网络存储与 UAMS 模式研究*

姚 渝 春
(重庆大学 自动化学院, 重庆 400030)

摘 要:在分散存储系统中,由于各子系统相互独立,资源和用户的管理难度大,用户对资源的访问不便,共享信息难以得到充分利用。本文提出通过设计一个用户认证和管理系统(UAMS),以虚拟账号方式管理用户,按照"资源分散存储、统一分配、用户集中管理"的模式整合分散存储资源。在这种模式中,UAMS 以中介的身份将用户和资源隔离,避免了各存储系统重复管理用户。它能在对各子系统无管理权限的前提下,对分散的存储资源实行集中用户管理,方便用户对分散存储资源的访问,有效地提高存储网络的可用性和信息的共享度,UAMS 提供的用户认证机制改善了存储系统的安全性。

关键词:网络存储技术;集中用户管理;信息系统安全
中图分类号:TP393.07 文献标识码:A 文章编号:1672-6693(2008)03-0042-4

1 概述

20 世纪 80 年代,随着 PC 机的兴起,主机/终端体系结构走向没落,数据的存储逐渐由一种功能相对专一的服务器来完成。存储系统在数据量、性能、安全性[1-2]等方面都有很大提高,网络存储的结构也逐渐从 DAS(Direct Attached Storage,直接连接存储)发展到当今广泛应用的 NAS(Network Attached Storage,网络附加存储)和 SAN(Storage Area Network,存储区域网络)。据预测,今后几年世界范围内磁盘存储系统的容量将以每年近 80% 速度递增,网络存储技术已成为继计算机技术、互联网技术之后的第三次浪潮[3-4]。

1.1 网络存储结构分类

依据硬件结构可将存储系统分为直接连接存储(DAS)、网络附加存储(NAS)、存储区域网络(SAN)三种类型。DAS 是一种典型的以服务器为中心的存储方式,数据存储设备完全以服务器为中心,其主要优势是技术成熟、价格便宜、应用难度低、安全控制容易实现,适合于存储量较小、数据交换少的环境。DAS 的突出缺点是:其总体性能受到服务器性能制约,扩展、升级、集成都很困难。NAS 是一种基于局域网的存储,它采用了专门设计用于网络存储的瘦服务器和经过优化的操作系统,整个系统的设置和管理较为简单,广泛支持多种标准化协议,具有很好的扩充性和兼容性,是当今中小型网络存储应用的主流产品,但 NAS 的性能会受到网络性能的制约。SAN 需要单独建立一个以光纤交换机为核心的光纤高速网络,连接所有的 SAN 存储设备和服务器,SAN 存储设备受 SAN 服务器的控制和管理。SAN 能以数据块(Data Block)的方式实现高速、大数据量传输。其不足之处是造价高、标准不统一、兼容性不理想[5]。

1.2 集中存储与分散存储

按照存储资源的管理模式可将网络存储系统分为集中存储和分散存储两种类型,不能简单地说哪种存储方式更好,它们有各自不同的用途和特点,对应用环境的要求也有差异。选择存储方式需要考虑的因素有:存储资源的相关度、资源所有者的业务关系、用户分布情况、网络性能。如果资源相关度高、资源所有者业务关系密切、用户分布集中、网络性能好,可以采用集中存储,反之,就应该考虑分散存储。

集中存储有利于资源的整合,便于对数据、用户、访问权限的统一管理,安全控制也容易实现。但集中存储对网络环境、存储系统的结构、设备性能都有较高要求。比如在由多个 DAS 子系统构成的存储系统中,由于 DAS 各自独立,相互之间难以管理对方的资源和用户,集中存储就很难实现。在一个

* 收稿日期:2008-05-04
资助项目:重庆市科技攻关计划资助项目(No. CSTC2007AB2046)
作者简介:姚渝春(1967-),男,高级工程师,研究方向为计算机应用技术。

NAS系统中,由于专用的NAS服务器可以同时管理多个连接在LAN上的NAS存储设备,系统的扩容也很方便,适合于集中存储,但如果数据流量很大,LAN的性能可能会成为整个系统的"瓶颈"[6-7]。

分散存储对网络性能、存储结构没有特殊的要求,存储资源可以广泛分布在网络的多个位置。但分散存储系统的资源和用户管理相当困难,用户对多个资源的访问也不方便,存储资源往往得不到有效利用。

