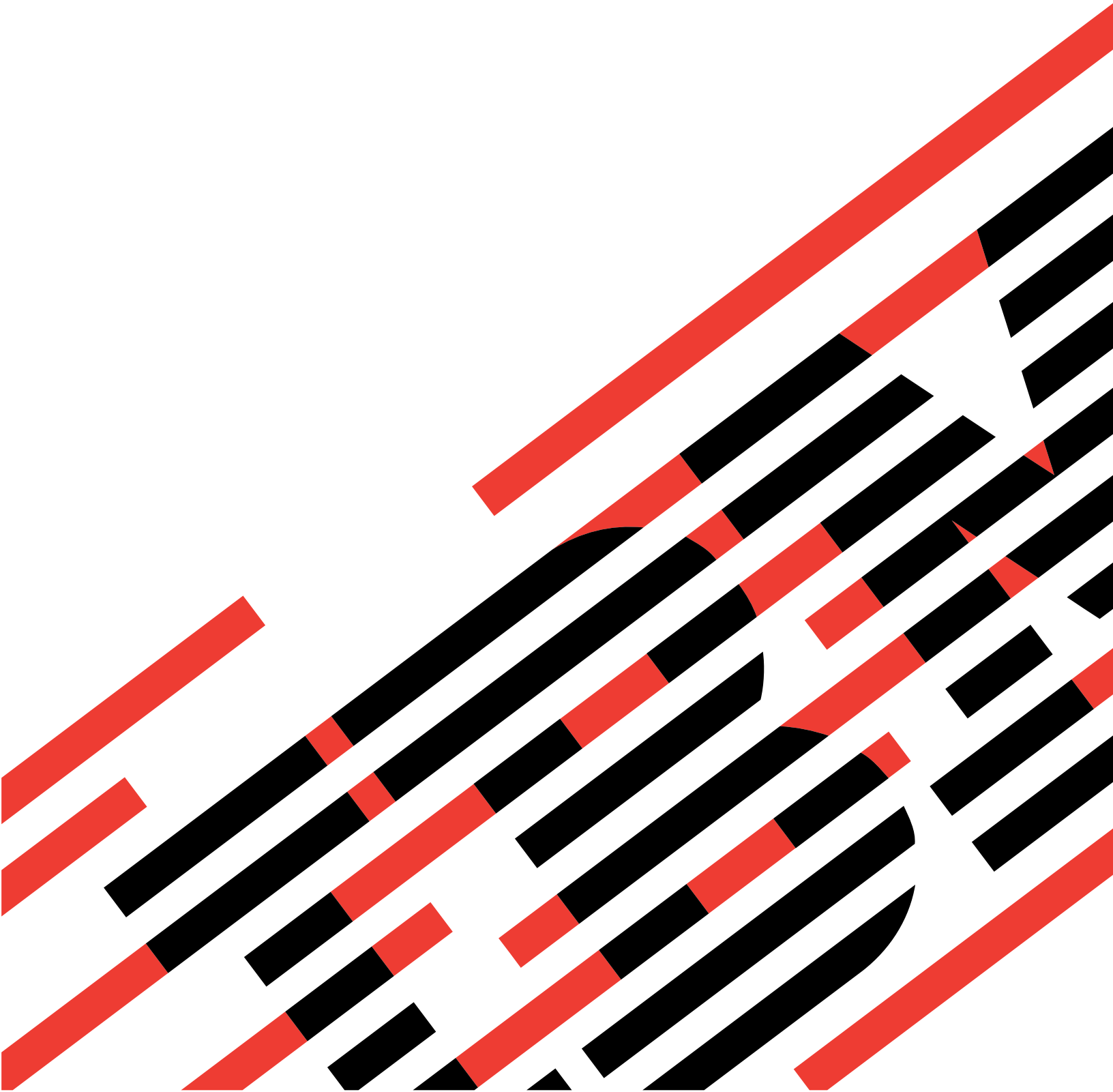
IBM

eserver

iSeries

Сетевые Службы каталогов (LDAP)



IBM

@server

iSeries

Сетевые Службы каталогов (LDAP)

Содержание

Часть 1. Службы каталогов (LDAP)

Службы каталогов обеспечивают поддержку сервера LDAP в системе iSeries. Протокол LDAP применяется в сетях TCP/IP как служба каталогов для Internet-приложений и других программных продуктов.

Если вы уже работали со Службами каталогов, то вам следует ознакомиться с информацией о новых возможностях этого выпуска. При необходимости можно просмотреть и напечатать файл с информацией о Службах каталогов в формате PDF.

Ниже перечислены разделы, содержащие информацию о Службах каталогов, необходимую для управления сервером LDAP в системе iSeries:

Дополнительная информация о Службах каталогов приведена на Web-сайте Служб каталогов  .

Службы каталогов применяют сервер LDAP IBM SecureWay Directory  .

Глава 1. Новое в версии V5R2

В новой версии были внесены следующие изменения в Службы каталогов:

- Начиная с версии V5R1, Службы каталогов входят в состав базовой операционной системы. В версиях V5R2 и выше компонент 32 не поддерживается.
- Предусмотрены более надежные средства защиты данных, хранящихся на сервере каталогов.
- Сервер каталогов LDAP теперь может применяться в качестве контроллера домена Enterprise Identity Mapping (EIM).
- Новая опция позволяет администраторам предоставлять права доступа администратора к серверу каталогов тем пользователям, которым с помощью программы Навигатор были предоставлены права доступа к идентификатору функции Администратор сервера каталогов (QIBM_DIRSRV_ADMIN) операционной системы.
- Сервер каталогов может применять все настроенные IP-адреса или только некоторые из них. Дополнительная информация приведена в разделе “Изменение номера порта или IP-адреса” на стр. 21.
- В версии V5R2 API **ldap_set_option** поддерживает новую функцию трассировки. Опция LDAP_OPT_DEBUG позволяет выполнять диагностику неполадок для клиентов, применяющих API LDAP на языке C. Дополнительная информация приведена в разделе “Трассировка ошибок с помощью опции LDAP_OPT_DEBUG” на стр. 67 и API Служб каталогов справочной системы iSeries Information Center  .

Выделение новой и измененной информации:

Для выделения технических изменений в этой документации применяются следующие обозначения:

- Значок  обозначает начало измененной информации.
- Значок  обозначает конец измененной информации.

Глава 2. Как напечатать этот раздел

Для просмотра или загрузки этого документа в формате PDF щелкните на следующей ссылке: Службы каталогов (LDAP) (около 323 Кб, или 66 страниц).

Прочая информация

Дополнительно можно загрузить следующие документы в формате PDF:

- *LDAP Implementation Cookbook*  .
- *Understanding LDAP*  .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*

- *Implementation and Practical Use of LDAP on the iSeries Server*  .

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

1. Откройте файл PDF в окне браузера (щелкните на приведенной выше ссылке).
2. В меню браузера выберите **Файл**.
3. Выберите **Сохранить как...**
4. Выберите каталог, в котором следует сохранить файл PDF.
5. Нажмите кнопку **Сохранить**.

Загрузка программы Adobe Acrobat Reader

Программу Adobe Acrobat Reader, необходимую для печати и просмотра файлов в формате PDF, можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Глава 3. Службы каталогов - Введение

Службы каталогов представляют сервер LDAP в системе iSeries. Протокол LDAP применяется в сетях TCP/IP как служба каталогов для Internet-приложений и других программных продуктов. Большинство задач по настройке и администрированию сервера каталогов LDAP на базе OS/400 можно выполнять с помощью графического интерфейса Навигатора. Для управления Службами каталогов на PC, подключенном к серверу iSeries, должен быть установлен Навигатор. Службы каталогов могут применяться приложениями с поддержкой LDAP, например, почтовыми программами, получающими адреса электронной почты с серверов LDAP.

Помимо сервера LDAP, Службы каталогов включают:

- Клиент LDAP на базе OS/400. Этот клиент содержит набор интерфейсов прикладных программ (API), с помощью которых можно создавать клиентские приложения в OS/400. Информация об этих API приведена в разделе Службы каталогов справочной системы iSeries Information Center, который относится к категории Программирование.
- Продукт IBM SecureWay Directory Client Software Development Kit (SDK) версии 3.2. В пакет SDK входят клиент LDAP Windows и следующие средства:
  - Средство управления каталогами IBM SecureWay, предоставляющее графический интерфейс для работы с данными каталога.
  - утилиты командной строки (ldapsearch, ldapadd, и т.д.)
  - API LDAP на языке C (библиотечные файлы, заголовочные файлы и примеры программ)
  - Продукт IBM JNDI LDAP (ibmjndi.jar)
  - Электронную документацию для перечисленных выше продуктов. Имена и каталоги соответствующих файлов HTML указаны в файле Readme.

Если вы работали со Службами каталогов в операционной системе OS/400 более раннего выпуска, обратитесь к разделу “Переход от более раннего выпуска Служб каталогов к V5R2” на стр. 12.

Общая информация о LDAP приведена в разделе “LDAP - основные понятия” на стр. 8. Если вы работали с серверами LDAP на других платформах, то вам следует ознакомиться с информацией об особенностях применения LDAP в OS/400, приведенной в этом разделе.

Ознакомившись с основной информацией, перейдите к разделу “Планирование конфигурации сервера каталогов LDAP” на стр. 11.

Информация об установке и настройке сервера каталогов приведена в разделе “Установка и настройка Служб каталогов” на стр. 14.

Документация

В разделе Службы каталогов справочной системы Information Center приведен обзор функции LDAP, причем особый акцент делается на управлении сервером каталогов LDAP в операционной системе OS/400. Эта документация также содержит полную информацию о продукте SecureWay Directory Client SDK. Дополнительная информация о LDAP приведена в следующих источниках:

- *LDAP Implementation Cookbook*  .
- *Understanding LDAP*  .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*

- *Implementation and Practical Use of LDAP on the iSeries server*  .

- Книга *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol* Тима Хоуза и Марка Смита.
- Книга *Understanding and Deploying LDAP Directory Services* Марка К. Смита, Гордона С. Гуда и Тима Хоуза.

Дополнительная информация о применении Служб каталогов на сервере iSeries приведена на Домашней странице Служб каталогов сервера iSeries .

Примечание: Некоторая информация из этого документа взята из документации по LDAP, предоставленной Мичиганским университетом.

LDAP - основные понятия

Простой протокол доступа к каталогам (LDAP) - это протокол служб каталогов, основанный на TCP/IP. Формальное описание протокола LDAP версии 2, созданное Рабочей группой Internet (IEFT), находится в документе RFC 1777, *Lightweight Directory Access Protocol*. Формальное описание протокола LDAP версии 3, созданное IETF, находится в документе RFC 2251, *Lightweight Directory Access Protocol (v3)*. Эти документы RFC можно просмотреть в сети Internet на следующем Web-сайте:

http://www.ietf.org

Служба каталогов LDAP основана на модели клиент-сервер. Один или несколько серверов LDAP содержат данные каталога. Клиент LDAP подключается к серверу LDAP и отправляет запрос. Сервер возвращает ответ или указатель (ссылку) на другой сервер LDAP.

Применение LDAP:

Так как LDAP - это служба каталогов, а не база данных, то информация LDAP обычно носит описательный характер и представляет собой набор атрибутов. Пользователи LDAP считывают информацию из каталога гораздо чаще, чем изменяют ее. Как правило, обновления представляют собой операции удаления или добавления записей. Чаще всего каталоги LDAP применяются как электронные телефонные справочники и адресные книги электронной почты.

Структура каталога LDAP:

Модель службы каталогов LDAP основана на **записях** (которые также называются **объектами**). Каждая запись состоит из одного или нескольких **атрибутов** и характеризуется **типом**. Обычно типы представлены мнемоническими сочетаниями символов, например, `cn` - common name (имя), а `mail` - адрес электронной почты.

Пример каталога в разделе рис. 1 на стр. 10 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. Для редактирования файлов схемы на сервере LDAP следует применять Средство управления каталогами (DMT) IBM SecureWay. Во время установки Служб каталогов эти файлы размещаются в каталоге `/QIBM/UserData/OS400/DirSrv`.

Примечание: Исходные копии файлов схемы по умолчанию находятся в каталоге `/QIBM/ProdData/OS400/DirSrv`. Для того чтоб заменить файлы в каталоге UserData, их можно скопировать из каталога /QIBM/ProdData/OS400/DirSrv.

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.

Кроме того, каждая запись каталога содержит следующие **операционные атрибуты**, автоматически создаваемые сервером LDAP:

- `CreatorsName` - содержит DN связывания, применявшийся при создании записи.
- `CreateTimestamp` - содержит время создания записи.
- `modifiersName` - содержит DN связывания, применявшийся при последнем изменении записи (изначально это имя совпадает со значением атрибута `CreatorsName`).
- `modifyTimestamp` - содержит время последнего изменения записи (изначально совпадает со значением атрибута `CreateTimestamp`).

Как правило, записи каталога LDAP расположены в соответствии с иерархической структурой политического, географического или юридического образования. (см. рис. 1 на стр. 10). Записи, соответствующие странам, 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.

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`.

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 рис. 1 на стр. 10, 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`.

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 разделе рис. 1 на стр. 10, 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.

