winbindd

Nazwa

winbindd -- Demon Przełączania Usług Nazewniczych (Name Service Switch) do odwzorowania nazw z serwerów NT

Synopsis

winbindd [-i] [-d <poziom debugowania>] [-s <plik konfiguracyjny smb>]

OPIS

Ten program jest częścią pakietu Samba.

winbindd jest demonem który dostarcza usług do funkcjonalności Przełącznika Usług Nazewniczych (Name Service Switch - dalej użyta jest oryginalna nazwa, przyp.tłum.) który jest obecny w większości nowych bibliotek C. Name Service Switch pozwala na uzyskanie informacji użytkownika i systemu z różnych usług bazodanowych, takich jak NIS lub DNS. Dokładne zachowanie może być skonfigurowane poprzez plik `/etc/nsswitch.conf`. Użytkownicy i grupy są alokowani, gdy tylko zostaną odwzorowani w obrębie zakresu identyfikatorów użytkowników i grup określonego przez administratora systemu Samba.

Usługa dostarczana przez winbindd nazywa się "winbind" i może być użyta do odwzorowania danych użytkownika i grupy z serwera Windows NT. Może również dostarczyć usług autentykacyjnych poprzez przypisany moduł PAM.

Następujące bazy danych nsswitch są implementowane przez usługę winbind:

passwd

Dane użytkownika tradycyjnie przechowywane w pliku `passwd(5)` i używane przez funkcje **getpwent(3)**.

group

Dane grup tradycyjnie przechowywane w pliku `group(5)` i używane przez funkcje **getgrent(3)**.

Na przykład, poniższa prosta konfiguracja w pliku `/etc/nsswitch.conf` może być użyta do odwzorowania danych użytkowników i grup najpierw z `/etc/passwd` i `/etc/group`, a potem z serwera Windows NT.

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

OPCJE

-d poziomdebugowania

Ustawia poziom debugowania na wartość całkowitą pomiędzy 0 i 100. 0 odpowiada

brakowi debugowania, a 100 odpowiada (?)absolutnym detalom(?). Aby wysłać raport o błędach do Zespołu Samba, użyj poziomu 100 (zobacz plik `BUGS.txt`).

-i

Mówi **winbindd** żeby nie zostawał demonem i nie odłączał się od bieżącego terminala. Ta opcja jest używana przez developerów podczas interaktywnego debugowania **winbindd** jeśli jest to wymagane.

ODWZOROWANIE ID I NAZWY

Użytkownicy i grupy w serwerze Windows NT są skojarzeni z identyfikatorem relatywnym (rid) który jest unikalny dla domeny gdy użytkownik lub grupa są tworzeni. Żeby konwertować użytkownika lub grupę Windows NT na użytkownika lub grupę unix, wymagane jest odwzorowanie pomiędzy rid'ami a identyfikatorami użytkownika lub grupy unix. Jest to jedno z zadań które wykonuje **winbindd**.

Jak tylko użytkownicy i grupy winbindd są odwzorowywani przez serwer, identyfikatory użytkowników i grup są alokowane z określonego przedziału. Jest to wykonywane przy pierwszym podejściu, oparte o serwer, choć wszyscy istniejący użytkownicy i grupy będą mapowani gdy tylko klient przeprowadzi enumerację użytkowników lub grup. Zaalokowane identyfikatory unix będą przechowywane w pliku bazy danych w katalogu blokad (lock) Samba i będą zapamiętane.

OSTRZEŻENIE:: Baza danych "rid na unix id" jest jedynym miejscem, gdzie odwzorowania użytkowników i grup są przechowywane przez winbindd. Jeśli ten plik zostanie usunięty lub uszkodzony, nie będzie żadnego sposobu żeby winbindd określił, które identyfikatory użytkowników i grup odpowiadają którym rid'om użytkowników i grup Windows NT.

KONFIGURACJA

Konfiguracja demona **winbindd** jest wykonywana przez parametry konfiguracyjne w pliku `smb.conf(5)`. Wszystkie parametry powinny być określone w sekcji [global] smb.conf.

winbind separator

Opcja separatora winbind pozwala ci określić jak nazwy domen NT i użytkowników są łączone w nazwę użytkownika unix gdy jest ona prezentowana użytkownikom. Domyślnie, **winbindd** będzie używał tradycyjnego separatora '\' tak, że nazwa użytkownika unix będzie wyglądała jak DOMENA\nazwauzytkownika. W niektórych przypadkach ten znak może powodować problemy, bo znak '\' ma specjalne znaczenie w powłokach unix. W takim wypadku możesz użyć opcji separatora winbind, aby określić alternatywny znak separatora. Dobrymi alternatywami mogą być '/' (aczkolwiek to konfliktuje z separatorem katalogów unix) lub '+'. Znak '+' wydaje się być najlepszym wyborem dla 100% kompatybilności z istniejącymi narzędziami unix, lecz może być złym wyborem z estetycznego punktu widzenia, zależnie od twojego gustu.

