**Samba高级服务器配置**

上面偶说了下samba滴常规配置哈，这些已经可以使用企业内部滴资料通过网络共享并分配适当滴共享权限来管理共享目录，但这仅仅对于 很多大型企业或安全要求高滴来说还是不能满足其需求哈，所以偶下面就来讲下samba滴高级服务器配置让我们搭建滴samba服务器功能更强大，管理更灵 活，我们滴数据也更安全哈~

4.1 用户账号映射

前面已经说过，samba的用户帐号信息是保存在smbpasswd文件中滴，而且可以访问samba服务器的帐号也必须对应一个同名的系统帐号。基于这 一点，所以哈，对于一些hacker来说，只要知道samba服务器滴samba帐号，就等于是知道了Linux系统帐号，只要crack其samba帐 号密码加以利用就可以攻击samba服务器哈。所以我们要使用用户帐号映射这个功能来解决这个问题哈~~~

用户帐号映射这个功能需要建立一个帐号映射关系表，里面记录了samba帐号和虚拟帐号的对应关系，客户端访问samba服务器时就使用虚拟来登录哈。

1）编辑主配置文件/etc/samba/smb.conf

在global下添加一行字段username map = /etc/samba/smbusers开启用户帐号映射功能。

2）编辑/etc/samba/smbusers

smbusers文件保存帐号映射关系，其有固定滴格式：

samba帐号 = 虚拟帐号（映射帐号）

帐号redking就是我们上面建立的samba帐号（同时也是Linux系统帐号），51cto及51blog就是映射滴帐号名（虚拟帐号），帐号 redking在我们访问共享目录时只要输入51cto或51blog就可以成功访问了，但是实际上访问samba服务器的还是我们滴redking帐 号，这样一来就解决了安全问题哈~我们继续。

3）重启samba服务：service smbd restart

4）验证效果哈~

输入我们定义的映射帐号51cto，注意我们没有输入帐号redking哈~，映射帐号51cto滴密码和redking帐号一样哈~

现在就可以通过映射帐号浏览共享目录了哈~

注意：强烈建议不要将samba用户的密码与本地系统用户的密码设置成一样哈，可以避免非法用户使用samba帐号登录系统非法破坏哈~~~

4.2 客户端访问控制

对于samba服务器的安全性，我们已经说过可以使用valid users字段去实现用户访问控制，但是如果企业庞大，存在大量用户的话，这种方法操作起来就显得比较麻烦哈~比如samba服务器共享出一个目录来访 问，但是要禁止某个IP子网或某个域的客户端访问此资源，这样滴情况使用valid users字段就无法实现客户端访问控制。

下面我们就讲下使用hosts allow和hosts deny两个字段来实现该功能。而用好这两个字段滴关键在于熟悉和清楚它们的使用方法和作用范围哈

hosts allow 和 hosts deny 的使用方法

1）hosts allow 和 hosts deny 字段的使用

hosts allow 字段定义允许访问的客户端

hosts deny 字段定义禁止访问的客户端

2）使用IP地址进行限制

比如公司内部samba服务器上共享了一个目录sales，这个目录是存放销售部的共享目录，公司规定192.168.0.0/24这个网段的IP地址禁止访问此sales共享目录，但是其中192.168.0.24这个IP地址可以访问。

先将安全级别模式由user改为share

这里我们添加hosts deny和hosts allow字段

hosts deny = 192.168.0. 表示禁止所有来自192.168.0.0/24网段的IP地址访问

hosts allow = 192.168.0.24 表示允许192.168.0.24这个IP地址访问

当host deny和hosts allow字段同时出现并定义滴内容相互冲突时，hosts allow优先。现在设置的意思就是禁止C类地址192.168.0.0/24网段主机访问，但是允许192.168.0.24主机访问。

