维普资讯 http://www.cqvip.com

基于 LDAP 的统一用户认证系统设计与实现*)

肖琬蓉　杨生举

(甘肃省科学技术情报研究所　兰州 730000)

摘　要　本文通过分析现有应用系统在用户管理上存在的问题,提出统一用户认证解决方案。利用 LDAP 目录服务,构建一套统一的身份认证机制及网络应用资源管理模式,实现对用户的统一身份认证、单点登录、集中鉴权以及对网络应用资源的统一管理。

关键词　目录服务,统一身份认证,单点登录,集中鉴权

Design and Implementation of Unified Identity Authentication System Based on LDAP

XIAO Wan-rong　YANG Sheng-ju

(Gansu Institute of Sci. & Tech. Information, Lanzhou 730000, China)

Abstract　This article puts forward the solution of unified Identity authentication by analyzing the questions of existing application system's user management. By LDAP directory service to construct a mechanism of unified identity authentication and a mode of network application resource management to realize unified identity authentication, single sign-on, concentrate on authorizing and unified management of network application resources.

Keywords　Directory services, Unified identity authentication, Single sign-on, Concentrate on authorizing

0　引言

近年来,随着网络信息化建设的不断深入,网络应用日益丰富,使得网络管理特别是用户管理变得越来越复杂[1]。由于现有网络应用系统的用户信息相互独立,用户管理与维护模式不尽相同,各应用系统采用独立的身份认证机制对用户进行认证授权,用户在进入不同系统时,需要多次输入帐号、口令等身份标识信息来通过系统的认证。这不仅给系统的日常运行维护带来很大不便,而且照成资源上的浪费和安全上的隐患。为此,亟需构建一个通用、完善、安全、易于管理、可扩展的统一用户认证管理体系,来实现用户的身份认证及网络应用资源的统一管理。基于 LDAP 目录服务的引入为统一身份认证和用户信息的集中管理提供了一个强有力的工具。

1　系统总体设计

本系统通过分析甘肃科技网络现有应用系统在用户管理上存在的问题,提出统一用户认证解决方案,利用 LDAP 目录服务中提供的分布式服务,将用户基本信息、用户管理信息、网络应用资源信息以及用户对网络应用资源的访问权限等以目录树的形式加以组织存储,并在此基础上提出一套统一的用户身份认证及网络应用资源管理模式,从而实现对用户的统一身份认证、单点登录(SSO)[2]、集中鉴权以及对网络应用资源的统一管理。有效解决了用户重复登录和多点帐号管理的问题,避免不同应用系统独立进行用户认证所造成的重复开发,方便了用户,简化了管理过程,提高新应用系统的开发效率和整体安全性。

1.1　系统体系结构

基于目录服务的统一认证系统是一个集中的用户认证管理集成环境,用来管理和分发用户的权限和身份,并为不同的应用系统提供用户和权限管理服务。如图 1 所示,统一认证系统主要包括 LDAP 目录数据库、目录服务系统和应用服务系统三部分,其中 LDAP 目录数据库是系统的核心,用于存储用户数据;目录服务系统用于提供基于 Web 方式的用户管理、身份认证和服务授权;应用服务系统由应用程序接口和若干应用服务器组成,围绕着 LDAP 的应用功能编写相应的程序接口,通过将应用服务器中的认证模块修改为使用接口的程序,来实现利用目录服务进行统一身份认证的功能。

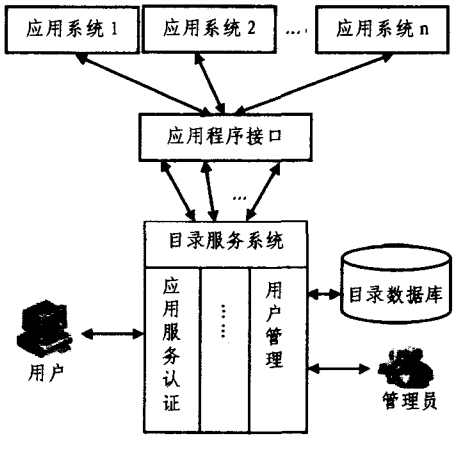

图 1　统一认证系统结构图

1.2　系统体系结构原理

使用统一身份认证平台来接管各个应用中的认证模块,从而将原先独立的应用系统有机地整合在一起。对于用户而言,只要登录统一身份认证服务后,即可使用所有支持统一身

*)基金项目:甘肃省自然科学基金项目"基于 LDAP 的甘肃科技网络统一用户认证系统应用基础研究"(编号:3ZS061-A25-041)。肖琬蓉　高级工程师,主要研究方向为 Web 开发研究;杨生举　硕士研究生,主要研究方向为计算机软件与数据库开发研究。

