleDES-168 | Алгоритм шифрования Тройной DES со 168-разрядным ключом и SHA-1 MAC |
| DES-56 | Алгоритм шифрования DES с 56-разрядным ключом и SHA-1 MAC |
| RC4-128-SHA | Алгоритм шифрования RC4 со 128-разрядным ключом и SHA-1 MAC |
| RC4-128-MD5 | Алгоритм шифрования RC4 со 128-разрядным ключом и MD5 MAC |
| RC2-40-MD5 | Алгоритм шифрования RC4 с 40-разрядным ключом и MD5 MAC |
| RC4-40-MD5 | Алгоритм шифрования RC4 с 40-разрядным ключом и MD5 MAC |
| AES | Шифрование AES |

**Синтаксис**
IA5 String

**Максимальная длина**
30

### ibm-slapdSslKeyDatabase

**Описание**
Задает имя файла базы данных ключей SSL сервера LDAP. Этот файл применяется для обработки запросов на установление защищенных соединений, поступающих от клиентов LDAP, а также для установления защищенных соединений с серверами-копиями LDAP.

**По умолчанию**
/etc/key.kdb

**Синтаксис**
Directory string with case-exact matching

**Максимальная длина**
1024

**Значение**
Одно значение

### ibm-slapdSslKeyDatabasePW

**Описание**
Задает пароль доступа к файлу базы данных ключей SSL сервера LDAP, указанному в параметре ibm-slapdSslKeyDatabase. Если с этим файлом связан файл паролей, то не указывайте параметр ibm-slapdSslKeyDatabasePW, либо укажите none.

**Примечание:** Файл паролей должен быть расположен в одном каталоге с файлом базы данных ключей. Кроме того, ему должно быть присвоено то же имя, что и файлу базы данных ключей, но с другим расширением (.sth вместо .kdb).

**По умолчанию**
none

**Синтаксис**
Binary

**Максимальная длина**
128

**Значение**
Одно значение

**ibm-slapdSslKeyRingFile**

**Описание**
Имя файла базы данных ключей SSL сервера LDAP. Этот файл применяется для обработки запросов на установление защищенных соединений, поступающих от клиентов LDAP, а также для установления защищенных соединений с серверами-копиями LDAP.

**По умолчанию**
key.kdb

**Синтаксис**
Directory String with case-sensitive matching

**Максимальная длина**
1024

**Значение**
Одно значение

**ibm-slapdSuffix**

**Описание**
Задает контекст имен, который должен хранится в этой базе данных.

**Примечание:** Имя совпадает с именем класса объектов.

**По умолчанию**
Значение по умолчанию отсутствует.

**Синтаксис**
DN

**Максимальная длина**
1000

**Значение**
Список значений

**ibm-slapdSupportedWebAdmVersion**

**Описание**
Этот атрибут задает самую младшую версию Web-инструмента администрирования, которая поддерживает сервер данной записи cn=configuration.

**По умолчанию**

**Синтаксис**
Directory String

**Максимальная длина**

**Значение**
Одно значение

**ibm-slapdSysLogLevel**

**Описание**

Задает уровень отладки и ведения протокола, хранящегося в файле slapd.errors. Допустимы значения l, m и h.

- h - высокий (наибольшее количество информации)
- m - средний (по умолчанию)
- l - низкий (наименьшее количество информации)

**По умолчанию**

m

**Синтаксис**

Directory string with case-insensitive matching

**Максимальная длина**

1

**Значение**

Одно значение

### ibm-slapdTimeLimit

**Описание**

Задает максимальное время выполнения операции поиска в секундах. Это ограничение распространяется на все операции поиска, независимо от того, какое значение задано в запросе клиента. Если в запросе клиента указано ограничение, то будет применяться наименьшее из двух значений: значения, переданного клиентом, и значения, заданного в файле **ibmslapd.conf**. Если в запросе клиента не указано ограничение, и подключение к базе данных установлено от имени администратора, то предполагается, что ограничение не установлено. Если в запросе клиента не указано ограничение, и подключение к базе данных установлено от имени обычного пользователя, то применяется ограничение, заданное в файле **ibmslapd.conf**. Значение 0 означает ″не ограничено″.

**По умолчанию**

900

**Синтаксис**

Integer

**Максимальная длина**

**Значение**

Одно значение

### ibm-slapdTransactionEnable

**Описание**

Если встраиваемый модуль транзакций загружен, но для параметра ibm-slapdTransactionEnable указано значение FALSE, то в ответ на запросы StartTransaction сервер будет отправлять сообщение `LDAP_UNWILLING_TO_PERFORM`.

**По умолчанию**

TRUE

**Синтаксис**

Boolean

**Максимальная длина**

5

**Значение**

Одно значение

**ibm-slapdUseProcessIdPw**

**Описание**
Если это значение включено, сервер игнорирует атрибуты ibm-slapdDbUserID и ibm-slapdDbUserPW и идентифицирует себя для DB2 с помощью собственного одноразового разрешения процесса.

**По умолчанию**
FALSE

**Синтаксис**
Boolean

**Максимальная длина**
5

**Значение**
Одно значение

**ibm-slapdVersion**

**Описание**
Версия IBM Slapd

**По умолчанию**

**Синтаксис**
Directory String with case-sensitive matching

**Максимальная длина**

**Значение**
Одно значение

**ibm-slapdWriteTimeout**

**Описание**
Задает тайм-аут в секундах для заблокированных записей. По достижении этого времени соединение аннулируется.

**По умолчанию**
120

**Синтаксис**
Integer

**Максимальная длина**
1024

**Значение**
Одно значение

**objectClass**

**Описание**
Значение атрибута objectClass задает тип объекта, связанного с записью.

**Синтаксис**
Directory string

**Максимальная длина**
128

**Значение**
Список значений

# Идентификаторы объектов (OID)

Идентификаторы объектов, применяемые на сервере каталогов, показаны в следующей таблице. Эти OID находятся в корневом DSE. Запись корневого DSE содержит информацию о самом сервере.

