Виталий Акулов

Корпоративный каталог

Каталог LDAP (Lightweight Directory Access Protocol) — отличное средство для хранения различной статистической информации, например деловых контактов. Если надо организовать подобную службу во внутренней сети компании, все, что вам понадобится, — это дистрибутив ОС Linux.

Каталог по своей функциональности достаточно сильно напоминает обычную СУБД. Но в отличие от нее предназначен в основном для чтения и быстрого поиска информации внутри базы, а потому не поддерживает такие функции современных СУБД как, например, механизм транзакций или «реляционные» отношения между таблицами. Если продолжать проводить параллели все с той же СУБД, то информация, предоставляемая пользователю службой каталога, больше всего напоминает служебные таблицы-справочники, например «материалов» или «поставщиков». Новые записи в такие таблицы добавляются достаточно редко, а изменение уже имеющейся в них информации выглядит как удаление записи и добавление на ее место новой.

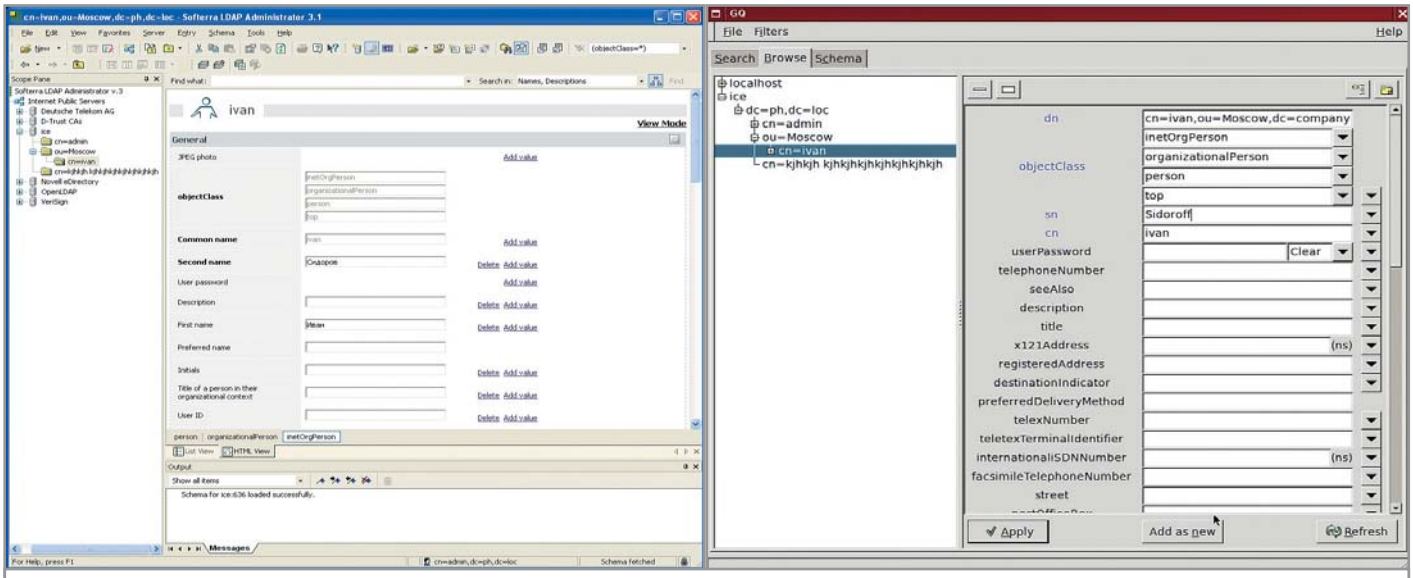
В сетях OSI (Open System Interchange networks) полная модель служб каталога описана стандартом X.500, который подробно рассматривает не только информационную модель хранения данных, но и сам протокол для оперирования ими — DAP (Directory Access Protocol). Однако модель каталога настолько богата, а DAP включает в себя такое количество самых разнообразных способов обработки данных, что его полная реализация на обычном компьютере — задача более чем нетривиальная. В основном именно по этой причине энтузиасты из Мичиганского университета, пользуясь рекомендациями консорциума ISODE, решили заняться разработкой нового, облегченного варианта DAP, который в итоге так и назвали — LDAP (Lite DAP).