2 分散存储资源整合

为了提高分散存储资源的可用性,对分散资源整合技术的研究已经成为网络存储技术发展的重要方向之一。从目前的情况看,解决方案主要分为3种类型:1)建立IP—SAN存储系统,用集中存储完全替换原有的分散存储系统;2)虚拟存储技术;3)整合存储技术。

在3个方案中,方案1是最彻底的解决办法,在IBM、HP等企业的大力推动下被广泛采用,但投资过高,不适合对价格敏感的客户;虚拟存储技术是指把多个物理上独立存在的存储体通过软件或硬件的手段集中管理起来,形成一个逻辑上的虚拟存储单元[8]。虚拟存储较好地解决了设备的整合问题,投资也不大,是一个不错的解决方案。但是以上两个方案必须满足一个前提——对被整合的资源或设备有管理的权限,两个方案都无法解决因管理体制造成的分散存储的整合问题,应用范围受到一定限制。

整合存储技术是近年来逐步发展起来的新的应用技术,具体做法是:用一个或多个存储管理服务器为访问者提供资源指向服务,通过地址映射(NAT)、IP隧道(IP Tunnel)、直接路由(Direct Routing)等技术手段,直接或间接地帮助用户访问存储资源[9]。整合存储技术主要依靠软件技术,投资小,适用范围广。但与前两个方案相比,由于缺乏硬件的支撑,并不能提高存储系统的性能。

目前整合存储技术主要解决了数据的访问,即帮助用户发现并访问资源,但较少考虑用户的集中管理,仍然存在各系统分别管理用户的局面,从用户的角度看,这些资源是分散的,可用性有待改善。为了解决这些问题,本文提出一个基于整合存储的新存储模型——UAMS,利用UAMS可以实现用户集中管理,资源统一分配、单点登录、安全认证。

准确地说,这是一种"资源分散存储、统一分配,用户集中管理"的存储模式。

3 UAMS结构模型

为了方便用户对资源的访问、降低用户管理的复杂性、提高分散存储资源的可用性,比较合理的办法之一就是将存储资源的管理与用户管理分离,单独建立一套用户认证和管理系统UAMS(Users Authentication and Management System),让UAMS成为访问者和存储资源的中介。设计UAMS是为了实现以下目标:1)用户集中管理;2)资源统一分配;3)用户单点登录;4)为用户对资源的访问提供安全认证和指向服务[10]。

存储资源和UAMS共同构成一个三层结构,UAMS包含了其中的两层——服务层和数据层(见图1)。服务层通过不同的接口为应用层提供用户管理、认证管理、日志管理、资源管理等服务,并为用户对资源的访问提供指向服务;数据层记录了用户信息和资源信息,包括用户基本信息、角色、资源位置、资源类型、访问方式、资源分配情况等[11]。

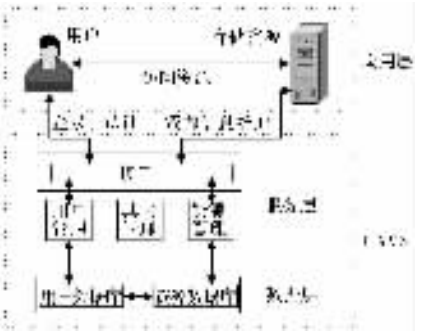

图1 UAMS结构模型

UAMS结构模型有如下特点:1)UAMS以虚拟账号方式对用户进行集中管理,将虚拟账号自动映射成多个存储系统的真实账号。存储系统不直接管理用户,降低了管理复杂程度;2)单点登录、统一访问界面。用户只需一次登录就能访问所有存储资源;3)安全认证机制提高存储系统安全性;4)认证和数据访问分离,UAMS只负责用户认证和资源指向,避免产生"瓶颈"。

4 UAMS在实际应用中的关键技术

4.1 Client/Server结构

UAMS可以设计成Client/Server或Brower/Server结构,虽然Brower/Server结构在应用范围和可维护性等方面有诸多优势,但考虑到存储管理系统对软件界面设计有较高要求,用Web设计符合要求的界面比较困难,因此,UAMS采用Client/Server

结构。整个系统包含客户端和服务端两部分。客户端为用户对资源的访问及维护提供统一的操作界面,客户端对应 UAMS 三层结构中的应用层和部分服务层的功能。服务端包括资源数据库、用户数据库、访问接口、日志管理等,最核心的内容是资源数据库和用户数据库。这两个数据库的设计非常关键,其结构是否合理直接关系到整个系统的性能和可维护性。

