异构网络文件打印共享及 Samba 安全管理研究

Research of Share Files and Printers in Isomerous Network and Security Management of Samba

王 海 李常先 徐鹏民 (山东莱阳农学院网络中心 青岛 266109)

摘要:通过对异构网络文件打印共享方式 NFS、CIFS 和 Samba 服务器的分析比较,提出了完整的 Samba 服务器管理体系及安全策略,使 Samba 服务器在异构网络环境中的应用更加稳定、安全。主要包括 5 个层次:Linux 系统管理、Samba 安全配置、访问控制、日志管理、系统备份与恢复,对于每个层次的安全管理策略进行了相应的分析讨论。实践证明,这种安全管理体系与策略具有很好的实用性,有助于异构网络环境下的应用性研究与开发。

关键词:异构网络 共享 NFS CIFS Samba 服务器 安全管理

1 引言

UNIX 和 Linux 把 TCP/IP 和 Internet 带到了桌面,而 Windows 则带来了数以亿计的用户。随着 Linux 的应用日益广泛,特别是在网络应用方面,有大量的网络服务器使用 Linux 操作系统。但在桌面应用方面,由于 Linux 和 Windows 相比还有一定的差距,所以在企业应用中往往是 Linux 和 Windows 操作系统共存形成异构网络。在服务器端大多使用 Linux 和 Unix,PC 端使用 Windows 9X/2000/XP。

在 Linux 和 Windows 两种操作系统之间实现资源共享有多种途径,像 NFS 和 CIFS,但应用较多的是通过 Samba 服务器。对于可以作为文件和打印服务器的 Samba Server 的构建与应用已有很多文章作了介绍,而对于如何高效、安全地对 Samba 服务器进行管理却很少讨论。处于异构网络中的 Samba 服务器方便了 Windows 和 Unix/Linux 系统之间资源共享的同时,也承担着可能遭受攻击的风险。因为从支持 Samba 的操作系统、TCP/IP 到 Samba 本身都存在着安全漏洞,尽管这些漏洞不断地得到修正,但是,未知的不安全因素无时不在,如何适应这种局面是系统管理员所面临的严峻挑战。因此,使用 Samba 服务器的同时,必须对其实施安全有效的管理,为用户提供更加方便、安全、高效的服务。

2 文件及打印共享

当前流行的 Windows/Linux 集成层次是通过运行 Windows 的 PC 共享位于 Linux 主机(或者专门的类似 Linux 的文件服务器)上的目录来取得的。被共享的目录在 Windows 系统下可以显得是透明的,要么作为驱动器,要么作为常规 Windows 网络文件树上的延伸。在 Linux 下也可以安装位于 Windows 上的文件系统,但是这种做法不太常见。NFS 和 CIFS 都可以实现这两种文件共享系统。

2.1 网络文件系统(NFS)

NFS 是为在 UNIX 主机间共享文件而设计的,UNIX 主机上的文件上锁机制以及安全规范与 Windows 系统中的有着显著不同。尽管市场上有各种各样在 Windows 客户端安装 NFS 共享目录的产品,但是应该努力避免使用它们,这既是因为规范不匹配,也因为 CIFS 做得更好。如果您坚持使用 Windows 文件服务器,那么用 Windows 的 NFS 服务器软件(如 microsoft 公司的 Services for UNIX(SFU))把 Windows 的文件系统共享给 Linux 客户机也是可行的。不过,下面介绍的 Linux SMBFS 文件系统往往是达到这种效果的一种更简单的方法。

2.2 公共 Internet 文件系统(CIFS)

CIFS 的基础是以前称为 SMB(Server Message Block,服务器消息块)的协议。SMB 是 Microsoft 早期给 DOS 增加的一种扩展,以便把磁盘 I/O 重定向到一

种叫做 NetBIOS(Network Basic Input/Output System,网络基本 I/O 系统)的系统上。NetBIOS 是由 IBM 和 Sytec 设计的,它是网络和应用程序间的一种原始接口。