维普资讯 http://www.cqvip.com

份认证服务的应用系统，统一认证模式流程如图 2 所示，工作原理如下：

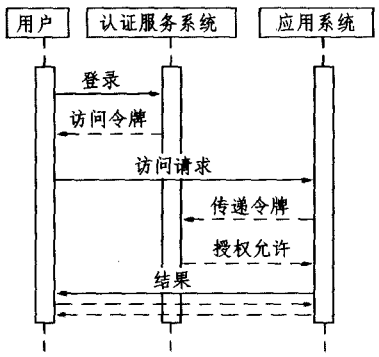

图 2　统一认证过程流程图

1)用户通过输入用户名和密码，向用户认证系统发出认证请求；

2)认证服务器验证用户提供的信息，如果匹配成功，它将返回令牌给客户端；

3)客户端向应用系统发出服务请求，同时向应用系统传送该令牌；

4)应用系统在收到请求后，将令牌传递给认证服务器；

5)认证服务器验证令牌是否存在，如果成功，将授权允许指令返回给应用系统；

6)应用系统接收到授权指令后处理客户的请求，并将结果返回给客户端。

1.3　系统功能模块

本系统包含两个子系统，即提供普通授权用户服务的前台统一认证服务子系统和用于系统管理员维护系统的后台统一认证管理子系统(如图 3 所示)。其中前台统一认证服务子系统功能模块包括：用户注册、统一认证、修改密码、信息维护；后台统一认证管理子系统功能模块包括：日志管理、用户管理和应用管理。

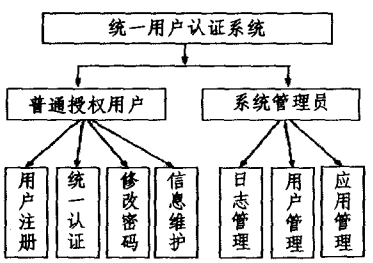

图 3　统一认证系统功能模块

1) 用户注册　授权用户的注册和帐号同步；

2) 统一认证　为不同应用系统提供单点登录界面；

3) 修改密码　授权用户对密码的变更；

4) 信息维护　授权用户对注册信息的更新及应用系统权限的修改；

5) 日志管理　对各种操作日志记录的保存与管理；

6) 用户管理　对所有用户信息及权限的管理；

7) 应用管理　对应用系统的设置管理。

1.4　LDAP 设计

1.4.1　LDAP 目录服务

LDAP(Light Directory Access Protocol，轻量级目录访问协议)是目录访问协议的一种，它是对 X.500 目录访问协议的移植，但是简化了实现方法，所以称为轻量级目录服务。目录服务就是按照树状信息组织模式，实现信息管理和服务接口的一种方法。它能够提供快速响应和大容量查询并且提供多个目录服务器的信息复制功能，具有广泛的数据整合和共享能力，支持分布式的信息访问和数据操作功能，并有着强大的授权认证机制和精细的访问控制，比一般的数据库更具安全性，同时元目录功能允许快速、简洁地与现存基础结构进行集成，从而使用户信息方便管理，访问起来速度快捷。LDAP 目录服务的这些特性使其成为实现统一用户认证管理的首选方案。

1.4.2　LDAP 类型定制

由于存放在 LDAP 目录中的数据形式的多样性与用户的实际应用需要，LDAP 提供了定制的功能[4]。由于甘肃科技网络用户的类型与一般 LDAP 目录中自带的有关人员的类型相比，需要一些特殊的属性，因此，定义甘肃科技网络用户类型为对象类型 gsinfouua，gsinfouua 用到了一些自定义的属性类型，也包含了一些 LDAP 自带的属性类型，该类型的定义如下：

```
objectclass ( 1.3.6.1.4.1.6056789.2.2.2.1 NAME'gsinfouua'
DESC'gsinfouua'
MUST ( uid $ userPassword $ email )
MAY (ufax $ uaddress $ uunit $ usernameGskjcgPerson $ usernameGskjcgUnit $ usernameMailAdmin $ usernameQKGL $ usernameMeeting $ usernameIOA $ usernameIPP $ usernameCX $ usernameUDRP $ usernameSiteShare $ usernameMail $ PasswordGskjcg Unit $ PasswordGskjcgPerson $ PasswordMailAdmin $ PasswordQKGL $ PasswordIOA $ PasswordMeeting $ PasswordCX $ PasswordIPP $ PasswordUDRP $ PasswordSiteShare $ PasswordMail $ authority $ streetAddress $ postalCode $ telephoneNumber $ fax MYMcustomerno $ uregdate $ ulogintime $ ulastlogindate $ token $ laibinzhanghao $ zhanghaoxuke $ houtaifabu $ uusername $ balance $ uusertype $ udepartment $ ucity $ ustate ))
```

