Вопросы интеграции информационных и сетевых служб. Варианты использования LDAP каталогов ♣

© А.В.Созыкин
ИМСС УрО РАН
sozykin@icmm.ru

Г.Ф.Масич
ИМСС УрО РАН
masich@icmm.ru

А.Г.Масич
ИМСС УрО РАН
mag@icmm.ru

А.Н. Бездушный
РАН ВЦ РАН
bezdushn@ccas.ru

Аннотация

В статье рассматривается деятельность, направленная на обеспечение интеграции информационно-справочных сервисов и сервисов сетевого управления учреждений РАН. Архитектура предлагаемого решения основывается на открытых стандартах, использовании многоуровневой компонентной архитектуры LDAP-систем и доступа к ним как через локальные, так и через глобальные сети. Проводится сравнение схем метаданных информационно-справочной системы ИСИР РАН и стандартных схем LDAP каталогов.

1. Взаимодействие сетевых служб с LDAP каталогами

В настоящее время большая часть сетевых сервисов способна использовать каталог LDAP в качестве хранилища конфигурационной информации. В их число входят операционные системы семейств Unix и Windows, почтовые серверы, DNS серверы, прокси серверы и серверы аутентификации и авторизации (Radius и Tacacs). Особо следует отметить, что существуют бесплатные реализации описанных выше служб, способные взаимодействовать с LDAP. Это делает возможным создание на базе LDAP централизованного хранилища конфигурационной и идентификационной информации.

Каждый производитель операционных систем и программного обеспечения имеет свою реализацию каталога LDAP и все программное обеспечение этого производителя, как правило, может взаимодействовать с этой реализацией. Так, в операционную систему Windows фирмы Microsoft встроен Active Directory Server, работающий по протоколу LDAP. Почтовый сервер Microsoft Exchange не имеет своего хранилища информации о пользователях, а вместо этого использует Active Directory. LDAP каталогами являются Sun ONE Directory Server, встроенный в Solaris и Novell eDirectory, встроенный в Netware. Также каждый производитель имеет решение, которое позволяет управлять всей совокупностью производимых им программных продуктов через единый интерфейс. Такие решения позволяют управлять только программными продуктами одного производителя. Сети в учреждениях РАН, как правило, гетерогенны, а с помощью системы управления одного производителя невозможно управлять всеми сервисами корпоративной сети. Учитывая это, а также высокую стоимость таких решений, их применение в рамках Академии Наук затруднено.

В организациях с большим количеством пользователей и машин управление учетными записями пользователей становится трудной задачей. Каталог LDAP позволяет создать единую централизованную систему аутентификации. Многие современные сетевые сервисы могут использовать LDAP для аутентификации пользователей. Механизмы взаимодействия с каталогом меняются от сервиса к сервису, но, как правило, функциональные возможности одни и те же.

До недавнего времени для распространения в сети информации об учетных записях пользователей наиболее широко использовался Network Information Service (NIS). NIS является распределенным сервисом, который позволяет создать центральный сервер, хранящий конфигурационную информацию о пользователях, группах, сетевых сервисах и т.д. Клиенты NIS обращаются к серверу NIS за этой информацией. LDAP может предложить ту же функциональность, что и NIS, но с дополнительными возможностями:

- Информация в каталоге LDAP может быть легко использована не только для аутентификации пользователей в Unix, но и для большого количества других целей;
- LDAP предоставляет комплексный механизм списков контроля доступа (access control lists), что позволяет легко управлять правами доступа пользователей и делегировать полномочия управления;

Труды 6ой Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» - RCDL2004, Пущино, Россия, 2004.

- Для защиты данных при передачи по сети от LDAP-сервера к клиенту может использоваться SSL;
- Управление всей информацией в сети осуществляется через «единую точку доступа».