SMB 包(packet)是由一种叫做 NBT(NetBIOS over TCP)的 NetBIOS 扩展承载的,尽管所有这些听上去非常烦琐,但结局是这些协议已经得以普及,而且能够在从 MVS 和 VMS,到我们的朋友 Linux 和 Windows 之间的各种平台上使用。各个系统现在都能用它。

2.3 安装远程的 CIFS 共享资源(SMBFS)

SMBFS 文件系统能让 Linux 把网络 CIFS 文件服务器只当作是另一个不同的文件系统类型,就像它对待 NFS 服务器那样。SMBFS 已经引入 Linux 内核好几年了。代码最初是由 Pal – Kristian Engstad 编写的,现在由 Samba 的作者 Andrew Tridgell 维护。因为内核里已经支持这种文件系统,所以,您可以使用普通的老命令 mount,把一个远程的 CIFS 资源安装到本地的安装点下。例如 mount –t smbfs –o username = ned / engserver/admin /home/ned/engadmin,而不要直接使用 smbmount 命令,因为采用 mount 命令会有更好的一致性,而且容易记忆(mount 调用 smbmount)。

2.4 Linux 的 CIFS 服务器(Samba)

Samba 是一种非常流行的软件包,它采用 GNU 公共许可证,在 Linux 主机上实现了 CIFS 的服务器端。它最初是由澳大利亚人 Andrew Tridgell 开发的,他用逆向工程的方法实现了 SMB 协议,并且在 1992 年公布了代码成果。

现如今,Samba 得到了很好的支持,而且处于活跃的开发之中,它的功能在不断扩大。它提供了一种稳定成熟的机制,可以把 Windows 机器集成到 Linux 网络中来。Samba 的真正动人之处则在于您只要在 Linux 机器上安装一个软件包就行了,在 Windows 端不需要任何特殊软件。

Samba 的 CIFS 提供 5 种基本服务:文件共享、网络打印、验证和授权、名字解析、服务声明(文件服务器和打印机"浏览")。

Samba 不仅能通过 CIFS 提供访问 Linux 文件的服务,而且它还能执行一个 Windows NT 4.0 主域控制器的所有基本功能。Samba 支持一些高级特性,包括 Windows NT 域登录、Windows 用户特性描述文件的漫游,以及 CIFS 假脱机打印。Samba 能让 Linux 和 Windows 的各个版本之间轻松共享文件。

Microsoft 没有公布有关它是如何实现 CIFS、NT 域和活动目录(Active Directory)这类技术的信息,所以参与 Samba 项目的有志人士实际上必须采用逆向工程的方法分析正在运行的 Microsoft 服务器,研究如何能让 Samba 工作。遗憾的是,这一局限性使得 Microsoft 的新功能在 Samba 上实现的时间有一定的滞后。

Samba 的大多数功能都是由两个守护进程实现的:smbd 和 nmbd。smbd 实现文件和打印服务,还有验证和授权功能。nmbd 提供其他的 CIFS 主要部件,名字解析和服务声明。另外 Samba 还包括一些管理工具,如 smbclient,smbtar,testparm,smbpasswd 等程序。

和 NFS 与内核相互深深地交织在一起不同,Samba 不要求对内核做任何修改,完全作为一个用户进程运行。它绑定到了用于 NBT 请求的套接口,并等待客户端访问资源的请求。一旦请求被提出并通过了认证,smbd 就派生出自身的一个实例,该实例以发出请求的用户的身份运行。结果,所有常规的 Linux 文件访问权限(包括组权限)都得到遵守。smbd 在这上面所添加的唯一一项特殊功能是文件上锁服务,该功能可向客户端 PC 提供它们所习惯的上锁语义。