4.2 资源数据库和用户数据库

资源数据库记录了存储资源的位置(IP 地址)、资源类型、访问方式、访问该资源所需的真实账号、密码等。用户数据库包含虚拟账号表、资源分配表、日志等多种数据,它们记录了虚拟账号的基本信息和资源分配情况(见图 2)。下面将几个关键问题重点阐述。

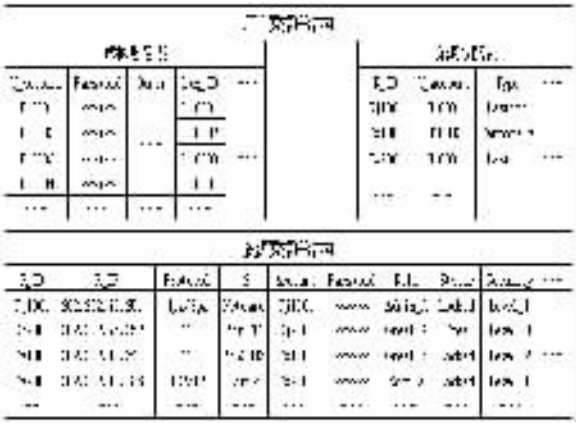

图 2　用户数据库和资源数据库

1)关于虚拟账号的含义。所谓虚拟账号不是存储资源所在系统中的真实账号,而是 UAMS 为访问者所建立的一个虚拟用户名,但虚拟账号与真实账号存在一对多的关联(即一个用户可以拥有多个存储资源)。设立虚拟账号是为了将访问者与存储资源隔离开来,使存储资源不直接面对使用者,而是通过 UAMS 这个中介。采用这种方法可以有效地实现用户的集中管理,避免了存储资源所在系统分别管理所有访问者的繁琐、重复的工作。

2)如何建立虚拟账号与真实账号的关联。存储资源所有者创建真实账号,UAMS 创建虚拟账号,并将虚拟账号与真实账号关联。以 Microsoft SQL Server 后台数据库为例,在用户数据库中设立一个资源分配表,该表记录了虚拟账号已经分配到的存储资源的相关信息。每个虚拟账号可以分配多个存储资源,具有相同 v_account 值的记录即为同一个用户所拥有的真实资源(如图 2 所示,在该图的资源分配表中,Cj1001 和 Tx2001 均为 U10001 所分配到的资源)。

3)为什么要将资源数据库和用户数据库独立设置。资源数据库记录存储资源的信息,主要由资源所有者维护,用户数据库记录用户信息,由 UAMS 维护。将两个数据库独立设置容易理清两者间的逻辑关系,数据库访问权限设置变得更简单,资源与用户之间的映射关系更清晰,且资源与用户信息的变化不会相互影响。

4.3 UAMS 的建立

UAMS 的建立分为以下几个步骤:1)设计资源数据库和用户数据库的结构。数据库建立在存储管理服务器上,由 UAMS 的管理者完成,数据库结构设计要以整个系统的运行模式为依据,设计得不合理将会给日后的运行维护带来很多麻烦。可以考虑选择 LDAP 或 SQL Server 作为后台数据库。LDAP 和 SQL Server 都具有良好的开放性和可扩展性,并为众多网络操作系统、组件系统和应用系统所支持[12]。2)资源所有者首先在存储系统中建立真实账号,并以角色(Role)的方式为账号分配权限(基于角色的权限分配可简化 UAMS 对用户的权限管理),角色定义要有统一的规划,避免出现管理上的混乱。然后通过客户端将以上信息上传至 UAMS 的资源数据库中。3)用户通过客户端向 UAMS 提出申请,UAMS 首先生成一个虚拟账号,再向资源数据库查询可供分配的存储资源,分配给该用户,并记录到用户数据库中。

4.4 UAMS 的安全措施

用户在访问存储资源时首先通过客户端向 UAMS 提交虚拟账号和密码,验证通过后 UAMS 向资源数据库查询该用户的真实账号、密码等,并将其传回客户端。但如果不采取任何安全措施,账号和密码的传递很容易在线路或节点上被截获或破译。

根据存储资源安全性需求的高低,可以采用两种类型的安全措施。一是基于一次性口令的认证机制(One-time Password),即 UAMS 和客户端每次通讯前,依据双方事先约定的规则,生成一个对称密钥,用这个密钥对传递的数据进行加密和解密。这种方法很简单,而且不需要资源所有者的配合,但安全性不高,只解决了传输线路上的安全问题,节点安全问题仍然存在。

