统一用户管理系统在气象行业的应用①

李 强, 何 遂, 李光兵, 吉 莉

(重庆市北碚区气象局, 重庆 400700)

摘 要: 研究了利用LDAP技术和单点登录技术在气象行业建立统一用户管理系统的思路和方法. 通过对气象业务应用系统现状进行分析, 提出了一种基于LDAP目录服务和单点登录技术的统一用户管理系统解决方案, 详细介绍了 LDAP 目录的建立、身份认证和单点登录的实现过程. 同时, 简要介绍了建立该系统的流程. 统一用户管理系统的应用, 可以有效实现气象系统网络信息资源的整合, 使得用户认证和访问控制更加高效, 管理更加方便.

关键词: LDAP; 统一用户管理; 单点登录; 气象业务

Application of the Unified User Management System in the Meteorological Industry

LI Qiang, HE Sui, LI Guang-Bing, JI Li

(Chongqing Beibei District Meteorological Bureau, Chongqing 400700, China)

Abstract: Study on the ideas and methods of using the technology of LDAP and single sign-on technology to establish a unified user management system in the meteorological industry. According to the analysis of the status of the existing meteorological business applications, this paper proposed a solutions program based on the LDAP directory services and single sign-on technology. Focus on the establishment of an LDAP directory, authentication and single sign-on. At the same time, it briefly introduces the establishment of the system flow, so that the user authentication and access control is more efficient, and management more convenient.

Key words: LDAP; unified user management; single sign-on; meteorological operations

随着信息技术的发展, 网络信息系统在气象行业得到了广泛应用, 并且有不断发展的趋势. 由于应用系统是在不同年代、由不同的团队、运用不同的技术开发建设的, 各系统间形成了各自独立的认证机制和访问控制, 对使用和维护都带来极大不便, 并且不利于扩展和级联. 随着业务系统的增加, 暴露出来的问题也越来越多, 并对气象事业的发展产生了不利影响, 建立一套统一的用户管理系统已显得迫切和重要. 大量研究[1-10]表明, 利用 LDAP 目录服务和单点登录技术是一个理想的解决方案, 可以有效的解决用户统一管理、统一认证、集中授权等一系列问题. 目前, 这类系统已经应用到学校[11]、保险[12]、互联网等行业的实际工作中. 本文就如何在气象行业中建立起统一的用户管理系统进行分析与研究.

1 背景和目标

对社会公众来说, 气象业务可能就是指天气预报, 然而事实并非如此. 一般情况下, 气象业务可分为大气探测、天气预报、气象服务、人工影响天气、气象行政执法等类别, 其中各项又可细分, 种类繁多. 比如大气探测可分为地基、天基、空基三种类型; 天气预报可以分为短期天气预报、短期气候预测、农业气象预报、海洋气象预报等; 气象服务可分为公众气象服务、决策气象服务、气象预警、气象保障服务等. 除此之外, 还有其它分类方式, 总而言之, 气象业务的特点就是种类多, 涉及面广泛.

面对这些气象业务工作, 管理部门或上级部门为了提升工作效率, 往往开发了与之相适应的业务系统. 通常情况下, 这些业务系统的使用范围是以省、市级

① 基金项目:重庆市气象局业务技术攻关项目(Ywgg-201217)
收稿时间:2012-12-25;收到修改稿时间:2013-01-23

行政辖区划定的，省、市级气象业务主管机构负责管理，具有典型的区域性特征(中国气象局统一要求的除外). 在一个新系统投入使用时，各业务主管部门会为业务人员分配用户 ID，而区、县气象部门人员较少，往往存在职能交叉和一人多岗的情况，这就意味着大多数工作人员拥有多个用户 ID，不利于识记. 另一方面，在每次分配 ID 的时候都遵循一定的组合原则，加上部分业务人员不修改密码的习惯，其他人可以很容易的登录某个系统进行非正常操作，容易造成安全隐患. 管理者和业务人员都希望对这种情况进行改进，建立一个统一的用户管理系统是有必要的.

针对气象业务系统的现状，建立统一的用户管理系统的目标是实现用户集中管理、统一认证、集中授权，支持正向扩展、反向兼容，同时保证系统的稳定性和安全性. 主要体现在三个方面:

管理者角度: 提供统一的用户管理方法，可以快速进行用户信息的维护以及权限的分配. 在一个新的业务系统投入使用时，只需简单操作就可以实现数据共享，不必每次进行 ID 的分配. 系统应具有很好的安全性和可扩展性，并且拥有图形化操作界面.