1.4.3　LDAP 目录设计

LDAP 是以目录信息树 (Directory Information Tree，DIT)为存储方式的树型存储结构，目录信息树及其相关概念构成了 LDAP 协议的信息模型。DIT 由条目(entry)构成，每个条目具有若干个属性(attribute)，每个属性可以有多个值(values)。条目由相对特异名 RDN(Relative Distinguished Name)来标识，RDN 和它所有祖先节点的 RDN 按从上到下的顺序串连起来，就是它的特异名 DN(Distinguished Name)，DN 用来唯一标识一个条目。DN 结构中，常用的属性有 dc(组织域名)、ou(组织单元)、cn(项普通名)、uid(用户标识)[5]。本系统中的目录信息包括组织结构、人员信息、资源和权限信息，并作为数字证书的存放库。应用系统在注册时，根据这些信息决定用户是否可以使用该服务，决定每个节点应具有哪些属性，以及这些节点怎样组织成一个结构合理的目录信息树是目录设计的目标，也是统一身份认证系统设计的关键步骤，图 4 给出了系统的目录树设计。

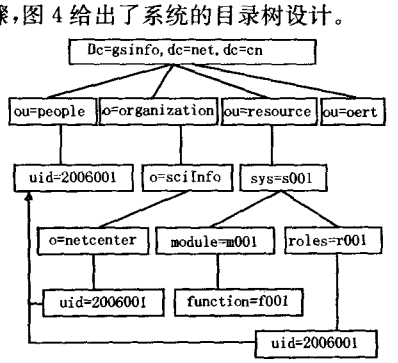

图 4　统一用户认证中 LDAP 目录结构设计

在这个 LDAP 目录结构中，dc＝gsinfo，dc＝net，dc＝cn

维普资讯 http://www.cqvip.com

作为整棵树的 Root DN。人员(ou=people)子树中每个项存放的是甘肃科技信息网中每个人的基本信息,其中还包括了该人在本系统内所属的角色列表。组织(o=organization)下的子树,是按照一般组织的分级结构组织存放,从概念上直观反映了组织间的上下级关系,非常易于理解。每个组织有自己的各种属性,组织下可以分为各个子组织,最低一级子组织子树下包含属于该组织的人员列表,这里每个人只是一个索引,指向人员子树下具体的某个人员。资源(ou=resource)子树下主要是分为甘肃科技网络内的各个系统,这棵子树控制着访问的权限。一个系统代表一个具体的服务,每个系统又划分为多个模块,每个模块可能还会有多个功能。

2 系统实现

2.1 前台统一认证服务系统

2.1.1 用户注册

用户注册分为两种情况:(1)用户已有信息发布系统、业务管理系统、异构检索系统、邮件系统其中的一个或多个帐号。在这种情况下,用户注册时,除了填写基本信息如登录名、密码、姓名、单位名称等等,还要进行帐号同步(或称之为帐号关联)。帐号同步就是把原有各系统的帐号跟本系统的帐号对应起来,做一次关联,以后进入各系统时,只需记住一个统一的帐号就可以了,但在本系统中通过链接进入各系统时,本质上还是调用的原来各系统的帐号。这样处理的好处是为了和以前的用户帐号相兼容。(2)全新注册,即没有上述系统的任何帐号。在这种情况下,用户只需填写基本信息如登录名、密码、姓名、单位名称等即可,这个统一的帐号包括了以上各系统帐号的所有属性。

2.1.2 统一认证

用户访问系统时,将用户名和密码提交给目录服务系统,目录服务器将其与目录数据库中的数据进行比较,合法用户可以通过 LDAP 认证。由于采用了异步 XML 调用(AJAX)技术,当用户输入用户名,光标离开输入框时,如果目录服务器中不存在该用户名,会弹出提示框,要求用户重新输入,并且光标直接定位在用户名输入框,本页面不刷新,方便用户操作;若密码或验证码不正确,会弹出提示框,要求用户重新登录,本页面并不刷新,正确的用户名的输入仍然保留,不用用户重新输入。

用户进入系统后,可通过统一登录界面,进入相应的应用系统。如果用户拥有该应用系统的访问权限,直接点击该系统名称的链接即可访问该系统;如果用户没有该应用系统的访问权限,则该应用系统的名称上没有链接,用户也就无法访问该系统。