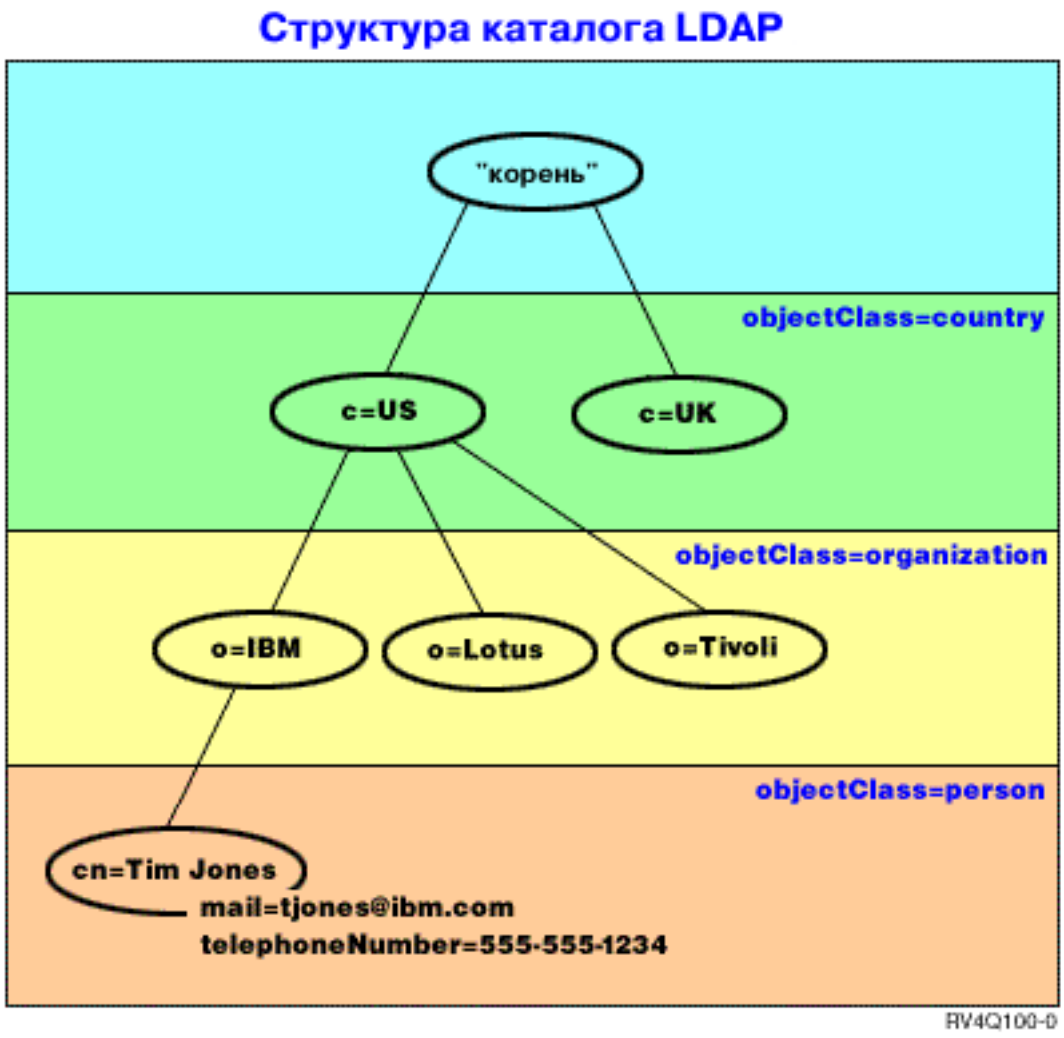


Рисунок 1. Базовая структура каталога LDAP

Примечания о LDAP и Службах каталогов:

- Начиная с версии V4R5, сервер LDAP OS/400 и клиент LDAP OS/400 применяют LDAP версии 3. Клиент версии 2 может применяться для работы с сервером версии 3. Клиент версии 3 может применяться для работы с сервером версии 2, если он подключается к серверу как клиент версии 2 и применяет только API версии 2. Более подробные сведения приведены в разделе Информация о LDAP версий 2 и 3.
- Клиент LDAP Windows также основан на протоколе LDAP версии 3.
- Так как протокол LDAP является стандартом, основные свойства всех серверов LDAP совпадают. Однако вследствие различий в реализации они не являются полностью совместимыми. Сервер LDAP Служб каталогов совместим с другими серверами LDAP из семейства продуктов IBM SecureWay Directory и IBM Directory. С другими серверами LDAP он может быть совместим лишь частично.
- Данные сервера LDAP Служб каталогов хранятся в базе данных OS/400.

Дополнительная информация:

Примеры каталогов LDAP приведены в следующих руководствах:

- Раздел 1.6, The Quick Start: A Public LDAP Example, руководства *Understanding LDAP*.

- Раздел 3.3, Example Scenarios, руководства Understanding LDAP.

Дополнительная информация о принципах работы LDAP приведена в разделе Глава 5, “Службы каталогов - основная и справочная информация” на стр. 35.

Информация о применении LDAP версий 2 и 3

Начиная с версии V4R5, сервер LDAP OS/400 и клиент LDAP OS/400 применяют LDAP версии 3. Клиент версии 3 не может применяться для работы с сервером версии 2. Однако с помощью API ldap_set_option() можно изменить версию клиента V3 на V2. Это позволит отправлять клиентские запросы на сервер V2.

Клиент V2 можно применять вместе с сервером V3. Однако следует учитывать, что в ответ на поисковый запрос сервер V3 может возвратить данные в формате UTF-8, в то время как клиент V2 поддерживает только набор символов IA5.

Примечание: Формальное описание протокола LDAP версии 2, созданное Рабочей группой Internet (IEFT), находится в документе RFC 1777, *Lightweight Directory Access Protocol*. Формальное описание протокола LDAP версии 3, созданное IETF, находится в документе RFC 2251, *Lightweight Directory Access Protocol (v3)*. Эти документы RFC можно просмотреть в сети Internet на следующем Web-сайте:

http://www.ietf.org 

Планирование конфигурации сервера каталогов LDAP

Перед установкой Служб 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.
- **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 Служб 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**. Службы каталогов позволяют использовать для защиты соединений протокол Secure Sockets Layer (SSL), цифровые сертификаты, а также протокол Translation Layer Security (TLS). В версиях V5R1 и выше также поддерживается функция идентификации Kerberos.
- Службы каталогов позволяют ограничивать доступ к объектам в каталоге с помощью списков управления доступом (ACL). Кроме того, для защиты каталога может применяться OS/400функция контроля за действиями.

Переход от более раннего выпуска Служб каталогов к V5R2

В Службы каталогов операционной системы OS/400 версии V5R2 добавлен ряд новых функций и возможностей. Эти изменения относятся как к серверу каталогов LDAP, так и к графическому пользовательскому интерфейсу Навигатора. Для работы с новыми функциями графического интерфейса необходимо установить Навигатор на PC, подключенном к серверу iSeries по соединению TCP/IP. Навигатор является компонентом продукта iSeries Access для Windows. Если в системе установлена более ранняя версия Навигатора, обновите ее до версии V5R2.

К OS/400 версии V5R2 можно перейти от версии V4R5 или V5R1. При переходе к OS/400 версии V5R2 данные каталога LDAP и файлы схемы каталога автоматически преобразуются в формат V5R2. Для обновления сервера LDAP Служб каталогов операционной системы OS/400 версии V4R3 или V4R4 до версии V5R2 необходимо выполнить дополнительные действия.

При переходе к OS/400 версии V5R2 следует обратить внимание на следующее:

- При переходе к версии V5R2 Службы каталогов автоматически переносят файлы схемы в V5R2 и удаляют старые файлы схемы. Однако если файл схемы были удалены или переименованы, преобразование не будет выполнено. В этом случае будет показано сообщение об ошибке, либо Службы каталогов будут считать, что эти файлы уже преобразованы.
- Службы каталогов преобразуют данные каталога в формат V5R2 при первом запуске сервера или импортировании файла LDIF. Планируя процедуру перехода к новой версии, отведите время на выполнение этой операции. При переходе к версии V5R2 от V4R4 или более ранней версии учтите, что в версии V5R2 данные каталога будут занимать примерно вдвое больше памяти. Это обусловлено тем, что в V4R4 и более ранних версиях Службы каталогов поддерживали только набор символов IA5 и хранили данные в CCSID 37 (однобайтный формат). В настоящий момент Службы каталогов поддерживают полный набор символов ISO 10646.

  После перехода к версии V5R2 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.
- V4R4 и более ранние выпуски Служб 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 версии V4R4 и более ранних версий к версии V5R2 Службы каталогов изменяют 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.
- 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.

Переход от Служб каталогов версии V4R3 или V4R4 к версии V5R2

Переход от OS/400 версии V4R3 к версии V5R2 не поддерживается. Для перехода от сервера LDAP Служб каталогов версии V4R3 или V4R4 к версии V5R2 выполните следующие процедуры:

- Установка промежуточного выпуска OS/400 поверх выпуска V4R3 или V4R4
- Сохранение библиотеки базы данных и установка OS/400 версии V5R2 после удаления версии V4R3 или V4R4

Установка промежуточного выпуска OS/400 поверх выпуска V4R3 или V4R4

Хотя переход от версии V4R3 или V4R4 операционной системы OS/400 к версии V5R2 не поддерживается, это процедуру можно выполнить в несколько этапов:

- переход от версии V4R3 или V4R4 к версии V4R5
- переход от версии V4R4 или V4R5 к версии V5R1
- переход от версии V4R5 или V5R1 к версии V5R2

Версию сервера Служб каталогов можно обновить путем перехода к промежуточному выпуску (V4R5 или V5R1) и последующего перехода к выпуску V5R2. Подробная информация о процедурах установки OS/400 приведена в разделе *Установка программного обеспечения*  . Для перехода к новой версии продукта выполните следующие действия:

1. Запишите изменения, внесенные в файлы схемы в каталоге /QIBM/UserData/OS400/DirSrv. Файлы схемы переносятся автоматически.
2. Установите OS/400 версии V4R5 или V5R1 поверх версии V4R4 или V4R3.
3. Поверх установленной версии установите OS/400 версии V5R2.
4. Запустите сервер Служб каталогов (если это еще не сделано).
5. С помощью Средства управления каталогами внесите записанные на шаге 1 изменения в файлы схемы.
6. Заново запустите сервер Служб каталогов.

Сохранение библиотеки базы данных и установка OS/400 версии V5R2 после удаления версии V4R3 или V4R4

Другим способом обновления сервера Служб каталогов является сохранение применяемой в версиях V4R3 и V4R4 библиотеки базы данных и ее восстановление после установки версии V5R2 ″с нуля″. При этом не приходится устанавливать промежуточный выпуск. Однако в ходе этой процедуры не переносятся параметры сервера, поэтому их придется настроить заново. Подробная информация о процедурах установки OS/400 приведена в разделе *Установка программного обеспечения*  . 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.
2. Запишите параметры конфигурации, заданные в свойствах сервера Служб каталогов, в том числе имя библиотеки базы данных.
3. Сохраните библиотеку базы данных, указанную в конфигурации сервера Служб каталогов.
4. Запишите параметры конфигурации функции публикации.
5. Установите OS/400 версии V5R2 ″с нуля″.
6. Настройте сервер Служб каталогов с помощью мастера EZ-Setup.
7. Восстановите библиотеку базы данных, сохраненную на шаге 3.
8. С помощью Средства управления каталогами внесите записанные на шаге 1 изменения в файлы схемы.
9. С помощью Навигатора внесите изменения в конфигурацию Служб каталогов. Укажите восстановленную базу данных.
10. С помощью Навигатора восстановите конфигурацию функции публикации.
11. Заново запустите сервер Служб каталогов.

Сведения о переходе к новой версии

При обновлении версии V4R3 необходимо обратить внимание на следующее:

- **Переход от файла ключей к базе данных ключей:**

  Для подключения к серверу каталогов LDAP по защищенному соединению SSL в продукте Client Access версии V3R2 применялся файл ключей. В продукте iSeries Access для Windows при работе с соединениями SSL применяются хранилища сертификатов, известные также как базы данных

ключей. Если ранее при работе с сервером LDAP применялся файл ключей, то для применения SSL в новой версии его необходимо преобразовать в базу данных ключей. При первой попытке установить соединение SSL с сервером каталогов LDAP Навигатор выдаст предупреждение об этом изменении. Если вы решите преобразовать ключ, то вам потребуется указать некоторую информацию о базе данных ключей.

В версии V4R3 сервер каталогов LDAP также применял файл ключей для собственных соединений SSL. В версии V4R4 и выше вместо файла ключей применяется хранилище сертификатов. Если на сервере версии V4R3 была настроена поддержка SSL, содержимое файла ключей будет перенесено в системное хранилище сертификатов.

- **Были удалены два потоковых файла:**

  Следующие потоковые файлы, применявшиеся Службами каталогов версии V4R3, больше не используются и автоматически удаляются при установке более позднего выпуска:

  ```
  /QIBM/ProdData/OS400/DirSrv/qgldcert.kyr
  /QIBM/ProdData/OS400/DirSrv/qgldcert.sth
  ```

  Никаких действий с этими файлами выполнять не требуется. Эта информация приведена исключительно для вашего сведения.

Кроме того, следует учитывать еще ряд особенностей, связанных с переходом от старых выпусков к текущему выпуску.

Установка и настройка Служб каталогов

Продукт Службы каталогов (LDAP) автоматически устанавливается при установке OS/400. Для сервера каталогов задается конфигурация по умолчанию, с которой он автоматически запускается при запуске TCP/IP. После запуска на сервере каталогов публикуется информация о системе. Для настройки параметров серверов каталогов LDAP запустите Мастер настройки Служб каталогов. Для применения этого мастера необходимы специальные права доступа *ALLOBJ и *IOSYSCFG.

Начиная с версии V5R1, Службы каталогов входят в состав базовой операционной системы. В версиях V5R2 и выше компонент 32 не поддерживается.

Настройка сервера каталогов LDAP

Если в системе не была настроена публикация информации на другом сервере LDAP, и на сервере DNS TCP/IP не определены серверы LDAP, то Службы каталогов автоматически устанавливаются с ограниченной конфигурацией по умолчанию. Вы можете настроить отдельные параметры сервера каталогов LDAP с помощью мастера Службы каталогов. Этот мастер можно запустить в процессе настройки EZ-Setup, либо 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 OS/400 дополнительно потребуются специальные права доступа *AUDIT.

Для запуска Мастера настройки Служб каталогов выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Настроить**.

Примечание: Если сервер каталогов уже настроен, выберите опцию **Изменить конфигурацию** вместо опции **Настроить**.

Настройте сервер каталогов LDAP, следуя указаниям Мастера настройки сервера каталогов.

Примечание: Библиотеку, содержащую данные каталога, может потребоваться разместить 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.