2. Метаданные сетевых сервисов

Сетевым сервисам требуется большое количество конфигурационных параметров. Но большинство таких параметров являются специфичными для данного сервиса и не представляют интереса для широкого круга пользователей и приложений. Существует только два типа ресурсов, представляющих широкий интерес – это «Учетная запись пользователя» («Account»), «Группа» и «Роль». Группы используются для упрощения управления доступом пользователей к сервисам. Пользователи объединяются в группы, которым разрешен доступ к определенным сервисам, например «Группа пользователей Интернет». Это снимает необходимость прописывать отдельные строки контроля доступа для каждого пользователя. Сервисы также могут объединяться в группы. Роли применяются для делегирования управления данными в каталоге. Некоторым пользователям назначаются роли администраторов. Администраторы могут управлять всеми или частью данных каталога.

3. Обзор стандартных LDAP схем

Поскольку LDAP каталоги часто используются в качестве корпоративных справочников общего назначения, чтобы осуществить принципы «единой точки доступа», «согласованной модификации данных» как информационной, так сетевой инфраструктур научного учреждения, необходимо иметь сопоставление схем метаданных информационно-справочных систем, например, ИСИР, и стандартных схем LDAP каталогов.

3.1 RFC 2256 A Summary of the X.500(96) User Schema for use with LDAPv3

Это самая широко используемая схема. Она основывается на стандартах ISO и ITU-T X.500. В схеме определен базовый для LDAP класс top. Все остальные LDAP схемы используют этот класс и схему RFC 2256. Кроме определения базовых классов, схема включает набор атрибутов и классов объектов для представления корпоративного справочника white pages.

3.2 RFC 1274 The COSINE and Internet X.500 Schema

Схема дополняет набор классов объектов и объектов, определенный в RFC 2256 и X.500, используемый для создания white pages организации. Кроме этого, вводит дополнительные классы объектов для описания документов и для управления сетевыми сервисами.

3.3 RFC 2798 Definition of the inetOrgPerson LDAP Object Class

Данная схема, как следует из названия, содержит определение всего одного класса inetOrgPerson. Этот класс является подклассом organizationalPerson из RFC 2256. В нем определены дополнительные атрибуты для характеристики персоны в организации, такие как идентификационный номер сотрудника организации, тип работы (постоянная, временная, основная, по совместительству и т.п.), номер водительского удостоверения, предпочитаемый персоной язык, имя для представления персоны.

3.4 RFC 2307 An Approach for Using LDAP as a Network Information Service

Схема определяет набор атрибутов и классов объектов для использования каталога LDAP в качестве сервиса имен для UNIX и TCP/IP.

4. Сравнение схемы метаданных ИСИР РАН со стандартными схемами LDAP

В ИСИР имеется RDFS-подсхема, содержащая набор прикладных классов и свойств, характерных для большинства информационных систем. Примеры включают базовую информацию о документах, организациях, людях и их деятельности. В стандартах RFC определен набор атрибутов и классов объектов для тех же целей. В данном разделе производится анализ стандартных схем LDAP и RDFS схемы метаданных ИСИР РАН с целью установить соответствие между ними.

ИСИР поддерживает следующие типы ресурсов: «Персона», «Проект», «Публикация», «Организационная единица». «Организационная единица» является базовым типом ресурсов для типов «Организация» и «Подразделение». Таким образом, в полный набор используемых типов ресурсов входят «Персона», «Проект», «Публикация», «Организация» и «Подразделение».

Стандартные LDAP схемы включают определения классов объектов, для представления сущностей, используемых в ИСИР. В табл. 1 приведены названия классов объектов LDAP, соответствующие типам ресурсов ИСИР.

Для каждого типа ресурсов ИСИР (кроме типа «Проект») существует несколько классов объектов LDAP. Для типа ресурсов «Проект» в стандартных схемах LDAP нет класса со сходным назначением.

