LDAP-КАТАЛОГ СО РАН

Д. Ю. Новоселов
Новосибирский государственный университет, Россия
С. П. Ковалев
Институт вычислительных технологий СО РАН, Новосибирск, Россия
e-mail: novodim@nsu.ru, kovalyov@nsc.ru

Growing SB RAS network increasingly requires a uniform access to the information about users and informational resources. In this article the implementation of such a system based on the LDAPv3 protocol is described.

Введение

При устройстве на работу нового сотрудника информация о нем сразу попадает в базу данных отдела кадров. На современных предприятиях каждый сотрудник имеет адрес электронной почты, логин и пароль для доступа к почтовому ящику, а также вход в корпоративный домен и т. д. Вся эта информация содержится в тех или иных базах данных, однако с большой степенью вероятности дублирует друг друга, поскольку, как правило, пользователь имеет одинаковую информацию доступа для всех систем. Для обеспечения доступа пользователя к какой-либо новой системе необходимо продублировать информацию о нем еще раз в базе данных пользователей этой системы.

Но можно привести и другой пример, когда новая система способна использовать информацию о пользователях из уже существующих баз данных. Это пример того, как можно сократить затраты на конфигурацию и поддержку доступа пользователей.

В предельном случае должен существовать единый регистр пользователей и ресурсов, способный предоставить все необходимые операции для управления доступом пользователей к ресурсам. Любые сервисы, требующие аутентификации и авторизации, способны взаимодействовать с этой системой и использовать ее как источник информации о пользователях, ресурсах и правах пользователей к этим ресурсам.

1. Постановка задачи

Основанием системы управления информацией о пользователях, ресурсах и правах доступа пользователей к ресурсам является единый каталог пользователей и ресурсов.

Исходя из реалий, когда информация о пользователях и ресурсах СО РАН уже существует в некотором виде в разнообразных базах данных, основными задачами каталога являются упорядочение, объединение уже имеющейся информации, предоставление

© Институт вычислительных технологий Сибирского отделения Российской академии наук, 2005.

унифицированного доступа к ней со стороны приложений и осуществление контроля за целостностью данных каталога.

Необходимо однозначно определить место нахождения информации каждого из подразделений СО РАН в рамках каталога. То есть каталог должен предоставлять систему именования, позволяющую осуществлять однозначный доступ к записи по ее идентификатору, уникальному во всем каталоге, а также обладать определенным потенциалом расширяемости для возможности включения новых подразделений в общий каталог.

Решение задачи унифицированного доступа к информации означает наличие общего протокола обмена информацией каталога с приложениями и ее однозначное описание, а также реализацию способов преобразования уже имеющейся информации в универсальный вид для СО РАН. Иными словами, должно быть согласовано представление информации о пользователях и ресурсах, описаны все необходимые сущности, для каждой из них перечислены обязательные и необязательные поля и способы задания их значений. При описании представления данных каталога необходимо учитывать требования круга приложений, которые будут осуществлять запросы к каталогу, и способы импортирования информации из уже имеющихся хранилищ в стандартное представление каталога. Универсальное представление информации в каталоге скорее всего будет уже, чем то, что применяется в отдельных организациях СО РАН.

Несмотря на то, что подавляющим большинством запросов к каталогу будут запросы на чтение, существует необходимость в достаточно гибком механизме управления доступом к данным каталога. Примером может служить ограничение доступа на чтение к некоторым полям записей для неавторизованного пользователя. Предоставляемые каталогом механизмы должны обеспечивать возможности ограничения прав на чтение и изменение данных как для целых организаций, так и для отдельных пользователей. Должно быть возможно управление правами доступа для одной или нескольких записей.

Желательны наличие поддержки современных способов аутентификации пользователей и обеспечение целостности и секретности пользовательских сессий, например аутентификация с участием сертификатов x.509 и возможность применения SSL.