用户角度: 登录所有应用系统都使用唯一的用户名和口令(或数字证书)；当用户登录后，可以在所有授权系统间进行切换，而不必重复登录；当一个新业务系统投入使用时，可以使用原来的 ID 登录；用户在一个系统内进行了信息修改，可以同步到其他所有系统，保持信息的高度一致性.

开发者角度: 系统具有较高的兼容性，对旧的业务系统能够尽量少改或不改程序就可以实现兼容；提供公共的访问接口，使新业务系统能快速接入服务.

2　关键技术

2.1　轻型目录访问协议

轻型目录访问协议[13](Lightweight directory access protocol，简称 LDAP)，是目录访问协议的一种，它是对 X.500 的目录访问协议的移植，对实现方法进行了简化. 同时 LDAP 是一种标准、开放、可扩展的目录访问协议，它把网络环境中的各种资源都作为目录信息，在目录树结构中分层存储，对这些信息可以存储、访问、管理并使用，是支持网络系统的重要底层基础技术之一[14]. 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.

2.2　单点登录技术

单点登录[15](Single Sign On，简称为 SSO)，是目前比较流行的企业业务整合的解决方案之一. SSO 的定义是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统. 它是企业应用集成在“身份认证”层面的整合.

3　详细设计

基于统一用户管理的目的，核心思想就是将用户身份、权限等信息集中在一起进行管理. 系统采用 LDAP 服务器存储与用户相关的信息，用关系数据库存放与各系统相关的业务数据. 当用户通过浏览器访问应用程序时，将用户名和密码提交给管理系统，管理系统与 LDAP 目录服务器进行信息比对确定用户身份的合法性，进而提供访问服务. 系统管理员拥有管理权限，可以对用户信息进行修改和权限分配. 图 1 是系统的总体结构图.

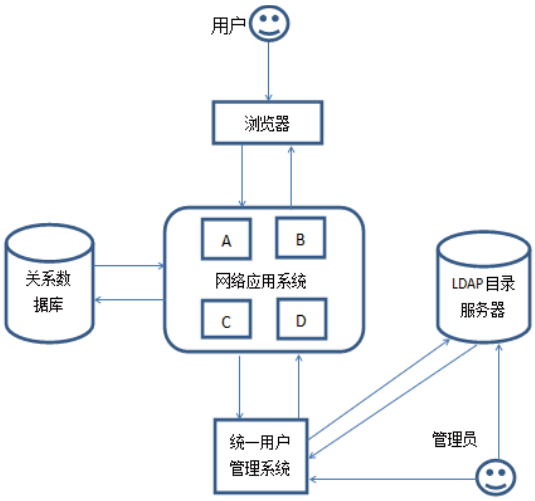

图 1　统一用户管理系统的总体结构图

3.1　LDAP 目录设计

LDAP 目录是统一用户管理系统的重要组成部分，它以树形结构进行组织. 实现统一用户管理系统的关键是如何将机构、角色、权限、网络资源、用户信息等数据利用 LDAP 目录树组织起来并进行有效管理.

LDAP 目录树中，一个结点对应一个项目实体，项目的命名称为标识 DN(Distinguished name). DN 由若干元素构成，每个元素称为相对标识(Relative Distinguished Name, RDN), RDN 由项目的一个或多个属性构成. 目录树中每个结点均有自己的惟一标识 DN，数据实体间的关系由 DN 来关联.

根据目录构成方法和系统的需要，定义五种元数据类型，分别为 o=组织结构，ou=人员，ou=组织角色，cn=网络资源，ou=权限，五个类型都是根目录(root)下的分支，构成根目录下的五棵子树. 组织(o=组织结构)下可建立分支机构，分支机构下可以建立部门，部门下面包含部门的人员索引；人员(ou=人员)子树下存放组织内所有人员的基本信息，包括角色信息、ID 号等；组织角色(ou=组织角色)是由多种角色组成，如管理员、二级管理员、普通用户等，角色具有三个属性“角色名”、“角色简介”、“与角色相关的权限”；网络资源子树(cn=网络资源)用于存放网络资源(如预报系统、防雷系统、服务系统等)的基本信息，包含“资源名”、“资源描述”、“URL”等属性，各资源结点下又可以包括子资源；权限(ou=权限)是各种权限的集合，权限由“权限名”、“权限资源”、“拥有该权限的角色”等属性组成. 整个目录中，人员不直接与权限产生关系，而是通过角色与权限进行关联，资源通过权限和角色进行关联，形成的完整的组织关系. 图 2 是 LDAP 树形目录结构图，目录通过属性进行关联，主要表达的意思是：组织中拥有若干人员，每个人员可以扮演一个或多个角色，每个角色拥有一个权限，每个权限可以访问一些授权的网络资源.

