文章编号:2095-6134(2015)05-0676-06

基于 AD 的私有云存储访问控制实现方案*

李从午†, 潘无穷, 林璟锵

(中国科学院数据与通信保护研究教育中心, 北京 100093)

(2014 年 9 月 1 日收稿; 2015 年 3 月 3 日收修改稿)

Li C W, Pan W Q, Lin J Q. An AD-based private cloud storage access control scheme[J]. Journal of University of Chinese Academy of Sciences, 2015,32(5):676-681.

摘 要 当前大多数企业的应用系统通常使用 AD(活动目录)实现统一身份管理及访问控制,但许多云存储设备不支持直接连入 AD. 本文提出一种将云存储设备连入 AD 的实现方案. 该方案使用 Samba 文件访问控制服务器来沟通 AD 服务器和云存储设备,使得用户可以通过 AD 域账户实现单点登录及访问控制,极大地提高了工作效率,增强了系统整体安全性.

关键词 AD; 云存储; 访问控制; Samba

中图分类号:TP309 **文献标志码**:A **doi**:10.7523/j.issn.2095-6134.2015.05.014

An AD-based private cloud storage access control scheme

LI Congwu, PAN Wuqiong, LIN Jingqiang

(*Data Assurance and Communication Security Research Center of Chinese Academy of Sciences*, *Beijing* 100093, *China*)

Abstract Nowadays, AD (active directory) is usually used to carry out the unified identity management and achieve access control systems of most enterprises, but many cloud storage devices do not support connection to the AD directly. We propose a scheme to connect cloud storage device and AD. The scheme uses the Samba file access control server to communicate with the AD server and the cloud storage device, and user achieves single sign-on and access control through the AD domain accounts, which greatly improves the work efficiency and enhances the overall security of the system.

Key words AD; cloud storage; access control; Samba

云存储[1]是云计算的一种衍生概念,是最近发展起来的一种新的存储方式. 随着云计算的大规模发展和云存储理念的广泛普及,越来越多的企业和单位开始搭建属于自己的云存储系统. 私有云[2]存储系统对比公有云具有数据安全和服务质量两方面的优势. 存储在公有云上的数据随时都有被攻击的危险,但是对企业而言,和业务有关的数据是不能受到任何形式的威胁的,而私有云一般构筑在防火墙后,它的数据安全相对有保障,服务质量也比较稳定. 另一方面,资源显示,全球前 1 000 家企业中,平均每家企业有 14 个数据库和 40 多个应用系统. 这么多的系统,如果用户

* 国家"973"计划项目(2014CB340603)和国家"863"计划项目(2013AA01A214)资助

† 通信作者,E-mail:cwli13@is.ac.cn

登录不同的系统需要切换账号和输入密码,非常影响工作效率. 当职员信息发生变更时,人事专员需要通知各应用系统管理员进行“人工同步”,如果通知不及时或权限取消不及时可能会造成信息泄露,而审计专员也很难确认某位职工是否在适合的系统拥有正确的权限[3]. 因此,绝大多数的企业和单位都部署了统一身份管理系统.

现在越来越多的企业使用 AD[4] 来实现统一身份管理,使用域管理具有方便管理、安全性高、可扩展性强、可冗余性等优势. 但是现有的许多云存储设备不支持直接连入 AD 服务器,如 H3C Neocean EX1500 系列 (IP-SAN), BUFFALO TeraStation (NAS)系列等. 另外,费用也是影响企业选择的一个重要因素. 本文提出一种方案使不支持直接连入 AD 的云存储设备通过一台 linux 服务器来获取 AD 域账户信息,在不更换云存储设备的前提下实现云环境统一身份管理,对企业管理具有重大意义.

本文首先介绍私有云环境下统一身份管理的需求,然后提出一种基于 AD 实现云存储访问控制实现方案,并详尽地介绍该方案的原理,随后通过实验验证该方案的可行性,最后对本文提出的方案进行总结.

