windows同步linux用户,用winbind实现windowsPDC和linux系统的帐号同步

转载 吹亚吹 于 2021-05-07 18:53:41 发布 320 收藏
文章标签： windows同步linux用户

测试环境：操作系统：redflagDC4.1 samba版本:samba-3.0.2a-9AX ip：172.16.100.2

(注意，一定要使用比较“干净”的DC4.1环境，就用自带的samba也可以成功，我们之前的测试因为操作系统已经被别人做过配置，所以换了好几个版本的samba都不行，不得已后来重新安装DC4.1，配置就很顺利了。)

PDC控制器：windows2000Server 测试域名tail 主机名pig ip:172.16.100.1

测试DNS ： windows2000Server 主机名pig (与PDC为同一台服务器)

测试过程：

一、准备工作：

配置windows2000Server为PDC，建立tail域，配置能够解析 tail 域的DNS，并用window2000或者windows98和客户端使用该DNS，能够正确登录windows2000Server的PDC域。

二、配置winbindd服务连接PDC抓到的域内的用户和组信息：

1、修改nsswitch.conf文件：

vi /etc/nsswitch.conf

做如下修改，使winbind成为passwd及group的认证信息源

passwd: files winbind

shadow: files

group: files winbind

2、配置DC4.1的DNS客户端文件：

vi /etc/resolv.conf

加上nameserver 172.16.100.1

ping一下pig.tail，确保可以连通

3、vi smb.conf，确保[global]段设置中有下面几行：

[global]

workgroup = TAIL

netbios name = rfdc41

server string = Samba Server

security = domain

password server = pig.tail

preferred master = no

domain master = no

domain logons = no

idmap uid = 10000-20000

idmap gid = 10000-20000

template shell = /bin/bash

template homedir = /home/%D/%U

winbind separator = %

winbind use default domain = Yes

idmap uid和idmap gid是设置winbind把win200x域用户、组map成本地用户、组所使用的ID号范围，如果用户很多，可以加大这两个值之间的差。

Template homedir是用户登录后的主目录，我设置成/home/域名/用户名。

Template shell是用户登录后的shell，如果你想用PDC给你的sshd做认证，就可以加上这个，给用户一个登录shell。

winbind separator是获取帐号的时候，域名与用户名之间的分隔符，比如tail%work

winbind use default domain设置它为yes是在显示的时候屏蔽掉域名与用户名之间的分隔符，否则用户在登录linux系统的时候，就要很烦琐地键入类似tail%work这样的用户名了。

5、用samba的net join命令把这台机器加入到windows200x域中(samba3.0以上的版本可以支持)