2.1.3 修改密码

授权用户在登录系统后,便可在修改密码界面变更自己的密码。密码是经过加密处理的,即使管理员也无法知道该用户的密码。

2.1.4 信息维护

注册用户的详细信息如单位地址、单位名称、电话号码、Email 等都可以在信息维护模块中进行修改。为了和原有的应用系统的帐号兼容,这里还提供了对访问应用系统的权限和帐号的修改。

2.2 后台统一认证管理系统

2.2.1 日志管理

本功能模块只对具有系统管理权限的管理员可见,用于系统的维护,对普通授权用户不可见。对各种操作保存完整日志记录,便于查找和管理。管理员可以根据登录名称和日期范围来查询日志信息,包括登录者的登录名、IP 地址,所访问的应用系统和访问日期等。管理员还可以对所查询到的日志信息进行删除操作。

2.2.2 用户管理

本功能模块只对具有系统管理权限的管理员可见,用于系统的维护,对普通授权用户不可见。管理员可根据登录名或用户姓名查询用户的详细信息,并可对详细信息或用户的权限进行修改或删除操作。

2.2.3 应用管理

应用系统要接入统一身份认证系统,必须在应用管理模块内注册其基本信息。统一身份认证系统确认应用系统的名称、域名、原登录地址和应用系统简介后,设置哪些用户可以访问该应用系统和指定某个用户是该应用系统的管理员。

2.3 目录服务器安装配置

2.3.1 目录服务器安装

1) 安装 Berkeley DB 4.2.52 由于 OpenLDAP 需要 Berkeley DB 来存放数据,因此需先安装 Berkeley DB 4.2.52:

```
# tar -zxvf db-4.2.52.tar.gz
```

解完压后,会生成一个 db-4.2.52 目录,进入该目录下的 build_unix 目录。执行以下命令进行配置安装:

```
# ../dist/configure
# make
# make install
```

该软件默认是安装在/usr/local/BerkeleyDB.4.2 目录下。安装完成后,要把/usr/local/BerkeleyDB.4.2/lib 的库路径加到/etc/ld.so.conf 文件内,添加完成后执行一次 ldconfig,使用配置文件生效。这样编译 OpenLDA 时才能找到相应的库文件,资料库也就安装完成了,接下来安装 OpenLDA。

2)安装 OpenLDAP,在 Linux AS release 4 的命令行下,直接输入命令 #./configure, # make, # make install 进行安装。安装完毕后,相应的执行文件主要包括:

/usr/local/openldap/libexec/slapd 是单独运行的 LDAP 守护进程,它监听客户端请求,端口号为 389。

/usr/local/openldap/sbin/slaptest 测试的配置文件语法是否正确。

/usr/local/openldap/bin/ldappasswd 为 LDAP 添加使用者密码。

/usr/local/openldap/sbin/slappasswd 设置管理员的密码。

/usr/local/openldap/libexec/slurpd 是单独运行的更新和复制进程,它能够把本地数据库的变化通知相关服务器进行更新。

/usr/local/openldap/bin/ldapadd,/usr/local/openldap/bin/ldapdelete,/usr/local/openldap/bin/ldapsearch,/usr/local/openldap/bin/modrdn 等是 LDAP 的客户端软件,能够完成对目录的查询、删除、修改、添加等功能。

2.3.2 目录服务器配置

OpenLDAP 把所有与 LDAP 服务器有关的配置项都放在 slapd.conf 文件中,该文件存放在/openldap/etc/openldap 目录下。配置文件如下所示:

```
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
```

维普资讯 http://www.cqvip.com

```
include /usr/local/openldap/etc/openldap/schema/core.schema
include /usr/local/openldap/etc/openldap/schema/cosine.schema
include /usr/local/openldap/etc/openldap/schema/nis.schema
include /usr/local/openldap/etc/openldap/schema/inetorgperson.schema
include /usr/local/openldap/etc/openldap/schema/dns.schema
include /usr/local/openldap/etc/openldap/schema/gsinfoaccount.schema
include /usr/local/openldap/etc/openldap/schema/gsinfouua.schema
# Define global ACLs to disable default read access.
pidfile /usr/local/openldap/var/run/slapd.pid
argsfile /usr/local/openldap/var/run/slapd.args
database bdb
suffix"dc=gsinfo,dc=cn"
rootdn"cn=root,dc=gsinfo,dc=cn"
# Cleartext passwords, especially for the rootdn, should
# be avoid. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw jsj322
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory /usr/local/openldap/var/openldap-data
# Indices to maintain
index objectClass eq
```