3 Samba 服务器的安全管理体系

Samba 服务器的安全管理体系应包括操作系统的安全管理、Samba 的安全配置、共享资源的控制管理、日志管理、系统备份与恢复等内容,如图 1 所示。

由于 Samba 服务器运行在 Unix/Linux 系统上,对操作系统的安全控制是管理 Samba 服务器的基础。其中 TCP/IP 协议的不安全/带来了 Samba 服务器管理上的难度。用户认证功能可由 Samba 服务器自身提供,也可以由代理认证服务器完成。访问控制的管理是对共享资源的读、写等控制。日志管理和系统备份与恢复是当系统受到攻击后的管理措施。

4 Samba 服务器的安全管理策略

4.1 操作系统管理

由于 Samba 服务器运行在 Unix/Linux 平台和 TCP/IP 协议之上,操作系统的漏洞和 TCP/IP 不安全会

带来 Samba 的不安全，因此更新操作系统补丁、启用防火墙是加强系统管理、防范攻击的必要措施。

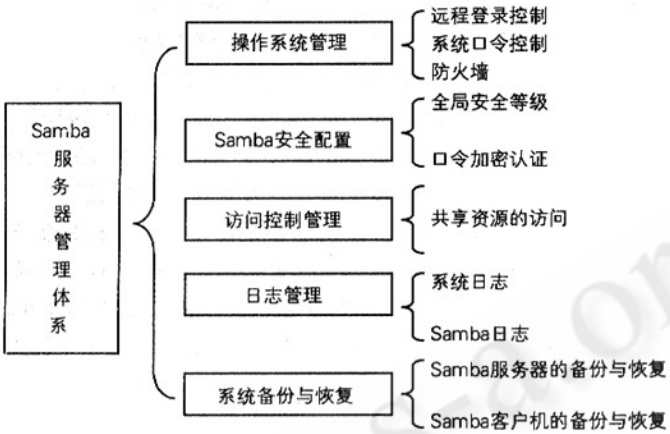

图 1　Samba 服务器的管理体系

Unix/Linux 中提供了防火墙保护来加强系统安全性能。以 Linux 系统为例，新的 Linux 中引入了 Netfilter 的模块化安全框架，使用 iptables 配置基于状态的防火墙、基于 TCP 标记和 MAC 地址的包过滤、强大而简单的 nat 功能等。Linux 系统防火墙的安全级别分为高级、中级和无防火墙 3 类。对于无防火墙级别，系统不会进行安全检查。在防火墙"信任的设备"选项中，任何被选中的网络设备到达的数据都会被系统接收，防火墙对该设备将不起任何作用。在 Samba 服务器的管理过程中，如果 Linux 防火墙设置不当，将会导致 Samba 用户找不到访问路径等问题。当然，你可以在边界防火墙上禁用对 Samba 访问的端口，只需关闭 TCP/445 和 TCP/139 端口，就可以有效的阻止局域网外围的主机对内部 Samba 服务器的访问。

4.2 Samba 安全管理

4.2.1 Samba 用户

Samba 服务器在使用过程中，经常涉及 3 类用户：Windows 用户、Unix/Linux 用户、Samba 用户。通常 Samba 用户是 Windows 用户与 Unix/Linux 用户共同包含的，但要注意这样几点：

（1）只有 Samba 用户才可以合法使用 Samba 服务器。

（2）Samba 用户必须首先是 Unix/Linux 用户，反之不一定成立。

（3）将 Unix/Linux 用户转换为 Samba 用户时，名称可以改变。

（4）Samba 用户可以不是 Windows 用户。此时当 Windows 主机对 Samba 服务器（全局安全等级不是 Share）访问时，如果当前 Windows 账户所用的用户名和密码与 Samba 服务器上的不同，就会出现连接对话框，要求输入 Samba 的合法用户名与密码。