По завершении работы мастера будет создана базовая конфигурация сервера каталогов LDAP. Если в системе установлен продукт Lotus Domino, то порт 389 (порт сервера LDAP по умолчанию) может быть занят функцией LDAP Domino. Выполните одно из следующих действий:
- Измените порт, применяемый функцией Lotus Domino
- Измените порт, применяемый Службами каталогов
- Укажите конкретные IP-адреса

Теперь можно запустить сервер. Перед этим можно выполнить следующие действия:
- Импортировать данные на сервер
- Настроить защиту Secure Sockets Layer (SSL)
- Настроить идентификацию Kerberos
- Настроить переадресацию

Настройка SSL на сервере каталогов LDAP

Если в системе установлен компонент Диспетчер цифровых сертификатов, то для защиты данных сервера каталогов LDAP можно настроить протокол Secure Sockets Layer (SSL). Перед настройкой SSL на сервере каталогов рекомендуется ознакомиться с обзором применения SSL совместно со Службами каталогов.

Если для управления сервером каталогов LDAP с помощью Навигатора или клиента LDAP Windows планируется применять соединение SSL, на PC должна быть установлена одна из клиентских программ шифрования (5722CE2 или 5722CE3).

Для настройки SSL на сервере LDAP воспользуйтесь программой Диспетчер цифровых сертификатов. Диспетчер цифровых сертификатов можно запустить из папки **Internet** Навигатора или со страницы **Сеть** окна диалога **Свойства** серверов каталогов.

Для запуска интерфейса Диспетчера цифровых сертификатов со страницы **Сеть** выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
5. Перейдите на страницу **Сеть**.

6. Нажмите кнопку **Диспетчер цифровых сертификатов**.
   Диспетчер цифровых сертификатов будет запущен в Web-браузере по умолчанию.

Инструкции по назначению цифрового сертификата серверу каталогов приведены в разделе Защита сервера каталогов LDAP.

После настройки SSL можно изменить порт, применяемый сервером каталогов LDAP для защищенных соединений.

Настройка идентификации Kerberos на сервере каталогов LDAP

Если в системе настроена Служба сетевой идентификации, то на сервере каталогов LDAP можно настроить функцию идентификации Kerberos. Перед настройкой Kerberos на сервере каталогов рекомендуется ознакомиться с обзором применения Kerberos совместно со Службами 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 пункте **Каталог** 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.

Конфигурация Служб каталогов по умолчанию

Сервер каталогов LDAP автоматически устанавливается в процессе установки OS/400. При этом создается конфигурация по умолчанию. Сервер каталогов применяет конфигурацию по умолчанию, если выполнены следующие условия:

- Администратор не запускал Мастер настройки Служб каталогов и не изменял параметры на странице Свойства.
- Функция публикации Служб каталогов не настроена.
- Серверу каталогов LDAP не удается обнаружить информацию о LDAP на сервере DNS.

При работе сервера каталогов LDAP с конфигурацией по умолчанию:

- Сервер каталогов LDAP автоматически запускается вместе с TCP/IP.
- Создается администратора по умолчанию - cn=Administrator. Устанавливается пароль, применяемый для выполнения внутренних операций. Другой пароль администратора можно задать на странице свойств Служб 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 LDAP применяет библиотеку данных по умолчанию 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.

Следующие параметры действуют по умолчанию для функции публикации Служб каталогов:

- Система публикует информацию на локальном сервере каталогов LDAP
- При публикации не применяется SSL
- Для публикации применяются контейнеры в суффиксе по умолчанию

- Для идентификации на сервере каталогов операционная система OS/400 применяет ИД cn=Administrator и созданный системой пароль.
- Публикуется только информация о системе.

Средство управления каталогами IBM SecureWay

Средство управления каталогами IBM SecureWay (DMT) предоставляет графический интерфейс для работы с данными каталога LDAP. С помощью DMT можно выполнять следующие задачи:

- Просмотр схемы каталога
- Добавление, изменение и удаление классов объектов
- Добавление, изменение и удаление атрибутов
- Просмотр и поиск в дереве каталогов
- Добавление, изменение, просмотр и удаление записей
- Изменение RDN записи
- Управление ACL

DMT является компонентом клиента LDAP Windows, входящего в состав Служб каталогов. Клиент поставляется в каталоге интегрированной файловой системы.

Для установки клиента LDAP Windows, включающего DMT, на PC выполните следующие действия:

1. В Навигаторе откройте **Файловые системы**.
2. Откройте **Общие каталоги**.
3. Дважды щелкните на значке **Qdirsrv**.
4. Дважды щелкните на значке **UserTools**.
5. Дважды щелкните на значке **Windows**.
6. Дважды щелкните на значке файла **setup.exe**, чтобы начать установку DMT. Выполните инструкции программы установки.

Документация по Средству управления каталогами IBM SecureWay (DMT) находится в файле `dparent.htm`. Этот файл копируется в папку IBM SecureWay Directory на PC во время установки клиента.

Глава 4. Администрирование сервера каталогов LDAP

Для администрирования сервера каталогов LDAP необходимы следующие наборы прав 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, роль администратора может играть спроецированный пользователь, у которого есть права доступа к ИД функции Администратор служб каталогов.

Ниже перечислены основные задачи администрирования сервера каталогов:

Запуск сервера каталогов LDAP

Для запуска сервера каталогов LDAP выполните следующие действия:

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** 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 файлы. Аналогично, первый запуск сервера каталогов после перехода от более ранней версии Служб каталогов может занять больше времени, чем обычно, так как сервер должен преобразовать файлы. Для того чтобы определить, запущен ли сервер, узнайте его состояние.

Примечание: Сервер каталогов можно запустить и в сеансе 5250 с помощью команды `STRTCPSVR *DIRSRV`.

Если сервер каталогов настроен для запуска вместе с TCP/IP, то его можно запустить с помощью команды STRTCP.

Завершение работы сервера каталогов LDAP

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 завершения работы сервера каталогов LDAP выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** 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. Для того чтобы определить, остановлен ли сервер, узнайте его состояние.

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

Состояние сервера каталогов указывается в столбце **Состояние** на правой панели окна программы Навигатор.

Для просмотра состояния сервера каталогов выполните следующие действия:
1. В Навигаторе откройте **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 дополнительной информации о состоянии сервера каталогов щелкните правой кнопкой мыши на пункте **Каталог** 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.

Проверка заданий на сервере каталогов LDAP

В некоторых случаях может понадобиться проконтролировать работу определенных заданий на сервере каталогов LDAP. Для этого выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Задания сервера**.

Включение функции уведомления о событиях

Службы каталогов поддерживают 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 Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите опцию **Свойства**.
5. Выберите **События**.
6. Выберите Опцию **Разрешить регистрацию клиентов для уведомления о событиях**.

Кроме того, можно указать максимальное число зарегистрированных записей для каждого соединения и максимальное число зарегистрированных записей для всего сервера.

Дополнительная информация о функции уведомления о событиях приведена в приложении C, Event Notification, руководства IBM SecureWay Directory Version 3.2: Client SDK Programming Reference  .

Настройка параметров транзакций

Службы каталогов поддерживают транзакции, объединяющие несколько операций с каталогом LDAP. Дополнительная информация приведена в разделе “Транзакции” на стр. 40.

Для настройки параметров транзакций на сервере выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
5. Выберите **Транзакции**.
6. Задайте параметры транзакций.

Примечание: Параметры транзакций могут влиять на производительность сервера LDAP, поэтому для достижения максимальной производительности следует попробовать различные сочетания значений параметров.

Изменение номера порта или IP-адреса

По умолчанию сервер каталогов LDAP Службб каталогов применяет следующие порты:
- 389 для незащищенных соединений.
- 636 для защищенных соединений (если вы разрешили Службам 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 Службб каталогов, либо, если приложением поддерживает связывание с определенным IP-адресом, задайте различные IP-адреса для двух серверов.

Пример конфликта сервера LDAP Domino с сервером LDAP Службб каталогов iSeries приведен в разделе Применение сервера LDAP Domino и сервера LDAP Службб каталогов в одной системе iSeries

Для изменения портов сервера каталогов LDAP выполните следующие действия:

1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** 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 пункте **Каталог** 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.

Перемещение данных каталога LDAP в другую систему

Сервер LDAP Служб каталогов может работать независимо от других серверов. Однако в некоторых случаях требуется, чтобы он работал совместно с другими серверами. Ниже перечислены некоторые из них:

- “Импорт файла LDIF”
- “Экспорт файла LDIF”
- “Настройка новой копии сервера каталогов” на стр. 23
- “Публикация информации на сервере каталогов” на стр. 27

Импорт файла LDIF

Для переноса информации между серверами каталогов LDAP применяются файлы Формата обмена данными LDAP (LDIF). Перед выполнением этой операции передайте файл LDIF на сервер iSeries как потоковый файл.

Для того чтобы импортировать файл LDIF на сервер каталогов LDAP, выполните следующие действия:

1. Если сервер каталогов запущен, остановите его. Информация о завершении работы сервера каталогов приведена в разделе “Завершение работы сервера каталогов LDAP” на стр. 20.
2. В Навигаторе откройте **Сеть**.
3. Откройте **Серверы**.
4. Выберите **TCP/IP**.
5. Щелкните правой кнопкой мыши на пункте **Каталог**, выберите опцию **Средства**, а затем - **Импортировать файл**.

Примечание: Файлы LDIF также можно импортировать с помощью утилиты ldapadd.

Экспорт файла LDIF

Для переноса информации между серверами каталогов LDAP применяются файлы Формата обмена данными LDAP (LDIF). Дополнительная информация приведена в разделе “Формат обмена данными LDAP” на стр. 36. 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 **Каталог**, выберите опцию **Средства**, а затем - **Экспортировать файл**.

   Примечание: Если вы не укажете каталог для экспорта файла LDIF, файл будет сохранен в каталоге по умолчанию, указанном в пользовательском профайле OS/400, под управлением которого выполняется эта операция. Если каталог по умолчанию не изменялся, то это корневой каталог.

Примечания:

1. 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**.
2. Файл LDIF можно также создать с помощью утилиты ldapsearch. Дополнительная информация приведена в разделе “Утилита ldapsearch” на стр. 56. Укажите опцию -L, чтобы перенаправить вывод в файл.

Настройка новой копии сервера каталогов

Вы можете создать копии сервера каталогов LDAP в других системах iSeries. Для репликации Службы каталогов применяют стандартный протокол LDAP версии 3.

Примечания:

1. В репликации не могут участвовать серверы LDAP версий 3 и 2. По этой причине в системе, для которой создается копия, должна применяться та же версия LDAP, что и в системе сервера-копии. Версии V4R3 и V4R4 операционной системы OS/400 поддерживают LDAP версии 2. Версия V4R5 и более поздние версии поддерживают LDAP версии 3
2. Каталог Служб каталогов можно скопировать на сервер IBM SecureWay V3.2 или более поздней версии, установленный в другой операционной системе. Для этого на сервере каталогов OS/400 должна быть настроена поддержка механизма 3.2 ACI. При возникновении неполадок во время создания копии процесс репликации прекращается. В этом случае создается неполная копия.

Для настройки новой копии сервера каталогов выполните следующие действия:

1. Настройте главный сервер и сервер-копию, если это еще не сделано.

   Примечание: Убедитесь, что схемы и суффиксы обоих серверов совпадают.
2. Остановите главный сервер.
3. (необязательно) Настройте данные LDAP для первоначальной репликации. Этот шаг можно пропустить при отсутствии данных, которые необходимо перенести на сервер-копию с главного сервера.
4. (необязательно) Перенесите данные LDAP на главный сервер. Этот шаг следует пропустить, если выполнено одно из следующих условий:
   - Создается копия нового сервера каталогов LDAP.
   - Сервер не содержит данных, которые необходимо сохранить.
5. Настройте новый сервер-копию.
6. Настройте главный сервер для работы с новой копией.
7. Убедитесь, что на главном сервере разрешено обновление каталога:
   a. В Навигаторе разверните значок системы, в которой находится главный сервер каталогов.
   b. Откройте **Сеть**.
   c. Откройте **Серверы**.
   d. Выберите **TCP/IP**.
   e. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
   f. Отметьте опцию **Разрешить обновление каталога**, если это еще не сделано.

Примечание: В приведенных выше инструкциях предполагается, что главный сервер и сервер-копия находятся в системах, управляемых с помощью Навигатора с одного PC. Если для управления этими системами применяются разные PC, то различные части этой

процедуры следует выполнять на соответствующих PC. Если один из серверов работает в операционной системе IBM, отличной от OS/400, то обратитесь за описанием процедуры настройки сервера к документации по соответствующей операционной системе.

Настройка данных LDAP для первоначальной репликации

На главном сервере каталогов LDAP могут быть данные, которые необходимо добавить на новый сервер-копию. Для этого необходимо экспортировать каталог в файл LDIF. На время экспортирования файла LDIF следует запретить обновление главного сервера. Это можно сделать одним из следующих способов:

- Остановить сервер каталогов LDAP. При большом объеме данных в каталоге работу сервера придется остановить на длительное время.
- Запретить обновления, изменив свойства сервера. При этом в процессе экспортирования файла LDIF сервер сможет обрабатывать запросы на поиск. Для применения этого способа выполните следующие действия:
  1. В Навигаторе разверните значок системы, в которой находится главный сервер каталогов.
  2. Откройте **Сеть**.
  3. Откройте **Серверы**.
  4. Выберите **TCP/IP**.
  5. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
  6. Если выбрана опция **Разрешить обновление каталога**, отмените ее выбор. Во время настройки репликации все запросы на обновление каталога будут отклоняться.
  7. Нажмите кнопку **OK**.
  8. Остановите, а затем повторно запустите сервер каталогов LDAP.

После того как вы завершите работу сервера или запретите обновление каталога, выполните следующие действия:

1. Экспортируйте каталог в файл LDIF.
2. Перенесите файл LDIF в систему, в которой находится сервер-копия.

После переноса файла LDIF в систему сервера-копии необходимо импортировать данные на этот сервер:

1. В Навигаторе разверните значок системы, в которой находится сервер-копия.
2. Завершите работу сервера-копии. Обновите информацию о состоянии серверов. Состояние сервера должно измениться на **Остановлен**.
3. Откройте **Сеть**.
4. Откройте **Серверы**.
5. Выберите **TCP/IP**.
6. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
7. Отметьте опцию **Разрешить обновление каталога**, если она еще не выбрана. Это позволит импортировать данные.
8. Нажмите кнопку **OK**.
9. Импортируйте файл LDIF, перенесенный на шаге 2.
10. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
11. Отмените выбор опции **Разрешить обновление каталога**.