测试下效果，如果是192.168.0.24的客户端就可以正常访问

如果是其他客户端滴话就是这样的效果

如果想同时禁止多个网段滴IP地址访问此服务器可以这样设置

hosts deny = 192.168.1. 172.16. 表示拒绝所有192.168.1.0网段和172.16.0.0网段的IP地址访问sales这个共享目录。

hosts allow = 10. 表示允许10.0.0.0网段的IP地址访问sales这个共享目录。

注意：当需要输入多个网段IP地址的时候，需要使用“空格”符号隔开。

3）使用域名进行限制

我们来看这样一个例子哈，公司samba服务器上共享了一个目录public，公司规定.sale.com域和.net域的客户端不能访问，并且主机名为free的客户端也不能访问。

hosts deny = .sale.com .net free 表示禁止.sale.com域和.net域及主机名为free的客户端访问public这个共享目录。

注意：域名和域名之间或域名和主机名之间需要使用“空格”符号隔开。

4）使用通配符进行访问控制

samba服务器共享了一个目录security，规定所有人不允许访问，只有主机名为boss的客户端才可以访问。对于这样一个实例哈，我们就可以通过使用通配符的方式来简化配置。

hosts deny = All 表示所有客户端，并不是说允许主机名为ALL的客户端可以访问哈~~~

常用的通配符还有“\*”，“？”，“LOCAL”等。

还有一种比较有意思的情况，如果我们规定所有人不能访问security目录，只允许192.168.0.0网段的IP地址可以访问，但是 192.168.0.100及192.168.0.78的主机是要禁止访问滴。我们可以使用hosts deny禁止所有用户访问，再设置hosts allow允许192.168.0.0网段主机，但当hosts deny和hosts allow同时出现而且冲突滴时候，hosts allow生效，如果这样滴话，那么允许192.168.0.0网段的IP地址可以访问，但是192.168.0.100及192.168.0.78的主 机禁止访问就无法生效了哈~我们可以使用EXCEPT进行设置。

hosts allow = 192.168.0. EXCEPT 192.168.0.100 192.168.0.78 表示允许192.168.0.0网段IP地址访问，但是192.168.0.100和192.168.0.78除外哈~

hosts allow 和 hosts deny 的作用范围

hosts allow和hosts deny设置在不同的位置上，它们的作用范围是不一样滴。如果设置在[global]里面，表示对samba服务器全局生效哈，如果设置在目录下面，则表只对这个目录生效。

这样设置表示只有192.168.0.88才可以访问samba服务器，全局生效哈~

这样设置就表示只对单一目录security生效，只有192.168.0.88才可以访问security目录里面的资料。

4.3 设置Samba的权限

到这里我们已经可以对客户端访问进行有效的控制，但是对于能访问的客户端来说，我们还是不能灵活方便滴控制他们访问共享资源的权限，比如boss或gm这 样的帐号可以对某个共享目录具有完全控制权限，其他帐号只有只读权限哈，这样的情况我们就可以使用write list字段来实现哈~

例如公司samba服务器上有个共享目录tech，公司规定只有boss帐号和tech组的帐号可以完全控制，其他人只有只读权限。如果只用 writable字段则无法满足这个实例的要求，因为当writable = yes时，表示所有人都可以写入了哈，而当writable = no时表示所有人都不可以写入。这时我们就需要用到write list字段哈~

write list = boss,@tech 就表示只有boss帐号和tech组成员才可以对tech共享目录有写入权限哈（其中@tech就表示tech组）。

我们来看下writable和write list之间的区别：

字段

值描述

writable

yes

所有帐号都允许写入

writable

no

所有帐号都禁止写入

write list

写入权限帐号列表

列表中的帐号允许写入

4.4 Samba的隐藏共享

我们还可以使用browseable字段实现隐藏共享的功能哈~~~

比如我们要把samba上的技术部共享目录隐藏，我们可以这样设置。

browseable = no表示隐藏该目录

现在就看不到tech共享目录了哈~

如果我们直接输入[url=file://..192.168.0.188.tech/]\\192.168.0.188\tech[/url]就可以访问了哈~

在有些特殊的情况下，browseable也无法满足企业的需求，比如，samba服务器上有个security目录，此目录只有boss用户可以浏览访 问，其他人都不可以访问。因为samba的主配置文件只有一个，所有帐号访问都要遵守该配置文件的规则，如果隐藏了该目录，那么所有人就都看不到该目录 了，就像上面演示的一样，要知道共享目录名称后输入[url=file://..192.168.0.188.tech/]\\192.168.0.188\tech[/url]才可以访问技术部资料。如果这样滴目录一多滴话，不可以叫boss去记那么多目录名称哈，那样还不被boss骂死哈~~~^\_^问题出在samba服务的主配置文件只有一个，而smb.conf没有提供字段允许部分人可以浏览隐藏目录的功能。