net rpc join -S pig.tail -U Administrator

然后输入域管理员密码，也就是Administrator的密码。

6、启动samba服务和winbindd服务

#service smb start

#service winbind start

7、用wbinfo命令查看用winbindd服务连接PDC抓到的域内

wbinfo -u

可以看到类似如下winbind抓取到的PDC用户信息：

Administrator

Guest

huaijinyang

jack

krbtgt

laohuai

user1

user2

user3

user4

user5

work

再执行：

wbinfo -g

可以看到类似如下winbind抓取到的PDC组信息：

BUILTIN%System Operators

BUILTIN%Replicators

BUILTIN%Guests

BUILTIN%Power Users

BUILTIN%Print Operators

BUILTIN%Administrators

BUILTIN%Account Operators

BUILTIN%Backup Operators

BUILTIN%Users

Domain Admins

Domain Users

Domain Guests

Domain Computers

Domain Controllers

Cert Publishers

Schema Admins

Enterprise Admins

Group Policy Creator Owners

DnsUpdateProxy

zzz

8、检查PDC用户(组)转换为本地用户(组)UID和GIU情况：

getent passwd

显示将PDC用户转换成系统用户的UID情况，显示最后类似如下信息：

Administrator:x:10000:10000::/home/TAIL/Administrator:/bin/bash

Guest:x:10001:10000::/home/TAIL/Guest:/bin/bash

huaijinyang:x:10002:10000:huai:/home/TAIL/huaijinyang:/bin/bash

jack:x:10003:10000:jack:/home/TAIL/jack:/bin/bash

krbtgt:x:10004:10000::/home/TAIL/krbtgt:/bin/bash

laohuai:x:10010:10000:laohuai:/home/TAIL/laohuai:/bin/bash

user1:x:10005:10000:user1:/home/TAIL/user1:/bin/bash

user2:x:10006:10000:user2:/home/TAIL/user2:/bin/bash

user3:x:10007:10000:user3:/home/TAIL/user3:/bin/bash

user4:x:10008:10000:user4:/home/TAIL/user4:/bin/bash

user5:x:10011:10000:user5:/home/TAIL/user5:/bin/bash

work:x:10009:10000:work:/home/TAIL/work:/bin/bash

PDC用户Administrator的UID从10000开始。

getent group

显示将PDC用户转换成系统用户的GID情况，显示最后类

Domain Admins:x:10003:Administrator

Domain Users:x:10000:Administrator,Guest,krbtgt,work,jack,user1,user2,user3,user4,huaijinyang,user5,laohuai

Domain Guests:x:10005:Guest

Domain Computers:x:10006:CALL-CENTER$,hjy$,localhost$,lishen$,HUAIJINYANG$,smb1$,rfas41$,lux$

Domain Controllers:x:10007:PIG$

Cert Publishers:x:10008:

Schema Admins:x:10002:Administrator

Enterprise Admins:x:10004:Administrator

Group Policy Creator Owners:x:10001:Administrator

DnsUpdateProxy:x:10009:

zzz:x:10010:

BUILTIN%System Operators:x:10011:

BUILTIN%Replicators:x:10012:

BUILTIN%Guests:x:10013:

BUILTIN%Power Users:x:10014:

BUILTIN%Print Operators:x:10015:

BUILTIN%Administrators:x:10016:

BUILTIN%Account Operators:x:10017:

BUILTIN%Backup Operators:x:10018:

BUILTIN%Users:x:10019:

PDC组Users 的UID从10000开始。

能够看到这样的信息，表示配置工作已经完成了大半，winbind服务已经在正常工作了。

这里有一点需要注意，如果在PDC域中新建了用户或者为某个用户修改了密码，需要重新刷新samba服务和winbind服务，过程如下：

service smb stop

service winbind stop

rm -f /etc/samba/*.tdb

rm -f /var/cache/samba/*.tdb

net rpc join -S pig.tail -U Administrator

service smb start

service winbind start

才能重新抓取到PDC的更新信息。

9、建立用户的登录主目录

samba的配置文件中指定了template homedir的路径，我们先要建立这个目录

mkdir /home/TAIL

注意PDC域名要大写！

三、配置PDC用户登录的pam认证

1

、备份原来的pam认证文件

mkdir /home/backup

cp /etc/pam.d/login /home/backup

cp /etc/pam.d/system-auth

2、修改login文件

vi /etc/pam.d/login

这个文件最后一句是

session optional pam_console.so

在这句后面加上

session required pam_mkhomedir.so skel=/etc/skel umask=0022

3、修改system-auth文件

vi /etc/pam.d/system-auth

a、找到以“auth”字符串开头并调用“pam_unix.so”的语句，如下：

auth sufficient /lib/security/$ISA/pam_unix.so likeauth nullok

在这一句最后加上字符串“use_first_pass”,如下：

auth sufficient /lib/security/$ISA/pam_unix.so likeauth nullok use_first_pass

然后在这一句上面加上语句：

auth sufficient /lib/security/pam_winbind.so

b、找到以“account”字符串开头并调用“pam_unix.so”的语句，如下：

account required /lib/security/$ISA/pam_unix.so

在这一句最后加上字符串“use_first_pass”,如下：

account required /lib/security/$ISA/pam_unix.so use_first_pass

然后在这一句上面加上语句：

account sufficient /lib/security/pam_winbind.so

四、用PDC用户登录测试

在linux中某个终端以PDC用户登录，能够看到$提示符，说明配置完成。

相关日志