

Integrating Suse Linux Enterprise Server 10 with Microsoft Active Directory and Server 2003

Disclaimer

The Origin of this information may be internal or external to Astera. Astera makes all reasonable efforts to verify this information. However, the information provided in this document is for your information only and is provided as is. Astera makes no explicit or implied claims to the validity of this information. Any trademarks referenced in this document are the property of their respective owners.

Scope

This how to was created to document the successful integration of user accounts between Linux and Active Directory. This configuration will allow you to use your Active Directory users as the primary accounts logging into Linux, including access to Samba shares on Linux. You can also create local Linux accounts for specific purposes. This document assumes a one forest, one domain AD environment. This document assumes you have a working knowledge of Linux.

Information / Fact

This configuration has been tested with the following configuration. With some tweaking, you might be able to apply the following with different versions of the operating systems and apps used, but for the purpose of this document, the following was used;

Microsoft Window Server 2003 Standard

Installed services / apps

- Active Directory (must be a DC)
- DNS

Suse Linux Enterprise Server 10.1 Sp1

Installed packages

Libsmbclient 3.0.24-2.23
Nautilus-share 0.6.4-31.8
Samba 3.0.24-2.23
Samba-client 3.0.24-2.23
Samba-winbind 3.0.24-2.23
Samba winbind Winbind daemon 3.0.24-2.23
Krb5 1.4.3-19.17
Krb5-apps-clients 1.4.3-19.17
Krb5-client 1.4.3-19.17
Pam_krb5 1.4.3-19.17
NTP

Once you have installed the Suse packages, and your windows environment is running, you can now integrate the two. Before you begin, please review this document and backup all files that will require modification. It is particularly important to backup the /etc/nsswitch.conf file. It is quite possible that modifying this file can render your Linux server unable to authenticate users, therefore do not reboot or log off unless you have tested the changes. Creating a recover disk for Linux would also be a good idea. It is **important that DNS is working properly** with reverse lookups, and that both Windows and Linux servers are able to properly resolve each other.

Configure Linux to communicate with AD via Kerberos. It is important that you configure time synchronization, in order to ensure your Windows DC and the SUSE server have the same time. In this example, NTP server is configured on the Windows DC, and the Linux NTP client is configured to sync with the Windows server. Below is the ntp.conf file in /etc.

Ntp.conf

```
##
server 127.127.1.0
# local clock (LCL)
fudge 127.127.1.0 stratum 10
# LCL is unsynchronized

##
## Outside source of synchronized time
##
## server xx.xx.xx.xx      # IP address of server
##
## Miscellaneous stuff
##
driftfile /var/lib/ntp/drift/ntp.drift
# path for drift file
logfile /var/log/ntp
server yourtimeserver.com
```

Once you have verified that time is synchronized, you need to configure Kerberos on the Linux server. You can use Yast or you can manually modify your krb5.conf file in /etc. Note that the domain name in the krb5 file is the name of your Active Directory domain name. The krb5.conf file should look something like this;

Krb5.conf

```
[libdefaults]
    default_realm = YOURDOMAIN.COM
    clockskew = 300

[realms]
YOURDOMAIN.COM = {
    kdc = windowsdcserver.yourdomain.com
    default_domain = yourdomain.com
    admin_server = windowsdcserver.yourdomain.com
}

[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON

[domain_realm]
    .yourdomain.com = YOURDOMAIN.COM

[appdefaults]
pam = {
```

```
ticket_lifetime = 1d
renew_lifetime = 1d
forwardable = true
proxiable = false
retain_after_close = false
minimum_uid = 1
try_first_pass = true
```

Once Kerberos is configured, you will then need to request a Kerberos ticket in order to join the Linux server to the AD domain. To request a ticket, type the following;

```
Kinit administrator@YOURDOMAIN.COM
```