1　背景知识

1.1　AD 简介

AD(活动目录)是 Windows2000 服务器版操作系统的一种目录服务,目录服务可将网络中存在的各种对象组织起来进行管理,有利于网络对象的查找,加强了网络的安全性,增强了管理.

域网是通过主从模式实现的,通过域控制器来集中管理域内用户帐号和权限,帐号信息保存在域控制器内,访问控制权限也由域控制器统一管理. 域控制器中包含由这个域的账户、密码、属于这个域的计算机等信息构成的数据库. 通过接入 AD,企业可以实现邮箱系统、办公系统、管理系统等多应用系统统一身份管理,用户只需使用域账户名和密码即可登录以上所有系统,提高了工作效率,易于同步管理与审计[5].

1.2　Samba 及其安全级别

Samba 是一种标准的提供 Windows 系统与 Linux/Unix 系统互操作性的开源软件包,是许多服务以及协议的实现. 它包括 TCP/IP 上的 NetBIOS、SMB、CIFS、MSRPC、NT 域协议套件等,其核心是 SMB 协议. 除此之外,Samba 还用于共享打印机.

Samba 一共有 5 种不同的安全级别, 包括 share、user、server、domain、ads. 安全级别不同,Samba 服务器的身份认证方式也不同.

share:不需要 Samba 账户就可登陆 Samba 服务器(不需要身份认证).

user:需要添加 Samba 账户才可以登陆 Samba 服务器.

server:由另外一台 Samba 服务器来对用户进行身份认证.

domain:把 Samba 服务器加入到 NT 域,由 NT 的域控制器来进行身份认证.

ads:活动目录服务是 Samba3.0 版本中新增的身份认证方式. 采用 ads 安全级别会将 Samba 服务器集成到活动目录中,即将 Samba 服务器作为一个域成员加入 AD 域.

通过配置 ads 模式下的 Samba 服务,可以让 Samba 服务器与 AD 服务器进行交互,且利用 windows 域控制器来完成身份认证.

2　基于 AD 的云存储访问控制实现原理

2.1　整体介绍

如果不把 AD 服务器接入网络拓扑中,整个系统将无法获得 AD 域用户信息,那么就不能使用 AD 域账户单点登录了. 由于 AD 服务器不能直接与云存储设备进行交互,但 AD 服务器和云存储设备都可以直接和 Linux 服务器进行交互,于是,我们设计加入一台 Linux 服务器来沟通 AD 服务器和云存储设备,然后将 AD 域用户映射为 Linux 用户并且在 Linux 服务器上添加访问控制策略[6],通过 Linux 用户操作的方式来访问挂载在 Linux 服务器上的云存储设备. 这个系统对用户是透明的. 图 1 显示了云存储访问控制的部署方案及 Linux 服务器内部组件层次结构.

Linux 服务器(Samba 文件访问控制服务器)上的核心组件是 Samba、Kerberos 和 iSCSI 用户空间组件.

图 2 显示了 Samba 交件访问控制服务器的安全体系层次模型. AD 域成员想要访问云存储设备上的资源必须通过 OS 安全——身份认证——

访问控制 3 层结构[7]才能实现.

本文部署的系统首先将 AD 域成员映射成为 linux 用户,这些用户必须符合 linux 账户管理要求. 然后,当一个用户登录时,要进行身份认证,以验证其是否为合法用户;除此之外,还需要在 linux 服务器上添加访问控制策略来实现 AD 域成员的访问控制.