那我们可以换个角度哈，既然单一滴配置文件无法实现要求，那么我们可以为不同需求的用户或组分别建立相应的配置文件并单独配置后实现其隐藏目录的功能哈，现在我们为boss帐号建立一个配置文件，并且让其访问的时候能够读取这个单独的配置文件。

（1）建立独立滴配置文件哈~

先为boss帐号创建一个单独的配置文件，我们可以直接复制/etc/samba/smb.conf这个文件并改名就可以了，如果为单个用户建立配置文件，命名时一定要包含用户名哈。

我们使用cp命令复制主配置文件，为boss帐号建立独立的配置文件。

（2）编辑smb.conf主配置文件哈~

在[global]中加入config file = /etc/samba/smb.conf.%U，表示samba服务器读取/etc/samba/smb.conf.%U文件，其中%U代表当前登录用户。命名规范与独立配置文件匹配哈~

（3）编辑smb.conf.boss独立配置文件

编辑boss帐号的独立配置文件smb.conf.boss，将tech目录里面的browseable = no删除，这样当boss帐号访问samba时，tech共享目录对boss帐号访问就是可见滴，这样主配置文件smb.conf和boss帐号的独立配 置文件相搭配就有实现其他用户访问时tech共享目录是隐藏滴，而boss帐号访问时就是可见滴。

（4）重新启动samba服务：service smbd restart

（5）测试效果哈~

现在我们以普通用户redking帐号登录samba服务器哈~~~

发现以redking帐号登录samba看不到tech共享目录哈~~证明tech共享目录对除boss帐号以外的人是隐藏共享滴。

现在我们以boss帐号登录来看看哈~~

我们发现以boss帐号登录之后，tech共享目录自动显示了哈~~~

这样以独立配置文件的方法来实现隐藏共享对不同帐号的可见性非常方便哈~

注意：目录隐藏了并不是说不共享了，只要知道共享名，并且有相应权限，还是可以访问滴，就像上面演示的一样，可以输入“\\IP地址\共享名”的方法就可以访问隐藏共享了。

5 Samba客户端配置

5.1 Linux客户端访问Samba共享

linux客户端访问服务器主要有两种方法

1）使用smbclient命令

在Linux中，samba客户端使用smbclint这个程序来访问samba服务器时，先要确保客户端已经安装了samba-client这个rpm包。

smbclient可以列出目标主机共享目录列表

smbclient命令格式：smbclient -L 目标IP地址或主机名 -U 登录用户名%密码

当我们查看rhel5(192.168.0.188)主机的共享目录列表时，提示输入密码，这时候可以不输入密码哈，我们直接按回车，这样表示匿名登录，然后就会显示匿名用户可以看到的共享目录列表了哈~

smbclient -L rhel5或者smbclient -L 192.168.0.188

如果想使用samba帐号相看samba服务器端共享了什么目录，我们可以加上-U参数哈~，后面跟上用户名%密码。

smbclient -L 192.168.0.188 -U boss%boss

这样就显示了只有boss帐号才显示的tech技术部共享目录。

注意：不同用户使用smblient浏览的结果可能是不一样滴，这要根据服务器设置的访问控制权限而定哈~

我们还可以在使用smbclient命令行共享访问模式浏览共享的资料哈

smbclient命令行共享访问模式命令格式：

smbclient //目标IP地址或主机名/共享目录 -U 用户名%密码

上面已经显示了服务器上有一个tech共享目录，我们来查看一下里面的内容哈~

另外smbclient登录samba服务器后，我们可以使用help查询所支持的命令。

2）使用mount命令挂载共享目录

mount命令挂载共享目录格式：

mount -t cifs //目标IP地址或主机名/共享目录名称 挂载点 -o username=用户名

[root@client ~]# mount -t cifs //192.168.0.188/tech /mnt/sambadata/ -o username=boss%boss