Несмотря на то, что почти для всех типов ресурсов ИСИР РАН нашлись стандартные классы LDAP, лишь небольшая часть свойств ИСИР РАН имеет аналоги среди атрибутов LDAP. Возможно, эти свойства следует отнести к самому базовому набору свойств, который представляет собой

Таблица 1.
Типы ресурсов «ИСИР» и классы объектов LDAP

Тип ресурсов ИСИР	Классы объектов LDAP	Стандарт	Описание
isir:Person	person	RFC 2256	Персона
	organizationalUnit	RFC 2256	
	pilotPerson	RFC 1274	
	inetOrgPerson	RFC 2713	
isir:Unit isir:Department	organizationalUnit	RFC 2256	Подразделение
	pilotOrganization	RFC 1274	
isir:Organization	organization	RFC 2256	Организация
	pilotOrganization	RFC 1274	
isir:Publication	document	RFC 1274	Публикация
	documentSeries	RFC 1274	

необходимый и разумный минимум, минимально достаточный для обмена метаданными и поддержки взаимосвязей ресурсов, в частности с LDAP каталогами стандартных схем.

Стандартные схемы LDAP разработаны с целью использования LDAP в качестве корпоративного справочника общего назначения, а ИСИР РАН - это информационно-справочная система, рассчитанная на использование в научных организациях. Схема ИСИР РАН содержит много атрибутов, характерных именно для научных организаций и результатов научных исследований, чего нет в стандартных схемах LDAP.

Также в стандартных схемах LDAP нет атрибутов для представления связей между объектами. Такие связи представляются с помощью иерархии объектов в каталоге. Например, вместо свойств isir:subOrganization и isir:superOrganization для указания вышестоящей и подчиненных организаций, создается дерево, в вершине которого головная организация, на уровень ниже расположены организации, подчиненные непосредственно ей, а на следующих уровнях организации, подчиненные этим организация. Тогда вышестоящая организация будет находиться в каталоге на уровень выше рассматриваемой организации, а подчиненные – на уровень ниже.

Таким образом, чтобы использовать каталог LDAP в качестве репозитория для ИСИР РАН недостаточно стандартных LDAP схем, необходимо дополнительно создать схему LDAP для ИСИР РАН, включающую определения необходимых атрибутов и классов объектов.

5. Использование LDAP каталогов как репозитория хранимых объектов информационно-справочных сервисов

Для описания используемых схем метаданных в ИСИР используется язык RDFS. Схема ИСИР содержит набор прикладных классов и свойств. В набор классов входит ряд абстрактных классов, обеспечивающих использование встроенных услуг ядра ИСИР по управлению хранимыми объектами, и два неабстрактных класса – «ИСИР-ресурс» и «структура». «Ресурс» - это логическая единица хранения, наделенная «самостоятельностью», в том смысле, что она может существовать вне зависимости от других информационных объектов, представлять первичный интерес пользователей. «Структура» - значение («зависимый объект»), существующее только в контексте логических единиц хранения (ресурсов).

Для каждого класса, как абстрактного, так и неабстрактного, задается набор допустимых свойств. Ряд свойств, называемых «ИСИР-атрибутами», используется для связывания с объектами (ресурсами или зависимыми объектами) его составных частей, которые не могут существовать независимо от объекта.

Существует возможность наследования, как для классов, так и для свойств. Для классов допускается множественное наследование, но при этом класс можно унаследовать только от одного неабстрактного класса, и от нескольких абстрактных классов.

При создании LDAP схемы ИСИР RDF- классы представляются LDAP- классами объектов, а RDF-свойства – LDAP-атрибутами. Абстрактные классы ИСИР представляются в LDAP классами типа auxiliary, а не абстрактные – классами типа structural.

Атрибуты LDAP описываются отдельно от определений классов. Для каждого класса указывается допустимый набор атрибутов. Атрибут с одним названием в разных классах имеет один и тот же смысл.