Перемещение данных LDAP на главный сервер

После преобразования сервера каталогов LDAP в сервер-копию его данные изменять нельзя. Если сервер LDAP, настраиваемый в качестве сервера-копии, содержит данные, то рекомендуется перенести эти данные на главный сервер. Для этого выполните следующие действия:

1. В Навигаторе разверните значок системы, в которой находится сервер-копия.
2. Откройте **Сеть**.
3. Откройте **Серверы**.
4. Выберите **TCP/IP**.
5. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.

6. Если выбрана опция **Разрешить обновление каталога**, отмените ее выбор. Во время настройки репликации все запросы на обновление каталога будут отклоняться.
7. Нажмите кнопку **OK**.
8. Завершите работу сервера каталогов LDAP.
9. Экспортируйте каталог в файл LDIF.
10. Перенесите файл LDIF в систему, в которой находится главный сервер.

После переноса файла LDIF в систему главного сервера необходимо импортировать данные на этот сервер:

1. В Навигаторе разверните значок системы, в которой находится главный сервер каталогов.
2. Завершите работу главного сервера, если это еще не сделано. Обновите информацию о состоянии серверов. Состояние сервера должно измениться на **Остановлен**.
3. Откройте **Сеть**.
4. Откройте **Серверы**.
5. Выберите **TCP/IP**.
6. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
7. Отметьте опцию **Разрешить обновление каталога**, если она еще не выбрана. Это позволит импортировать данные.
8. Нажмите кнопку **OK**.
9. Импортируйте файл LDIF, перенесенный на шаге 10 предыдущей процедуры.
10. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
11. Отмените выбор опции **Разрешить обновление каталога**.

Настройка новой копии

Для настройки нового сервера-копии выполните следующие действия.

Примечание: Перед выполнением этой процедуры необходимо настроить и завершить работу сервера-копии.

1. В Навигаторе разверните значок системы, в которой находится сервер-копия.
2. Откройте **Сеть**.
3. Откройте **Серверы**.
4. Выберите **TCP/IP**.
5. При необходимости завершите работу сервера. Обновите информацию о состоянии серверов. Состояние сервера должно измениться на **Остановлен**.
6. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
7. Перейдите на страницу **Репликация**.
8. Выберите опцию **Применять сервер-копию**.
9. В поле **Имя, применяемое главным сервером для обновления** укажите имя, которое будет применять главный сервер при подключении к серверу-копии для обновления. Это может быть отличительное имя (DN), либо имя пользователя Kerberos.

   Если выбрано DN:

   - Нажмите кнопку **Пароль**, расположенную рядом с полем **Имя, применяемое главным сервером для обновления**. Введите пароль, который будет применять главный сервер при подключении к серверу-копии для обновления данных.

     Примечание: Запишите этот пароль и имя, указанное на шаге 9. Они понадобятся при настройке репликации на главном сервере.

   Если выбрана опция **Добавить пользователя Kerberos**:

   - Программа выдаст приглашение для ввода имени Kerberos (в формате `LDAP/ имя-хоста`, где *имя-хоста* - полное имя хоста главного сервера) и области по умолчанию (например, ACME.COM) главного сервера.

     Примечание: Для применения пользователя Kerberos поддержка протокола Kerberos должна быть настроена как на главном сервере, так и на сервере-копии.

10. В поле **URL главного сервера** введите имя главного сервера в формате URL. Если главный сервер применяет порт, отличный от указанного по умолчанию, задайте номер этого порта в URL.
11. Перейдите на страницу **База данных**/**Суффиксы**. Если список не содержит необходимый суффикс, добавьте его.
12. (необязательно) Для применения протокола SSL во время репликации настройте функцию защиты SSL на сервере с помощью Диспетчера цифровых сертификатов. Диспетчер цифровых сертификатов можно запустить со страницы **Сеть**. Дополнительная информация о настройке SSL на сервере каталогов приведена в разделе “Настройка SSL на сервере каталогов LDAP” на стр. 15.
13. Нажмите кнопку **OK**.

Настройка главного сервера для работы с новой копией

Настройте главный сервер для работы с новой копией, выполнив следующие действия.

Примечание: Для выполнения этой процедуры необходимо настроить и запустить главный сервер.

1. В Навигаторе разверните значок системы, в которой находится главный сервер каталогов.
2. Откройте **Сеть**.
3. Откройте **Серверы**.
4. Выберите **TCP/IP**.
5. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
6. Отметьте опцию **Разрешить обновление каталога**, если это еще не сделано.
7. Нажмите кнопку **OK**.
8. Остановите, а затем повторно запустите сервер каталогов LDAP. Обновите информацию о состоянии серверов. Состояние сервера должно измениться на **Запущен**.
9. Еще раз щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
10. Перейдите на страницу **Репликация**. Навигатор может выдать приглашение для ввода информации о соединении. Задайте эту информацию и нажмите кнопку **OK**.
11. Нажмите кнопку **Добавить.**
12. В поле **Сервер** введите имя сервера-копии в формате URL.
13. Выберите способ идентификации.

    Для применения отличительного имени (DN) и пароля:

    a. Выберите **Применять DN и пароль**.

    b. В поле **Подключаться как** введите имя, указанное на шаге 9 на стр. 25 при настройке сервера-копии.

    c. Нажмите кнопку **Пароль** и введите пароль, заданный на шаге 9 на стр. 25 при настройке сервера-копии.

    Для применения Kerberos:

    - Выберите опцию **Применять учетную запись Kerberos главного сервера**. Главный сервер будет применять для идентификации свое имя субъекта Kerberos.

      Примечание: Для применения Kerberos поддержка Kerberos должна быть включена как на главном сервере, так и на сервере-копии.
14. Для применения протокола SSL во время репликации настройте на сервере функцию защиты SSL с помощью Диспетчера цифровых сертификатов. Диспетчер цифровых сертификатов можно запустить со страницы **Сеть**. Дополнительная информация о настройке SSL на сервере каталогов приведена в разделе “Настройка SSL на сервере каталогов LDAP” на стр. 15.
15. Если сервер-копия не применяет порт по умолчанию, укажите номер порта в поле **Порт**.
16. Если сервер-копию не нужно обновлять при каждом изменении записей на главном сервере, выберите **Время**. Затем укажите частоту обновления сервера-копии.
17. Нажмите кнопку **OK**.
18. Перейдите на страницу **База данных**/**Суффиксы**. Если список не содержит необходимый суффикс, добавьте его.
19. Разрешите обновлять каталог на всех серверах-копиях:

a. В Навигаторе разверните значок системы, в которой находится сервер-копия.
b. Откройте **Сеть**.
c. Откройте **Серверы**.
d. Выберите **TCP/IP**.
e. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
f. Отметьте опцию **Разрешить обновление каталога**, если она еще не выбрана.
g. Нажмите кнопку **OK**.

20. Если серверы-копии не запущены, запустите их.

Примечание: Сервер не может являться и главным сервером, и сервером-копией.

Публикация информации на сервере каталогов

Систему можно настроить для публикации определенной информации на локальном или удаленном сервере каталогов LDAP. OS/400 автоматически публикует эту информацию на сервере каталогов LDAP, когда в нее вносятся изменения с помощью Навигатора. Публикуемая информация может включать системные сведения (системы и принтеры), информацию об общих принтерах, пользователях, а также стратегии QoS TCP/IP. Дополнительная информация о Quality of service приведена в разделе Конфигурация LDAP и QoS .

Если родительское DN, в котором публикуются данные, не существует, то Службы каталогов автоматически создают это DN. В системе также могут быть установлены другие приложения OS/400, публикующие информацию в каталоге LDAP. Кроме того, пользовательские программы могут публиковать в каталоге LDAP информацию других типов с помощью интерфейсов прикладных программ (API).

Примечания:

1. Если в OS/400 разрешена публикация информации типа Пользователи, на сервер LDAP 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 Службы каталогов OS/400 справочной системы iSeries Information Center. Он относится к категории Программирование. Этот раздел содержит следующие сведения:
   - Инструкции по вызову API.
   - Инструкции по исключению отдельных пользователей из списка пользователей, информация о которых экспортируется на сервер LDAP.
   - Описание процедуры экспорта полей системного каталога рассылки.
2. Если в OS/400 разрешена публикация информации типа Система, и выбраны некоторые принтеры, то система автоматически синхронизирует данные каталога LDAP с изменениями, вносимыми в конфигурацию принтеров в системе. На сервере публикуется следующая информация о принтере: расположение принтера, скорость работы (число страниц в минуту), поддержка двусторонней и цветной печати, тип и модель, а также описание принтера. Эта информация берется из описания устройства в системе. Пользователи могут руководствоваться этой информацией при выборе принтера.
3. Информацию OS/400 можно опубликовать на сервере каталогов LDAP, расположенном в другой операционной системе, при условии, что на этом сервере настроена схема IBM.

Для настройки в операционной системе OS/400 функции публикации информации на сервере каталогов LDAP выполните следующие действия:

1. В Навигаторе щелкните правой кнопкой мыши на значке системы и выберите пункт **Свойства**.
2. Перейдите на страницу **Службы каталогов**.
3. Выберите типы информации, которую необходимо 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 LDAP, на котором следует публиковать информацию OS/400, и нажмите кнопку **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 OS/400 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 “Применение идентификации Kerberos на сервере каталогов LDAP” на стр. 42.
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 OS/400 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 Служб каталогов. Определения схемы IBM SecureWay Directory, включая Службы каталогов iSeries, можно найти на Web-странице Служб каталогов.

Информация об общих принтерах должна публиковаться на сервере каталогов, поддерживающем схему Active Directory фирмы Microsoft. Публикация такой информации в Active Directory позволяет пользователям настраивать принтеры iSeries непосредственно на рабочей станции Windows 2000 с помощью мастера добавления принтера. Для этого при работе с мастером нужно выбрать принтер в каталоге Active Directory Windows 2000.

API для публикации информации OS/400 на сервере каталогов

Службы каталогов предоставляют встроенную функцию публикации пользовательской и системной информации. Ее можно настроить на странице **Службы каталогов** окна **свойств системы**. API настройки и публикации сервера LDAP позволяют создавать программы OS/400 для публикации информации других типов. Эти типы информации также показаны на странице **Службы 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 **Службы 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 Службы 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 **Службы 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.

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 пункте **Каталог** и выберите **Свойства**.
5. Нажмите кнопку **Добавить**.
6. 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.
7. Нажмите кнопку **OK**.

Добавление суффиксов на сервер каталогов LDAP

Добавление суффикса на сервер каталогов LDAP позволяет серверу работать с указанной 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 пункте **Каталог** 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.

Удаление суффиксов с сервера каталогов

Для удаления суффикса с сервера каталогов LDAP выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** 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 Служб каталогов

Службы каталогов хранят информацию в следующих объектах:

- В библиотеке базы данных (по умолчанию, QUSRDIRDB), содержащей информацию серверов каталогов.
- 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.

Информация о сохранении и восстановлении данных OS/400 приведена в руководстве Резервное копирование и восстановление, SH43-0080  .

Управление принадлежностью и доступом к данным каталога

Управление принадлежностью и доступом к данным каталога предполагает выполнение следующих задач:

- “Работа со свойствами принадлежности объектов каталога”
- “Работа со списками управления доступом (ACL)” на стр. 31
- “Работа с группами ACL” на стр. 31

Работа со свойствами принадлежности объектов каталога

Для того чтобы задать свойства принадлежности объектов каталога, выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.

4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Права доступа**.

   Если соединение с сервером каталогов не установлено, то появится окно диалога **Подключение к серверу каталогов**. Подключитесь к серверу как администратор или владелец объекта.
5. В списке содержимого каталога выберите объект, со свойствами которого вы хотите работать, и нажмите кнопку **OK**.

Работа со списками управления доступом (ACL)

Работа со списками управления доступом (ACL) предполагает выполнение таких задач, как назначение явных и неявных ACL объектам каталога, добавление пользователей в ACL, удаление пользователей из ACL, а также поиск объектов каталога. Начиная с версии V5R1, Службы каталогов поддерживают новую модель ACL, поэтому с информацией о списках управления доступом рекомендуется ознакомиться всем пользователям, в том числе тем, кто ранее уже работал с ACL.

Для работы с ACL выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Права доступа**.

   Если соединение с сервером каталогов не установлено, то появится окно диалога **Подключение к серверу каталогов**. Подключитесь к серверу как администратор или владелец объекта, с ACL которого вы планируете работать.
5. В списке содержимого каталога выберите объект, с ACL которого вы хотите работать, и нажмите кнопку **OK**.
6. Перейдите на страницу **ACL**.

Работа с группами ACL

Для выполнения операций с группами ACL:
1. В Навигаторе выберите **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Группы ACL**.

Работа с правами доступа администраторов

В версии V5R2 и старше права доступа администратора можно предоставлять пользовательским профайлам, у которых есть доступ к ИД функции Администратор Служб каталогов (QIBM_DIRSRV_ADMIN).

Например, если у пользовательского профайла JOHNSMITH есть права доступа к ИД функции Администратор Служб 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. 43.

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 Администратор Служб 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 **OS/400**.
4. Выберите опцию **Администратор Служб каталогов**.
5. Нажмите кнопку **Настроить**.
6. Откройте папку **Пользователи**, **Группы** или **Пользователи вне групп** в зависимости от категории пользователя.
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**.

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 пункте **Каталог** и выберите **Свойства**.
5. Перейдите на страницу **База данных/Суффиксы**.
6. Выберите опцию **Заносить в протокол сведения об изменении каталога**.
7. (необязательно) В поле **Максимальное число записей** укажите максимальное число записей протокола изменений.

   Примечание: Хотя этот параметр не является обязательным, рекомендуется его указать. Если ограничение на число записей не будет задано, протокол изменений может достигнуть очень большого размера.