这表示挂载192.168.0.188主机上的共享目录tech到/mnt/sambadata目录下，cifs就是samba所使用的文件系统哈

5.2 Windows客户端访问Samba共享

这个就比较简单了哈，我们也一直用这个访问微软的共享目录哈，上面其他也已经讲过了哈，方法就是在开始运行里面使用UNC路径直接进行 访问哈~~也可以到网上邻居里面找，但是偶不太喜欢用这个方法，因为速度太慢哈。还是觉得在开始--运行或是直接在资源管理器或IE的地址栏里面输入 UNC路径比较快哈~

1）在开始--运行里面使用UNC路径直接进行访问

2）映射网络驱动器访问samba服务器共享目录

输入tech共享目录的地址

输入可以访问tech共享目录的samba帐号和密码

这时在我的电脑的网络驱动器中就可以看到映射的Z盘了哈~

打开Z盘就可以访问tech共享目录里面的资源。

6 Samba的打印共享

默认情况下，samba的打印服务是开放滴~所以我们只要把打印机安装好后客户端的用户就可以使用打印机了。

1）设置global配置项

修改smb.conf全局配置，开启打印共享功能

2）设置printers配置项

使用默认设置就可以让客户端正常使用权打印机了哈，需要注意的就是printable一 定要设置成yes哈，如果不设置成yes那还打什么哈~~~path字段定义打印机队列，可以根据需要自己定制哈，另外共享打印和共享目录不一样哈，安装 完打印机后必须重新启动samba服务，否则客户端可能无法看到共享的打印机。如果设置只允许部分员工使用打印机，我们可以使用valid users、hosts allow或hosts deny字段来实现哈，这些在讲共享目录时已经说过了，不清楚可以再翻翻看哈~~下面进入samba企业实战与应用。

7 Samba企业实战与应用

7.1 企业环境及需求

samba服务器目录：

企业数据目录：/companydata

公共目录：/companydata/share

销售部目录：/companydata/sales

技术部：/companydata/tech

企业员工情况：

总经理：gm

销售部：销售部经理 redking、员工 sky、员工 jane

技术部：技术部经理 michael、员工 bill、员工 joy

搭建samba文件服务器，建立公共共享目录，允许所有人访问，权限为只读，为销售部和技术部分别建立单独的目录，只可以总经理和相应部门员工访问，并且公司员工禁止访问非本部门的共享目录。这是个典型的企业文件服务器案例哈。

总经理-----------------------

|

销售部-------------------交换机--------------------samba服务器

|

技术部-----------------------

7.2 需求分析

对于建立公共目录public字段就可以实现匿名访问，员工只能访问本部门的共享目录，禁止访问非本部门的共享目录，我们可以通过设置 目录共享字段“browseable = no”及字段“valid users”来实现其隐藏功能和相应的访问权限。这样设置不能很好得解决同一目录多种需求的权限设置，所以我们需要建立独立配置文件，为每个部门建立一个 组后并为每个组建立配置文件来实现隔离用户权限会比较灵活哈~

7.3 解决方案

1）建立各部门专用共享目录

使用mkdir建立需求的共享目录以便分门别类的存储相应资料。

同时设置/companydata共享目录的用户权限

2）添加samba服务器描述及设置smbpasswd文件

默认/etc/samba/目录下没有smbpasswd文件,我们要先关闭samba的tdbsam验证。

解决方法：在smb.conf文件中注释掉passdb backend = tdbsam 一行，加上smb passwd file = /etc/samba/smbpasswd，然后保存退出。