**Управляющие элементы**

*Таблица 8. Управляющие элементы, поддерживаемые сервером каталогов*

| Имя | OID | Самый ранний выпуск i5/OS или OS/400 | Самый ранний выпуск IBM Directory Server | Описание |
|---|---|---|---|---|
| Управление DSA IT | 2.16.840.1.1137.30.3.4.2 | V4R5 | V3.2 | Считать записи переадресации обычными записями. |
| “Транзакции” на стр. 50 | 1.3.18.0.2.10.5 | V4R5 | V3.2 | Пометить операцию как часть транзакции. |
| os400-dltusrprf-ownobjopt | 1.3.18.0.2.10.8 | V5R2 | | Удалить пользовательский профайл для владельца объекта. См. раздел “Спроецированная база данных операционной системы” на стр. 80. |
| os400-dltusrprf-pgpopt | 1.3.18.0.2.10.9 | V5R2 | | Удалить пользовательский профайл для основной группы. См. раздел “Спроецированная база данных операционной системы” на стр. 80. |
| Поиск с сортировкой | 1.2.840.113556.1.4.473 (запрос) и 1.2.840.113556.1.4.474 (ответ) | V5R2 с PTF | V4.1 | Упорядочивать результаты поиска перед возвратом записей клиенту. См. раздел “Параметры поиска” на стр. 47. |
| Постраничный поиск | 1.2.840.113556.1.4.319 | V5R2 с PTF | V4.1 | Возвращать записи клиенту постранично, а не все сразу. См. раздел “Параметры поиска” на стр. 47. |

*Таблица 8. Управляющие элементы, поддерживаемые сервером каталогов (продолжение)*

| Имя | OID | Самый ранний выпуск i5/OS или OS/400 | Самый ранний выпуск IBM Directory Server | Описание |
|---|---|---|---|---|
| Удаление дерева | 1.2.840.113556.1.4.805 | V5R3 | V5.1 | Этот управляющий элемент включается в запрос на удаление и указывает на необходимость удаления заданной записи вместе со всеми ее дочерними записями. Пользователь должен быть администратором каталога. Удаляемая запись не может быть контекстом копирования. |
| “Стратегия управления паролями” на стр. 73 | 1.3.6.1.4.1.42.2.27.8.5.1 | V5R3 | V5.1 | Возврат клиенту дополнительной информации об ошибке стратегии управления паролями. |
| Управление сервером | 1.3.18.0.2.10.15 | V5R3 | V5.1 | Разрешает администратору выполнять обычно запрещенные операции восстановления (например: обновление копии, предназначенной только для чтения, обновление стабилизированного сервера или установка некоторых операционных атрибутов). |
| “Proxy-идентификация” на стр. 60 | 2.16.840.1.113730.3.4.18 | V5R4 | V5.2 | Клиентское приложение может подключиться к каталогу со своим идентификатором, и при этом получает возможность действовать от имени другого пользователя. |
| Управление подключением поставщика копирования | 1.3.18.0.2.10.18 | V5R3 | V5.2 | Этот управляющие элемент добавляется поставщиком-шлюзом. |

**Расширенные операции**

*Таблица 9. OID для расширенных операций*

| Имя | OID | Самый ранний выпуск i5/OS или OS/400 | Самый ранний выпуск IBM Directory Server | Описание |
|---|---|---|---|---|
| Регистрация событий | 1.3.18.0.2.12.1 | V4R5 | V3.2 | Регистрация запросов для событий в SecureWay V3.2 Event Support |
| Отмена регистрации событий | 1.3.18.0.2.12.3 | V4R5 | V3.2 | Отмена регистрации событий, зарегистрированных посредством запроса регистрации событий. |
| Начало транзакции | 1.3.18.0.2.12.5 | V4R5 | V3.2 | Начало контекста транзакции для SecureWay V3.2 |
| Конец транзакции | 1.3.18.0.2.12.6 | V4R5 | V3.2 | Конец контекста транзакции (фиксация/откат) для SecureWay V3.2 |
| Запрос нормализации DN | 1.3.18.0.2.12.30 | V5R3 | V5.1 | Запрос на нормирование DN или последовательности DN. |
| StartTLS | 1.3.6.1.4.1.1466.20037 | V5R4 | V5.2 | Запрос на начало соединения TLS. |

Существует также набор дополнительных расширенных операций, которые не предназначены для запуска клиентом. Такие операции применяются в утилите ldapexop, а также в операциях, выполняемых Web-инструментом администрирования. Эти операции и необходимые для их запуска права доступа перечислены в следующей таблице:

*Таблица 10. Дополнительные расширенные операции*

| Имя | OID | Самый ранний выпуск i5/OS | Самый ранний выпуск IBM Directory Server | Описание |
|---|---|---|---|---|
| Управление копированием | 1.3.18.0.2.12.16 | V5R3 | V5.1 | Выполняет запрошенное действие на сервере, на котором операция была запущена, а также каскадным образом передает запрос всем потребителям этого сервера, подчиненным ему в топологии копирования. Клиент должен быть администратором каталога или иметь права доступа на запись в объект ibm-replicagroup=default соответствующего контекста копирования. |
| Управление очередью копирования. | 1.3.18.0.2.12.17 | V5R3 | V5.1 | Операция помечает объект как уже скопированный в соответствии с указанным соглашением. Эта операция допустима только в том случае, если у клиента есть права доступа на запись для соглашения о копировании. |