为了解决两种系统的用户名之间不匹配的问题，Samba 服务器采用建立映射表的方法实现。Samba 服务器定义的所有用户映射关系保存在文件/etc/samba/smbusers 中，可以使用 vi 编辑。建立映射的格式是：samba 用户名 = Windows 用户名。这样当 Windows 客户机提出服务请求时，Samba 服务器若发现当前的 Windows 用户不是 Samba 用户，就去查找映射表，提高了客户机的访问效率。

Samba 的最新版本带有一个可选的工具，它叫做 Winbind，以实现统一 Windows 和 Linux 的登录验证。通过插入底层的名字服务开关库（name service switch library）模块，Winbind 能让 Linux 服务器从 Windows 的域控制器获得用户和组的信息。Winbind 也能让用户从 Linux 改变他们的 Windows 域口令。另外，Winbind 还包括一个 PAM 模块，使用 Windows 的域来验证本地的 Linux 登录。虽然 Winbind 是 Samba 工具集里一种相当新的工具，但是它是把少数几台 Linux 主机引入一个 Windows 占优的网络中的理想方案。

4.2.2 Samba 用户的安全等级

（1）安全等级

Samba 中可以设置 4 种安全等级，从低到高分别为 Share，User，Server，Domain。Share 模式下用户访问 Samba 服务器不需要提供用户名和口令，安全性能较低；User 是 Samba 服务器默认的安全等级，每一个共享目录只能被一定的用户访问，并由 Samba 服务器负责检查帐号和密码的正确性；Server 为服务器安全级别，依靠其他 Windows NT/2000 或 Samba 服务器来验证用户的帐号和密码，是一种代理验证 Server 为服务器级安全，此种安全模式下，系统管理员可以把所有的 Windows 用户和口令集中到一个 NT 系统上，使用 Windows NT 进行 Samba 认证，远程服务器可以自动

认证全部用户和口令，如果认证失败，Samba 将使用用户级安全模式作为替代的方式；Domain 为域安全级别，使用主域控制器（PDC）来完成认证。要想安全管理 Samba 服务器，后两种方式具有较强的安全性，尤其是 domain 等级。

为了更好说明问题，下面以 Server 安全等级方式的认证机制为例加以介绍。

（2）Server 安全级别的认证机制

Server 安全级别可以充分利用已有网络中已存在的服务器资源来进行用户认证。使用 Server 安全级别时，必须同时使用全局参数"password server"，Password Server 可以指定一台机器，也可以是以逗号分隔的计算机列表或"*"，"*"号由 Samba 服务器去尝试定位网络中的主或备份控制器。采用这种方式时，需要先将 Samba 服务器配置文件 smb. conf 中的[global]节做修改：

Security = server

password server = 10.10.10.100

这里给出了 Password Server 的机器的 IP 地址，也可以用机器名。这种方式的具体认证步骤如下。

① Windows 客户机向 Samba 服务器发出服务请求；

② Samba 服务器验证 Windows 当前用户是否为合法 Samba 用户，若不是，出现连接窗口，请求输入合法的 Samba 用户名和密码；

③ 将合法的 Samba 用户名和密码提交 Samba 服务器；

④ Samba 服务器判断认证服务器是否启动并正常工作，若为否，由 Samba 服务器按照 User 安全等级进行用户验证及服务，否则，将用户名及密码提交 Password Server；

⑤ Password Server 将验证后得到的 Token 令牌返回 Samba 服务器；

⑥ Samab 服务器再将验证的 Token 令牌返回 Windows 客户端；

⑦ Windows 客户端得到 Token 令牌后，访问 Samba 服务器。

（3）基于口令的认证

在 Windows 95 及以前的版本，在访问 Samba 服务器时使用普通的明文密码，从而造成很大的安全漏洞。从 Windows 98 和 Windows NT 4.0 SP3 之后的 Samba 客户机均使用加密的口令认证方式，但 Samba 服务器无法区分明文密码和加密密码，口令在网络上明文传输的安全漏洞问题仍然存在。解决这个问题的最好方法是让 Samba 支持加密口令认证，使用独立于 Linux 系统口令文件之外的认证系统，表示在进行身份认证时，要对用户的密码进行加密。RedHat 中的 Samba 软件包已经预先编译成支持加密口令认证功能，可直接使用。为使 Samba 服务器识别加密的口令，须对配置文件中全局部分的 security，encrypt passwords，null passwords，smb passwd file 4 个参数进行设定（以 user 安全等级为例）。