第二种方法是基于数字证书的认证机制。在这种机制下,UAMS 充当了 CA(Certificate Authority)的

角色,它向客户端和资源所在系统发放包含密钥的数字证书,双方都能通过 UAMS 获得对方的公钥。双方在通信前先用 HASH 函数(散列函数)生成摘要,并用私钥加密摘要生成数字签名。如果需要对正文加密,则随机生成一个 DES 对称密钥,并用对方的公钥加密随机生成的密钥。对方收到数据后,将以上过程逆向进行,就能在获得数据的同时验证发送者的身份(见图 3)。基于数字证书的认证机制使通讯的双方能实现相互验证,很好地保证通信的安全性、完整性和不可抵赖性,并且不需要专门的安全传输线路[13]。

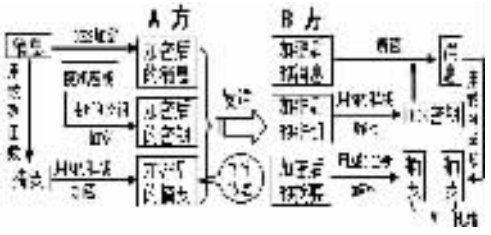

图 3 数字证书机制下的通讯过程

虽然数字证书在安全性方面有巨大的优势,但实施难度比较大,它要求存储资源所在的系统支持公钥体系。在有众多分散存储系统的大型网络中,实现起来并不容易。因此,在 UAMS 的资源数据库设计时,要考虑到这个问题,应该允许资源所有者根据资源的重要程度自行选择安全措施。

参考文献:

[1] 肖丹燕,肖嵬. 校园网络安全的管理对策[J]. 重庆师范学院学报(自然科学版),2002,19(4):40-43.

[2] 刘益和,王锦,陈静科. 一个基于 C/S 模式信息系统的安全描述[J]. 西华师范大学学报(自然科学版),2005,26(2):170-174.

[3] 李战怀. 海量存储的关键技术[J]. 中国教育网络,2006,5:58-59.

[4] INTEL. The Future of Network Storage [EB/OL]. (2002-02-02). http://www.intel.com/network/connectivity/resources/doc_library/white_papers/iSCSI_networkstorages.pdf.

[5] EDELSON E. Security in Network Attached Storage (NAS) for Workgroups[J]. Network,2004,2004(4):8-12.

[6] GIBSON G A,METER R V. Network Attached Storage Architecture [J]. Communications of the ACM, 2000, 43(Ⅱ):27-33.

[7] 张献华. 主流数字存储技术的发展[J]. (2007-11-8). http://www.lrn.cn/bookscollection/magazines/magi-nformatization/2002maginformatization/2002_1/200711/t20071108_166039.htm.

[8] 刘玉山. 虚拟存储技术及其应用[J]. 有线电视技术,2003,12:45-50.

[9] 曾国兵. 分散服务集中管理的 NAS 集群方案研究与实现[J]. 计算机应用研究,2004,2:163-165.

[10] 张学平. 统一用户管理解决方案[J]. 信息安全与通信保密,2005,9:43-44.

[11] 徐永祥. 统一用户管理系统的设计[J]. Computer Engineering,2003,29(8):120-123.

[12] 肖爱华. 统一用户管理设计与实现[D]. 国防科学技术大学硕士学位论文,2005.

[13] HUNT R. Technological Infrastructure for PKI and Digital Certification [J]. Computer Communications, 2001, 24(14):1460-1471.

Research into Network Storage Technology & UAMS

YAO Yu-chun

(College of Automation, Chongqing University, Chongqing 400030, China)

Abstract: Individual resource is independent of each other in the dispersive storage system, which brings about difficulty to managing resources and inconvenience to users to access resources, as well as reduction of availability of shared information. Considering the proldem as mentioned above, this article proposes integrating disperse storage resources based on the mode of "disperse storage, unified allocation and centralized user management" through establishing an UAMS (User Authentication and Management System) and managing users with virtual account. In this mode, UAMS acts as intermediate to separate users from resources. This provides convenience to users for accessing many dispersive resources and avoids repetitive management to users in each storage system. It can realize uniform user management of dispersive storage system on the precondition of preserving intrinsic management model. It's convenient for users to access information. The UAMS can highly increase the usability of network storage system and the information resource sharing. The use of users authentication improves the security of storage system.

Key words: network storage technology; centralized user management; information system security

(责任编辑 游中胜)