

# Winbind Ties Linux and Windows Sign-Ons Together

by Carla Schroder

You keep hearing "Linux is like way cool! Use Linux!" Linux is cool, and even useful, but migrating from other platforms or integrating Linux hosts into an existing network takes a bit more work and knowledge than giving a careless wave of your hand, which is a minor detail that seems to escape the attention of enthusiastic Linux evangelists. Most sysadmins do not have the luxury of starting from scratch, and must make do with existing setups of varying (in)sanity and (il)logic.

The premier program for integrating Windows and Linux is Samba, which ace admins already know and love. Samba can be a cross-platform print and file server, a primary domain controller for a Windows LAN, and even a full member of an NT or Active Directory domain. The difficulty with running mixed Linux and Windows networks is managing user and group accounts and logins. The two platforms manage them in very different ways, which makes it difficult to integrate the two. A common method is to maintain two duplicate sets of users, groups, and passwords, which of course is less than ideal. (The word "sucks" can be confidently applied to this scenario.)

Fortunately the brainiacs behind Samba invented **winbind** to provide a unified logon, thus saving overworked admins from silliness like doing everything twice, and users from the horrors of trying to track what they are logging into, and which login to use. Winbind lets a Linux box become a full member of a Samba, Windows NT4 or Active Directory domain, and view Windows users and groups as Linux users and groups. All user and group queries from a Linux box are resolved by the domain controller.

Winbind is ideal for admins who wish to add Linux workstations or servers to an existing Windows domain. This allows a graceful introduction with a minimum of hassle. Servers and workstations slide right in without troubling users or bothering pointy-haired bosses.

You should also use winbind when you have hosts that are not members of the domain accessing a Samba or Windows domain. This is an important step to prevent unauthorized access from same-named foreign user accounts. For example, without winbind user Carla who is not a member of the domain will be able to access the files of user Carla who is a member of the domain. This, of course, is bad. Winbind does not allow this to happen; the foreign Carla will be given a different SID (security identifier) and so will not be able to get into the wrong files.

If you're using a simple peer network without user authentication, don't bother with winbind. Just for you bullet-point aficionados, here is a summary of what winbind does:

- Authenticates users
- Manages passwords
- Allows Linux users to use Windows domain resources as though they were native Linux resources
- User and group ID allocation

## Underlying Protocols

Winbind makes use of both the Windows NT RPC (remote procedure calls) and the native protocols of Active Directory. The Samba team received no assistance from Microsoft in decoding these calls, but somehow through persistence and tireless effort captured and decoded the signals over the wire. Moral: if interoperability and customer service are your desire, stick with the free/open source world.

# Winbind Ties Linux and Windows Sign-Ons Together

by Carla Schroder

For a NT4/Samba domain, you need Samba 3, winbind, NSS (name service switch), and PAM (pluggable authentication modules). For Active Directory you need Samba 3, winbind, LDAP, and Kerberos.

Using PAM allows authentication and password management to take place on the domain controller. PAM also lets the stern, controlling sysadmin set different authentication policies for different situations, such as for applications, or for users from different locations.

NSS provides a mechanism for hostnames, mail aliases, and user data to be resolved from various sources. Active Directory uses LDAP and Kerberos natively, which Linux can also do.

Windows uses RIDs (relative identifiers) for users and groups. Winbind converts these to Linux user and group numbers in a persistent database file called *winbind\_idmap.tdb*. This is not used when LDAP is used. Additionally, to speed up performance, winbind uses caching. The cache responds to requests, rather than hitting the domain controller for every request.

## Requirements

Samba and Winbind also work for just about any Unix variant. We'll use Linux in this series.

Collecting the necessary bits will vary depending on which Linux distribution you are using. You definitely want the latest stable version of Samba. Debian's Samba package includes everything you need, including support for PAM already compiled in. Most RPMs do the same. If you want to build from sources, see Resources.

If you are modifying an existing Samba server, back up everything! Back up *smb.conf*, */etc/pam.d*, and */etc/nsswitch.conf*. Messing up your PAM configuration means you may not be able to log in at all, so you must also have a rescue disk, such as Knoppix, at hand. Come back next week to learn how to configure all these things to make winbind do the heavy lifting for you.

## Resources

- Chapter 22 of The Official Samba-3 HOWTO and Reference Guide, "Winbind: Use of Domain Accounts"