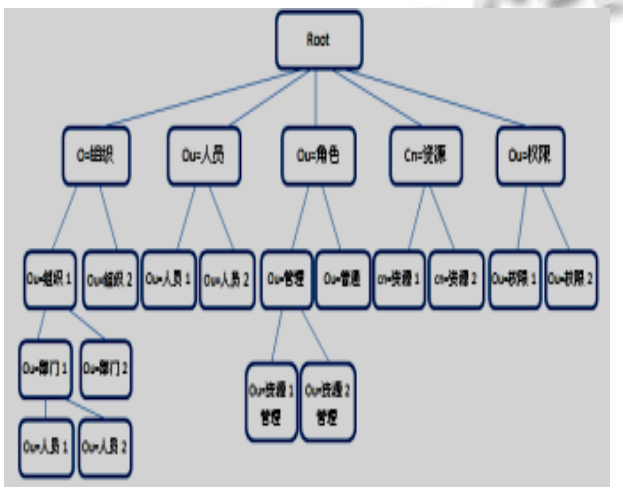

图 2 LDAP 目录树形结构图

3.2 身份认证与单点登录

前一节介绍了如何建立起一个 LDAP 服务目录，本节主要介绍如何利用这个目录实现身份认证与单点登录. 身份认证是指对用户的身份信息进行验证，确认用户身份的合法性. 用户访问一个网络应用时，必须经过身份验证并确认合法后，才可以成功登录进行相关操作. 通常情况下，用户的身份信息是与其它业务数据一起存储在关系数据库里的，用户提交访问请求时将用户名和密码与数据库中存储的信息进行比对，以此来验证用户身份的合法性. 这种情况在一个业务系统中是可行的，当业务系统比较多时，问题就变得相对复杂了，而利用 LDAP 服务目录则正好可以解决这种问题. 图 3 是用户身份认证的流程图，下面分条进行陈述:

(1) 用户通过浏览器访问一个业务系统;

(2) 将用户的身份认证信息(用户名和密码)提交到业务系统;

(3) 业务系统接到登录请求后，将用户信息提交到统一用户管理系统进行认证;

(4) 将用户身份信息到 LDAP 目录中进行验证，如果是合法用户，返回到统一用户管理系统;

(5) 认证成功，获得证书或授权，并将所有的授权信息一并获取，为单点登录作准备;

(6) 将认证信息返回到业务系统;

(7) 用户成功登录;

(8) 内容通过浏览器显示出来，用户可以使用，还可以切换到其它已授权的业务系统.

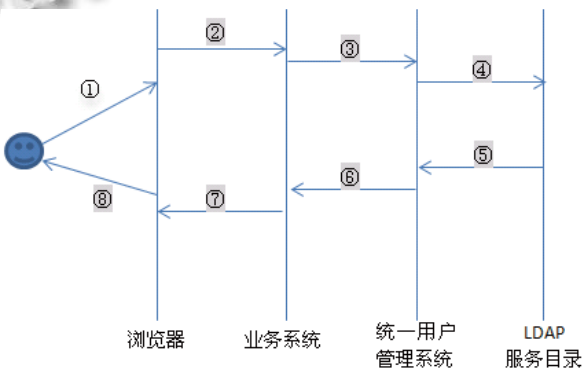

图 3 用户认证流程图

图 3 是基于 LDAP 的统一用户管理系统的身份认证和单点登录的一般过程. 单点登录的产品很多，如 IBM Tivoli、Oracle Esso 等，还有大量的开源 SSO 产品，

实现的技术主要是采用 Cookie 和 Session.

3.3 登录方案设计

在整个业务体系内，有的用户要使用多个业务系统，有的用户只使用其中一个或两个业务系统. 为了满足用户需求的多样性，需要一个完善的登录方案. 对于多需求用户，通过一个统一的入口获得授权系统列表，再进行下一步的操作；对于需求单一的用户，可以直接通过感兴趣的系统进行登录，然后使用. 图 4 就是针对两种用户提出的两种访问方式，可以很好的满足不同用户的需求.