2.4 目录信息数据导入

目录信息导入有两种方法：即从命令行手工输入和通过数据库交换文件 LDIF 导入。从命令行手工输入是最直接的一种，但是对于大批量的数据，工作量很大；LDAP 提供一种更加简明的目录信息表达方法——数据库交换文件 LDIF，用于导入和导出目录信息。它是目录交换格式文件，以文本方式来表示 LDAP 中的条目。采用这种方法不需要启动目录服务进程，当需要创建大批量的条目时，使用这种方法比较适合。

总而言之，比起从命令行手工输入数据，LDIF 文件有着明显的优势，但必须遵守正确的语法来将用户信息输入文件，并将它导入目录中。

结束语 目前，本系统已应用于甘肃科技信息网的网络运行中，并在甘肃科技网络的建设中发挥着重要的作用。一方面降低了网络应用系统中用户管理的成本，提高了新应用系统的开发效率，尤其提供包括单点登录在内的认证服务，在应用系统集成中发挥了显著的作用，成为甘肃科技网络构架中不可缺少的一部分。另一方面有了通用的用户信息基础结构，可以集中管理用户角色，制定安全策略，减少各应用系统权限管理的维护量，提高工作效率和整体安全性。

参 考 文 献

[1] 焦静，李勇. 基于 LDAP 的统一身份认证的设计与实现[J]. 科学技术与工程，2007，7(4)：646-649

[2] 胡毅时，怀进鹏. 基于 Web 服务的单点登录系统的研究与实现[J]. 北京航空航天大学学报，2004，30(3)：236-239

[3] 涂德志. LDAP 协议研究与 LDAP 服务器的设计与实现[D]. 电子科技大学，2002(5)

[4] 许鑫，苏新宁，陆炯. 数字化校园身份认证系统的设计. 现代图书情报技术[J]，2005(4)：51-57

[5] 宋志伟. LDAP 协议研究[D]. 南京理工大学，2003(1)

(上接第 287 页)

其中 288 项功能(占总功能项数的 92%)由自动生成平台生成，自动生成的功能中有 11 项进行了二次定制与维护。

表 1 治安管理信息系统功能简表

	修理业	报废业	印刷业	合计
录入/编辑	46 项	42 项	44 项	132 项
查询	31 项	28 项	25 项	84 项
统计	22 项	19 项	18 项	59 项
布控报警	16 项	16 项	7 项	39 项
合计	115 项	105 项	94 项	314 项

上述系统借助自动生成平台用时 4 个月即开发调试完成，并通过了公安部关于此类治安管理信息系统的现场测试，目前已在陕西省咸阳、榆林等地市实施运行。

结束语 本文提出了一种基于代码生成的 Web 信息系统工程化开发方法，实践证明可以有效缩短以数据库为核心的 Web 信息系统开发周期。提出了类似编译器基础架构的特定域软件体系结构，实现了前端与后端的共享；提出的专用代码方法将生成的业务逻辑代码与界面呈现代码分离，提高了目标系统的可定制性与可维护性；并采用多表关联、基本操作组合以及数据库驱动的目标平台无关工作流机制支持了复杂模式业务逻辑的自动生成，适应了复杂 Web 信息系统的实际开发需要。

同一类业务的不同目标平台后端的核心逻辑是类似的，主要区别是待生成的目标平台的基本语句语法不同，因此后端的可重用性有待进一步加强。此外，在实际的 Web 信息系统中，仍存在一些第 5 节中采用的手段无法支持的复杂业务模式，这些业务模式在一定应用领域内具有较强的通用性。如何增强代码生成后端的可重用性以及支持应用领域内通用的复杂业务模式，是下一步的研究重点。

参 考 文 献

[1] Struts. http://struts.apache.org/

[2] Hibernate. http://www.hibernate.org/

[3] Ruby on Rails. http://www.rubyonrails.org/

[4] .NET Maker. http://www.hkvstore.com/aspnetmaker/

[5] UCML. http://www.ucml.com.cn/cpzx.asp

[6] 徐世莲. 基于软件体系结构的 WEB_MIS 应用平台设计. 计算机科学，2006，33(9)

[7] 刘坚. 编译原理基础. 第 1 版. 西安：西安电子科技大学出版社，2002：64

[8] Christopher A，Simmon C，Catherine A C. 关系数据库和 SQL 编程. 第 1 版. 皮人杰，等译. 北京：清华大学出版社，2005：164

[9] http://www.wisdomstock.com/web/hmrj.asp