NAME

winbindd - Name Service Switch daemon for resolving names from NT servers

SYNOPSIS

winbindd [-D|--daemon] [-F|--foreground] [-S|--stdout] [-i|--interactive] [-d <debug level>] [-s <smb config file>] [-n|--no-caching] [--no-process-group]

DESCRIPTION

This program is part of the **samba**(7) suite.

winbindd is a daemon that provides a number of services to the Name Service Switch capability found in most modern C libraries, to arbitrary applications via PAM and ntlm_auth and to Samba itself.

Even if winbind is not used for nsswitch, it still provides a service to smbd, ntlm_auth and the pam_winbind.so PAM module, by managing connections to domain controllers. In this configuration the **idmap config * : range** parameter is not required. (This is known as ‘netlogon proxy only mode’.)

The Name Service Switch allows user and system information to be obtained from different databases services such as NIS or DNS. The exact behaviour can be configured through the /etc/nsswitch.conf file. Users and groups are allocated as they are resolved to a range of user and group ids specified by the administrator of the Samba system.

The service provided by winbindd is called ‘winbind’ and can be used to resolve user and group information from a Windows NT server. The service can also provide authentication services via an associated PAM module.

The pam_winbind module supports the *auth*, *account* and *password* module-types. It should be noted that the *account* module simply performs a getpwnam() to verify that the system can obtain a uid for the user, as the domain controller has already performed access control. If the libnss_winbind library has been correctly installed, or an alternate source of names configured, this should always succeed.

The following nsswitch databases are implemented by the winbindd service:

hosts
: This feature is only available on IRIX. User information traditionally stored in the hosts(5) file and used by gethostbyname(3) functions. Names are resolved through the WINS server or by broadcast.

passwd
: User information traditionally stored in the passwd(5) file and used by getpwent(3) functions.

group

Group information traditionally stored in the group(5) file and used by getgrent(3) functions.

For example, the following simple configuration in the /etc/nsswitch.conf file can be used to initially resolve user and group information from /etc/passwd and /etc/group and then from the Windows NT server.

```
passwd:         files winbind
group:          files winbind
## only available on IRIX: use winbind to resolve hosts:
# hosts:        files dns winbind
## All other NSS enabled systems should use libnss_wins.so like this:
hosts:          files dns wins
```

The following simple configuration in the /etc/nsswitch.conf file can be used to initially resolve hostnames from /etc/hosts and then from the WINS server.

```
hosts:              files wins
```

OPTIONS

-D|--daemon

If specified, this parameter causes the server to operate as a daemon. That is, it detaches itself and runs in the background on the appropriate port. This switch is assumed if winbindd is executed on the command line of a shell.

-F|--foreground

If specified, this parameter causes the main winbindd process to not daemonize, i.e. double-fork and disassociate with the terminal. Child processes are still created as normal to service each connection request, but the main process does not exit. This operation mode is suitable for running winbindd under process supervisors such as supervise and svscan from Daniel J. Bernstein’s daemontools package, or the AIX process monitor.

-S|--stdout

If specified, this parameter causes winbindd to log to standard output rather than a file.

-d|--debuglevel=level

level is an integer from 0 to 10. The default value if this parameter is not specified is 0.

The higher this value, the more detail will be logged to the log files about the activities of the

server. At level 0, only critical errors and serious warnings will be logged. Level 1 is a reasonable level for day-to-day running - it generates a small amount of information about operations carried out.

Levels above 1 will generate considerable amounts of log data, and should only be used when investigating a problem. Levels above 3 are designed for use only by developers and generate HUGE amounts of log data, most of which is extremely cryptic.

Note that specifying this parameter here will override the **log level** parameter in the smb.conf file.

-V|--version
Prints the program version number.

-s|--configfile=<configuration file>
The file specified contains the configuration details required by the server. The information in this file includes server-specific information such as what printcap file to use, as well as descriptions of all the services that the server is to provide. See smb.conf for more information. The default configuration file name is determined at compile time.

-l|--log-basename=logdirectory
Base directory name for log/debug files. The extension **".progname"** will be appended (e.g. log.smbclient, log.smbd, etc...). The log file is never removed by the client.

--option=<name>=<value>
Set the **smb.conf**(5) option "<name>" to value "<value>" from the command line. This overrides compiled-in defaults and options read from the configuration file.

-?|--help
Print a summary of command line options.

--usage
Display brief usage message.

-i|--interactive
Tells winbindd to not become a daemon and detach from the current terminal. This option is used by developers when interactive debugging of winbindd is required. winbindd also logs to standard output, as if the -S parameter had been given.

-n|--no-caching
Disable some caching. This means winbindd will often have to wait for a response from the

domain controller before it can respond to a client and this thus makes things slower. The results will however be more accurate, since results from the cache might not be up-to-date. This might also temporarily hang winbindd if the DC doesn’t respond. This does not disable the samlogon cache, which is required for group membership tracking in trusted environments.

--no-process-group
Do not create a new process group for winbindd.

NAME AND ID RESOLUTION

Users and groups on a Windows NT server are assigned a security id (SID) which is globally unique when the user or group is created. To convert the Windows NT user or group into a unix user or group, a mapping between SIDs and unix user and group ids is required. This is one of the jobs that winbindd performs.

As winbindd users and groups are resolved from a server, user and group ids are allocated from a specified range. This is done on a first come, first served basis, although all existing users and groups will be mapped as soon as a client performs a user or group enumeration command. The allocated unix ids are stored in a database and will be remembered.