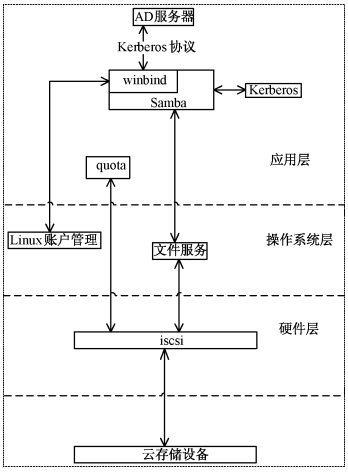

图 1 云存储访问控制的部署方案及 Linux 服务器内部组件层次结构

Fig. 1 Cloud storage access control scheme and internal component hierarchical structure of Linux server

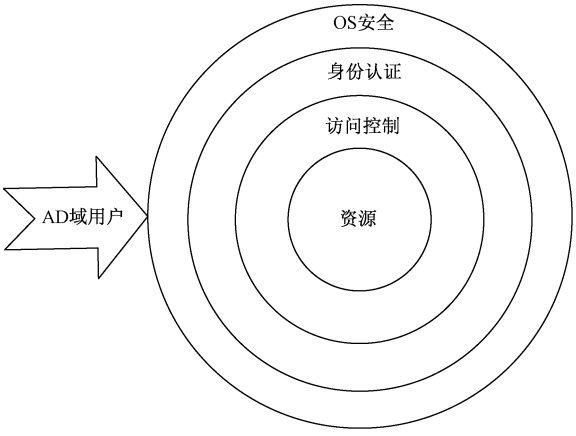

图 2 Samba 文件访问控制服务器的安全体系层次模型

Fig. 2 Safety system hierarchical structure model of Samba file access control server

本文部署的系统实现思路如下:

1)使用 Winbind 将 AD 域用户和组映射成为 Linux 用户和组.

2)利用 Kerberos 协助 Samba 完成身份认证.

3)通过 iSCSI 用户空间组件完成 Linux 服务器与云存储设备间 initiator-target 关联.

4)在 Linux 服务器上配置访问控制策略和资源分配策略.

2.2 用户和组的映射

既然 AD 域用户无法直接与云存储设备进行联系,而 Linux 用户可以轻松地实现对云存储设备的访问(像操作本地磁盘一样),如果能够把 AD 域用户映射成为 Linux 用户,那么就能将 AD 服务器与云存储设备之间的桥梁搭上. Winbind 是 Samba 套件的功能之一. 它允许 Linux 系统利用 Windows server 的用户帐号信息. 可以把 winbind 看作是 Samba 作为 Windows 域成员的一个中介,它可以把 Windows 域帐号里的用户和组映射成 Linux 的用户和组.

2.3 身份认证

身份认证用来验证用户身份的合法性,只有合法的用户才能访问相应资源. 我们主要依赖 Kerberos[8]来完成身份认证. Kerberos 是一种以对称密码体制为基础, 对用户及网络连接进行认证的协议,提供了网络通讯方之间相互身份认证的手段,主要应用于分布式网络环境.

图 3 显示了 ads 安全级别下的身份认证过程. 在 ads 安全级别[9]下,Samba 服务器将验证工作交给 Windows 域控制器来完成,需要通过 Kerberos 协助完成身份认证工作. 此时,Samba 服务器是作为 Windows AD 域的一个域成员,并不是 AD 域控制器[10].

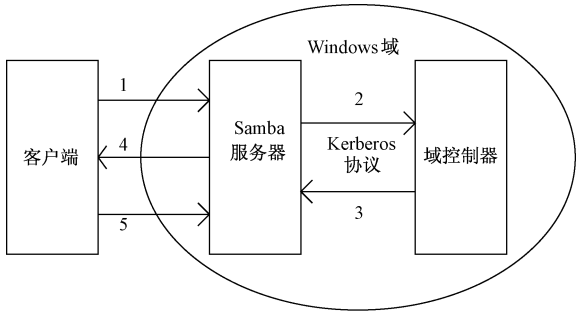

图 3 Ads 安全级别下的身份认证

Fig. 3 Identification authentication under ads security level

ads 安全级别下的身份认证过程如下:

1)客户端将用户名和密码发给 Samba 服务器;

2)Samba 服务器将这两项信息发给域控制器验证;

3)域控制器将验证的 token 令牌返回 Samba 服务器;

4)Samba 服务器将验证的 token 令牌返回客

户端;

5)客户获得 token 令牌,依据该令牌访问 Samba 服务器.