Класс объектов `changeLogEntry` представляет изменения, внесенные на сервере каталогов. Набор изменений представляется в виде упорядоченного набора записей объекта changelog 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 функции контроля объектов для сервера каталогов

Службы каталогов поддерживают функцию контроля за действиями OS/400. Если системное значение QAUDCTL равно *OBJAUD, в программе Навигатор можно включить функцию контроля за объектами.

Для включения функции контроля за объектами для Служб каталогов выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
5. Перейдите на страницу **Контроль**.
6. Выберите необходимое значение контроля для сервера.

Изменения, внесенные в параметры контроля, вступают в силу сразу после нажатия кнопки **OK**. Перезапускать сервер каталогов LDAP не нужно. Дополнительная информация приведена в разделе “Средства защиты Служб каталогов” на стр. 41

Повышение производительности сервера каталогов LDAP

Для повышения производительности сервера каталогов LDAP следует настроить следующие параметры:
- Размер результатов поиска
- Ограничение на длительность поиска
- Параметры транзакций сервера
- Число соединений с базой данных и нитей сервера

Для настройки параметров производительности сервера каталогов выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
5. Перейдите на страницу **Производительность**.

Производительность сервера каталогов также можно повысить путем настройки числа соединений с базой данных и нитей сервера. Для этого выполните следующие действия:
1. В Навигаторе откройте **Сеть**.
2. Откройте **Серверы**.
3. Выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Каталог** и выберите **Свойства**.
5. Перейдите на страницу **База данных/Суффиксы**.

Глава 5. Службы каталогов - основная и справочная информация

Для работы с сервером LDAP Служб каталогов ознакомьтесь со следующей общей и справочной информацией:

Информация об основных понятиях LDAP и планировании конфигурации сервера LDAP также приведена в разделе Глава 3, “Службы каталогов - Введение” на стр. 7.

Списки управления доступом LDAP (ACL)

Во многих случаях ограничивать доступ к данным на сервере каталогов LDAP не требуется. Например, сервер LDAP в корпоративной сети Intranet может содержать справочник телефонов всех работников компании. Доступ к данным этого каталога, скорее всего, будет предоставлен всем работникам.

Однако президент компании не хочет, чтобы любой работник мог узнать его номер телефона. В этом случае можно создать **список управления доступом (ACL)**. В этом ACL можно предоставить доступ к номеру телефона президента только тем работникам, от которых президент хочет принимать телефонные звонки.

В ACL можно задать права доступа на добавление и удаление объектов каталога. Кроме того, в них определяются права пользователей на чтение, запись, поиск и сравнение атрибутов каталога. Существует два типа ACL: унаследованные и заданные явно. То есть, ACL могут применяться одним из следующих способов:

- Можно явно задать ACL для конкретного объекта.
- Можно указать, что объекты наследуют ACL от объектов более высокого уровня в иерархии каталога LDAP.

Например, в предыдущем примере президент компании не хотел бы, чтобы любой сотрудник мог узнать его номер телефона. Однако у всех менеджеров должен быть доступ к этому номеру телефона. В этом случае для упрощения настройки прав доступа менеджеров может применяться **Группа ACL**. Группа ACL позволяет предоставить права доступа одновременно группе пользователей. Эта функция особенно полезна в том случае, если группе пользователей необходим доступ к нескольким наборам объектов. Если группе менеджеров, которым известен номер телефона президента, позже понадобится предоставить доступ к информации о заработной плате, это можно сделать с помощью той же группы ACL.

Модели ACL

Все версии Служб каталогов поддерживают модель прав доступа на основе уровня класса доступа. Согласно этой модели, каждый тип атрибутов LDAP относится к одному из следующих классов: Обычный, Промежуточный и Полный. Эта классификация задается в файлах схемы атрибутов. При добавлении пользователя в ACL указывается, к каким классам у пользователя есть права на чтение,

запись, поиск и сравнение. В большинстве схем номер телефона относился бы к классу Обычный. Таким образом, чтобы предоставить менеджерам в приведенном выше примере доступ к номеру телефона президента, необходимо предоставить им права на чтение атрибутов класса Обычный из объекта каталога президента. При этом у менеджеров не будет доступа к атрибутам класса Промежуточный и Полный. Настройка прав доступа на уровне классов доступа поддерживается во всех версиях Служб каталогов.

Службы каталогов также поддерживают модель прав доступа на уровне атрибутов. Согласно этой модели, права на чтение, запись, поиск и сравнение отдельных атрибутов предоставляются независимо от класса доступа. Вернемся к приведенному выше примеру. Согласно модели прав доступа на уровне атрибутов, менеджерам можно предоставить права доступа к атрибуту `telephoneNumber`, даже если у них нет доступа к классу Обычный.

Модель прав доступа на уровне атрибутов поддерживается только серверами SecureWay Directory Services версии 3.2 и более поздними версиями. По умолчанию эта модель не применяется. Разрешить применение этой модели можно при работе с ACL. После того как модель будет активизирована, для отказа от ее применения потребуется заново настроить сервер или восстановить базу данных каталога. При выборе этой модели следует учитывать, что клиенты LDAP V2 (включая версии Навигатора младше V5R1) не поддерживает работу с этой моделью, и их применение может привести к повреждению записей ACL.

Специальные значения ACL

Первоначально для всех объектов на сервере каталогов задан ACL, содержащий специальную группу ACL, `CN=Anybody`, включающую всех пользователей каталога. По умолчанию у этой группы есть права на чтение, поиск и сравнение атрибутов всех объектов, относящихся к обычному классу.

В некоторых случаях всем идентифицированным пользователям сервера каталогов требуется предоставить одинаковые права доступа к ряду объектов каталога. Это можно сделать с помощью особой группы списков управления доступом (ACL) `cn=Authenticated`.

Для определения прав доступа объекта к самому себе предназначено специальное DN `cn=this`. Оно позволяет автоматически предоставлять дочерним записям, наследующим ACL, права доступа к родительским объектам.

Дополнительная информация

Для управления ACL с помощью программы Навигатор не нужно знать всех тонкостей реализации ACL в Службе каталогов. Однако для того чтобы указывать атрибуты ACL при работе с файлами LDIF и применять ACL в в утилитах LDAP командной строки необходимо ознакомиться с атрибутами, применяемыми в ACL. Информация об атрибутах ACL приведена в справочном документе Access Control Lists Документации по программе IBM SecureWay Directory Management Tool.

Дополнительную информацию о создании и изменении ACL и групп ACL можно найти в следующих разделах:

“Работа со списками управления доступом (ACL)” на стр. 31
“Работа с группами ACL” на стр. 31

Формат обмена данными LDAP

Формат обмена данными LDAP (LDIF) обеспечивает простой способ обмена информацией из каталога между серверами каталогов LDAP. Файлы LDIF содержат записи каталога LDAP в простом текстовом формате. В версии V4R5 Служб каталогов формат файлов LDIF, применяемых сервером каталогов, был несколько изменен. Файлы LDIF состоят из последовательности строк, описывающих

запись каталога или набор изменений, внесенных в запись каталога. Эти строки не могут содержать информацию о записях и изменениях одновременно.

Запись LDIF задается в следующем формате:

```
version: 1
dn: отличительное имя
тип-атрибута-1: значение-атрибута-1
...
```

где:

- *version* указывает версию формата файла LDIF. Версия должна быть равна 1. Если номер версии отсутствует, то считается, что это файл LDIF старого формата. Содержимое файла LDIF версии 1 должно быть записано в кодировке UTF-8.
- *отличительное имя* - отличительное имя записи каталога
- *тип-атрибута-1* - тип атрибута LDAP (например, cn или ou)
- *значение-атрибута-1* - значение атрибута

Запись может содержать несколько атрибутов. Каждый атрибут указывается на отдельной строке. Если значение атрибута не умещается на одной строке, то оно переносится на следующую строку, в начале которой указывается пробел или символ табуляции.

Записи в файле LDIF разделяются пустыми строками. Строки, начинающиеся со знака фунта (#), являются комментарием и игнорируются при обработке файла LDIF.

Отличительные имена и значения атрибутов, отвечающие хотя бы одному из приведенных ниже условий, должны задаваться в кодировке base-64:
- Содержат символы новой строки или возврата каретки.
- Начинаются с двоеточия (:), ПРОБЕЛА или знака меньше (<).
- Оканчиваются пробелом.

Между именем и значением атрибута в кодировке base-64 указывается два символа двоеточия.

Внешние ссылки задаются в формате file:// URL. Между типом атрибута и значением внешней ссылки должны быть указаны двоеточие и знак меньше (:<).

Примеры файлов LDIF:

Пример 1: Простой файл LDAP с двумя записями

```
version: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
   sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   description: A big sailing fan.

   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
```

```
   telephonenumber: +1 408 555 1212
   description:Babs is a big sailing fan, and travels extensively in
   search of perfect sailing conditions.
   title:Product Manager, Rod and Reel Division
```

Пример 2: Файл, содержащий значение в кодировке base-64

```
version: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Gern Jensen
   cn: Gern O Jensen
   sn: Jensen
   uid: gernj
   telephonenumber: +1 408 555 1212
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

Пример 3: Файл, содержащий несколько записей об изменениях и комментарии

Примечание: Файлы LDIF, содержащие записи об изменениях, нельзя напрямую импортировать на сервер. Однако они поддерживаются утилитами оболочки LDAP.

```
version: 1
   # Добавление новой записи
   dn: cn=Fiona Jensen, ou=Rochester, o=Big Company, c=US
   changetype: add
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Fiona Jensen
   sn: Jensen
   uid: fiona
   telephonenumber: +1 408 555 1212
   jpegphoto:< file:///usr/local/directory/photos/fiona.jpg

   # Удаление существующей записи
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # Изменение относительного отличительного имени записи
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

Порядок расположения записей в файле LDIF играет важную роль. Для успешного добавления записи из файла LDIF в каталог LDAP пространство имен каталога должно содержать ее родительскую запись. В приведенном выше примере вторую и третью запись невозможно добавить, если не существует первая запись.

Аналогично, для импорта файла LDIF на сервер, поддерживающий определенные суффиксы, файл LDIF должен содержать записи для этих суффиксов. Например, если на сервере есть суффикс `ou=Rochester, o=Big Company, c=US`, то приведенный выше файл LDIF можно импортировать. Но если вместо этого на сервере есть суффикс `o=Big Company, c=US`, то для этого суффикса потребовалось бы задать запись в файле LDIF:

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

Формат и содержимое отдельных файлов LDIF определяются схемой того сервера, с которого они экспортируются. Файл LDIF можно импортировать на любой сервер LDAP, схема которого совпадает со схемой сервера, с которого был экспортирован данный файл. Серверы LDAP различных вендоров применяют разные схемы (с разными классами объектов и атрибутами). В связи с этим не всегда можно импортировать файл LDIF, созданный на другом сервере.

Документ RFC, содержащий спецификации файлов LDIF, можно просмотреть на следующем Web-сайте:

http://www.ietf.org/rfc/rfc2849.txt 

Связанные процедуры:

“Импорт файла LDIF” на стр. 22
“Экспорт файла LDIF” на стр. 22

Информация о поддержке национальных языков (NLS)

Начиная с версии V4R5, сервер LDAP Служб каталогов OS/400 и клиент LDAP OS/400 применяют протокол LDAP версии 3. При этом применяются следующие правила работы с NLS:

- Сервер обменивается данными с клиентами LDAP в формате UTF-8. Поддерживаются все символы ISO 10646.
- Для хранения информации в базе данных сервер LDAP Служб 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 справочной системы iSeries Information Center, относящемся к категории Планирование.

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.

Службы 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`.

Связанная процедура:

“Работа со свойствами принадлежности объектов каталога” на стр. 30

Переадресация в каталоге LDAP

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

Службы 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: В Службах каталогов объекты переадресации должны содержать только атрибуты Отличительное имя (`dn`), objectClass (`objectClass`) и переадресация (`ref`). Применение этого ограничения продемонстрировано в примере, приведенном в разделе “Утилита ldapsearch” на стр. 56.

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

После настройки сервера каталогов LDAP в системе клиенты могут применять транзакции. 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.

Транзакции могут включать следующие операции 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.

Дополнительная информация о транзакциях приведена в Приложении Limited Transaction Support руководства IBM SecureWay Directory Client SDK Programming Reference.

Серверы-копии LDAP

На сервере-копии LDAP хранится та же информация, что и на главном сервере каталогов LDAP. Создание копий каталога LDAP предоставляет следующие преимущества:

- Наличие копий ускоряет поиск в каталоге. Поисковые запросы клиентов отправляются не на один сервер, а распределяются между главным сервером и серверами-копиями.
- Серверы-копии хранят резервные копии информации главного сервера. В случае, если главный сервер недоступен, сервер-копия может выполнить запрос и предоставить доступ к данным каталога.

Серверы-копии поддерживают только операции чтения. Если пользователь с соответствующими правами доступа пытается изменить запись на сервере-копии, то этот сервер переадресует запрос на главный сервер каталогов.

Связанная процедура:

“Настройка новой копии сервера каталогов” на стр. 23

Средства защиты Служб каталогов

Контроль за действиями

Начиная с версии V5R1, Службы каталогов поддерживают функцию контроля за действиями OS/400. Возможен контроль следующих операций:

- Связывание и удаление связей с сервером каталогов.
- 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.

Для включения контроля за записями каталога может потребоваться изменить параметры контроля OS/400. Если системное значение QAUDCTL равно *OBJAUD, функцию контроля за объектами можно включить с помощью Навигатора. Дополнительная информация о функции контроля приведена в книге *Security - Reference*  , а также в разделе Контроль за действиями справочной системы iSeries Information Center.

Идентификация и защита соединения

Службы каталогов предоставляют следующие средства защиты соединений, установленных между клиентами и сервером каталогов LDAP:

- Соединения Secure Sockets Layer (SSL)
- Идентификация Kerberos
- Шифрование пароля CRAM-MD5

Применение протоколов SSL и TLS на сервере каталогов LDAP

Для защиты соединений с сервером каталогов LDAP в Службах каталогов может применяться протокол SSL.