По сути, LDAP заимствовал из X.500 как модель хранения данных, так и протокол для работы с ними. Существенным же отличием от прародителя стало именно то, что LDAP был реализован только лишь для стека TCP/IP, а потому не поддерживал различные экзотические функции оригинального DAP. Еще раз отметим, что LDAP — это протокол, описывающий способ доступа к информации, которая хранится в каталоге. Системой, которая хранит эту информацию, может быть любая СУБД. Однако как только СУБД начинает поддерживать интерфейс протокола LDAP, она может уже выступать и в роли службы каталога. Забегая немного вперед, можно сказать, что некоторые из служб LDAP-каталогов имеют реализацию интерфейса LDAP для обслуживания клиентов, а все данные хранят в какой-либо распространенной СУБД.

Если взглянуть на каталог изнутри, отдельные записи в нем удобнее всего рассматривать как объекты. Каждая запись в каталоге представляет собой набор атрибутов и их значений. Информация об атрибутах хранится в схеме каталога (directory schema), которая описывает хранящуюся в нем информацию с помощью классов (classes), используя при этом объектно-ориентированный подход.

Класс объекта (objectclass) описывает наименования атрибутов объекта, а также типы их значений. Некоторые атрибуты обязательны (must) для создания записи этого класса, остальные же являются опциональными (may). Кроме того, классы вполне могут наследовать атрибуты других классов. В качестве примера приведем описание структуры абстрактного класса account:

```
account OBJECT-CLASS
SUBCLASS OF top
MUST CONTAIN {
userid}
MAY CONTAIN {
description,
seeAlso,
localityName,
organizationName,
```



Вносим новые контакты в каталог через LDAP Administrator и GQ соответственно

organizationalUnitName,
host}

Как видите, класс account наследуется от класса top. Для создания класса account должен быть указан необходимый атрибут userid, также могут быть обозначены необязательные атрибуты description, seeAlso, localityName.

Одна запись в каталоге может хранить атрибуты нескольких классов объекта. Информация о том, атрибуты каких классов хранит та или иная запись каталога, указывается отдельным, обязательным для каждой записи атрибутом objectclass. Другим обязательным атрибутом каждой записи считается ее DN (distinguished name). Это уникальный атрибут, который является своего рода ключевым полем и имеет мнемоническое представление, которое необходимо читать справа налево. Например:

DN: Cn=Admin, Ou=IT, dc=Company, dc=com

Формат обмена данными между сервером LDAP и клиентом или же между двумя серверами LDAP называется LDIF (LDAP Data Interchange Format). С помощью данного формата можно описывать значения атрибутов для вновь создаваемых объектов или изменения атрибутов для уже существующих. Подводя итог нашей немного затянувшейся вводной части, скажем, что примеры реализации и использования LDAP-совместимых каталогов сейчас можно встретить практически в любой операционной системе. В Novell Netware это NDS (Novell Directory Service). В Microsoft Windows — AD (Active Directory). Ну а в Unix — проект OpenLDAP.

Адресная книга на LDAP-сервере slapd

Как уже было сказано в самом начале, мы продемонстрируем установку LDAP-сервера на базе платформы Linux. Такой выбор был обусловлен сразу двумя факторами — доступностью дистрибутива и необходимых средств, а также относительной легкостью в установке, во всяком случае по сравнению с тем же Microsoft Active Directory. Итак, чтобы установить службу каталога, вам понадобится добавить в систему три следующих пакета:

- **openldap-servers** — сервер slapd;
- **openldap-clients** — клиентские утилиты (ldapsearch, ldapadd);
- **openldap** — общие библиотеки для утилит из первых двух пакетов.