*Таблица 10. Дополнительные расширенные операции (продолжение)*

| Имя | OID | Самый ранний выпуск i5/OS | Самый ранний выпуск IBM Directory Server | Описание |
|---|---|---|---|---|
| Стабилизировать или Отменить стабилизацию | 1.3.18.0.2.12.19 | V5R3 | V5.1 | Эта операция переводит поддерево в состояние, в котором получаемые от клиентов обновления не обрабатываются (или выводит поддерево из такого состояния), за исключением клиента, идентифицированного как администратор каталога, и передавшего управляющий элемент Управление сервером. Клиент должен быть идентифицирован как администратор каталога или иметь права доступа на запись в объект ibm-replicagroup=default соответствующего контекста копирования. |
| Каскадное управление копированием | 1.3.18.0.2.12.15 | V5R3 | V5.1 | Выполняет запрошенное действие на сервере, на котором операция была запущена, а также каскадным образом передает запрос всем потребителям этого сервера, подчиненным ему в топологии копирования. Клиент должен быть администратором каталога или иметь права доступа на запись в объект ibm-replicagroup=default соответствующего контекста копирования. |
| Обновление конфигурации | 1.3.18.0.2.12.28 | V5R3 | V5.1 | Эта операция указывает серверу, что он должен повторно считать перечисленные параметры конфигурации. Операция разрешена только в том случае, если клиент является администратором каталога. |
| Уничтожение запроса на установление соединения | 1.3.18.0.2.12.35 | V5R4 | V5.2 | Запрос на уничтожение соединения на сервере. |
| Запрос уникального атрибута | 1.3.18.0.2.12.44 | V5R4 | V5.2 | Запрашивает с сервера список всех неуникальных значений атрибута с заданным именем. См. “ldapexop” на стр. 210 -op uniqueattr. |
| Запрос типа атрибута | 1.3.18.0.2.12.46 | V5R4 | V5.2 | Запрашивает с сервера список имен атрибутов, соответствующих заданному признаку. См. “ldapexop” на стр. 210 -op getattributes |
| Управление трассировкой сервера | 1.3.18.0.2.12.40 | V5R3 | V5.2 | Включает или выключает трассировку в IBM Directory Server. |
| Запрос типа пользователя | 1.3.18.0.2.12.37 | V5R3 | V5.2 | Запрашивает тип подключенного пользователя. |

**Поддерживаемые и разрешенные возможности**

В следующей таблице показаны OID для поддерживаемых и разрешенных функций. По этим OID можно определить, поддерживаются ли эти функции конкретным сервером.

*Таблица 11. OID для поддерживаемых и разрешенных функций*

| Имя | OID | Описание |
|---|---|---|
| Расширенная модель копирования | 1.3.18.0.2.32.1 | Обозначает действующую в IBM Directory Server v5.1 модель копирования, включая копирование поддеревьев и каскадное копирование. |
| Контрольная сумма записи | 1.3.18.0.2.32.2 | Означает поддержку на сервере функций ibm-entrychecksum и ibm-entrychecksumop. |
| UUID записи | 1.3.18.0.2.32.3 | Обозначает, что сервер поддерживает операционный атрибут ibm-entryuuid. |
| ACL с фильтрами | 1.3.18.0.2.32.4 | Обозначает, что этот сервер поддерживает модель ACL с фильтрами IBM. |
| Стратегия управления паролями | 1.3.18.0.2.32.5 | Обозначает, что сервер поддерживает стратегии управления паролями |
| Сортировка по DN | 1.3.18.0.2.32.6 | Обозначает, что сервер поддерживает сортировку по DN посредством атрибута ibm-slapdDn. |
| Делегирование группы администраторов | 1.3.18.0.2.32.8 | Сервер поддерживает перенаправление группы администраторов сервера в группу, указанную в конфигурации базовой программы. |
| Предотвращение отказа в обслуживании | 1.3.18.0.2.32.9 | Сервер поддерживает компонент для предотвращения отказа в обслуживании. Сюда входят тайм-ауты чтения-записи и аварийная нить. |
| Динамическое обновление записи и поддерева | 1.3.18.0.2.32.15 | Сервер поддерживает динамическое обновление записей и поддеревьев |
| Опция учета псевдонимов | 1.3.18.0.2.32.10 | Сервер поддерживает опцию, которая по умолчанию не раскрывает псевдонимы |
| Ограничения на поиск для групп | 1.3.18.0.2.32.17 | Функция Групповые ограничения на поиск поддерживает расширенные ограничения поиска для групп пользователей |
| Динамическая трассировка | 1.3.18.0.2.32.14 | Сервер поддерживает активную трассировку с расширенной операцией LDAP. |
| Средства TLS | 1.3.18.0.2.32.28 | Обозначает, что сервер действительно поддерживает TLS. |
| Контроль демона администрирования | 1.3.18.0.2.32.11 | Сервер поддерживает контроль демона администрирования. |
| Средства Kerberos | 1.3.18.0.2.32.30 | Обозначает, что сервер действительно поддерживает Kerberos. |
| Копирование без блокирования | 1.3.18.0.2.32.29 | Если сервер-приемник возвращает ошибку, поставщик не всегда повторяет попытки отправки изменения |
| Операционные атрибуты ibm-allMembers и ibm-allGroups | 1.3.18.0.2.32.31 | Базовая программа поддерживает поиск статических, динамических и вложенных групп посредством операционных атрибутов ibm-allMembers и ibm-allGroups. Поиск по атрибуту ibm-allMembers позволяет получить состав статической, динамической и/или вложенной группы. Путем поиска по атрибуту ibm-allGroups можно получить статическую, динамическую и/или вложенную группу, к которой относится участник с заданным DN. |