Domyślnie: **winbind separator = **

Przykład: **winbind separator = +**

winbind uid

Parametr winbind uid określa zakres identyfikatorów użytkowników które są alokowane

przez demona winbind. Zakres ten nie powinien zawierać istniejących użytkowników lokalnych lub nis, bo w przeciwnym wypadku mogą wystąpić dziwne konflikty.

Domyślnie: **winbind uid = <pusty łańcuch znakowy>**

Przykład: **winbind uid = 10000-20000**

winbind gid

Parametr winbind gid określa zakres identyfikatorów grup które są alokowane przez demona winbind. Zakres ten nie powinien zawierać istniejących grup lokalnych lub nis, bo w przeciwnym wypadku mogą wystąpić dziwne konflikty.

Domyślnie: **winbind gid = <pusty łańcuch znakowy>**

Przykład: **winbind gid = 10000-20000**

winbind cache time

Ten parametr określa liczbę sekund przez które demon **winbindd** będzie cache'ował dane użytkowników i grup przed ponownym pytaniem serwera Windows NT. Gdy jakiś element w tym cache'u jest starszy niż podany tu czas, winbindd poprosi kontroler domeny o numer sekwencyjny bazy danych kont na serwerze. Jeśli numer sekwencyjny nie zmienił się, wtedy cache'owany element jest oznaczany jako ważny (aktualny, przyp.tłum.) na następne *winbind cache time* sekund. W przeciwnym wypadku, element jest pobrany z serwera. Oznacza to że tak długo, jak baza danych kont nie jest zmieniana, winbindd będzie musiał wysyłać tylko jeden pakiet z pytaniem o numer sekwencyjny co *winbind cache time* sekund.

Domyślnie: **winbind cache time = 15**

winbind enum users

W wielkich instalacjach może być konieczne powstrzymanie enumeracji użytkowników poprzez grupę wywołań systemowych **setpwent()**, **getpwent()** i **endpwent()**. Jeśli parametr *winbind enum users* jest ustawiony na `false`, wywołania systemowe **getpwent** nie zwrócą żadnych danych.

Ostrzeżenie: Wyłączanie enumeracji użytkowników może spowodować, że niektóre programy będą zachowywać się dziwnie. Przykładowo, program finger jest zależny od posiadania dostępu do pełnej listy użytkowników podczas szukania pasujących nazw użytkowników.

Domyślnie: **winbind enum users = yes**

winbind enum groups

W wielkich instalacjach może być konieczne powstrzymanie enumeracji grup poprzez grupę wywołań systemowych **setgrent()**, **getgrent()** i **endgrent()**. Jeśli parametr *winbind enum groups* jest ustawiony na `false`, wywołania systemowe **getgrent** nie zwrócą żadnych danych.

Ostrzeżenie: Wyłączanie enumeracji grup może spowodować, że niektóre programy będą

zachowywać się dziwnie.

Domyślnie: **winbind enum groups = no**

template homedir

Przy wypełnianiu informacji o użytkowniku Windows NT, demon **winbindd** używa tego parametru do wpisania katalogu domowego dla tego użytkownika. Jeśli obecny jest tu łańcuch znakowy *%D* jest on zastępowany nazwą domeny tego użytkownika Windows NT. Jeśli obecny jest łańcuch *%U* jest on zastępowany nazwą użytkownika Windows NT.

Domyślnie: **template homedir = /home/%D/%U**

template shell

Przy wypełnianiu informacji o użytkowniku Windows NT, demon **winbindd** używa tego parametru do wpisania powłoki dla tego użytkownika.

PRZYKŁADOWE USTAWIENIE

Aby ustawić winbindd na szukanie użytkowników i grup plus autentykację z kontrolera domeny, użyj ustawień podobnych do poniższych. To było testowane na systemie RedHat 6.2 Linux.

W `/etc/nsswitch.conf` wstaw to:

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

W `/etc/pam.d/*` zastąp linie *auth* czymś podobnym:

```
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_pwdb.so use_first_pass shadow nullok
```

Zwróć uwagę w szczególności na użycie słowa kluczowego `sufficient` i `use_first_pass`.

Teraz zastąp linie konta (account) tym:

account required /lib/security/pam_winbind.so

Następnym krokiem będzie przyłączenie się do domeny. Aby to zrobić użyj programu **smbpasswd** w ten sposób:

smbpasswd -j DOMENA -r PDC -U Administrator

Nazwa użytkownika po *-U* może być nazwą każdego użytkownika Domeny który ma przywileje administracyjne. Zastąp nazwę "DOMENA" swoją nazwą domeny, a nazwę "PDC" nazwą swojego PDC.

Następnie skopiuj `libnss_winbind.so` do `/lib`, a `pam_winbind.so` do `/lib/security/`. Potrzebne jest

dowiązanie symboliczne z `/lib/libnss_winbind.so` do `/lib/libnss_winbind.so.2`. Jeśli używasz starszej wersji glibc, wtedy celem dowiązania powinien być `/lib/libnss_winbind.so.1`.