Для применения SSL в Службах каталогов в системе должна быть установлена одна из программ шифрования Cryptographic Access Provider (5722-ACx). Для применения SSL в Навигаторе на PC должна быть дополнительно установлена одна из клиентских программ шифрования Client Encryption (5722-CEx). Это программное обеспечение необходимо для:

- Настройки и администрирования Служб каталогов с рабочей станции с помощью соединения SSL. К этой категории относятся задачи, выполняемые с помощью Навигатора.
- Применения соединения SSL в приложениях, использующих API клиентов Windows.

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 OS/400. 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. Информация о поддержке SSL на сервере iSeries приведена в разделе Защита приложений с помощью SSL. Информация о поддержке TLS на сервере iSeries приведена в разделе Поддерживаемые протоколы SSL и TLS.

Применение идентификации Kerberos на сервере каталогов LDAP

Службы каталогов позволяют настроить на сервере каталогов LDAP функцию идентификации Kerberos. Kerberos - это протокол сетевой идентификации, обеспечивающий надежную идентификацию приложений клиент-сервер с помощью шифрования личным ключом.

Для настройки идентификации Kerberos в системе должна быть установлена одна из программ шифрования Cryptographic Service Provider (5722AC2 или 5722AC3). Кроме того, должна быть настроена сетевая служба идентификации.

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

Имя субъекта Kerberos, применяемое сервером, имеет следующий вид:

```
имя-службы/имя-хоста@область
```

имя-службы - LDAP, 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). В соответствии с принятым соглашением, имена областей Kerberos задаются прописными буквами, а имена хостов - строчными. Строка LDAP/ задается строчными буквами. Если область по умолчанию не задана, то на сервере каталогов нельзя настроить функцию идентификации Kerberos.

Если применяется идентификация Kerberos, то сервер каталогов LDAP 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. Поиск записи каталога, содержащей заданный идентификатор Kerberos, выполняется по следующим правилам:
  - Сервер ищет в каталоге объект krbRealm-V2 с атрибутом krbRealmName-V2, соответствующим области Kerberos. При наличии такой записи сервер пытается найти в списке DN из атрибута princSubtree запись с атрибутом krbPrincipalName, значение которого совпадает с именем субъекта и именем области. Если в атрибуте krbAliasedObjectName указано DN обнаруженной до этого записи, то применяется это DN. В противном случае применяется DN записи. Этот способ обычно применяется в том случае, когда центр рассылки ключей (KDC) Kerberos хранит информацию о субъектах в каталоге LDAP.
  - Если найти необходимую запись не удается, то сервер выполняет поиск записи каталога со вспомогательным классом ibm-securityIdentities и атрибутом altSecurityIdentities, значение которого равно KERBEROS:субъект@область. Этот способ позволяет связать идентификаторы Kerberos с записями каталогов в том случае, если KDC не хранит информацию о субъектах в каталоге.

У вас должен 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.

Спроецированная база данных операционной системы

Спроецированная база данных системы обеспечивает отображение объектов OS/400 в качестве записей дерева каталогов LDAP. Спроецированные объекты являются представлениями объектов OS/400 в виде объектов LDAP, а не записями в базе данных сервера LDAP. В версии V5R2 в записи дерева каталогов проецируются только пользовательские профайлы OS/400. Отображение объектов пользовательских профайлов называется спроецированной базой данных пользователей OS/400.

Для выполнения операций LDAP над объектами OS/400 применяются функции операционной системы. 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:

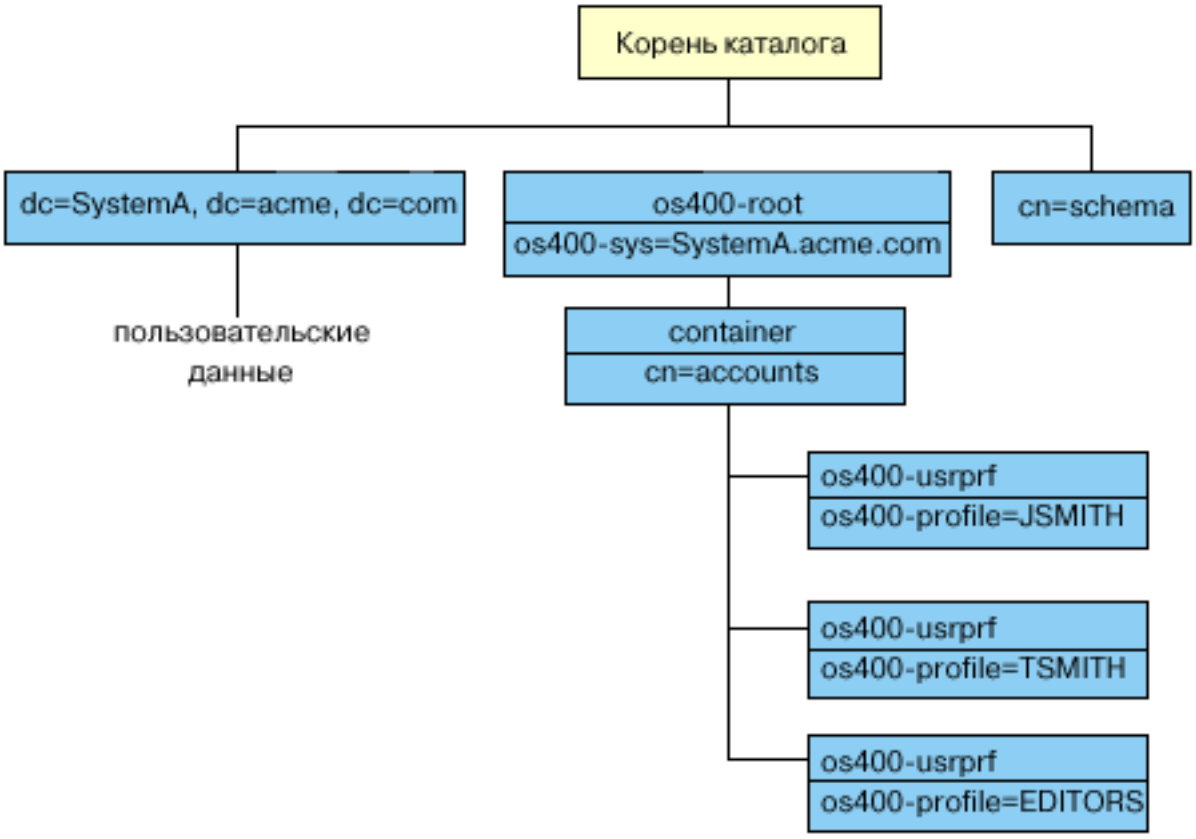
- “Дерево информации спроецированного каталога пользователей OS/400”
- “Операции LDAP” на стр. 44
- “DN связывания администратора и копии” на стр. 49
- “Схема спроецированной базы данных пользователей OS/400” на стр. 49

Дерево информации спроецированного каталога пользователей OS/400

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 каталога 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.

Связывание

Клиент LDAP может указать спроецированный пользовательский профайл при связывании с сервером LDAP (во время идентификации). Для этого нужно задать пароль пользовательского профайла OS/400 и DN спроецированного пользовательского профайла в качестве DN связывания. Пример DN, указанного в запросе на связывание: `os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com`.

Для получения доступа к спроецированной базе данных клиент должен подключиться как спроецированный пользователь. 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 связывание указан спроецированный пользовательский профайл, то доступен только простой метод связывания.

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 1. 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.
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.

Таблица 1. Операции поиска для спроецированной базы данных системы (продолжение)

Запрошенный поиск	База поиска	Область поиска	Фильтр поиска	Комментарии
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 1. 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:
  - 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 определено следующим образом:

    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 следует 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 импортирование и экспортирование данных в спроецированной базе данных системы.

DN связывания администратора и копии

В качестве DN связывания 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 “Работа с правами доступа администраторов” на стр. 31.

Схема спроецированной базы данных пользователей OS/400

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 (например, CRTUSRPRF или CHGUSRPRF) в командах пользовательских профайлов. Дополнительная информация приведена в разделе “Дерево информации спроецированного каталога пользователей OS/400” на стр. 43.

Службы каталогов и поддержка ведения журнала OS/400

Службы каталогов применяют для хранения информации каталога базу данных OS/400. При добавлении записей каталога в базу данных Службы каталогов применяют управление фиксацией. Для этого необходима поддержка ведения журнала OS/400.

При первом запуске сервера или функции импортирования 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, вызовите следующую команду OS/400:

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

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

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

Информация о командах для работы с журналом приведена в разделе Команды OS/400 справочной системы iSeries Information Center, относящемся к категории Программирование.

Глава 6. Утилиты LDAP командной строки

Службы каталогов содержат пять утилит, позволяющих работать с сервером каталогов LDAP в командной оболочке Qshell операционной системы OS/400. Эти утилиты применяют API LDAP. Их можно вызвать из командной строки qsh или из пользовательского приложения. Они также могут послужить полезными примерами программ. При установке клиента LDAP Windows, входящего в состав Служб каталогов, можно установить исходный код, незначительно отличающийся от исходного кода утилит командной оболочки.

Эти утилиты перечислены ниже:
- Утилита “Утилиты ldapmodify и ldapadd” предназначена для добавления и изменения записей каталогов LDAP.
- Утилита “Утилита ldapdelete” на стр. 54 предназначена для удаления записей из каталога LDAP.
- Утилита “Утилита ldapsearch” на стр. 56 предназначена для поиска записей в каталоге LDAP.
- Утилита “Утилита ldapmodrdn” на стр. 61 предназначена для изменения Относительных отличительных имен (RDN) записей каталога LDAP.

Информация о поддержке SSL в утилитах командной строки приведена в разделе “Сведения о применении SSL в утилитах командной строки LDAP” на стр. 63.

Утилиты ldapmodify и ldapadd

Утилита ldapmodify позволяет добавлять и изменять записи на сервере каталогов LDAP из командной оболочки QSH. Она применяет интерфейсы прикладных программ (API) ldap_modify, ldap_add и ldap_delete. Утилита ldapadd практически идентична утилите ldapmodify, однако флаг -a включается автоматически.

Формат:

ldapmodify [-a] [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *набор-символов***] [-d** *уровень-отладки***] [-D** *DN-связывания***] [-w** *пароль* **] [-m***механизм***] [-O***число-транзитных-участков***] [-h** *хост-ldap***] [-p** *порт-ldap***] [-f** *файл***] [-Z] [-K** *файл-ключей***] [-P** *пароль-файла-ключей* **] [-N** *имя-сертификата***]**

ldapadd [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *набор-символов***] [-d** *уровень-отладки***] [-D** *DN-связывания* **] [-w** *пароль***] [-m***механизм***] [-O***число-транзитных-участков***] [-h** *хост-ldap***] [-p** *порт-ldap* **] [-f** *файл***] [-Z] [-K** *файл-ключей***] [-P** *пароль-файла-ключей***] [-N** *имя-сертификата***]**

Примечание: Если вы не укажете *файл* с помощью опции **-f**, утилита будет ожидать ввода данных со стандартного устройства ввода. Для выхода из состояния ожидания нажмите клавишу SysReq, а затем выберите `2. Завершить предыдущий запрос`.

Диагностика:

При отсутствии ошибок код завершения равен 0. При возникновении ошибок код завершения отличен от нуля, и создаются сообщения об ошибках.

Щелкните здесь, чтобы просмотреть примеры работы с этими утилитами.

Параметры:

-V	Указывает версию LDAP, применяемую утилитой для подключения к серверу LDAP. По умолчанию применяется соединение LDAP V3. Для того чтобы явно выбрать LDAP V3, укажите -V 3. Для применения версии LDAP V2 укажите -V 2.

-a	Этот параметр поддерживается только утилитой ldapmodify. Он означает, что утилита будет по умолчанию добавлять записи, а не изменять их. Применение этого параметра эквивалентно применению утилиты ldapadd.
-b	Все значения, начинающиеся с символа `/, интерпретируются как двоичные значения, заданные в файле, полное имя которого задано вместо значений.
-c	Режим непрерывной работы. Сообщения об ошибках отправляются, однако утилиты ldapmodify и ldapadd продолжают выполнять операции изменения и добавления. По умолчанию после отправки сообщения об ошибке работа утилиты завершается.
-r	Заменять существующие значения по умолчанию.
-M	Считать объекты переадресации обычными записями.
-n	Показать результаты выполнения операции, но не вносить изменения в записи. Применяется для отладки вместе с параметром -v.
-v	Подробный вывод, при котором создается множество диагностических сообщений.
-F	Принудительное применение всех изменений, независимо от содержимого входных строк, начинающихся со слова replica: (по умолчанию строки replica: сравниваются с текущим хостом и портом сервера LDAP, чтобы определить, следует ли применять запись протокола репликации).
-R	Отключает автоматический переход по ссылкам.
-C *набор-символов*	Указывает, что входные данные для утилиты заданы в локальном наборе символов (*набор-символов*), и требуется преобразование в UTF-8. Опцию **-C** набор-символов следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Информация о допустимых значениях *набора-символов* приведена в документации по API ldap_set_iconv_local_charset().
-d *уровень-отладки*	Задает *уровень-отладки*.
-D *DN-связывания*	*DN-связывания* применяется для подключения к каталогу LDAP. *DN-связывания* задается в виде строки.
-w *пароль*	*Пароль* для идентификации.
-m *механизм*	Параметр *механизм* указывает механизм SASL, применяемый клиентом для подключения к серверу. Клиент применяет API ldap_sasl_bind_s(). Допустимы следующие значения: CRAM-MD5 (шифрование пароля), EXTERNAL (применяется для SSL) и GSSAPI (Kerberos). Команда игнорирует параметр **-m**, если задан параметр **-V 2**. Если параметр **-m** опущен, выполняется обычная процедура идентификации.
-O*число-транзитных-участков*	Параметр *число-транзитных-участков* позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.
-h *хост-ldap*	Укажите альтернативный хост, на котором работает сервер LDAP.
-p *порт-ldap*	Укажите альтернативный порт TCP, через который принимает запросы сервер LDAP. 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.
-f *файл*	Считывать 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.
-Z	Применять защищенное соединение SSL для обмена данными с сервером LDAP. Опция **-Z** может применятся только в тех версиях утилиты, которые поддерживают SSL.