Каждое из отделений СО РАН будет ответственно за соответствующую ему часть каталога, поэтому требуются механизмы для объединения этих частей в единый каталог СО РАН. Учитывая значительную географическую распределенность СО РАН, эти механизмы должны обеспечивать устоичивость каталога к сетевым сбоям для минимизации потерь в обслуживании.

Необходимой частью каталога является система контроля за актуальностью, целостностью и непротиворечивостью информации. Например, при необходимости изменить записи, соответствующие одному и тому же физическому объекту, требуется корректное изменение всех копий записей об этом объекте. Правила корректности данных определяются в значительной мере семантикой описываемых объектов.

2. Стандарты построения систем директорий

Системы, предназначенные для хранения разнородной информации, например о сотрудниках, компьютерах и ресурсах сети, сегодня принято реализовывать в виде сервиса директорий. Наиболее полным описанием того, что называется сервисом директорий, является стандарт x.500. Это полновесное описание всех аспектов построения систем директорий, включая вопросы взаимодействия клиента и сервера и описания формата данных [1]. По-

строение систем на базе стандарта x.500 было сочтено достаточно сложным. Этим обусловлено появление облегченного стандарта систем директорий, в частности протокола обмена данными из директорий x.500 и спецификации схем данных, совместимой с x.500. Применение нового стандарта позволило снизить удельные затраты на содержание одной записи в каталоге и упростить клиентские приложения. Этот стандарт получил название LDAP. К настоящему времени существует 3-я версия LDAP, которая стала стандартом протокола доступа к системам директорий в Интернет.

Система директорий стандарта x.500 представляет собой деревообразную структуру, состоящую из записей. Каждая из них может иметь потомков, т. е. служить директорией. Записи имеют имена, образованные составлением имени родителя, а также имени и значения своего атрибута, уникального среди "братьев" этой записи, т. е. потомков первого уровня того же предка. Такое имя называется Distinguished Name (DN), оно уникально в пределах всего дерева. Например, объект, соответствующий отделу marketing, может иметь DN: ou=marketing,o=company,dc=com, а DN отдела продаж будет выглядеть так: ou=sales,o=company,dc=com.

Записи системы директорий имеют некоторый набор атрибутов. Разрешенный набор атрибутов описывается с помощью объектной модели, позволяющей осуществлять наследование, при котором результирующий класс наследует все атрибуты родительских. Для описания атрибутов определяются типы, такие как цифровое поле, строка символов или бинарные данные. Для каждого из типов определены операции сравнения для осуществления сортировки объектов с использованием в качестве ключа значения атрибутов данного типа. Стандарт LDAPv3 поддерживает строки многобайтных символов для атрибутов, т. е. это позволяет описывать объекты в национальных языках. Совокупность описаний типов и объектов, принятых в системе директорий, называется схемой данных.

Протокол LDAP рекомендован для обмена информацией систем директорий. Но создатели стандарта не рекомендуют его использовать для изменения записей в системах директорий. Это связано с тем, что в стандарте LDAP пока не описаны механизмы аутентификации клиентов в той степени, которая необходима для обеспечения безопасности этих операций. Поэтому взаимодействие систем, способных не только читать информацию из сервисов директорий, но и изменять ее посредством LDAP, может быть затруднено или невозможно совсем из-за того, что уровень безопасности таких сессий может стать ниже допустимых пределов. В таких ситуациях авторы стандарта LDAP рекомендуют использовать другой, не связанный с протоколом LDAP способ изменения данных в директории, который способен обеспечить достаточный уровень безопасности [2, 3].

В стандарте LDAPv3 содержится описание процедуры сшивания различных частей директорий посредством использования специального объекта, называемого ссылкой (referral) [4]. Этот объект содержит LDAP URL [5], по которому находится часть дерева директорий с корнем на месте этого объекта. LDAP URL содержит сетевые координаты ссылаемого сервиса директорий, т. е. IP адрес и порт, и DN корня ссылаемого поддерева системы директорий. Это делает допустимым делегирование поддержки части каталога другим серверам. Если для завершения запроса клиента его необходимо выполнить на части дерева директорий, присоединенной ссылкой, то стандартом LDAPv3 предписано серверу возвратить клиенту ссылку на это поддерево и окончание запроса выполняется именно клиентом. Такой механизм позволяет сбалансировать нагрузку между серверами и организовать распределенную систему директорий.