*Таблица 11. OID для поддерживаемых и разрешенных функций (продолжение)*

| Имя | OID | Описание |
|---|---|---|
| Глобально уникальные атрибуты | 1.3.18.0.2.32.16 | Функция сервера для присвоения значений глобально уникальным атрибутам. |
| Мониторинг количества операций | 1.3.18.0.2.32.24 | На сервере предусмотрена возможность отслеживания количества начатых и завершенных операций. |
| Мониторинг количества записей протокола | 1.3.18.0.2.32.20 | На сервере предусмотрена возможность отслеживания количества записей протокола для добавляемых на сервер сообщений, CLI, а также количества файлов протокола контроля. |
| Мониторинг количества типов соединений | 1.3.18.0.2.32.22 | На сервере предусмотрены счетчики типов соединений SSL и TLS. |
| Мониторинг данных об активных обработчиках | 1.3.18.0.2.32.21 | На сервере предусмотрена возможность отслеживания данных об активных обработчиках (cn=workers,cn=monitor). |
| Мониторинг данных о соединениях | 1.3.18.0.2.32.23 | На сервере предусмотрена возможность отслеживания соединений не по IP-адресу, а по ИД соединения (cn=connections, cn=monitor). |
| Мониторинг данных трассировки | 1.3.18.0.2.32.25 | На сервере предусмотрена возможность отслеживания данных трассировки текущего параметра. |
| Кэширование атрибутов для обработки фильтра поиска | 1.3.18.0.2.32.13 | Сервер поддерживает кэширование атрибутов для обработки фильтра поиска. |
| Proxy-идентификация | 1.3.18.0.2.32.27 | Сервер поддерживает для группы пользователей возможность действовать от чужого имени. |
| Поддержка языковых тегов | 1.3.6.1.4.1.4203.1.5.4 | Обозначает, что сервер поддерживает языковые теги согласно спецификации RFC 2596. |
| Срок давности записей протокола изменений | 1.3.18.0.2.32.19 | Обозначает, что на сервере предусмотрена возможность хранения записей протокола изменений в зависимости от их давности. |
| Поддерево копирования IBMpolicies | 1.3.18.0.2.32.18 | Сервер поддерживает копирование поддерева cn=IBMpolicies. |
| Поиск в поддереве с пустой базой | 1.3.18.0.2.32.26 | На сервере разрешен поиск в поддереве с пустой базой. Пустая база означает поиск во всем поддереве DIT сервера. |
| Автоматическое кэширование атрибутов | 1.3.18.0.2.32.50 | Поддержка автоматического кэширования атрибутов |
| ibm-entrychecksumop | 1.3.18.0.2.32.56 | Функции ibm-entrychecksumop системы IDS 6.0 |

### OID для ACL

В следующей таблице приведены OID для различных типов ACL.

*Таблица 12. OID для ACL*

| Имя | OID | Описание |
|---|---|---|
| Модель ACL IBM SecureWay V3.2 | 1.3.18.0.2.26.2 | Обозначает, что сервер LDAP поддерживает модель ACL IBM SecureWay V3.2 |
| IBM ACL на основе фильтров | 1.3.18.0.2.26.3 | Обозначает, что сервер LDAP поддерживает списки ACL на основе фильтров для IBM Directory Server v5.1 |

*Таблица 12. OID для ACL (продолжение)*

| Имя | OID | Описание |
|---|---|---|
| Поддержка системных и ограниченных ACL | 1.3.18.0.2.26.4 | Означает, что в списках ACL сервера разрешены системный и ограниченный классы доступа. |

# Глава 9. Устранение неполадок сервера каталогов

К сожалению, при работе даже самых надежных серверов, таких как сервер каталогов, иногда возникают неполадки. Приведенная ниже информация поможет вам найти и устранить причину возникшей неполадки сервера каталогов.

Коды возврата, свидетельствующие об ошибках LDAP, описаны в файле ldap.h, расположенном в библиотеке QSYSINC/H.LDAP.



Дополнительная информация о типичных неполадках сервера каталогов приведена на домашней странице сервера каталогов (www.iseries.ibm.com/ldap).

Сервер каталогов применяет несколько серверов языка структурных запросов (SQL), которым в iSeries соответствуют задания QSQSRVR. При возникновении ошибки SQL в протокол задания QDIRSRV обычно заносится следующее сообщение:

```
Возникла ошибка SQL -1
```

В этих случаях протокол задания QDIRSRV будет содержать ссылку на протоколы заданий сервера SQL. Однако в некоторых случаях при возникновении ошибки сервера SQL в протокол задания QDIRSRV не заносится указанное сообщение. В таких случаях следует знать, что какие задания серверов SQL запустил сервер каталогов. Это позволит вам выбрать протоколы заданий QSQSRVR, в которых следует искать дополнительные сообщения об ошибках.

При успешном запуске сервер каталогов создает следующие сообщения:

```
                                                    Система:  MYISERIES
Задание . :   QDIRSRV      Пользователь . :   QDIRSRV      Число . :  174440

  >> CALL PGM(QSYS/QGLDSVR)
     Задание 057448/QUSER/QSQSRVR применяется для обработки в режиме сервера SQL.
     Задание 057340/QUSER/QSQSRVR применяется для обработки в режиме сервера SQL.
```

```
Задание 057448/QUSER/QSQSRVR применяется для обработки в режиме сервера SQL.
Задание 057166/QUSER/QSQSRVR применяется для обработки в режиме сервера SQL.
Задание 057279/QUSER/QSQSRVR применяется для обработки в режиме сервера SQL.
Задание 057288/QUSER/QSQSRVR применяется для обработки в режиме сервера SQL.
Сервер каталогов запущен успешно.
```

В этих сообщениях перечислены задания QSQSRVR, запущенные сервером. Число сообщений может быть различным, в зависимости от конфигурации и от числа заданий QSQSRVR, необходимых для обработки процедуры запуска.

На странице **База данных/Суффиксы** окна свойств сервера каталогов в Навигаторе задается общее число серверов SQL, применяемых сервером каталогов для работы с каталогом после запуска сервера. Для копирования запускаются дополнительные серверы SQL.

## Отслеживание ошибок и контроль доступа с помощью протокола задания сервера каталогов

Путем просмотра протокола задания сервера каталогов можно получить информацию об ошибках и обращениях к серверу. Протокол заданий содержит следующие сообщения:

- Сообщения о работе сервера и о любых связанных с ним неполадках, например, об ошибках заданий серверов SQL и об ошибках копирования.
- Сообщения о системе защиты, информирующие об операциях, выполняемых клиентами, например, о вводе неправильных паролей.
- Сообщения с подробными сведениями об ошибках клиентов, например, об отсутствующих обязательных атрибутах.

Если вы не выполняете отладку, то заносить в протокол сообщения о клиентских ошибках не рекомендуется. Для управления занесением таких ошибок в протокол перейдите на вкладку **Общие** свойств сервера каталогов в Навигаторе iSeries.

Если сервер запущен, то для просмотра протокола задания QDIRSRV нужно выполнить следующие действия:

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **IBM Directory Server** и выберите **Задания сервера**.
5. В меню **Файл** выберите пункт **Протокол задания**.

Если сервер остановлен, то для просмотра протокола задания QDIRSRV нужно выполнить следующие действия:

1. В Навигаторе откройте **Основные операции**.
2. Выберите **Вывод на принтер**.
3. В столбце **Пользователь** на правой панели Навигатора будет показан элемент QDIRSRV. Для просмотра протокола задания дважды щелкните на имени **Qpjoblog**, которое находится слева от QDIRSRV.