2.4 Samba 服务器与云存储设备之间的关联

iSCSI 技术是一种新型储存技术,该技术是将 SCSI 接口与以太网络技术结合,使服务器可与使用 IP 网络的储存设备互相传输资源. iSCSI 驱动使主机拥有了通过 IP 网络访问存储的能力,驱动在 initiator 和 target 间使用 iSCSI 协议在 TCP/IP 网上传输 SCSI 请求和响应. 虽然 Linux 2.6 提供了 iSCSI 驱动,但还需要使用用户空间组件来初始化 iSCSI 驱动. 本文部署的系统采用 open-iscsi 提供的 iscsi-initiator-utils 工具作为 iSCSI 用户空间组件来初始化 iSCSI 驱动,此工具作为 iSCSI 连接的发起端,而云存储设备作为 iSCSI 连接的服务端,两者关联之后就能像使用本地磁盘一样将云存储设备挂载到 Samba 服务器的指定目录下,进而可以在 Samba 服务器上像使用本地磁盘一样使用云存储设备,实现 Samba 服务器与云存储设备基于 iSCSI 协议的访问.

2.5 访问控制与资源分配

用户通过身份认证后,并不代表他拥有所有权限,该用户可以访问哪些资源,能否读、写、执行还需要受到访问控制权限的限制. 将云存储设备与 Samba 文件控制服务器关联之后,可通过 quota 工具进行磁盘配额,实现资源分配. Quota 是 Linux 上专门用来实现磁盘配额的一种工具,借助这个工具,可以给不同用户分配不同大小的磁盘空间,以满足不同用户的需求.

3 方案实现

首先将 AD 服务器以及云存储设备连接到 Linux 服务器,在 Linux 服务器上下载并安装必要组件 Samba、Kerberos、iscsi-initiator-utils. 然后配置 Samba 的配置文件 smb. conf 来使 winbind 获取 AD 域成员信息:

```
1  winbind use default domain = true
2  winbind offline logon = true
3  winbind enum groups = true
4  winbind enum users = true
5  winbind separator = /
```

再配置 nsswitch. conf 来添加控制搜索信息类型的方法:

```
1  passwd: files winbind
2  shadow: files winbind
3  group: files winbind
```

通过以上配置,就能使用 winbind 将 AD 域用户映射成为 Linux 用户,只需要再把 winbind 服务开启即可:

```
1  #service winbind start
```

随后,还需要将 Samba 用户与 Linux 本地用户区分开(只有 Samba 用户才是合法用户). 通过配置 smb. conf,设置 encrypt password = yes,使得 Samba 服务器与 Linux 采用不同的密码文件,Linux 用户不同于 Samba 用户. 不仅如此,还需要结合 Samba 和 Kerberos 来实现身份认证. 在 smb. conf 中设置 security = ads 来完成 ads 安全级别的配置.

```
1  [global]
2  workgroup = LOIS0
3  server string = Samba Server Version% v
4  password server = 192.168.0.191 // AD 服务器
5  realm = LOIS. LOCAL // 活动目录服务器域名
6
7  security = ads // 采用活动目录认证方式
8  idmap uid = 16777216 - 33554431
9  idmap gid = 16777216 - 33554431
10 template shell = /bin/bash
   template homedir = /test/% U
```

需要注意的是:ads 认证方式必须结合 realm 参数,这样,Samba 和 Kerberos 才能正确识别 AD 域.

然后在 krb5. conf 中进行以下配置:

```
1  [libdefaults]
2  default_realm = LOIS. LOCAL // 默认域名
3  dns_lookup_realm = false
4  dns_lookup_kdc = true
5  forwardable = true
6  [realms]
7  LOIS. LOCAL = {
8  kdc = 192.168.0.191:88 // AD 域服务器 ip
9  admin_server = 192.168.0.191:749
10 default_domain = LOIS. LOCAL
11 }
12 [domain_realm]
13 lois. local = LOIS. LOCAL
14 lois. local = LOIS. LOCAL
```

方案进行到这一步,就完成了 Samba 服务器与 AD 服务器沟通的各组件的基本配置,可通过 net ads join-U administrator@ LOIS. LOCAL 命令将 Samba 服务器加入 AD 域.