-K *файл-ключей*	Укажите 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**.
-P *пароль-файла-ключей*	Укажите пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей (включая личный ключ). Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и этот параметр указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.
-N *имя-сертификата*	Укажите метку, связанную с сертификатом клиента в файле базы данных ключей. Если сервер LDAP выполняет только идентификацию сервера, то сертификат клиента не нужен. Сертификат клиента требуется указать в том случае, если сервер LDAP настроен для идентификации клиента и сервера. Параметр *имя-сертификата* не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр *имя-сертификата* не нужно указывать, если указанный файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.

Альтернативный формат ввода:

Для совместимости с более ранними версиями утилита ldapmodify поддерживает альтернативный формат ввода. Этот формат представляет собой одну или несколько записей, разделенных пустыми строками. Каждая запись задается в следующем формате:

```
Отличительное имя (DN)
атрибут=значение
[атрибут=значение ...]
```

где *атрибут* - имя атрибута, а *значение* - значение атрибута. По умолчанию значения добавляются. Если указан флаг **-r**, то по умолчанию существующие значения заменяются новыми. Один и тот же атрибут можно указать несколько раз (например, можно добавить несколько значений для одного атрибута). Для переноса строк и сохранения символа новой строки в значении применяется символ обратной косой черты (\). Для удаления значения перед *атрибутом* следует указать знак минус (-). Для удаления всего атрибута не указывайте знак равно (=) и значение. Если задан флаг **-r**, то для добавления значений перед *атрибутом* необходимо указывать знак плюс (+).

Примеры: ldapmodify и ldapadd

Пример 1:

Предположим, 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:< file:///tmp/modme.jpeg
-
delete: description
-
```

Команда `ldapmodify -b -r -f /tmp/entrymods` выполнит следующие действия:

- Заменит содержимое почтового атрибута записей Modify Me на значение `modme@student.of.life.edu`.
- Добавит заголовок `Grand Poobah`.
- Добавит содержимое файла **/tmp/modme.jpeg** в качестве объекта jpegPhoto.
- Удалит атрибут `description`.

Эту же операцию можно выполнить, применяя старый формат ввода 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
```

Для старого формата следует задать следующую команду:

```
ldapmodify -b -r -f /tmp/entrymods
```

Пример 2:

Предположим, 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: Manager
mail: johndoe@student.of.life.edu
uid: jdoe
```

Команда `ldapadd -f /tmp/entrymods` добавит запись John Doe, применяя значения из файла /tmp/newentry.

Пример 3:

Предположим, что существует файл **/tmp/newentry**, содержащий следующую информацию:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
changetype: delete
```

Команда `ldapmodify -f /tmp/entrymods` удалит запись John Doe.

Утилита ldapdelete

Утилита ldapdelete позволяет удалить одну или несколько записей с сервера каталогов LDAP. Она выполняется в командной оболочке QSH OS/400. Эта команда применяет интерфейс прикладных программ (API) ldap_delete.

Формат:

ldapdelete [-V] [-M] [-n] [-v] [-c] [-R] [-C набор-символов] [-d *уровень-отладки***] [-f***файл***] [-D** *DN-связывания***] [-w** *пароль* **] [-m** *механизм***] [-O***число-транзитных-участков***] [-h** *хост-ldap***] [-p** *порт-ldap***] [-Z] [-K** *файл-ключей* **] [-P** *пароль-файла-ключей***] [-N** *имя-сертификата***] [***DN***]...**

Примечание: Если не указан параметр *dn*, то утилита ldapdelete считывает список DN из стандартного ввода. Для выхода из состояния ожидания нажмите клавишу SysReq, а затем выберите `2. Завершить предыдущий запрос`.

Диагностика:

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

Щелкните здесь, чтобы просмотреть примеры работы с утилитой ldapdelete.

Параметры:

-V	Указывает версию LDAP, применяемую утилитой для подключения к серверу LDAP. По умолчанию применяется соединение LDAP V3. Для того чтобы явно выбрать LDAP V3, укажите -V 3. Для применения версии LDAP V2 укажите -V 2.
-M	Считать объекты переадресации обычными записями.
-n	Показать результаты выполнения операции, но не удалять записи. Применяется для отладки вместе с параметром **-v**.
-v	Подробный вывод, при котором создается множество диагностических сообщений.
-c	Режим непрерывной работы. Утилита ldapdelete отправляет сообщения об ошибках, но продолжает выполнять удаление. По умолчанию после отправки сообщения об ошибке работа утилиты завершается.
-R	Отключает автоматический переход по ссылкам.
-C *набор-символов*	Указывает, что отличительные имена (DN) для утилиты ldapdelete заданы в локальном наборе символов (*набор-символов*). Опция **-C** *набор-символов* позволяет переопределить значение по умолчанию, UTF-8. Опцию **-C** набор-символов следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Информация о допустимых значениях *набора-символов* приведена в документации по API ldap_set_iconv_local_charset().
-d *уровень-отладки*	Задает *уровень-отладки*.
-f *файл*	Утилита считывает последовательность строк из *файла*, выполняя одну операцию удаления LDAP для каждой из этих строк. Каждая строка в файле должна содержать одно отличительное имя (DN).
-D *DN-связывания*	*DN-связывания* применяется для подключения к каталогу LDAP. *DN-связывания* задается в виде строки.
-w *пароль*	*Пароль* для идентификации.
-m *механизм*	Параметр *механизм* задает механизм SASL, применяемый для связывания с сервером. Применяется API ldap_sasl_bind_s(). Допустимы следующие значения: CRAM-MD5 (шифрование пароля), EXTERNAL (применяется для SSL) и GSSAPI (Kerberos). Если задан параметр -V 2, то параметр -m игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации.
-O *число-транзитных-участков*	Параметр *число-транзитных-участков* позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.
-h *хост-ldap*	Укажите альтернативный хост, на котором работает сервер LDAP.
-p *порт-ldap*	Укажите альтернативный порт TCP, через который принимает запросы сервер LDAP. 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.
-Z	Применять защищенное соединение SSL для обмена данными с сервером LDAP. Опция **-Z** может применятся только в тех версиях утилиты, которые поддерживают SSL.

-K *файл-ключей*	Укажите 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**.
-P *пароль-файла-ключей*	Укажите пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей (включая личный ключ). Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и этот параметр указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.
-N *имя-сертификата*	Укажите метку, связанную с сертификатом клиента в файле базы данных ключей. Если сервер LDAP выполняет только идентификацию сервера, то сертификат клиента не нужен. Сертификат клиента требуется указать в том случае, если сервер LDAP настроен для идентификации клиента и сервера. Параметр *имя-сертификата* не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр *имя-сертификата* 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.
dn	Задает один или несколько аргументов *dn*. В параметре *dn* должно быть задано отличительное имя в виде строки.

Пример: ldapdelete

Следующая команда удаляет запись с именем commonName Delete Me из записи University of Life:

```
ldapdelete cn=Delete Me, o=University of Life, c=US
```

Может потребоваться указать *DN-связывания* и *пароль* (см. описание опций **-D** и **-w**).

Утилита ldapsearch

Утилита ldapsearch позволяет запустить поиск записи на сервере каталогов LDAP из командной оболочки QSH операционной системы OS/400. Она применяет API ldap_search.

Во время поиска применяется фильтр, соответствующий строковому представлению фильтров LDAP. Дополнительная информация о фильтрах поиска LDAP приведена в описании API ldap_search, которое можно найти в разделе Службы каталогов OS/400 из категории Программирование справочной системы iSeries Information Center.

Утилита ldapsearch получает атрибуты найденных записей, указанные в параметре *attrs*, и выводит записи и значения на стандартное устройство вывода. Если атрибуты не указаны, то возвращаются значения всех атрибутов.

Формат:

ldapsearch [-V] [-n] [-v] [-t] [-A] [-B] [-L] [-M] [-R] [-C *набор-символов***] [-d** *уровень-отладки***] [-F** *разделитель***] [-f** *файл* **] [-D** *DN-связывания***] [-w** *пароль-связывания***] [-m** *механизм***] [-O** *число-транзитных-участков***] [-h** *хост-ldap* **] [-p** *порт-ldap***] [-Z] [-K** *файл-ключей***] [-P** *пароль-файла-ключей***] [-N** *имя-сертификата* **] [-b** *база-поиска* **] [-s** *область* **] [-a** преобразование**] [-l** *ограничение-по-времени***] [-z** *ограничение-по-размеру***]** *фильтр* **[***атрибуты...***]**

Диагностика:

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

Формат вывода:

Найденные записи утилита ldapsearch записывает на стандартное устройство вывода в следующем формате:

```
Отличительное имя (DN)
имя-атрибута=значение
имя-атрибута=значение
имя-атрибута=значение
...
```

Записи разделяются пустыми строками. Если в опции **-F** указан символ-разделитель, то он выводится вместо символа равно (=). Если указана опция **-t**, то имя временного файла заменяет фактическое значение. Если указана опция **-A**, то выводится только `имя-атрибута`.

Щелкните здесь, чтобы просмотреть примеры работы с утилитой ldapsearch.

Параметры:

-V	Указывает версию LDAP, применяемую утилитой для подключения к серверу LDAP. По умолчанию, применяется соединение LDAP V3. Для того чтобы явно выбрать LDAP V3, укажите -V 3. Для применения версии LDAP V2 укажите -V 2.
-n	Показать результаты операции, но не выполнять поиск. Применяется для отладки вместе с параметром **-v**.
-v	Подробный вывод, при котором создается множество диагностических сообщений.
-t	Записать полученные значения в набор временных файлов. Эта опция применяется для работы с двоичными значениями, такими как jpegPhoto и audio.
-A	Получить только атрибуты (без значений). Эта опция применяется в случае, если нужно проверить наличие атрибутов в записи.
-B	Не подавлять вывод двоичных значений. Эта опция применяется при работе со значениями с другим набором символов, например, ISO-8859.1. Она неявно задается, если указана опция **-L**
-L	Вывести результаты поиска в формате LDIF. Если указана эта опция, то применяется и опция **-B**, а опция **-F** игнорируется.
-M	Считать объекты переадресации обычными записями.
-R	Отключает автоматический переход по ссылкам.
-C *набор-символов*	Указывает, что входные данные для утилиты ldapsearch заданы в локальном наборе символов (*набор-символов*). Входные данные включают в себя фильтр, DN-связывания и базовое DN. При выводе данных утилита ldapsearch преобразует полученную от сервера LDAP информацию в указанный набор символов. Опцию **-C** набор-символов следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Информация о допустимых значениях *набора-символов* приведена в документации по 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 вывод утилиты ldapsearch должен быть сохранен в кодировке UTF-8 или base 64, если обнаружены непечатаемые символы. Эти опции согласуются между собой, так как стандартные файлы LDIF содержат только строковые данные в формате UTF-8 (или UTF-8 с кодировкой base 64).
-d *уровень-отладки*	Задает *уровень-отладки*.
-F *разделитель*	Указанный *разделитель* отделяет имена атрибутов от их значений. По умолчанию применяется разделитель `=. Если указан флаг **-L**, то эта опция игнорируется.

-f *файл*	Утилита считывает последовательность строк из файла, выполняя функцию поиска LDAP для каждой строки. Каждая строка в файле должна содержать одно отличительное имя (DN).
-D *DN-связывания*	*DN-связывания* применяется для подключения к каталогу LDAP. *DN-связывания* задается в виде строки.
-w *пароль*	*Пароль* для идентификации.
-m *механизм*	Параметр *механизм* указывает механизм SASL, применяемый для связывания с сервером. Применяется API ldap_sasl_bind_s(). Допустимы следующие значения: CRAM-MD5 (шифрование пароля), EXTERNAL (применяется для SSL) и GSSAPI (Kerberos). Если задан параметр **-V** 2, то параметр **-m** игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации.
-O *число-транзитных-участков*	Параметр *число-транзитных-участков* позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.
-h *хост-ldap*	Укажите альтернативный хост, на котором работает сервер LDAP.
-p *порт-ldap*	Укажите альтернативный порт TCP, через который принимает запросы сервер LDAP. 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.
-Z	Применять защищенное соединение SSL для обмена данными с сервером LDAP. Опция **-Z** может применятся только в тех версиях утилиты, которые поддерживают SSL.
-K *файл-ключей*	Укажите 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**.
-P *пароль-файла-ключей*	Укажите пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей (включая личный ключ). Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и этот параметр указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.
-N *имя-сертификата*	Укажите метку, связанную с сертификатом клиента в файле базы данных ключей. Если сервер LDAP выполняет только идентификацию сервера, то сертификат клиента не нужен. Сертификат клиента требуется указать в том случае, если сервер LDAP настроен для идентификации клиента и сервера. Параметр *имя-сертификата* не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр *имя-сертификата* 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.
-b *база-поиска*	Опция *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.
-s *область*	Задает область поиска. *Область* может принимать значения `base`, `one` и `sub`, обозначающие базовый объект, поиск на одном уровне и в поддереве, соответственно. По умолчанию применяется значение `sub`.
-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.

-l *ограничение-по-времени*	*Ограничение* на время поиска.
-z *ограничение-по-размеру*	Число записей, возвращаемых в результате поиска, не должно превышать значение, указанное в параметре *ограничение-по-размеру*. С его помощью можно задать максимальное число записей, возвращаемых в результате поиска.
фильтр	Указывает имя фильтра, применяемого для поиска.
атрибуты...	Указывает атрибуты, возвращаемые утилитой при обнаружении искомых записей. Если в параметре *атрибуты* не указаны значения, то утилита возвращает все атрибуты.