   **Примечание:** В Навигаторе iSeries может быть задан фильтр, разрешающий показывать только буферные файлы. Если в списке QDIRSRV отсутствует, то выберите **Вывод на принтер**, затем выберите пункт **Включить в список** в меню **Опции**. Укажите значение **Все** в поле **Пользователь** и нажмите кнопку **OK**.

**Примечание:** Для выполнения некоторых задач сервер каталогов применяет ресурсы других систем. При возникновении ошибки в одном из этих ресурсов в протоколе задания будет указана ссылка на источник информации об этой ошибке. В некоторых случаях сервер каталогов не может указать такой объект. Для того чтобы определить, не связана ли возникшая неполадка с серверами SQL, просмотрите протокол задания серверов SQL.

## Обнаружение неполадок с помощью TRCTCPAPP

Сервер поддерживает функцию трассировки соединения, обеспечивающую сбор данных о линии связи, например об интерфейсе локальной (LAN) или глобальной (WAN) сети. Правильно интерпретировать записи трассировки может только специально обученный пользователь. Однако с помощью записей трассировки можно легко определить, передавались ли данные между двумя точками.

Команда Трассировка приложения TCP/IP (TRCTCPAPP) с опцией *DIRSRV может применяться для обнаружения неполадок клиентов или приложений сервера каталогов.

Дополнительная информация о применении команды TRCTCPAPP при работе с сервером LDAP и необходимых правах доступа приведена в описании команды TRCTCPAPP (Трассировка приложения TCP/IP).

Общая информация о работе с функцией трассировки соединения приведена в разделе Трассировка соединения.

## Трассировка ошибок с помощью опции LDAP_OPT_DEBUG

Для трассировки неполадок на клиентах, применяющих API LDAP на языке C, может использоваться опция LDAP_OPT_DEBUG API **ldap_set_option()**. Эта опция поддерживает несколько уровней отладки и может применяться для устранения неполадок в приложениях.

Ниже приведен пример включения опции отладки.

```
int debugvalue= LDAP_DEBUG_TRACE | LDAP_DEBUG_PACKETS;
ldap_set_option(  1d, LDAP_OPT_DEBUG, &debugvalue);
```

Помимо параметра `debugvalue` API **ldap_set_option()**, уровень отладки можно задать с помощью переменной среды `LDAP_DEBUG` задания, в котором выполняется приложение клиента.

Ниже приведен пример включения трассировки клиента с помощью переменной среды LDAP_DEBUG:

```
ADDENVVAR ENVVAR(LDAP_DEBUG) VALUE(0x0003)
```

После запуска клиента, в работе которого возникает ошибка, введите в командной строке iSeries:

```
DMPUSRTRC  ClientJobNumber
```

где `ClientJobNumber` - номер задания клиента.

Для просмотра информации в интерактивном режиме введите в командной строке iSeries:

```
DSPPFM QAP0ZDMP QP0Znnnnnn
```

где `QAP0ZDMP` содержит ноль, а `nnnnnn` - номер задания.

Для того чтобы сохранить информацию для последующей отправки в сервисное представительство, выполните следующие действия:

1. Создайте файл SAVF с помощью команды Создать SAVF (CRTSAVF).
2. Введите в командной строке iSeries:

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   где `QAP0ZDMP` содержит ноль, а *xxx* - имя файла сохранения SAVF.

## Идентификаторы сообщений GLEnnnn

Идентификаторы сообщений представляются в формате GLEnnnn, где nnnn - десятичный код ошибки. Например, описание кода возврата 50 (0x32) можно посмотреть с помощью команды:

```
DSPMSGD MSGID(GLE0050) MSGF(QGLDMSG)
```

Вы получите описание ошибки LDAP_INSUFFICIENT_ACCESS.

Идентификаторы сообщений GLE и их описания приведены в таблице.

| Идентификатор сообщения | Описание |
|---|---|
| GLE0000 | Запрос успешный (LDAP_SUCCESS) |
| GLE0001 | Ошибка при выполнении операций (LDAP_OPERATIONS_ERROR) |
| GLE0002 | Ошибка протокола (LDAP_PROTOCOL_ERROR) |
| GLE0003 | Превышено ограничение по времени (LDAP_TIMELIMIT_EXCEEDED) |
| GLE0004 | Превышен максимальный размер (LDAP_SIZELIMIT_EXCEEDED) |
| GLE0005 | Сравниваемые тип и значение в записи отсутствуют (LDAP_COMPARE_FALSE) |
| GLE0006 | В записи найдены сравниваемые тип и значение (LDAP_COMPARE_TRUE) |
| GLE0007 | Способ идентификации не поддерживается (LDAP_AUTH_METHOD_NOT_SUPPORTED) |
| GLE0008 | Требуется строгая идентификация (LDAP_STRONG_AUTH_REQUIRED) |
| GLE0009 | Получены частичные результаты и возвращена переадресация (LDAP_PARTIAL_RESULTS) |
| GLE0010 | Возвращена переадресация (LDAP_REFERRAL) |
| GLE0011 | Превышено административное ограничение (LDAP_ADMIN_LIMIT_EXCEEDED) |
| GLE0012 | Критичное расширение не поддерживается (LDAP_UNAVAILABLE_CRITICAL_EXTENSION) |
| GLE0013 | Требуется конфиденциальность (LDAP_CONFIDENTIALITY_REQUIRED) |
| GLE0014 | Выполняется подключение SASL (LDAP_SASLBIND_IN_PROGRESS) |
| GLE0016 | Атрибут не найден (LDAP_NO_SUCH_ATTRIBUTE) |
| GLE0017 | Неопределенный тип атрибута (LDAP_UNDEFINED_TYPE) |
| GLE0018 | Неправильное соответствие (LDAP_INAPPROPRIATE_MATCHING) |
| GLE0019 | Нарушение ограничения (LDAP_CONSTRAINT_VIOLATION) |
| GLE0020 | Тип или значение существует (LDAP_TYPE_OR_VALUE_EXISTS) |
| GLE0021 | Недопустимый синтаксис (LDAP_INVALID_SYNTAX) |
| GLE0032 | Объект не найден (LDAP_NO_SUCH_OBJECT) |