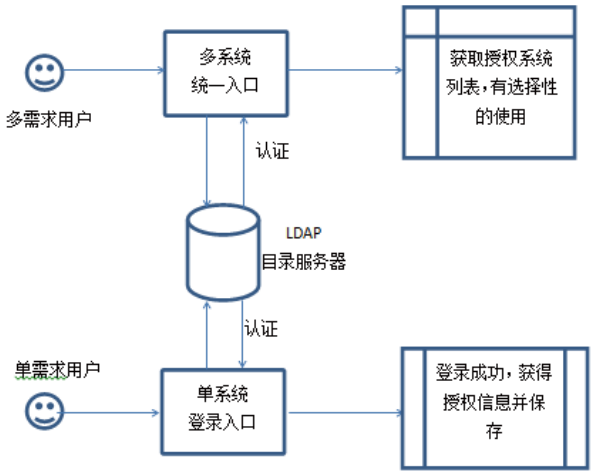

图 4 两种用户访问方式

3.4 兼容性和扩展性

针对目前已经建成的业务系统，实现两者之间的兼容性值得进一步讨论. 当然，重新开发是不现实的，这里有两种方法可以解决这个问题：一是修改各系统的登录认证程序，将认证模块指向统一用户管理系统和 LDAP 目录，然后重新分配权限；另一种是建立起各系统的用户与 LDAP 目录间的映射，引入认证代理模块实现登录认证. 笔者更倾向于使用第一种方法. 不管是哪个系统，身份认证部份的程序都不复杂，修改起来比较容易，并且效果更好；另一方面，气象部门的人员数量不大，重新分配权限也不需要太多的时间.

对于新系统的扩展，比起兼容性来说那要简单得多. 当在开发一个新系统时，不必再建立用户信息数据库，只需要将登录认证的程序指向 LDAP 目录即可，利用 LDAP 的目录服务实现访问控制. 因此，基于 LDAP 的系统是易于扩展的，并且节约开发成本.

4 系统实现方案

通过分析，利用 LDAP 技术在气象行业建立统一用户管理系统是可行的. 由于气象台站分布广泛，受气候和行政辖区的影响，各地使用的业务系统并不完全一样，具有典型的地域性特征. 因此，在省或市辖区建立统一用户管理系统是合理的思路，既可以满足管理的需要，又可以满足业务的需要. 然而，气象业务是一种日常工作，同时也是非常重要的工作，不能随便被中止和影响，因而在建立系统的同时需要全方位考虑，制订切实可行的实施方案.

首先，确定统一用户管理系统的覆盖区域. 比如在重庆市气象系统内建立统一用户管理系统，这个区域就是重庆市的各级气象部门，包括市级机关、职能处室、直属事业单位、区县级气象部门.

第二，搜集用户信息和已建成的业务系统信息，以便于前期规划的后期工作. 用户信息应包括全面，包括个人基本信息、职能信息和所处的单位信息. 业务系统信息应包括系统的名称、功能作用、URL、用户信息、认证方式、开发语言等.

第三，整理用户信息和业务系统信息，建立统一用户管理系统. 这里指的是建立 LDAP 目录服务器，对用户进行授权.

第四，修改原有业务系统的认证方式. 对业务系统进行修改时，必须保证不影响业务工作的正常开展.

第五，对业务系统进行整合，建立统一的用户认证系统及引导界面.

第六，系统测试，优化完善.

5 结语

气象部门业务种类众多，大量业务系统的开发应用在某些情况下对工作效率有一定的提高，但同时也增加了管理和使用的麻烦. 建立基于 LDAP 目录的统一用户管理系统可以实现用户信息与网络资源的整合，具有安全、快速、高效、可扩展的特点，可以很好的解决统一用户管理、统一用户认证、集中权限分配等问题. 应用这个系统，可极大的方便人事部门对人员的管理，提高管理效率，节约管理成本，保持用户信息的高度一致性；业务系统的使用者可以很方便的使用已授权的业务系统，不再需要识记大量的用户名和密码，给用户提供了便利；当引入一个新的系统时，不必再建立用户数据库，不必再编写认证代码，只需

(下转第 80 页)

仅提高信道利用率和识别标签速度, 还从根本上提供系统吞吐率, 该算法系统吞吐率明显优于其它各种ALOHA 算法.