После установки в каталоге /etc/openldap должны будут появиться следующие конфигурационные файлы:

- **/etc/openldap/ldap.conf** — настройки клиентских утилит;
- **/etc/openldap/slapd.conf** — настройки сервера slapd;
- **/etc/openldap/schema/*.schema** — схемы хранения данных.

Конфигурация сервера состоит из двух частей — глобальные директивы и директивы, относящиеся к каждой конкретной базе данных, в которой хранятся записи каталога. Изначально конфигурационный файл slapd.conf выглядит следующим образом:

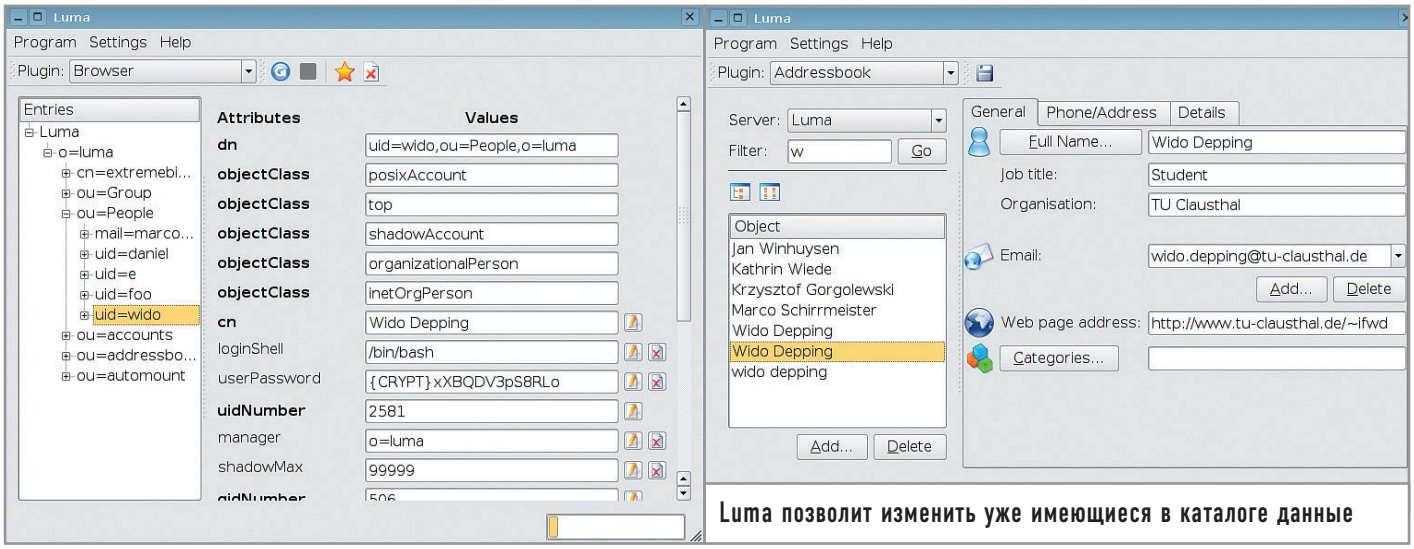
```
# Глобальные директивы
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/redhat/rfc822-MailMember.schema
include /etc/openldap/schema/redhat/autofs.schema
include /etc/openldap/schema/redhat/kerberosobject.schema

# Настройки БД на основе LDBM
database ldbm      # БД на базе LDBM
suffix «dc=my-domain,dc=com»      # Суффикс каталога
rootdn «cn=Manager,dc=my-domain,dc=com» # DN для root
directory /var/lib/ldap      # Где хранятся файлы БД
index objectClass,uid,uidNumber,gidNumber,memberUid  eq
# Атрибуты, для которых
index cn,mail,surname,givenname  eq,subinitial
# строятся индексы
```

В текущую конфигурацию необходимо добавить еще одну директиву:

```
rootpw «secret»    # Пароль для root
```