| Идентификатор сообщения | Описание |
|---|---|
| GLE0033 | Ошибка псевдонима (LDAP_ALIAS_PROBLEM) |
| GLE0034 | Недопустимый синтаксис DN (LDAP_INVALID_DN_SYNTAX) |
| GLE0035 | Объект является листовым (LDAP_IS_LEAF) |
| GLE0036 | Ошибка учета псевдонимов (LDAP_ALIAS_DEREF_PROBLEM) |
| GLE0048 | Неправильная идентификация (LDAP_INAPPROPRIATE_AUTH) |
| GLE0049 | Неправильные идентификационные данные (LDAP_INVALID_CREDENTIALS) |
| GLE0050 | Недостаточно прав доступа (LDAP_INSUFFICIENT_ACCESS) |
| GLE0051 | Сервер каталогов занят (LDAP_BUSY) |
| GLE0052 | Недоступен агент Службы каталогов (LDAP_UNAVAILABLE) |
| GLE0053 | Серверу каталогов не удается выполнить запрошенную операцию (LDAP_UNWILLING_TO_PERFORM) |
| GLE0054 | Обнаружен цикл (LDAP_LOOP_DETECT) |
| LE0064 | Нарушение присвоения имен (LDAP_NAMING_VIOLATION) |
| LE0065 | Нарушение класса объектов (LDAP_OBJECT_CLASS_VIOLATION) |
| GLE0066 | Операция над ветвью не разрешена (LDAP_NOT_ALLOWED_ON_NONLEAF) |
| GLE0067 | Операция над относительным отличительным именем не разрешена (LDAP_NOT_ALLOWED_ON_RDN) |
| GLE0068 | Запись уже существует (LDAP_ALREADY_EXISTS) |
| GLE0069 | Невозможно изменить класс объектов (LDAP_NO_OBJECT_CLASS_MODS) |
| GLE0070 | Слишком большой объем результатов (LDAP_RESULTS_TOO_LARGE) |
| GLE0071 | Задействовано несколько серверов. (LDAP_AFFECTS_MULTIPLE_DSAS) |
| GLE0080 | Неизвестная ошибка (LDAP_OTHER) |
| GLE0081 | Не удалось соединиться с сервером LDAP (LDAP_SERVER_DOWN) |
| GLE0082 | Локальная ошибка (LDAP_LOCAL_ERROR) |
| GLE0083 | Ошибка кодирования (LDAP_ENCODING_ERROR) |
| GLE0084 | Ошибка расшифровки (LDAP_DECODING_ERROR) |
| GLE0085 | Время запроса истекло (LDAP_TIMEOUT) |
| GLE0086 | Неизвестный способ идентификации (LDAP_AUTH_UNKNOWN) |
| GLE0087 | Неправильный фильтр поиска (LDAP_FILTER_ERROR) |
| GLE0088 | Операция отменена пользователем (LDAP_USER_CANCELLED) |

| Идентификатор сообщения | Описание |
|---|---|
| GLE0089 | Неправильный параметр в процедуре LDAP (LDAP_PARAM_ERROR) |
| GLE0090 | Недостаточно памяти (LDAP_NO_MEMORY) |
| GLE0091 | Ошибка соединения (LDAP_CONNECT_ERROR) |
| GLE0092 | Функция не поддерживается (LDAP_NOT_SUPPORTED) |
| GLE0093 | Не найден управляющий элемент (LDAP_CONTROL_NOT_FOUND) |
| GLE0094 | Нет результатов (LDAP_NO_RESULTS_RETURNED) |
| GLE0095 | Больше результатов (LDAP_MORE_RESULTS_TO_RETURN) |
| GLE0096 | URL не является адресом LDAP (LDAP_URL_ERR_NOTLDAP) |
| GLE0097 | URL не содержит DN (LDAP_URL_ERR_NODN) |
| GLE0098 | Недопустимое значение области URL (LDAP_URL_ERR_BADSCOPE) |
| GLE0099 | Ошибка выделения памяти (LDAP_URL_ERR_MEM) |
| GLE0100 | Клиентский цикл (LDAP_CLIENT_LOOP) |
| GLE0101 | Превышено ограничение переадресации (LDAP_REFERRAL_LIMIT_EXCEEDED) |
| GLE0112 | Среда SSL уже инициализирована (LDAP_SSL_ALREADY_INITIALIZED) |
| GLE0113 | Ошибка вызова инициализации (LDAP_SSL_INITIALIZE_FAILED) |
| GLE0114 | Среда SSL не инициализирована (LDAP_SSL_CLIENT_INIT_NOT_CALLED) |
| GLE0115 | Указано недопустимое значение параметра SSL (LDAP_SSL_PARAM_ERROR) |
| GLE0116 | Ошибка согласования защищенного соединения (LDAP_SSL_HANDSHAKE_FAILED) |
| GLE0118 | Не удается найти библиотеку SSL (LDAP_SSL_NOT_AVAILABLE) |
| GLE0128 | Не найден явный владелец (LDAP_NO_EXPLICIT_OWNER) |
| GLE0129 | Не удалось получить блокировку на требуемый ресурс (LDAP_NO_LOCK) |
| GLE0133 | В DNS не найдены сервера LDAP (LDAP_DNS_NO_SERVERS) |
| GLE0134 | Результаты DNS усечены (LDAP_DNS_TRUNCATED) |
| GLE0135 | Не удалось проанализировать данные DNS (LDAP_DNS_INVALID_DATA) |
| GLE0136 | Не удалось обработать системный домен или сервер имен (LDAP_DNS_RESOLVE_ERROR) |
| GLE0137 | Ошибка в файле конфигурации DNS (LDAP_DNS_CONF_FILE_ERROR) |
| GLE0160 | Переполнение выходного буфера (LDAP_XLATE_E2BIG) |
| GLE0161 | Входной буфер усечен (LDAP_XLATE_EINVAL) |

| Идентификатор сообщения | Описание |
|---|---|
| GLE0162 | Введен недопустимый символ (LDAP_XLATE_EILSEQ) |
| GLE0163 | Не удается определить позицию в кодовом наборе для символа (LDAP_XLATE_NO_ENTRY) |

## Ошибки клиента LDAP

Зная причины, по которым обычно возникают ошибки на клиенте LDAP, вы сможете быстро устранить неполадки на своем сервере. Полный список ошибок клиентов LDAP приведен в разделе “API сервера каталогов” в главе Программирование iSeries Information Center.

