

Join Linux to Active Directory With Winbind

By Carla Schroder

Two weeks ago we gave the high-level view of what **windbind** is for. Today we'll walk through using winbind to provide a single sign-on for Linux servers and workstations joined to a Windows Active Directory domain.

Join Samba Servers to Active Directory

See Join Samba 3 to Your Active Directory Domain for how to do this. Additionally, there is one more step you should take after editing your configuration files. You should delete all *.tdb* files to get rid of stale data. You may want to back them up first; look for */etc/samba/secrets.tdb* (which may not exist) and in */var/lib/samba*.

Another important step is to make sure all systems are keeping the same time; Kerberos is especially sensitive to time synchronization. Setting up a local time server on Linux is easy, see Keeping Accurate Time on Linux. Configuring a local time server is easier than ever -- instead of listing individual time servers as the article says to do, configure */etc/ntp.conf* to use the NTP server pool:

```
server pool.ntp.org
server pool.ntp.org
server pool.ntp.org
```

Listing it three times creates performance redundancy -- if you hit a bad server, it will quickly try a different one. Then configure the local clients to point to your local NTP server.

Join Linux Workstations to Active Directory: PAM Fun

Samba and winbind provide authentication and identity resolution for Linux hosts that are part of an Active Directory domain, since Active Directory does not deign to provide a method for authenticating them directly. Follow the steps for joining a Samba server to AD. Then comes the hairy part -- if your Linux users require access to network services that require authentication, you'll have to configure PAM (pluggable authentication modules). This can be a bit vexing, but the advantage is it saves users from having to manage multiple logins. And it allows you to control access to services very precisely. In the olden days there was but a single */etc/pam.conf* file. Then it was improved and gained all kinds of flexibility, using a single file for each service in */etc/pam.d*. Adding to the fun is Red Hat, SuSE, Debian, and doubtless other distributions configure PAM a little differently, bless their individualistic little souls. Note to distribution maintainers: just because you can be different doesn't mean you have to.

Your very first job is to make a backup of */etc/pam.d*, because any mistake can prevent you from being able to login. So keep a bootable rescue disk handy or boot to single-user if you get in trouble, and restore your original configuration.

Stop both the **smbd** and **windbindd** services, if they are running. At the very least you must configure winbind authentication in */etc/pam.d/login*. Here is a sample configuration that works on Debian:

```
auth      required      /lib/security/pam_securetty.so
auth      sufficient   /lib/security/pam_winbind.so
auth      sufficient   /lib/security/pam_unix.so use_first_pass
auth      required     /lib/security/pam_nologin.so
account   sufficient   /lib/security/pam_winbind.so
```

Join Linux to Active Directory With Winbind

By Carla Schroder

```
session    required    /lib/security/pam_mkhomedir.so skel=/etc/skel
umask=0022
@include common-auth
@include common-account
@include common-session
session    optional    /lib/security/pam_console.so
@include common-password
```

The order of the directives is important. Make sure that `pam_winbind.so` is either copied or linked to `/lib/security`. PAM automatically looks in `/lib/security` for modules so you don't have to spell out the full path, but it's a good habit to get into anyway. The files `common-auth`, `common-account`, `common-session`, and `common-password` define common settings for all services.

The `use_first_pass` argument tells PAM to re-use the previously entered password. This works only for `auth` and `password` modules.

`session required /lib/security/pam_mkhomedir.so skel=/etc/skel umask=0022` is a slick little PAM feature that creates home directories for users on the fly.

This does the same thing on Red Hat:

```
#/etc/pam.d/login
auth        required    /lib/security/pam_securetty.so
auth        sufficient  /lib/security/pam_winbind.so
auth        sufficient  /lib/security/pam_unix.so use_first_pass
auth        required    /lib/security/pam_stack.so service=system-auth
auth        required    /lib/security/pam_nologin.so
account     sufficient  /lib/security/pam_winbind.so
account     required    /lib/security/pam_stack.so service=system-auth
password    required    /lib/security/pam_stack.so service=system-auth
session     required    /lib/security/pam_stack.so service=system-auth
session     required    /lib/security/pam_mkhomedir.so skel=/etc/skel
umask=0022
session     optional    /lib/security/pam_console.so
```

What if you want to authenticate SSH logins via PAM? Do this in `/etc/pam.d/ssh`:

```
auth        required    /lib/security/pam_securetty.so
auth        sufficient  /lib/security/pam_winbind.so
auth        sufficient  /lib/security/pam_unix.so
auth        required    /lib/security/pam_pwdb.so use_first_pass
account     sufficient  /lib/security/pam_unix.so
account     required    /lib/security/pam_winbind.so
session     required    /lib/security/pam_unix.so
session     required    /lib/security/pam_winbind.so
password    required    /lib/security/pam_unix.so
password    required    /lib/security/pam_winbind.so
```

How to configure other services? As a general rule, stick your `pam_winbind.so` module next to any existing line that references a standard Linux `auth`, `account`, `session`, or `password` module. I don't

Join Linux to Active Directory With Winbind

By Carla Schroder

promise that this will always work, but it's a good starting point. Or you can study the PAM documentation. Or wait for my detailed PAM howto.

Make sure that you do not have more than one account that has UID=0 in the password database. If there are two accounts in the passwd backend that have the same UID, winbind will break.

Now you can restart **smbd** and **windbindd** and try logging in from a Linux workstation. If you run into trouble look for help in Resources. The Samba mail list archives contain a wealth of excellent information.

Resources

- The Linux-PAM System Administrators' Guide
- man 7 pam
- Chapter 22 of The Official Samba-3 HOWTO and Reference Guide, "Winbind: Use of Domain Accounts"
- Chapter 26. "PAM-Based Distributed Authentication"
- Samba mail list
- Chapter 19 of the Linux Cookbook, "Keeping Time With NTP", and chapter 23 "File and Printer Sharing, and Domain Authentication With Samba"