security = user

encrypt passwords = yes

null passwords = no

smb passwd file = /etc/samba/smbpasswd

Samba 服务器也允许使用未经加密的用户密码，但既麻烦又不安全。勿庸置疑，允许你的用户使用空口令会将你的整个主机暴露在潜在的敌人面前。但仍有许多企业允许使用空口令。Samba 可以使你通过让管理员拒绝空口令或无效口令的用户进行连接来鼓励用户选择一个口令。这一点通过增加上面的 null Passwords 属性并设置为 no 来实现。

4.3 资源访问控制管理

经过身份认证表明该用户是一个合法的 Samba 用户，但对于 Samba 服务器上共享资源是否能够访问及访问的方式，Samba 服务器可以通过资源控制进行管理。资源控制管理主要考虑 3 个层面：

（1）Unix/Linux 系统中的哪些资源可以共享。

（2）共享的资源对哪些主机或用户开放。

（3）用户对共享资源的使用设置何种访问权限。

对 3 个层面的管理主要通过设置 smb. conf 中的对应的参数，参数的具体含义可参考有关文献。

4.4 日志管理

日志分为系统日志和 Samba 日志。日志中记录了大量有利于管理的信息。系统日志的设置与管理可参阅 Unix/Linux 有关文献。这里主要讨论 Samba 的日志管理。Samab 服务器的日志用于记录 Samba 的使用情况，设置恰当的日志参数可以对 Samba 服务器

（下转第 88 页）

(上接第 83 页)

进行事后监督并进一步提高管理水平。在 smb. conf 的[global]节中可以设置有关日志参数,例如 Debuglevel、Log file、Timestamp logs 等。

4.5 系统备份与恢复

当 Samba 服务器出现问题后,用户希望尽快恢复系统,使之正常工作。做到这一点,应当在 Samba 服务器正常工作时,对系统进行备份,以防患于未然。系统备份的方式可以通过本地完成也可以远程操作。备份内容的选择上既可以整个系统也可以是仅与 Samba 服务器有关的配置文件和日志文件。完成备份工作后,一旦 Samba 服务器出现问题,可以及时恢复。Samba 客户机的备份相对较简单,因为 Samba 对客户机只要求支持 TCP/IP,有必要的情况下,可对 Windows 用户进行备份。

5 结束语

我们在实际工作中选用了 Linux + Samba 服务器作为文件与打印服务器,同时采用了上述 Samba 服务器的管理体系及安全策略。经过长期的运作,Samba 服务器在我们的异构网络一直工作正常,没有受到黑客的攻击和 Windows 下的蠕虫病毒的破坏,Samba 服务器的安全运行,极大地方便了教学、科研工作。

高效地解决异构网络中的文件和打印共享,保障数据的安全,是网络管理工作中的一项重要任务,Linux 系统下的 Samba 服务器是最好的解决方案。同时,在具体应用过程中,用户可以根据不同的安全要求,构建完整的 Samba 服务器安全管理体系,并从各个层次实施安全管理策略,以使 Samba 服务器运行更加稳定、安全、方便。

参考文献

1 谭良 等,Samba 服务器共享资源安全层次模型研究,计算机应用,2004 年 24 期。
2 陈旭、温阳东,Linux 系统网络安全问题分析及对策,合肥工业大学学报,2002 年 25 期。
3 宋利军,RedHat Linux 9.0 实用教程,科学出版社,2003 年。