Сообщения об ошибках клиента выдаются в следующем формате:

```
[Сбой операции LDAP]:[ошибки API клиента LDAP]
```

**Примечание:** В описании этих сообщений об ошибках предполагается, что клиент обменивается данными с сервером LDAP в системе i5/OS. Аналогичные ошибки могут возникать на клиенте, работающем с сервером на базе другой платформы, однако причины их возникновения и способы устранения будут, скорее всего, другими.

Чаще всего встречаются следующие сообщения:

- “ldap_search: Превышено ограничение времени”
- “[Сбой операции LDAP]: Ошибка при выполнении операции”
- “ldap_bind: Объект не найден”
- “ldap_bind: Неправильные идентификационные данные” на стр. 294
- “[Сбой операции LDAP]: Нет прав доступа” на стр. 294
- “[Сбой операции LDAP]: Не удалось подключиться к серверу LDAP” на стр. 294
- “[Сбой операции LDAP]: Не удалось подключиться к серверу SSL” на стр. 294

## ldap_search: Превышено ограничение времени

Эта ошибка возникает при низкой скорости выполнения поиска в каталоге. Для ее исправления попробуйте выполнить следующие действия:

- Увеличьте ограничение на время поиска для сервера каталогов. Подробные инструкции приведены в разделе “Настройка параметров производительности” на стр. 137.
- Сократите количество задач, выполняемых в системе. Кроме того, можно сократить число активных заданий клиентов LDAP.

## [Сбой операции LDAP]: Ошибка при выполнении операции

Эта ошибка может быть вызвана различными причинами. Для получения сведений о причинах ошибки в каждом конкретном случае просмотрите протоколы заданий QDIRSRV (см. раздел “Отслеживание ошибок и контроль доступа с помощью протокола задания сервера каталогов” на стр. 288) и протоколы заданий серверов SQL (см. раздел Глава 9, “Устранение неполадок сервера каталогов”, на стр. 287).

## ldap_bind: Объект не найден

Чаще всего эта неполадка возникает в том случае, если пользователь ошибается при вводе данных во время выполнения операции. Кроме того, эта неполадка часто возникает при попытке клиента LDAP подключиться от имени несуществующего DN. Зачастую это происходит, если пользователь указывает неправильное DN администратора. Например, пользователь может указывать `QSECOFR` или `Administrator`, в то время как настоящее DN администратора равно cn=Administrator.

Для получения более подробной информации об этой ошибке просмотрите протокол задания QDIRSRV, следуя указаниям, приведенным в разделе “Отслеживание ошибок и контроль доступа с помощью протокола задания сервера каталогов” на стр. 288.

## ldap_bind: Неправильные идентификационные данные

Если указаны неверный пароль или DN, сервер возвращает сообщение об ошибке Недействительное разрешение. Сообщение о неправильных идентификационных данных возвращается в том случае, если при попытке подключения клиент указал одну из следующих записей:

- Запись без атрибута пароля пользователя.
- Запись, представляющую пользователя i5/OS с атрибутом UID, но без пароля. При этом указанный пароль не совпадает с паролем пользователя i5/OS.
- Запись, представляющую спроецированного пользователя, причем указан метод подключения, отличный от простого.

Обычно эта ошибка связана с тем, что пользователь указал неверный пароль. Для получения более подробной информации об этой ошибке просмотрите протокол задания QDIRSRV, следуя указаниям, приведенным в разделе “Отслеживание ошибок и контроль доступа с помощью протокола задания сервера каталогов” на стр. 288.

## [Сбой операции LDAP]: Нет прав доступа

Обычно эта ошибка возникает в том случае, когда у подключающегося DN нет необходимых прав доступа для выполнения запрошенной операции (например, для добавления или удаления). Для получения более подробной информации об этой ошибке просмотрите протокол задания QDIRSRV, следуя указаниям, приведенным в разделе “Отслеживание ошибок и контроль доступа с помощью протокола задания сервера каталогов” на стр. 288.

## [Сбой операции LDAP]: Не удалось подключиться к серверу LDAP

Ниже перечислены наиболее вероятные причины ошибки:

- Клиент LDAP отправил запрос, когда сервер LDAP в указанной системе не запущен или не находится в состоянии ожидания.
- Пользователь задал неверный номер порта. Например, сервер принимает запросы через порт 386, а клиент отправил запрос через порт 387.

Для получения более подробной информации об этой ошибке просмотрите протокол задания QDIRSRV, следуя указаниям, приведенным в разделе “Отслеживание ошибок и контроль доступа с помощью протокола задания сервера каталогов” на стр. 288. Если сервер каталогов был запущен успешно, то протокол задания QDIRSRV будет содержать соответствующее сообщение.

## [Сбой операции LDAP]: Не удалось подключиться к серверу SSL

Эта ошибка возникает в том случае, когда сервер LDAP отклоняет запрос клиента на установление соединения SSL. Это может быть вызвано следующими причинами:

- Функция Управление сертификатами отклонила запрос клиента на подключение к серверу. С помощью Диспетчера цифровых сертификатов проверьте правильность настройки сертификатов, а затем перезапустите сервер и попытайтесь установить соединение еще раз.
- Возможно, у пользователя нет прав на чтение данных из хранилища сертификатов *SYSTEM (по умолчанию - /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Для приложений i5/OS на языке C доступна дополнительная информация об ошибках SSL. Подробные сведения приведены в разделе “API сервера каталогов” в главе Программирование.

## Ошибки, связанные со стратегией управления паролями

Если на сервере действует несколько стратегий управления паролями, то могут возникнуть ошибки, которые не всегда очевидны. Приведенная ниже информация поможет устранить ошибки, связанные со стратегией управления паролями.