Na koniec, utwórz `smb.conf` zawierający dyrektywy jak poniżej:

```
[global]
        winbind separator = +
        winbind cache time = 10
        template shell = /bin/bash
        template homedir = /home/%D/%U
        winbind uid = 10000-20000
        winbind gid = 10000-20000
        workgroup = DOMENA
        security = domain
        password server = *
```

Teraz uruchom **winbindd** i powinieneś zauważyć, że twoja baza danych użytkowników i grup jest powiększona o twoich użytkowników i grupy NT, oraz że możesz zalogować się do twojego systemu unix jako użytkownik z domeny, przy użyciu składni DOMENA+użytkownik jako nazwa użytkownika. Możesz chcieć skorzystać z poleceń **getent passwd** i **getent group** żeby potwierdzić poprawne funkcjonowanie **winbindd** .

NOTATKI

Poniższe notatki są przydatne podczas konfigurowania i uruchamiania **winbindd**:

nmbd musi działać na lokalnej maszynie żeby **winbindd** działał. **winbindd** sprawdza listę zaufanych domen (trusted domains) dla serwera Windows NT przy starcie i gdy odbierze sygnał SIGHUP. W ten sposób, aby działający **winbindd** dowiedział się o nowych relacjach zaufania między serwerami, musi otrzymać sygnał SIGHUP.

Procesy klienckie odwzorowujące nazwy poprzez moduł nsswitch **winbindd** czytają zmienną środowiskową o nazwie `$WINBINDD_DOMAIN`. Jeśli ta zmienna zawiera listę nazw domen Windows NT odddzielonych przecinkami, to winbindd odwzoruje tylko użytkowników i grupy w tych domenach Windows NT.

Naprawdę łatwo jest zdekonfigurować PAM. Upewnij się że wiesz co robisz, modyfikując jego pliki konfiguracyjne. Można ustawić PAM w taki sposób, że nie będziesz się już mógł zalogować do systemu.

Jeśli na więcej niż jednej maszynie UNIX działa **winbindd** wówczas - generalnie - identyfikatory użytkowników i grup alokowane przez winbindd nie będą takie same. Będą one poprawne tylko dla lokalnej maszyny.

Jeśli plik mapujący Windows NT RID na id użytkownika i grupy UNIX zostanie uszkodzony lub zniszczony, wtedy mapowania będą stracone.

SYGNAŁY

Poniższe sygnały mogą być wykorzystane do manipulowania demonem **winbindd**.

SIGHUP

Przeładuj plik `smb.conf(5)` i wprowadź wszystkie zmiany parametrów do działającej wersji winbindd. Ten sygnał również oczyszcza cache'owane dane użytkowników i grup. Lista innych domen zaufanych przez winbindd jest również przeładowana.

SIGUSR1

Sygnał SIGUSR1 spowoduje, że **winbindd** zapisze informacje o statusie do pliku logu winbind, włącznie z informacjami o liczbie użytkowników i grup alokowanych przez **winbindd**.

Pliki logu są przechowywane pliku określonym parametrem *`log file`*.

PLIKI

`/etc/nsswitch.conf(5)`

Plik konfiguracyjny przełącznika usług nazewniczych (name service switch, dalej używana jest nazwa oryginalna)

/tmp/.winbindd/pipe

Łącze UNIX przez które klienci komunikują się z programem **winbindd**. Z powodu bezpieczeństwa klient winbind będzie próbował połączyć się z demonem winbindd tylko, jeśli zarówno katalog `/tmp/.winbindd` jak i plik `/tmp/.winbindd/pipe` będą własnością root'a.

/lib/libnss_winbind.so.X

Implementacja biblioteki name service switch.

$LOCKDIR/winbindd_idmap.tdb

"Magazyn" mapowania Windows NT rid na id użytkownika/grupy UNIX. Katalog blokad jest określony przy użyciu opcji *`--with-lockdir`* gdy Samba jest na początku kompilowana. Domyślnie jest to katalog `/usr/local/samba/var/lock`.

$LOCKDIR/winbindd_cache.tdb

"Magazyn" dla cache'owanych danych użytkowników i grup.

WERSJA

Ta strona podręcznika jest poprawna dla wersji 2.2 pakietu Samba.

ZOBACZ TEŻ

`nsswitch.conf(5)`, samba(7), wbinfo(1), smb.conf(5)

AUTOR

Pierwotnie, Samba i związane z nią oprogramowanie były stworzone przez Andrew Tridgella . Samba jest teraz rozwijana przez Zespół Samba jako projekt Open Source podobnie jak jądro

Linux.

wbinfo i **winbindd** zostały napisane przez Tima Pottera.

Konwersja do DocBook dla Samba 2.2 została wykonana przez Geralda Cartera. Tłumaczenie na język polski wykonał Rafał Szcześniak.