This is your AD administrator username and when requested, you will need to type in the password. You will then be returned to the command prompt. This means that the Linux server received a valid ticket. You can view the ticket by typing “*klist*”. The system should return something that is similar to the following;

```
Ticket cache: FILE:/tmp/krb5cc_10000
Default principal: administrator@YOURDOMAIN.COM
```

```
Valid starting Expires Service principal
08/03/07 13:42:47 08/03/07 23:42:54 krbtgt/ YOURDOMAIN.COM @ YOURDOMAIN.COM
renew until 08/04/07 13:42:47
```

```
Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

Now that you have a valid Kerberos ticket, you can join the Linux server to the Windows domain. To do this, type the following;

```
net join -U administrator@YOURDOMAIN.COM
```

The Linux server will now appear be visible in “Active Directory Users and Computers”. You can now move to the next step, configuring Samba / Winbind. It will be a good idea to backup the following files;

```
/etc/nsswitch.conf
/etc/samba/*
```

Stop the samba and winbind services by issuing the following commands;

```
rcsmb stop
rcwinbind stop
```

You will now need to modify the files that follow. Once again, you should always backup your originals. Once these files are modified, we will then proceed to the step in the authentication process.

/etc/samba/smb.conf

[global]

```
workgroup = NETBIOSDOMAINNAME
printing = cups
printcap name = cups
printcap cache time = 750
cups options = raw
map to guest = Bad User
include = /etc/samba/dhcp.conf
logon path = \\%L\profiles\.msprofile
logon home = \\%L\%U\.9xprofile
logon drive = P:
usershare allow guests = No
idmap gid = 10000-20000
idmap uid = 10000-20000
realm = YOURDOMAIN.COM
security = ads
password server = windowsdcserver.yourdomain.com
template homedir = /home/%D/%U
template shell = /bin/bash
winbind offline logon = yes
winbind refresh tickets = yes
winbind use default domain = yes
add machine script = /usr/sbin/useradd -c Machine -d /var/lib/nobody -s /bin/false %m$
domain logons = No
domain master = No
netbios name = linuxservername
passdb backend = smbpasswd
wins support = No
```

Share disabled by YaST

[profiles]

```
# comment = Network Profiles Service
# path = %H
# read only = No
# store dos attributes = Yes
# create mask = 0600
# directory mask = 0700
```

Share disabled by YaST

[users]

```
# comment = All users
# path = /home
# read only = No
# inherit acls = Yes
# veto files = /aquota.user/groups/shares/
```

Share disabled by YaST

[groups]

```
# comment = All groups
# path = /home/groups
# read only = No
# inherit acls = Yes
```

[printers]

```
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No
```

[print\$]

```
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @ntadmin root
force group = ntadmin
create mask = 0664
directory mask = 0775
```

Share disabled by YaST

[netlogon]

/etc/samba/smbusers

```
# This file allows you to map usernames from the clients to the server.
# Unix_name = SMB_name1 SMB_name2 ...
#
# See section 'username map' in the manual page of smb.conf for more
# information.
#
# This file is not included in the default configuration as it makes the
# usage of an user named administrator impossible.
```

```
root = administrator
;nobody = guest pcguest smbguest
```

/etc/nsswitch.conf

```
passwd: compat winbind
group: compat winbind
```

```
hosts: files dns
networks: files dns
```

```
services: files
protocols: files
rpc: files
ethers: files
netmasks: files
netgroup: files nis
publickey: files
```

```
bootparams: files
```

automount: files nis
aliases: files

Once the above files have been modified, run the following commands:

In order to activate changes done to the nsswitch.conf file, run

```
/sbin/ldconfig
```

You now need to make sure that samba and winbind services are on, specifically they need to be run on runlevels 3 and 5. Change to the /etc/rc.d directory, and verify if samba and winbind are running and in which runlevels by typing the following;

```
chkconfig -- list smb  
chkconfig -- list winbind
```

If these services are not already set to on for runlevels 3 and 5, turn them on by running the following commands;

```
chkconfig smb on  
chkconfig winbind on
```

Next, start the samba and winbind services on your server by running the following commands;

```
rcsmb start (you can also issue ./smb start)  
rcwinbind start (you can also issue ./winbind start)
```

You can now test to see if your Linux server sees Active Directory users and groups. To verify if your Linux Server can see users, type