LDAP, как и RDFS поддерживает наследование классов и атрибутов. В LDAP схеме определяется базовый класс объектов, являющийся предком всех классов ИСИР isirTop. От него наследуются три класса isirAbstract, isirResource и isirStructure, служащих для представления абстрактных классов, ресурсов и структур соответственно. От этих классов наследуются все классы объектов LDAP схемы ИСИР. Также определяется базовый атрибут ИСИР isirAttribute, от которого наследуются все атрибуты ИСИР.

Полученная таким образом схема позволяет максимально использовать возможности LDAP для представления иерархии классов и свойств RDFS. Однако такая схема не использует стандартных схем LDAP, а значит, затрудняет интероперабельность с большим числом распространенных приложений LDAP, использующих стандартные схемы. Поэтому была разработана альтернативная схема LDAP для ИСИР, на основе стандартных схем.

Классы объектов для описания ресурсов ИСИР наследуются от классов стандартных схем (см. табл. 1) Определяется дополнительный класс для ресурса «Проект», классы объектов для структур и абстрактных классов ИСИР и атрибуты, которых нет в стандартных схемах. Такой подход не позволяет точно передать иерархию классов и свойств RDFS схемы ИСИР, но за счет использования стандартных схем обеспечивает интероперабельность с распространенными приложениями.

6. Виртуальный администратор

«Виртуальный администратор» - это интегрированная система управления сетевыми сервисами. Основные возможности системы включают:

- управление различным сетевым оборудованием и программным обеспечение через единую точку доступа;
- управление доступом пользователей организации к сетевым сервисам и делегирование полномочий управлении;
- сбор статистики использования сетевых ресурсов.

Большая часть современного сетевого оборудования и программного обеспечения поддерживает управление через web-интерфейс. У каждого устройства или программы своя специализированная система управления, рассчитанная на его особенности. Но доступ ко всем этим системам осуществляется с помощью обычного web-браузера. Такой подход позволяет легко создать единую точку доступа для управления объектами сети. Это просто страница, содержащая ссылки системы web управления всех объектов сети, используемых в организации.

Кроме системы управления, сетевое оборудование и программное обеспечение, как правило, имеет систему управления доступом пользователей к реализующим сетевой сервис объектам. Аналогично системам управления объектами сети, выполняющими различные и специфичные для каждого объекта сети операции записи и чтения конфигурационных параметров, системы управления доступом выполняют схожие действия. В простейшем случае это разрешение пользователю доступа к сервису, или запрет доступа. В более сложном случае, это может быть доступ только для чтения, или возможность изменения только части данных. Но хотя действия для различных объектов сети похожи, выполняются они через различные системы управления доступом с разным интерфейсом. При большом количестве объектов сети и пользователей, управление становится трудным процессом. Например, если в организации используется десять различных систем управления доступом, и необходимо поменять параметры доступа к сетевым сервисам для 20 сотрудников, то всего надо выполнить 200 действий.

Описанная выше проблема решается созданием в сети централизованного хранилища информации о пользователях, к которому могут обращаться все объекты сети. Управление доступом пользователей ведется в едином хранилище. Изменения в хранилище доступны всем сетевым объектам, что делает возможным управление через единую точку доступа. В качестве централизованного хранилища информации о пользователях в сети удобно использовать каталог LDAP.

Обладание статистическими данными работы сети помогает решить такие актуальные вопросы как разработка политики маршрутизации, учет работы отдельных пользователей, анализ безопасности сети, принятие решений о переконфигурировании сети.

Система «Виртуальный администратор» внедрена в ИМСС УрО РАН. Централизованным хранилищем информации о пользователях служит OpenLDAP - бесплатная реализация каталога LDAP. С ним взаимодействуют телекоммуникационные ресурсы института: почтовый сервер (SMTP, POP3, WebMail), прокси-сервер, обеспечивающий доступ в Интернет из института, модемный пул, обеспечивающий доступ в Интернет сотрудникам института из дома. С каталогом LDAP взаимодействует вычислительный ресурс ИМСС УрО РАН – многопроцессорный кластер МВС-1000. В каталоге LDAP хранит данные справочная система института, содержащая сведения об организационной структуре института, его сотрудниках, их публикациях и проектах. Сотрудники института имеют всего один идентификатор и пароль, с которым они могут получить доступ к любому из перечисленных сервисов.