Протокол LDAPv3 не определяет того, как должна проводиться авторизация пользователей, определяя ее только как применение информации о пользователе, полученной в

процессе аутентификации. Использование внешних средств для авторизации и аутентификации не противоречит спецификации протокола LDAPv3.

Кроме того, задачи осуществления репликации, т. е. создания копии поддерева системы директорий для обеспечения устойчивости к сбоям и уменьшению времен отклика системы, и контроля за свойствами данных, гарантирующими непротиворечивость и целостность информации, не описываются стандартом LDAPv3 и должны решаться на уровне хранения данных.

На сегодняшний день протокол LDAP v3 принят большинством производителей программного обеспечения в качестве стандартного способа обмена информацией из систем директорий в сети Интернет независимо от способа ее хранения [6].

3. Особенности доступных решений

Существующие на рынке коммерческие системы директорий сходны в том, что предоставляют доступ по протоколу LDAPv3 к данным из директории, но по-своему реализуют хранилище данных, приемы аутентификации и контроля доступа. От конкретной реализации системы директорий зависят и возможности интеграции с другими продуктами и платформами.

Как правило, системы директорий поддерживают больший набор способов аутентификации клиентов, чем описано в рамках LDAPv3, и предоставляют средства для осуществления авторизации. Обычно есть в наличии поддержка анонимного доступа, доступа с использованием пароля и SSL v3 аутентификация с участием x509 сертификатов. Некоторые продукты способны осуществлять биометрическую аутентификацию пользователей с использованием микропроцессорных карт. Средства авторизации позволяют ограничивать доступ к записям директорий на уровне пользователя, групп пользователей или поддерева системы директорий. Права доступа могут быть определены на поддерево, отдельную запись, набор записей или некоторые атрибуты записей. Вариации приемов авторизации изменяются от продукта к продукту.

Все системы директорий на рынке так или иначе поддерживают репликацию данных, т. е. возможность воспроизводить точную копию всего дерева или его части в другом месте. Надо заметить, что репликация не имеет ничего общего с описанием стандарта LDAPv3, поскольку касается вопроса хранения данных, однако протокол LDAPv3 может быть использован в качестве транспорта для распространения изменений между репликами. В разных продуктах репликация может осуществлять синхронизацию изменений данных или схемы данных, работать в режиме single-master или multi-master. Распространение изменений происходит за небольшое время, порядка нескольких минут, однако оно зависит от конкретного продукта, объема изменений и наличия сетевой коннективности между репликами. Репликация в режиме single-master, как следует из названия, позволяет иметь только одну выделенную реплику, предназначенную для внесения изменений в данные системы директорий. Все изменения, произведенные в одних репликах, не распространяются на другие реплики. А в режиме multi-master изменения могут производиться на любой из реплик, помеченных как мастер, при этом они попадут на все другие реплики.

Коммерческие продукты также осуществляют контроль за целостностью данных в системе директорий в соответствии с требованиями этой системы.

Все вышеперечисленное может быть отнесено на счет коммерческих систем директорий Microsoft Active Directory, Novell eDirectory и Oracle Internet Directory и других, а также

на реализацию системы директорий с открытым кодом — OpenLdap [7 – 10].

Таким образом, предпочтительность определенного продукта в качестве основы для системы директорий СО РАН зависит от других их особенностей, таких как требования к программно-аппаратному окружению, хранилищу данных или, в конце концов, доступности продукта.

Если рассматривать требования к окружению, то, например, система директорий Microsoft Active Directory естественно способна работать только на платформе Windows 2000/Windows 2003, в то время как OpenLdap работает в Unix-подобном окружении, которое охватывает значительный спектр платформ. Многоплатформенностью также отличаются и продукты от Novell и Oracle.