WARNING: The SID to unix id database is the only location where the user and group mappings are stored by winbindd. If this store is deleted or corrupted, there is no way for winbindd to determine which user and group ids correspond to Windows NT user and group rids.

CONFIGURATION

Configuration of the winbindd daemon is done through configuration parameters in the **smb.conf**(5) file. All parameters should be specified in the [global] section of smb.conf.

- **separator**
- **config * : range**
- **config * : backend**
- **cache time**
-

enum users

- **enum groups**

- **homedir**

- **shell**

- **use default domain**

- **rpc only** Setting this parameter forces winbindd to use RPC instead of LDAP to retrieve information from Domain Controllers.

EXAMPLE SETUP

To setup winbindd for user and group lookups plus authentication from a domain controller use something like the following setup. This was tested on an early Red Hat Linux box.

In /etc/nsswitch.conf put the following:

```
passwd: files winbind
group:  files winbind
```

In /etc/pam.d/* replace the *auth* lines with something like this:

```
auth  required    /lib/security/pam_securetty.so
auth  required      /lib/security/pam_nologin.so
auth  sufficient  /lib/security/pam_winbind.so
auth  required    /lib/security/pam_unix.so \
                use_first_pass shadow nullok
```

Note

The PAM module pam_unix has recently replaced the module pam_pwdb. Some Linux systems use the module pam_unix2 in place of pam_unix.

Note in particular the use of the *sufficient* keyword and the *use_first_pass* keyword.

Now replace the account lines with this:

account required /lib/security/pam_winbind.so

The next step is to join the domain. To do that use the net program like this:

net join -S PDC -U Administrator

The username after the *-U* can be any Domain user that has administrator privileges on the machine. Substitute the name or IP of your PDC for "PDC".

Next copy libnss_winbind.so to /lib and pam_winbind.so to /lib/security. A symbolic link needs to be made from /lib/libnss_winbind.so to /lib/libnss_winbind.so.2. If you are using an older version of glibc then the target of the link should be /lib/libnss_winbind.so.1.

Finally, setup a **smb.conf**(5) containing directives like the following:

```
[global]
        winbind separator = +
    winbind cache time = 10
    template shell = /bin/bash
    template homedir = /home/%D/%U
    idmap config * : range = 10000-20000
    workgroup = DOMAIN
    security = domain
    password server = *
```

Now start winbindd and you should find that your user and group database is expanded to include your NT users and groups, and that you can login to your unix box as a domain user, using the DOMAIN+user syntax for the username. You may wish to use the commands getent passwd and getent group to confirm the correct operation of winbindd.

NOTES

The following notes are useful when configuring and running winbindd:

nmbd(8) must be running on the local machine for winbindd to work.

PAM is really easy to misconfigure. Make sure you know what you are doing when modifying PAM

configuration files. It is possible to set up PAM such that you can no longer log into your system.

If more than one UNIX machine is running winbindd, then in general the user and groups ids allocated by winbindd will not be the same. The user and group ids will only be valid for the local machine, unless a shared **idmap config * : backend** is configured.

If the Windows NT SID to UNIX user and group id mapping file is damaged or destroyed then the mappings will be lost.

SIGNALS

The following signals can be used to manipulate the winbindd daemon.

SIGHUP

Reload the **smb.conf**(5) file and apply any parameter changes to the running version of winbindd. This signal also clears any cached user and group information. The list of other domains trusted by winbindd is also reloaded.

Instead of sending a SIGHUP signal, a request to reload configuration file may be sent using **smbcontrol**(1) program.

SIGUSR2

The SIGUSR2 signal will cause winbindd to write status information to the winbind log file.

Log files are stored in the filename specified by the log file parameter.

FILES

/etc/nsswitch.conf(5)

Name service switch configuration file.

/tmp/.winbindd/pipe

The UNIX pipe over which clients communicate with the winbindd program. For security reasons, the winbind client will only attempt to connect to the winbindd daemon if both the /tmp/.winbindd directory and /tmp/.winbindd/pipe file are owned by root.

$LOCKDIR/winbindd_privileged/pipe

The UNIX pipe over which ’privileged’ clients communicate with the winbindd program. For security reasons, access to some winbindd functions - like those needed by the ntlm_auth utility - is restricted. By default, only users in the ’root’ group will get this access, however the administrator may change the group permissions on $LOCKDIR/winbindd_privileged to allow programs like ’squid’ to use ntlm_auth. Note that the winbind client will only attempt to connect

to the winbindd daemon if both the $LOCKDIR/winbindd_privileged directory and $LOCKDIR/winbindd_privileged/pipe file are owned by root.

/lib/libnss_winbind.so.X
: Implementation of name service switch library.

$LOCKDIR/winbindd_idmap.tdb
: Storage for the Windows NT rid to UNIX user/group id mapping. The lock directory is specified when Samba is initially compiled using the *--with-lockdir* option. This directory is by default /usr/local/samba/var/locks.

$LOCKDIR/winbindd_cache.tdb
: Storage for cached user and group information.

VERSION

This man page is part of version 4.13.17 of the Samba suite.

SEE ALSO

nsswitch.conf(5), **samba**(7), **wbinfo**(1), **ntlm_auth**(8), **smb.conf**(5), **pam_winbind**(8)

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.

wbinfo and winbindd were written by Tim Potter.

The conversion to DocBook for Samba 2.2 was done by Gerald Carter. The conversion to DocBook XML 4.2 for Samba 3.0 was done by Alexander Bokovoy.