3)添加用户和组

先建立销售部组sales，技术部组tech，然后使用useradd命令添加总经理帐号gm及各个员工的帐号并加入相应的用户组。

接着使用smbpasswd命令添加samba用户

呃~~~不好意思哈~~~帐号gm的samba用户忘记添加了，现在补上哈~

4）配置smb.conf文件

（1）建立单独配置文件

用户配置文件使用用户名命令哈，组配置文件使用组名命令。

（2）设置主配置文件smb.conf

这里我们配置smb.conf主配置文件，在global中添加相应字段哈，确保samba服务器的主配置文件可以调用独立的用户配置文件和组配置文件。

include = /etc/samba/%U.smb.conf表示使samba服务器加载/etc/samba目录下格式为“用户名.smb.conf”的配置文件。

include = /etc/samba/%G.smb.conf表示使samba服务器加载/etc/samba目录下格式为“组名.smb.conf”的配置文件。

设置共享目录/companydata/share

（5）设置总经理gm配置文件

vim /etc/samba/gm.smb.conf

（6）设置销售部组sales配置文件

vim /etc/samba/sales.smb.conf

（7）设置技术部组tech配置文件

vim /etc/samba/tech.smb.conf

（8）开启samba服务

service smb start

（9）测试

我们先用gm帐号登录测试

可以全部看到共享目录。

/companydata/share目录只读

注意：

最好禁用RHEL5中的selinux功能，否则会出现些莫名其妙滴问题，比如下面的帐号gm明明对共享目录sales和tech是777的权限，但就是只能创建文件却不能创建文件夹哈~

关闭selinux，打开selinux配置文件/etc/selinux/config设置selinux = disabled后保存退出并重启系统。

查看selinux当前状态sestatus -v

现在我们就可以创建文件夹了

现在我们以其他帐号测试，就用技术部joy吧

在这里技术部的员工就看不到销售部的共享目录。同时对public目录只读权限，对tech目录有读写权限。

因为禁止对共享目录sales访问，就算知道了[url=file://..rhel5.sales/]\\rhel5\sales[/url]路径也是不能访问滴

8 Samba排错

1）Linux服务一般滴排错方法

（1）错误信息

一般仔细看下显示的错误信息，根据错误提示一般滴问题就可以判断问题出在什么地方了。

（2）配置文件

第2个我们可以查配置文件，有时可能误操作导致配置失误，服务无法正常运行，我们可以通过检查配置文件来确认问题。现在很多服务的软件包有自带配置文件检查工具，我们可以通过这些工具对配置文件进行检查哈~

（3）日志文件

如果服务出现问题，我们还可以使用tail命令来动态监控日志文件（在CLI状态下可以使用Ctrl+Alt+F1~F6切换到另一个CLI文字终端下查看）。

tail -F /var/log/messages

2）samba服务故障排错

（1）使用testparm命令检查

上面偶提到软件包有自带的配置文件检查工具，我们可以使用testparm命令检测smb.conf文件的语法，如果报错，说明smb.conf文件设置有错误哈，这样我们可以根据提示信息来修改主配置文件和独立配置文件。

testparm /etc/samba/smb.conf

[root@rhel5 ~]# testparm /etc/samba/smb.conf

Load smb config files from /etc/samba/smb.conf

Can't find include file /etc/samba/.smb.conf

Can't find include file /etc/samba/%G.smb.conf

Processing section "[homes]"

Processing section "[printers]"

Processing section "[public]"

Loaded services file OK.

Server role: ROLE\_STANDALONE

Press enter to see a dump of your service definitions

[global]

workgroup = COMPANYDOMAIN

server string = Company Samba File Server

cups options = raw

include = /etc/samba/%G.smb.conf

[homes]

comment = Home Directories

read .ly = No

browseable = No

[printers]

comment = All Printers

path = /var/spool/samba

printable = Yes

browseable = No

[public]

comment = public data

path = /companydata/share

guest ok = Yes

[root@rhel5 ~]# testparm /etc/samba/gm.smb.conf

Load smb config files from /etc/samba/gm.smb.conf

Processing section "[homes]"

Processing section "[printers]"

Processing section "[sales]"

Processing section "[tech]"

Loaded services file OK.