Данные систем директорий могут храниться в некотором внутреннем формате или в стандартных базах данных. Например, Microsoft Active Directory использует внутренее представление для хранения данных директорий, а продукт от Oracle способен хранить информацию директорий только в СУБД Oracle. Продукт OpenLdap позволяет хранить данные системы директорий практически в любом виде благодаря возможности осуществления доступа к данным через программируемые perl или shell интерфейсы. Однако возможно и хранение данных в БД Berkeley DB [10].

В принципе, для каждой из систем возможен импорт данных в формате LDIF, являющемся текстовым представлением записей директории, в который можно привести любые текстовые или бинарные данные. При этом главным вопросом является соответствие полей исходного хранилища и атрибутов LDAP объектов. То есть теоретически любое представление данных может быть доступно через протокол LDAPv3 независимо от используемой системы, однако это достигается путем различных трудозатрат.

Заключение

Таким образом, каталог пользователей и ресурсов СО РАН можно представить в виде мозаики из отдельных частей, которые управляются различными системами директорий, но предоставляют единообразный доступ к данным по протоколу LDAPv3 в соответствии с принятой схемой данных каталога. При этом обеспечение целостности информации гарантируется применением единой схемы данных, а вопрос обеспечения непротиворечивости данных в глобальном масштабе каталога остается открытым. Например, в ситуации, когда одному и тому же физическому объекту соответствует несколько записей в каталоге, неясно, каковы должны быть механизмы обеспечения одновременного изменения свойств этих записей при необходимости и, вообще говоря, насколько корректна ситуация существования в директориях нескольких записей для одного и того же физического объекта.

Возможно, что пилотная реализация каталога на базе нескольких организаций ННЦ позволит более конкретно сформулировать эти требования и станут понятными пути их выполнения.

В свете вышесказанного нет каких-либо веских причин настаивать на применении только одного определенного продукта для организации сервиса директорий СО РАН. Благодаря усилиям по стандартизации и взаимодействию систем, в принципе, возможно реализовать систему директорий СО РАН на базе продуктов, уже применяемых для реализации системы директорий в отдельно взятом институте, или путем организации доступа к имеющимся базам данным пользователей по протоколу LDAPv3 с использованием наиболее удобного для поддержки и конфигурирования продукта.

Скорее всего для создания центральной инфраструктуры системы директорий будет использован OpenLdap-2.2 благодаря своей доступности, гибкости организации интерфейсов к конечным базам данным, а также его соответствия духу сети СО РАН, где широко применяются и другие свободно распространяемые продукты, в то время как отдельные институты должны только лишь обеспечить доступ к информации о своих пользователях в соответствии с определенной схемой данных по протоколу LDAPv3.

Список литературы

[1] The directory. CCIT REC. X.500-X.521 ISO/IEC STANDARD 9594:1993.

[2] Wahl M., Howes T., Kille S. RFC 2251, Lightweight Directory Access Protocol (v3), раздел 1, December 1997.

[3] Wahl M., Alvestrand H., Hodges J., Morgan R. RFC 2829, Authentication Methods for LDAP, May 2000.

[4] Wahl M., Howes T., Kille S. RFC 2251, Lightweight Directory Access Protocol (v3), раздел 4.1.11, December 1997.

[5] Howes T., Smith M. RFC 2255, The LDAP URL Format, December 1997.

[6] More than 40 companies join Netscape and U. Michigan to support lightweight directory ACCESS protocol as proposed standard for Internet directories. Netscape Company Press Relations. http://wp.netscape.com/newsref/pr/newsrelease126.html

[7] Microsoft Active Directory.
http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp

[8] Understanding Novell eDirectory.
http://www.novell.com/documentation/edir873/edir873/data/fbadjaeh.html

[9] Oracle Internet Directory 10g.
http://www.oracle.com/technology/products/oid/index.html

[10] OpenLDAP 2.2 Administrator's Guide.
http://www.openldap.org/doc/admin22/

Поступила в редакцию 18 марта 2005 г.