```
wbinfo -u
```

and for groups

```
wbinfo -g
```

In both cases, you should see Active Directory objects appear as if they were local accounts. Note: If you do not see the users and or groups, you need to verify dns, Kerberos and your config files. Troubleshooting possible communication issues is beyond the scope of this document.

You can now test to see if you are able to log in using your windows credentials. Open up a telnet session, and at login, type in your windows username, and then enter your windows password. Your session should look something like this;

```
Welcome to SUSE Linux Enterprise Server 10 SP1 (i586) - Kernel 2.6.16.46-0.12-sm p (1).
```

```
Linuxservername login: windowsusername
```

```
Password:
```

```
Creating directory '/home/DOMAIN/windowsusername'.
```

```
Creating directory '/home/DOMAIN/windowsusername/bin'.
```

```
Creating directory '/home/DOMAIN/windowsusername/Documents'.
```

```
Creating directory '/home/DOMAIN/windowsusername/.mozilla'.
Creating directory '/home/DOMAIN/windowsusername/public_html'.
Creating directory '/home/DOMAIN/windowsusername/.xemacs'.
Creating directory '/home/DOMAIN/windowsusername/.fonts'.
Last login: Wed Jul 22 14:48:22 EDT 2007 from pc on pts/1
windowsusername@Linuxservername:~>
```

Congrats, this indicates that the Linux server is using Active Directory for user credentials, and is working fine. For each new user that logs onto Linux via winbind, a home directory is automatically created under /home/DOMAIN. Here you can modify the .profile for the users, etc.

You can now create Samba shares if you wish to publish Linux directories to your Windows systems. Follow the instructions below. Once again, backup any file you will modify prior to changing it.

By default ACL support is already built into the Suse 10.X kernel, as long as your using a file system that supports ACL. To enable ACL we will simply edit our /etc/fstab file and add the ACL option to the mount command of the volume where we will be exporting our Samba shares. In my configuration, the ACL option was already there, so no modification was required on my end. Here is an example of my fstab file.

```
/dev/sda2    /                reiserfs acl,user_xattr    1 1
/dev/sda1    swap             swap      defaults          0 0
proc         /proc            proc      defaults          0 0
sysfs        /sys             sysfs     noauto            0 0
debugfs      /sys/kernel/debug debugfs    noauto            0 0
devpts       /dev/pts         devpts    mode=0620,gid=5   0 0
/dev/fd0     /media/floppy    auto      noauto,user,sync  0 0
```

If your file does not include the acl option, add it by modifying the fstab file, and reboot the server. Once the server has come up, you can then create a directory that you wish to share, change the owner / group and then create a samba share. To do this, perform the following;

```
# mkdir directory
# chmod 770 directory
# chown -R DOMAINUSER directory
```

Next, backup your smb.conf file, and for each directory you want to share, create a similar entry in the smb.conf file, using the following format;

```
[share]
comment = share
path = /home/share
fstype = NTFS
browseable = Yes
writeable = Yes
acl support = Yes
security mask = 0750
directory mask = 0750
force security mode = 0750
force directory security mode = 0750
directory security mask = 0750
```

After you have setup your shares, save the smb.conf file and restart both your smb and winbind services located in /etc/rc.d directory.

```
# ./smb restart (you can also use rcsmb restart from any directory)
# ./winbind restart (you can also use rcwinbind restart from any directory)
```

From your windows machine map to your share(s) using the account you gave ownership to on the Linux side. Once your mapped you can right click on the share itself to define the share defaults for file creation and default permissions. Individual folders can be manipulated as you would normally. Use a few accounts to connect as different users to test your setting to ensure it works as you intend it to.

ACL from the Linux Side:

A standard ls or dir command will not show you the ACL info from the linux side , you can use the getfacl and the setfacl command to query or manipulate ACL information from the console.

```
# getfacl DirectoryName
```

This concludes this how to document. If you require further information, there are numerous resources available on the Internet, specifically www.samba.org, which was extremely helpful in our successful implementation. If you require further information or assistance from us, please do not hesitate to contact us via www.astera.net.