Примеры: ldapsearch

Пример 1:

Команда `ldapsearch cn=john doe cn telephoneNumber` выполняет поиск в поддереве записей с атрибутом commonName, равным `john doe` (применяется база поиска по умолчанию). Функция поиска возвращает значения commonName и telephoneNumber и записывает их на стандартное устройство вывода. Если в результате поиска будет обнаружено две записи, то вывод будет выглядеть приблизительно 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
```

Пример 2:

Команда `ldapsearch -t uid=jed jpegPhoto audio` выполняет поиск записей с ИД пользователя jed в поддереве, применяя базу поиска по умолчанию. Функция поиска получает объект jpegPhoto и звуковые данные и записывает их во временный файл. Если функция поиска обнаружит одну запись с одним значением для каждого из указанных атрибутов, то вывод будет выглядеть 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
```

Пример 3:

Команда `ldapsearch -L -s one -b c=US o=university* o description` выполняет поиск на уровне `c=US`. Эта функция поиска находит все организации, у которых значение атрибута organizationName начинается со строки `university` . Функция поиска возвращает значения в формате LDIF. Она получает значения атрибутов organizationName и description и записывает их на стандартное устройство вывода 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
...
```

Пример 4:

Как уже говорилось в разделе “Переадресация в каталоге LDAP” на стр. 39, каталоги LDAP Служб каталогов могут содержать объекты переадресации, содержащие только следующие элементы:

- Отличительное имя (`dn`).
- Атрибут objectClass (`objectClass`).
- Атрибут переадресации (`ref`).

В этом примере продемонстрирован поиск с применением объекта переадресации.

Предположим, 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
```

Если клиент отправляет запрос в систему System_A без управляющего значения manageDsaIT, то сервер возвращает ссылку. Например, если утилита ldapsearch запущена с параметром -M, то сервер LDAP системы System_A в ответ на запрос клиента отправит следующий адрес:

```
ldap://System_B:389/cn=Barb Jensen,
 ou=Rochester, o=Big Company, c=US
```

На основе полученной информации клиент отправляет запрос в систему System_B. Все атрибуты записи в системе System_A, помимо `dn`, `objectclass` и `ref`, игнорируются сервером.

Получив от сервера в ответ на запрос ссылку, клиент отправляет новый запрос на сервер с указанным адресом. Если поиск выполнялся на одном уровне, то в переадресованном запросе применяется базовая область поиска. Результаты этого поиска зависят от указанного значения области поиска (**-b**).

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 функция поиска возвращает атрибуты всех записей, содержащих атрибут sn=Jensen, которые находятся не выше суффикса `ou=Rochester, o=Big Company, c=US` в системах System_A и System_B. Клиент получает ссылку от сервера системы System_A и выполняет поиск в системе System_B, в результате чего получает `cn=Barb Jense,ou=Rochester,o=Big Company,c=US`.

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??base
```

В этом случае клиент отправит следующий запрос:

```
 ldapsearch -h System_B -b cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
     -s base sn=Jensen
```

В результате будет возвращена запись `cn=Barb Jensen,ou=Rochester,o=Big Company,c=US`.

Утилита ldapmodrdn

Утилита ldapmodrdn позволяет изменить Относительное отличительное имя (RDN) записи сервера каталогов LDAP. Эта утилита применяется в командной оболочке QSH операционной системы OS/400. Она применяет интерфейс прикладных программ (API) ldap_modrdn.

Формат:

ldapmodrdn [-V] [-r] [-M] [-n] [-v] [-c] [-R] [-C *набор-символов*] **[-d** *уровень-отладки*] **[-D** *DN-связывания*] **[-w** *пароль*] **[-m** *механизм*] **[-O** *число-транзитных-участков*] **[-h** *хост-ldap*] **[-p** *порт-ldap* **] [-Z] [-K** *файл-ключей*] **[-P** *пароль-файла-ключей*] **[-N** *имя-сертификата*] **[-f** *файл* **] [***dn rdn***]**

Примечания:

1. Если в командной строке будут заданы аргументы *dn* и *rdn*, то значение *rdn* заменит RDN записи, соответствующей указанному *dn*. В противном случае, файл (или стандартный ввод, если не указан флаг **-f**) должен содержать записи.

   ```
   Отличительное имя (DN)

   Относительное отличительное имя (RDN)
   ```

   Пары DN/RDN должны быть отделены друг от друга пустыми строками.
2. Если вы не укажете *файл* с записями в опции **-f** (и не укажете в командной строке аргументы *dn* и *rdn*), то команда ldapmodrdn будет ожидать ввода записей со стандартного устройства ввода. Для выхода из состояния ожидания нажмите клавишу SysReq, а затем выберите опцию `2. Завершить предыдущий запрос`.

Диагностика:

При отсутствии ошибок код завершения равен 0. При наличии ошибок код завершения отличен от нуля, и создаются сообщение об ошибках.

Щелкните здесь, чтобы просмотреть пример работы с утилитой ldapmodrdn.

Параметры:

-V	Указывает версию LDAP, применяемую утилитой для подключения к серверу LDAP. По умолчанию применяется соединение LDAP V3. Для того чтобы явно выбрать LDAP V3, укажите -V 3. Для применения версии LDAP V2 укажите -V 2.
-r	Удалить прежние значения относительного отличительного имени (RDN) из записи. По умолчанию старые значения сохраняются.
-M	Считать объекты переадресации обычными записями.
-n	Показать результаты выполнения операции, но не вносить изменения в записи. Применяется для отладки вместе с параметром **-v**.
-v	Подробный вывод, при котором создается множество диагностических сообщений.
-c	Режим непрерывной работы. Утилита ldapmodrdn отправляет сообщения об ошибках, но продолжает вносить изменения. По умолчанию после отправки сообщения об ошибке работа утилиты завершается.
-R	Отключает автоматический переход по ссылкам.
-C *набор-символов*	Указывает, что входные данные для утилиты заданы в локальном наборе символов (*набор-символов*), и требуется преобразование в UTF-8. Опцию **-C** набор-символов следует применять в том случае, если кодовая страница входных данных отличается от кодовой страницы задания. Информация о допустимых значениях *набора-символов* приведена в документации по API ldap_set_iconv_local_charset().
-d *уровень-отладки*	Задает *уровень-отладки*.
-D *DN-связывания*	*DN-связывания* применяется для подключения к каталогу LDAP. *DN-связывания* задается в виде строки.
-w *пароль*	*Пароль* для идентификации.
-m *механизм*	Параметр *механизм* указывает механизм SASL, применяемый для связывания с сервером. Используется API ldap_sasl_bind_s(). Допустимы следующие значения: CRAM-MD5 (шифрование пароля), EXTERNAL (применяется для SSL) и GSSAPI (Kerberos). Если задан параметр -V 2, то параметр -m игнорируется. Если параметр **-m** опущен, выполняется обычная процедура идентификации.
-O *число-транзитных-участков*	Параметр *число-транзитных-участков* позволяет ограничить число транзитных участков, применяемых библиотекой клиента при переадресации. По умолчанию применяется значение 10.
-h *хост-ldap*	Укажите альтернативный хост, на котором работает сервер LDAP.
-p *порт-ldap*	Укажите альтернативный порт TCP, через который принимает запросы сервер LDAP. 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.
-Z	Применять защищенное соединение SSL для обмена данными с сервером LDAP. Опция **-Z** может применятся только в тех версиях утилиты, которые поддерживают SSL.
-K *файл-ключей*	Укажите 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**.

-P *пароль-файла-ключей*	Укажите пароль базы данных ключей. Этот пароль необходим для работы с зашифрованной информацией в файле базы данных ключей (включая личный ключ). Если с файлом базы данных ключей связан файл пароля, пароль считывается из файла, и этот параметр указывать не нужно. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.
-N *имя-сертификата*	Укажите метку, связанную с сертификатом клиента в файле базы данных ключей. Если сервер LDAP выполняет только идентификацию сервера, то сертификат клиента не нужен. Сертификат клиента требуется указать в том случае, если сервер LDAP настроен для идентификации клиента и сервера. Параметр *имя-сертификата* не нужно указывать, если применяется сертификат и личный ключ по умолчанию. Кроме того, параметр *имя-сертификата* не нужно указывать, если указанный файл базы данных ключей содержит только один сертификат и личный ключ. Если не указаны параметры **-Z** и **-K**, то этот параметр игнорируется.
-f *файл*	Считывать информацию об изменении записей из файла LDIF вместо стандартного ввода или аргументов командной строки (*dn* и нового *rdn*). Стандартный ввод можно перенаправить в файл (< файл).
dn rdn	Указывает отличительное имя и новое относительное отличительное имя записи.

Пример: ldapmodrdn

Предположим, что создан текстовый файл/**tmp**/**entrymods**, содержащий следующую информацию:

```
cn=Modify Me, o=University of Life, c=US
cn=The New Me
```

Команда:

```
ldapmodrdn -r -f /tmp/entrymods
```

изменяет RDN записи `Modify Me` с `Modify Me` на `The New Me`. Прежнее значение cn, `Modify Me`, удаляется.

Сведения о применении SSL в утилитах командной строки LDAP

Для применения функций протокола Secure Sockets Layer (SSL) в утилитах командной строки необходимо установить одну из программ шифрования Cryptographic Access Provider (5722-ACx).

Раздел “Применение протоколов SSL и TLS на сервере каталогов LDAP” на стр. 41 содержит информацию о применении SSL на сервере LDAP Служб 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 связывания с сервером 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 связывания с сервером 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.

Глава 7. Устранение неполадок Служб каталогов

Хотя сервер LDAP Служб каталогов считается очень надежным, при работе с ним время от времени возникают неполадки. Приведенная ниже информация поможет вам найти и устранить причину возникшей неполадки сервера каталогов LDAP.

Дополнительная информация о наиболее часто встречающихся неполадках Служб каталогов приведена на Домашней странице Служб каталогов:

```
http://www.iseries.ibm.com/ldap
```

Основная процедура устранения неполадок Служб каталогов

Коды возврата, свидетельствующие об ошибках LDAP, описаны в файле ldap.h, расположенном в библиотеке QSYSINC/H.LDAP.

Для получения подробных сведений об ошибке сервера каталогов LDAP следует также просмотреть протокол задания QDIRSRV. Для трассировки воспроизводимых ошибок можно воспользоваться командой Трассировка приложения TCP/IP (TRCTCPAPP APP(*DIRSRV)). Дополнительная информация приведена в разделе “Обнаружение неполадок с помощью TRCTCPAPP” на стр. 66.

Службы каталогов применяют несколько серверов Языка структурных запросов (SQL). 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 этих случаях важно знать, какие серверы SQL должны быть запущены и для чего они применяются Службами каталогов.

При успешном запуске сервер каталогов LDAP создает следующие сообщения:

Примечание: Сообщения и число заданий серверов SQL могут отличаться от указанных в следующих случаях:
- Сервер запускается в первый раз.
- Должен быть выполнен переход к новой версии.
- Сервер применяет протокол изменений.
- На сервере увеличено число соединений с базой данных.

```
Система:   WARMERS
 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 Служб каталогов запущен успешно.
```

Первый сервер SQL, 057448/QUSER/QSQSRVR, применяется во время запуска сервера LDAP. Службы каталогов могут запустить дополнительные серверы SQL в случае, если сервер запускается впервые, необходимо выполнить переход к новой версии, либо если сервер применяет протокол изменений. После запуска эти серверы SQL удаляются.

В этом примере никакие дополнительные серверы не применялись, то есть предполагается, что сервер запускается не в первый раз, обновлять версию не требуется, и протокол изменений не настроен. Следующий сервер SQL (057340/QUSER/QSQSRVR) применяется Службами каталогов для репликации.

Самое последнее соединение в этом примере (057288/QUSER/QSQSRVR) применяется для выполнения операций добавления, изменения, удаления, а также изменения относительного DN. Другие соединения применяются для поиска, связывания и сравнения.

На странице **База данных**/**Суффиксы** окна свойств сервера каталогов в Навигаторе задается общее число серверов SQL, применяемых Службами каталогов для работы с каталогом после запуска сервера. Кроме того, один сервер SQL всегда настроен для репликации.

Отслеживание ошибок и контроль доступа с помощью протокола задания Служб каталогов

Путем просмотра протокола задания сервера LDAP можно получить информацию об ошибках и обращениях к серверу.

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 пункте **Каталог** 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**, расположенном слева от QDIRSRV.

   Примечание: В Навигаторе может быть задан фильтр, разрешающий показывать только буферные файлы. Если QDIRSRV отсутствует в списке, выберите **Вывод на принтер**, а затем выберите пункт **Включить в список** в меню **Опции**. Укажите значение **Все** в поле **Пользователь** и нажмите кнопку **OK**.

Примечание: Для выполнения некоторых задач Службы каталогов применяют 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 Службы каталогов не могут 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 LDAP.

Дополнительная информация о применении команды TRCTCPAPP при работе с сервером LDAP и необходимых правах доступа приведена в разделе Описание 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

В версиях V5R2 и выше 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 QAPOZDMP QPOZnnnnnn
```

где `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(QAPOZDMP LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   где *xxx* - имя созданного файла SAVF.

Ошибки клиента LDAP

Зная причины, по которым обычно возникают ошибки на клиенте LDAP, вы сможете быстро устранить неполадки на своем сервере. Полный список ошибок клиента LDAP приведен в разделе Службы каталогов OS/400 справочной системы iSeries Information Center. Этот раздел относится к категории Программирование.

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 OS/400. 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”
- “[Сбой операции LDAP]: Нет прав доступа” на стр. 69
- “[Сбой операции LDAP]: Не удалось подключиться к серверу LDAP” на стр. 69
- “[Сбой операции LDAP]: Не удалось подключиться к серверу SSL” на стр. 69

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 LDAP. Соответствующие инструкции приведены в разделе “Повышение производительности сервера каталогов LDAP” на стр. 33.
- 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 информации о причинах возникновения ошибки в конкретном экземпляре просмотрите протоколы заданий серверов QDIRSRV и SQL, следуя инструкциям, приведенным в разделе “Основная процедура устранения неполадок Служб каталогов” на стр. 65.

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 “Основная процедура устранения неполадок Служб каталогов” на стр. 65.

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 OS/400 с атрибутом UID, но без пароля. При этом указанный пароль не совпадает с паролем пользователя OS/400.
- Запись, представляющую спроецированного пользователя, причем указан метод связывания, 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 “Основная процедура устранения неполадок Служб каталогов” на стр. 65.

[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 “Основная процедура устранения неполадок Служб каталогов” на стр. 65.

[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 “Основная процедура устранения неполадок Служб каталогов” на стр. 65. Если сервер Служб каталогов был запущен, 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 OS/400 на языке C доступна дополнительная информация об ошибках SSL. Более подробные сведения приведены в документации по отдельным API Служб каталогов.

Напечатано в Дании