**При подключении с правильным паролем возвращается ошибка ″Неправильные идентификационные данные″:** Возможно, пароль устарел или учетная запись заблокирована. Проверьте атрибуты pwdchangedtime и pwdaccountlockedtime записи, как описано в разделе “Советы по стратегии управления паролями” на стр. 163.

**После успешного подключения при отправке запроса возвращается ошибка ″unwilling to perform″:** Возможно, сброшен пароль. В этом случае подключение будет успешным, но пользователь сможет выполнить на сервере только одну операцию - изменить пароль. До тех пор пока пароль не будет изменен, остальные запросы будут возвращать ошибку ″невозможно выполнить″.

**Непредвиденное поведение идентификации со сброшенным паролем:** Если пароль был сброшен, то подключение будет успешным, как говорилось выше. Это значит, что пользователь может идентифицироваться со сброшенным паролем неограниченное количество раз.

## Устранение неполадок QGLDCPYVL API

Этот API записывает свои операции с помощью пользовательского трассировщика. Если возникает или ожидается ошибка, то по записям трассировщика можно определить, очевидная это ошибка или необходимо обслуживание. Трассировку можно получить следующим образом:

```
STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
CALL QGLDCPYVL PARM(...)
ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTTRC(*YES)
```

Для того чтобы сохранить информацию для последующей отправки в сервисное представительство, выполните следующие действия:

1. Создайте файл SAVF с помощью команды Создать SAVF (CRTSAVF).
2. Введите в командной строке iSeries:

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   где QAP0ZDMP содержит ноль, а *xxx* - имя файла сохранения SAVF.

# Глава 10. Связанная информация

В этом разделе перечислены руководства IBM Redbooks (в формате PDF), Web-сайты и разделы Information Center, содержащие сведения о сервере каталогов. Вы можете просматривать и печатать эти документы PDF.

**Redbooks** (www.redbooks.ibm.com)

- Understanding LDAP, SG24-4986 .
- Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino, SG24-6163 .
- Implementation and Practical Use of LDAP on the iSeries Server, SG24-6193 .

**Web-сайты**

- Web-сайт IBM Directory Server iSeries (www.ibm.com/servers/eserver/iseries/ldap)
- Обучающий Web-сайт по JNDI (java.sun.com/products/jndi/tutorial/)

**Прочая информация**

“API сервера каталогов” в категории Программирование.

# Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако ответственность за проверку работы любых продуктов, программ и услуг других фирм несет пользователь.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

**Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству:** ФИРМА INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этой информации лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM, Лицензионного соглашения на машинный код IBM или любого другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Все указанные цены IBM являются предварительными розничными ценами IBM, которые действуют на данный момент и могут изменяться без предварительного уведомления. Цены дилеров могут быть другими.

Эта информация предназначена только для целей планирования. Приведенная информация может измениться до того, как описанные в ней продукты станут доступными.

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 на продукты, защищенные авторским правом:

В настоящей документации приведены примеры исходных текстов прикладных программ, иллюстрирующие некоторые приемы программирования в различных операционных платформах. Разрешается бесплатно копировать, изменять и распространять в любой форме эти примеры с целью разработки, использования и распространения прикладных программ для интерфейсов, соответствующих той операционной платформе, для которой созданы примеры. Эти примеры не были тщательно и всесторонне протестированы. По этой причине IBM не может гарантировать их надежность и пригодность для какой-либо цели.

Если вы просматриваете электронную версию этой информации, то фотографии и цветные иллюстрации могут быть недоступны.

## Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в Соединенных Штатах и/или других странах:

Application System/400
AS/400
DB2
e(эмблема)server
eServer
i5/OS
IBM
iSeries
Lotus
Lotus Notes
Operating System/400
OS/400
Redbooks
SecureWay
WebSphere
400

Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками Microsoft Corporation в США и/или других странах.

Java и все товарные знаки, включающие в себя слово Java, принадлежат фирме Sun Microsystems, Inc. в США и/или других странах.

UNIX - зарегистрированный товарный знак фирмы The Open Group в США и других странах.

Другие названия фирм, продуктов и услуг могут быть товарными или сервисными знаками других фирм.

## Сроки и условия

Разрешение на использование данных публикаций предоставляется на следующих условиях.

**Использование в личных целях:** Разрешается воспроизведение этих публикаций для личного, некоммерческого использования при условии сохранения в них всех заявлений об авторских правах. Запрещается распространение, демонстрация и использование этой публикации в качестве основы для последующих произведений, полностью или частично, без явного согласия на то фирмы IBM.

**Использование в коммерческих целях:** Разрешается воспроизведение, распространение и демонстрация этих публикаций исключительно в пределах организации при условии сохранения в них всех заявлений об авторских правах. Запрещается использование этих публикаций в качестве основы для последующих произведений, а также воспроизведение, распространение и демонстрация этих публикаций, полностью или частично, за пределами предприятия без явного согласия на то фирмы IBM.

За исключением явно оговоренных в данном разрешении случаев, на публикацию и любые содержащиеся в ней данные, программное обеспечение и другие объекты интеллектуальной собственности не предоставляются никакие разрешения, лицензии и права, ни явные, ни подразумеваемые.

Фирма IBM оставляет за собой право в любой момент по своему усмотрению аннулировать предоставленные настоящим разрешением права, если сочтет, что использование этой публикации наносит ущерб интересам фирмы IBM или что указанные инструкции не соблюдаются должным образом.

Загружать, экспортировать и реэкспортировать эту информацию разрешается только при условии полного соблюдения всех надлежащих законов, правил и предписаний, включая все действующие в Соединенных Штатах Америки законы и законодательные акты об экспорте.

ФИРМА IBM НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ ОТНОСИТЕЛЬНО СОДЕРЖИМОГО ЭТИХ ПУБЛИКАЦИЙ. ПУБЛИКАЦИИ ПРЕДОСТАВЛЯЮТСЯ ″КАК ЕСТЬ″, БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, КАК ЯВНЫХ, ТАК И ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ, СОБЛЮДЕНИЯ АВТОРСКИХ ПРАВ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО КОНКРЕТНОЙ ЦЕЛИ.

Напечатано в Дании