通过 wbinfo-u 命令可以看到:在搜索本地文件、列出 Linux 本地用户之后,Samba 会通过 winbind 将 AD 域用户列出来. 由于 winbind 将 AD 域用户映射成为 Lnux 用户,AD 域用户就成了 Samba 服务器上用户中的一部分. 已登录的 AD 域用户就可以通过 Samba 文件访问控制服务器访问云存储设备,获取资源.

用户通过身份认证后,说明他是应用系统一个合法用户,即 AD 域用户. 但该用户可以访问哪些资源,能否读、写、执行必须受到访问控制权限的限制. 通过配置 smb. conf 中的相关参数结合建立用户主目录时给该目录设置的权限可以实现访问控制策略.

表 1 显示了各项共享资源的访问控制参数,通过这些参数可以控制不同用户对资源的访问.

表 1 共享资源的访问控制参数

Table 1 Access control parameters of the shared resource

参数	功能
Writeable	共享资源是否可写
Browseable	共享资源是否可浏览
read only	共享资源是否可读
print able	用户是否可打印
Available	是否启用共享资源
Public	用户是否不需帐号和密码即可使用
guest ok	用户是否不需帐号和密码即可使用
only guest	共享资源是否只对 guest 用户使用
valid user	允许登录的用户
invalid user	禁止登录的用户
host allow	允许连接的主机地址
host deny	不允许连接的主机地址

在建立用户主目录时,通过 chmod 命令给这个文件夹设置权限(对用户抽象为磁盘). 例:

```
#mkdir user1home
#chown user1/user1home
#chmod 777/user1home
#mkdir user2home
#chown user2/user2home
#chmod 750/user2home
#mkdir user3home
#chown user3/user3home
#chmod 700/user3home
```

通过以上设置,所有人都可以对 user1home 的资源进行读、写、执行操作; user2 可对 user2home 的资源读、写、执行,同组用户可读、执行,不可写,其他用户无法操作; user3 可对 user3home 的资源读、写、执行,同组用户和其他用户都无法进行操作.

然后,还需要将 Samba 服务器与云存储设备关联才能使用云存储设备. 首先使用 PC 连接云存储设备,通过云存储设备控制器建立 target. 接着在 Samba 服务器使用 iscsi-initiator-utils 登录并连接 target.

```
#iscsiadm-m discovery-t sendtargets-p 192. 168. 0. 1
#scsiadm-m node-T iqn. 1994-05. com. redhat:b45be5af6021-login
```

完成关联之后,可通过 quota 进行磁盘配额,实现资源分配. 首先将关联的云存储设备挂载,然后进行配额设置. 这里以分配 5 G 空间为例.

```
#mount/dev/sdb3/test/
#vim/etc/fstab
/dev/sdb3/test ext4 defaults,usrquota,grpquota 0 0
#mount-o remount /test
#mount-o usrquota,grpquota /test
#quotacheck-cmug /test
#quotaon-av
#edquota-u user1
Disk quotas for user user1(uid 16777216):
Filesystem blocks quota limit grace files quota limit grace
/dev/sdb1 0 5000000 5120000 10 0 0
```

4 实验

首先进行功能实验. 建立 3 个用户,分别给他们的主目录设置 777、750 以及 700 权限,将他们加入同一个组,再在 smb. conf 中进行以下设置:

```
[user1home]
browsable = yes
writable = yes
[user2home]
browsable = yes
writable = yes
[user3home]
browsable = yes
writable = yes
```

尝试分别使用 user1,user2 和 user3 登录系

统,然后对他们的主目录进行操作.

表 2 显示了不同权限的用户访问控制结果.