Администрирование данных о пользователях и прав доступа к сервисам ведется с помощью разработанной консоли управления. Консоль позволяет через Web интерфейс без детального знания механизма конфигурирования сервисов создавать, удалять, редактировать учетные записи пользователей, объединять их в группы, назначать права доступа к сервисам.

Консоль позволяет делегировать полномочия управления данными в каталоге на основе организационной иерархии. Существует четыре уровня доступа к данным: администратор системы, администратор организации, администратор

подразделения и пользователь. Пользователи могут вводить и редактировать информацию только о себе. Сюда входит персональная информация, контактная информация, место работы и т.п. Пользователям доступна для редактирования не вся информация о них, а только ее часть. Например, они сами не могут назначать и удалять себе права на доступ к сервисам. Администратор подразделения имеет доступ к любой информации обо всех сотрудниках своего подразделения. Он может не только менять данные о сотрудниках подразделения, но и управлять их правами доступа. Администратор организации имеет те же возможности, что и администратор подразделения, но для всей организации. Кроме этого, администратор организации назначает администраторов подразделений. Администратор системы может менять любую информацию в каталоге и назначать администраторов организаций и подразделений. Одновременно в каждой организации или подразделении может быть несколько администраторов.

В целом, система «Виртуальный администратор» существенно упрощает управление объектами сети в организации за счет интеграции с информационными сервисами ИСИР РАН, создание единой точки доступа, через которую ведется все управление и делегирования полномочий управления доступа пользователей к ресурсом от администраторов ресурсов к руководителям подразделений.

Литература

[1] A Summary of the X.500(96) User Schema for use with LDAPv3. http://www.ietf.org/rfc/rfc2256.txt

[2] The COSINE and Internet X.500 Schema http://www.ietf.org/rfc/rfc1274.txt

[3] Definition of the inetOrgPerson LDAP Object Class. http://www.ietf.org/rfc/rfc2798.txt

[4] An Approach for Using LDAP as a Network Information Service. http://www.ietf.org/rfc/rfc2307.txt

[5] А. Н. Бездушный, А.М.Меденников, А. М. Серебряков, А. А.Филиппова. Метаданные ИСИР: определение и использование. // *Электронные библиотеки - 2001 - Том 4 - Выпуск 4*

[6] Бездушный А. Н., Масич Г.Ф., Масич А.Г., Серебряков В.А., Созыкин А.В. Интеграция сервисов управления объектами сети с информационными ресурсами посредством службы каталогов LDAP // *Тез. докл. Всероссийской научной конференции «Научный сервис в сети Интернет», г.Новороссийск*, 23-28 сентября, 2002 г.

[7] Масич А.Г., Масич Г.Ф., Созыкин А.В. Использование каталога LDAP для управления данными о пользователях сервисами корпоративной сети научного центра РАН / *Труды XXXV Молодежной школы конференции «Проблемы теоретической и прикладной математики», Екатеринбург, 2004, - с. 323-327.*

[8] Шабат В. Стратегический ВЗГЛЯД на Identity Management // Директор информационной службы, «Открытые системы», № 1 2003 г

Problems of network and information services integration. Using LDAP directories

A.V. Sozykin G.F. Masich A.G. Masich
A.N. Bezdushny

The method of the integration the identity management for the network, computation and information services is presented. The architecture of the solution is based on the open standards and multilevel component architecture of LDAP directories. Among the available configuration information of the network services, there are data ("network service metadata") that are of interest to information services. The schemes of ISIR information system metadata and standard LDAP directories are compared. The attention is given to using the LDAP directories as the repository for stored objects of information systems. The ways of RDFS schemes mapping to LDAP schemes are proposed

♣ Работа поддержана грантами РФФИ 03-07-90140в и 02-07-90305ск.