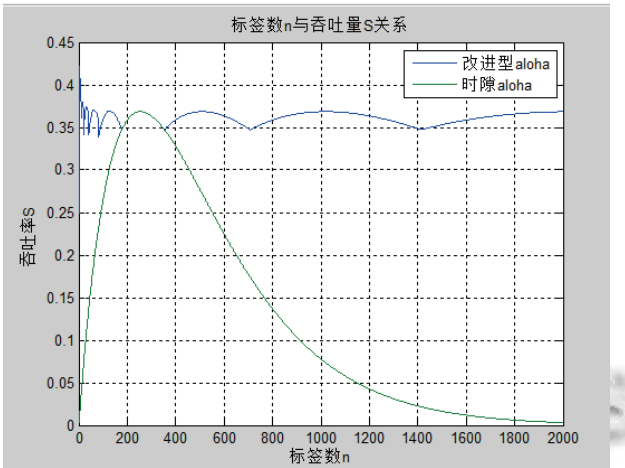

图4 改进分组动态时隙 ALOHA 算法与时隙 ALOHA 算法吞吐率对比

4 结语

本文提出一种改进分组动态时隙 ALOHA 算法, 该算法通过每一帧结束后对下一帧时隙标签数量进行预估, 并根据预估标签数量对标签进行分组, 同时动态匹配最佳帧长. 改进后算法系统吞吐率不仅不受标签数量限制, 也提高系统吞吐率.

参考文献

1 游战胜,刘克胜.无线射频识别技术(RFID)理论与应用.北京:电子工业出版社,2004.1–18.
2 尹君,何怡刚,李兵.基于分组动态帧时隙的 RFID 防碰撞算法.计算机工程,2009,35(20):267–269.
3 曹新宇,杨虹蓁,赵云峰.RFID 技术中防碰撞算法研究与改进.北华航天工业学院学报,2010,20(1):6–8.
4 Hale WK. Frequency assignment: Theory and applications. Proc. of the IEEE,1980,68(12):658–661.
5 Vogt H. Efficient Object Identification with Passive RFID Tags. Pervasive 2002, LNCS 2414, 2002:98–113.
6 王永,基于 EDFSA 算法的改进研究.计算机与数字工程,2011,3(39):18.
7 徐海峰,姜晖.RFID 系统实时高效 ALOHA 防冲突算法研究与仿真.计算机与数字工程,2011,5:19–26.
8 徐圆圆,曾隽芳,刘禹.基于 Aloha 算法的帧长及分组数改进研究.计算机应用,2008,28(3):588–590.

(上接第 48 页)

在用户管理系统的里进行授权即可. 因此, 这对气象工作的开展是非常有益的.

参考文献

1 肖琬蓉,杨生举.基于 LDAP 的统一用户认证系统设计与实现.计算机科学,2008,35(5):298–301.
2 沈阳,杜中军.基于 Kerberos 协议的单点登录研究与设计.计算机工程与设计,2011,32(7):2249–2350.
3 夏明忠,夏以轩,等.统一用户认证和授权管理的实现.计算机与应用化学,2011,28(8):1087–1090.
4 朱亚兴.异构环境中基于 EJB 和 CORBA 的统一用户管理系统设计.微型机与应用,2010,29(15):6–9.
5 张海藩.软件工程导论.第 5 版.北京:清华大学出版社,2008.
6 刘鹂娟.统一用户数据库的分析和设计.现代电信科技,2009(4):57–60.
7 张秋余,蔡志鹏,袁占亭.一种安全的单点登录系统口令同步方案.计算机工程,2011,37(17):122–123.
8 卫建国,王建林,庄立伟.气象软件设计模式的研究与实现.计算机工程,2010,36(9):59–64.
9 王佳倩,李润娥,李庭晏.统一用户管理和身份认证服务的设计与实现.实验技术与管理,2004,21(3):7–12.
10 张辉,杨岳湘,汪诗林.数字校园中基于 LDAP 的统一用户身份管理技术研究.计算机工程与科学,2005,27(1):14–16.
11 申军霞.统一身份论证开启区域教育信息化的新篇章.数字校园,2011:65–67.
12 杨智楠.浅谈统一用户管理系统的建设方案.计算机光盘软件与应用,2011,21:172–173.
13 赵曦,丁建国.基于 LDAP 的统一用户管理系统的研究与实现.情报杂志,2008,(12):80–82.
14 Howe T, Smith M.The LDAP Application Program Interface. RFC1823. 2002(8):82–86.
15 张开.基于 Cookie 的单点登录实现.价值工程,2012,(5):154–155.