Кроме того, необходимо выбрать суффикс каталога, который был бы созвучен с названием вашей компании. Например:



Luma позволит изменить уже имеющиеся в каталоге данные

suffix «dc=company,dc=ru» # Суффикс каталога

Таким образом, суффикс указывал бы на принадлежность каталога к вашей компании, если бы этот каталог был частью другого, более глобального каталога. Однако, изменяя суффикс, надо не забывать и о смене «rootdn»:

rootdn «cn=admin,dc=company,dc=ru» #DN для root

После этого можно запускать сервер, используя скрипт, находящийся в /etc/init.d:

/etc/init.d/slapd start

После того как стартовал сервер, необходимо сделать первую запись в нашем каталоге, а именно для «dc=company,dc=ru». Для этого мы воспользуемся утилитой ldapadd. Как можно догадаться, эта консольная программа предназначена для добавления записей в каталог. Входная информация для нее должна быть представлена в формате LDIF, поэтому давайте создадим файл first.ldif следующего содержания:

dn: dc=company, dc=ru
objectClass: dcObject
objectClass: organization
dc: company
o: Company LTD, Russia

Как видите, структура LDIF-файла сама по себе довольно проста: слева указаны наименования атрибутов, справа — их значения. Обязательными являются атрибуты dn и objectClass, указывающие DN вновь создаваемой записи и набор классов, описывающих атрибуты, значения которых должна будет хранить эта запись. Далее должны быть указаны атрибуты, обязательные для каждого выбранного класса. В данном случае это dc — для dcObject и o — для organization. LDIF-файл также может содержать сведения о нескольких записях. Благодаря этому весь имеющийся LDAP-каталог может быть экспортирован в один LDIF-файл. Теперь запишем полученный файл в наш каталог:

ldapadd -D 'cn=admin,dc=company,dc=ru' -f first.ldif -W
Enter LDAP Password: secret

Опция -D указывает DN подключения к серверу. Чтобы осуществлять запись в каталог, необходимо подключаться с rootdn и паролем rootpw, которые мы указали в файлах конфигурации сервера. Теперь попробуем создать подкаталог для хранения записей адресной книги — файл addressbook.ldif:

dn: ou=addressbook, dc=company, dc=ru
objectClass: organizationalUnit
ou: addressbook

Ну а теперь сделаем первую запись с контактной информацией о конкретной персоне в файле ivan_smirnoff.ldif:

dn: cn=Ivan Smirnoff, ou=addressbook, dc=company, dc=ru
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Ivan Smirnoff
gn: Ivan
sn: Smirnoff
mail: ismirnoff@company.ru
ou: addressbook
telephoneNumber: +7-095-123-4567
mobile: +7-777-1234567

Атрибуты mail, ou, telephoneNumber и mobile не являются обязательными. После загрузки файла ivan_smirnoff.ldif мы получим адресную книгу в LDAP-каталоге, правда, пока что состоящую всего лишь из одной записи. Проверить работоспособность полученного каталога можно с помощью утилиты ldapsearch, которая отобразит содержимое каталога все в том же LDIF-формате:

ldapsearch -b «dc=company,dc=ru»

Если значения параметров в LDIF-файле используют не только латинский алфавит, то они должны быть представлены в кодировке UTF-8.

Настройка Outlook

Для того чтобы воспользоваться нашей адресной книгой, необходимо настроить почтовый клиент таким образом, чтобы он сверял вводимые пользователем адреса электронной почты с данными в LDAP-каталоге. Покажем это на примере наиболее распространенного почтового клиента Outlook Express. Для начала создадим в нем новую учетную запись для «Службы каталогов»: для этого потребуется перейти в меню «Сервис → Учетные записи». Далее на вкладке свойств «Дополнительно» для этой учетной записи необходимо указать базу поиска «ou=adressbook,dc=company,dc=ru» — то есть DN

нашей адресной книги, который при поиске будет являться суффиксом для всех контактов.