Server role: ROLE\_STANDALONE

Press enter to see a dump of your service definitions

[global]

workgroup = COMPANYDOMAIN

server string = Company Samba File Server

cups options = raw

[homes]

comment = Home Directories

read .ly = No

browseable = No

[printers]

comment = All Printers

path = /var/spool/samba

printable = Yes

browseable = No

[sales]

comment = sales data

path = /companydata/sales

valid users = gm

read .ly = No

[tech]

comment = tech data

path = /companydata/tech

valid users = gm

read .ly = No

[root@rhel5 ~]# testparm /etc/samba/sales.smb.conf

Load smb config files from /etc/samba/sales.smb.conf

Processing section "[homes]"

Processing section "[printers]"

Processing section "[sales]"

Loaded services file OK.

Server role: ROLE\_STANDALONE

Press enter to see a dump of your service definitions

[global]

workgroup = COMPANYDOMAIN

server string = Company Samba File Server

cups options = raw

[homes]

comment = Home Directories

read .ly = No

browseable = No

[printers]

comment = All Printers

path = /var/spool/samba

printable = Yes

browseable = No

[sales]

comment = sales data

path = /companydata/sales

valid users = @sales, gm

read .ly = No

[root@rhel5 ~]# testparm /etc/samba/tech.smb.conf

Load smb config files from /etc/samba/tech.smb.conf

Processing section "[homes]"

Processing section "[printers]"

Processing section "[tech]"

Loaded services file OK.

Server role: ROLE\_STANDALONE

Press enter to see a dump of your service definitions

[global]

workgroup = COMPANYDOMAIN

server string = Company Samba File Server

cups options = raw

[homes]

comment = Home Directories

read .ly = No

browseable = No

[printers]

comment = All Printers

path = /var/spool/samba

printable = Yes

browseable = No

[tech]

comment = tech data

path = /companydata/tech

valid users = @tech, gm

read .ly = No

[root@rhel5 ~]#

2）使用ping命令测试

samba服务器主配置文件排除错误后重启smb服务，如果客户端仍然无法连接samba服务器，我们在客户端可以使用ping命令进行测试,这个我们微软的系统中排障一样哈，根据出现的不同情况可以进行分析哈。

（1）如果没有收到任何提示，说明客户端TCP/IP协议安装有问题，需要重新安装客户端TCP/IP协议，然后重新测试。

（2）如果提示“host not found”则检查客户端DNS或者/etc/hosts文件有没正确设置，确保客户端能够使用名称访问samba服务器。

（3）无法ping通还可能是防火墙设置滴问题，需要重新设置防火墙的规则，开启samba与外界联系的端口。

（4）当然还有一种低级的情况，那就是由于主机名输入错误导致不能ping通，请更正后重试哈~~~O(^\_^)O

3）使用smbclient命令进行测试

如果客户端与samba服务器可以ping通，说明客户端与服务器间的连接没有问题哈，如果还是不能访问samba共享资源，可以执行smbclient命令进一步测试服务器端的配置。

如果测试samba服务器正常，并且输入了正确的帐号和密码，那么执行smbclient命令就可以获得共享列表。

smbclient -L 192.168.0.188 -U joy%123

如果我们看到了错误信息提示“tree connect failed”则说明可以在smb.conf文件中设置了host deny字段拒绝了客户端的IP地址或域名，我们可以修改smb.conf配置文件允许客户端访问就可以了哈~

如果返回信息是“connection refused”提示拒绝连接则说明是samba服务器smbd进程可以没有被开启哈~我们必须确保smbd和nmbd进程处于开启状态，并使用netstat -a检查netbios使用的139端口是否处于监听状态哈。

检查samba服务

开启smb服务

netbios-ssn 会话管理

netbios-ns 名字解析

netbios-dgm 数据报

如果提示“session setup failed”连接建立失败则说明服务器拒绝了连接请求，这是因为输入的用户名和密码错误引起滴，我们输入正确的帐号和密码就ok了哈~

有时也会收到比如“Your server software is being unfriendly”错误信息，提示服务器软件存在问题，这个故障一般是因为配置smbd时使用了错误的参数或者启用smbd时遇到的类似严重破坏错 误，我们可以使用testparm来检查相应的配置文件并同时检查相关日志文件哈。