表 2　不同权限的用户访问控制结果

Table 2　Results of the different access authority users

	user1 home	user2 home	user3 home
user1	可读可写可访问	可读不可写可访问	不可读不可写不可访问
user2	可读可写可访问	可读可写可访问	不可读不可写不可访问
user3	可读可写可访问	可读不可写可访问	可读可写可访问

当参数 browsable = no 时,所有人都无法浏览该文件夹;当参数 writable = no 时,所有人都无法写该文件夹.

使用本文部署的系统后用户从输完帐号、密码点击登录到登录进系统完成身份认证的时间很短(不足 1 s,由于该操作涉及用户按键,精确到毫秒级误差较大),与云存储设备直接连入 AD 的方式相比,性能差异极小.

在 Samba 服务器设置 share 安全级别(不进行身份认证),通过管理服务器直接连接 Samba 服务器向云存储设备写入、读出资源时间与 ads 安全级别下 AD 域账户通过瘦客户端在管理服务器登录后向云存储设备写入、读出资源时间进行对比,进行系统性能实验(读出、写入均为 3.00 G 文件)(见表 3).

通过分析表 3 的实验数据,可以得出:经过身份认证的 ads 安全级别与不经过身份认证的 share 安全级别在读写文件的时间上差异很小,部署本文提出的系统不会影响整体性能.

表 3　性能实验结果

Table 3　Results of the performance experiment　　s

	写入时间 1	写入时间 2	写入时间 3	写入时间 4	写入时间 5	读出时间 1	读出时间 2	读出时间 3	读出时间 4	读出时间 5
直接连接 Samba 服务器后操作(share)	56.7	57.3	57.0	58.2	60.2	113.7	114.5	108.5	108.7	107.8
AD 域用户登录后操作(ads)	53.3	59.6	58.9	58.5	61.5	117.0	115.3	114.5	108.9	112.4

5　结束语

本文分析云环境下统一身份管理的必要性和现状,提出一种利用 AD 实现云存储的访问控制方案. 该方案能够使用户通过 AD 域账户实现单点登录以及访问控制,极大提高了工作效率,增强了系统整体安全性,也便于系统管理员实施更有效的管理,减轻维护时的负担. 除此之外,该方案还便于审计专员进行审计. 通过加入一台 Samba 服务器,将 AD 域用户映射成为 Linux 用户然后进行访问控制,为异构系统的统一身份管理提出一种新的思路.

参考文献

[1] 江伟玉, 刘丽敏, 查达仁. 面向云存储的访问控制服务研究[J]. 信息网络安全, 2013 (10): 34-37.

[2] 王冠,范红,杜大海. 云存储访问控制方案的安全性分析与改进[J]. 计算机应用, 2014, 34(2): 373-376.

[3] 傅颖勋, 罗圣美, 舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展, 2013, 50(1): 136-145.

[4] 王安俊, 刘萍, 武涛. Windows2000 活动目录技术的分析与研究[J]. 计算机工程与设计, 2003, 24(4): 21-24.

[5] 李发旭, 卫良. Windows2000 活动目录技术及其应用[J]. 青海师范大学学报: 自然科学版, 2004 (1): 36-39.

[6] 邹念, 唐宁九. 用 Samba 实现 Linux 和 Windows 之间的文件共享[J]. 计算机应用研究, 2002, 19(1): 152-153.

[7] 谭良, 蒲红梅, 周明天. Samba 服务器共享资源安全系统层次模型研究[J]. 计算机应用, 2004, 24(2): 115-117.

[8] 齐忠厚. Kerberos 协议原理及应用[J]. 计算机工程与科学, 2000, 22(5): 11-13.

[9] 刘承凌, 刘发贵. 基于 Samba 的文件共享及安全认证机制的研究[J]. 计算机应用与软件, 2006, 23(1): 122-124.

[10] 邱航, 权勇. 基于 Kerberos 的单点登录系统研究与设计[J]. 计算机应用, 2003, 23(7): 142-144.