Теперь, если при создании нового письма в строке адреса написать лишь начальную часть имени, фамилии или электронного адреса персоны, Outlook Express, произведя поиск по каталогу, автоматически «допишет» адрес или же предложит на выбор несколько вариантов, в случае если результаты поиска окажутся неоднозначными. Аналогичным способом можно настроить и другие почтовые клиенты. Ключевыми параметрами здесь являются IP-адрес сервера и база поиска.

Редактирование каталога

Все существующие приложения для редактирования каталога, построенного на базе сервера OpenLDAP, можно разделить на три типа: консольные, графические и основанные на технологиях WWW/CGI. Пример использования консольных утилит мы демонстрировали немного выше. Однако такое решение может сгодиться только в том случае, если LDIF-файлы генерируются автоматически другим приложением, например на основании записей отдела кадров в корпоративной информационной системе (КИС). При достаточном опыте можно создавать LDIF-файлы и вручную, используя предварительно подготовленные для этого шаблоны. Однако если решение выходит на корпоративный уровень, а обновление информации может лечь на плечи секретариата или отдела кадров, то без хорошего графического клиента обойтись вряд ли получится.

LDAP Administrator 3.1

Наиболее качественно реализованный LDAP-клиент для Windows — LDAP Administrator от компании Softerra (www.ldap-administrator.com). Большое количество функций, удобный интерфейс, наличие мастеров, а также умение работать с LDAP-каталогами корпоративных масштабов делают этот продукт единственным достойным выбором для Windows-платформы.

GQ 0.6.0

Данный клиент создан для платформы X-Windows на основе библиотек GTK+ и является одним из первых GUI-клиентов для LDAP под Unix-системы. Как правило, его можно отыскать в любом дистрибутиве ОС Linux.

GQ обладает достаточной функциональностью для редактирования каталогов среднего по масштабам предприятия, поддерживает русский язык и создание новых записей на основе существующих (замена механизма шаблонов). Однако разработчики проекта или совсем удовлетворились созданным детищем, или попросту про него забыли, но так или иначе последний его релиз датирован ноябрем позапрошлого года.

LUMA 1.6

Это относительно новый и весьма перспективный LDAP-клиент для X-Windows, написанный на языке Python с использованием библиотек python-ldap и python-qt. Он обладает достаточно приятным и простым в работе интерфейсом, довольно функционален, а кроме всего прочего поддерживает русский язык. Программа имеет серьезные шансы стать оптимальным выбором для небольших компаний.

Заключение

Несомненно, применение каталога в масштабах пусть даже небольшой организации облегчит жизнь не только пользователям, но и системным администраторам. Хотя бы по той простой причине, что LDAP-каталоги довольно легко масштабируемы, а благодаря использованию общего протокола практически не зависят от платформы реализации. Кроме того, при применении встроенных средств для репликации без особого труда можно построить собственную внутреннюю распределенную систему каталогов, которая будет полностью соответствовать территориальным разделениям филиалов вашей компании.

Альтернатива

Управление LDAP через веб-интерфейс

Среди множества LDAP-клиентов, написанных на различных высокоуровневых языках программирования, отдельно следует выделить те, которые построены на основе технологий WWW/CGI. Приведем лишь несколько наиболее распространенных примеров: *LDAP-ABOOK* (http://ldap-abook.sf.net), написанный на Perl; phpldapadmin (http://sf.net/projects/phpldapadmin), а также *LABE* (www.savoirfairelinux.com/labe), основанные на PHP. К несомненным достоинствам таких клиентов стоит отнести независимость от платформы. То есть редактировать LDAP-каталог вы сможете при помощи любого браузера. С другой стороны, для того чтобы установить такие клиенты, понадобятся как минимум веб-сервер и модуль реализации протокола LDAP для того языка программирования, на котором написан клиент. Однако этот «недостаток» в умелых руках превращается в неоспоримое достоинство, позволяя программисту изменять вид LDAP-каталога под стандарты и нужды компании.

Веб-интерфейс — наиболее удобное средство управления каталогом