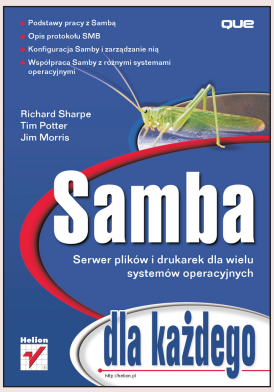
Samba dla każdego



Autorzy: Richard Sharpe, Tim Potter, Jim Morris
Tłumaczenie: zbiorowe
ISBN: 83-7197-498-1
Tytuł oryginału: Special Edition Using Samba
Format: B5, stron 666

Podobnie jak Linux, Samba to historia międzynarodowego sukcesu. Jest to darmowy, powszechnie dostępny (i licencjonowany na zasadach GPL) serwer plików i drukarek dla wielu systemów operacyjnych. Konkuruje on bezpośrednio z systemem operacyjnym Microsoft Windows NT i jest lepszy od niego pod wieloma względami.

Jednakże Sambie nie można odmówić krytyki. Wymaga dużego nakładu czasu poświęconego jej nauce i wiele osób twierdzi, że jest trudna w używaniu i ciężko nią zarządzać, a mimo to jest używana w dużych i małych korporacjach, organizacjach rządowych, organizacjach non-profit, małym biznesie i – dzięki sukcesowi Linuksa – również na domowych komputerach.

Fakt, że pakiet z tak skromnymi początkami jak Samba mógł, pomimo powtarzających się trudności, osiągnąć taki sukces, świadczy dobitnie o potędze Internetu, który każdemu zapewnia dostęp do użytecznego oprogramowania.

Niezbędny podręcznik dla wszystkich użytkowników Samby!

- Ustaw współdzielenie plików i drukarek.
- Zwiększ bezpieczeństwo systemu poprzez zarządzanie hasłami.
- Zautomatyzuj pracę przy użyciu rozbudowanych makr i skryptów.
- Połącz klientów sieciowych używających całej gamy systemów operacyjnych (od starych i nowych Windows, aż po Unix?a).
- Wyśrubuj swój system aby osiągnąć najwyższą możliwą wydajność sieci.
- Dowiedz się jak pracuje Samba w przedsiębiorstwie.
- Uzyskaj dostęp do najbardziej kompletnego opisu poleceń i parametrów Samby.
- Znajdź i napraw problemy sieciowe.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 5.

Zarządzanie i konfiguracja Samby

Richard Sharpe

W tym rozdziale:

- Modele bezpieczeństwa
- Struktura Samby
- Działający plik smb.conf
- Pliki dziennika zdarzeń a usuwanie usterek
- Najczęstsze problemy podczas korzystania z Samby
- Graficzne narzędzia konfiguracyjne
- Dodatkowe informacje

Samba może spełniać wiele funkcji, a między innymi:

- udostępniać usługi serwera plików i drukarek;
- pracować jako serwer logowania (ang. *logon server*);
- pracować jako podstawowy kontroler domeny;
- działać jako serwer przeglądania lub główny serwer przeglądania domeny.

Ponadto Samba umożliwia całkowitą kontrolę nad wieloma wykonywanymi przez nią funkcjami. Na przykład, można mieć kontrolę nad tym, kto jest właścicielem nowo utworzonego pliku i jakie określono dla niego prawa dostępu. Można także — za każdym razem, kiedy użytkownik połączy się lub rozłączy z określonym zasobem — uruchamiać odpowiednie polecenia na serwerze.

Wielu użytkowników zainteresuje się możliwościami Samby jako serwera plików i drukarek. Szybko jednak będą oni chcieli uzyskać więcej informacji na temat zarządzania Sambą i tego, w jaki sposób wykorzystać Sambę do wykonywania bardziej skomplikowanych czynności.

W tym rozdziale poznamy sposób zarządzania Sambą. Po pierwsze, przyjrzymy się modelom bezpieczeństwa Samby i omówimy sposób przeprowadzania uwierzytelniania. Następnie omówimy:

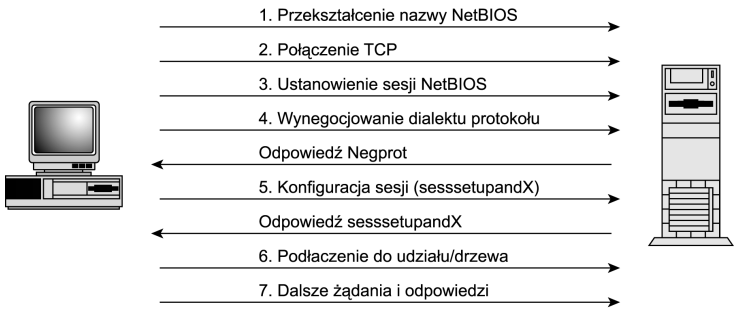
- strukturę Samby w aspekcie procesów obsługujących żądania klientów,
- strukturę pliku *smb.conf* i przeznaczenie poszczególnych sekcji,
- pliki dzienników tworzone przez Sambę i sposób korzystania z nich w celu rozwiązywania problemów,
- narzędzia ułatwiające konfigurację z graficznym interfejsem użytkownika dostępne dla Samby.

Modele bezpieczeństwa

Zadaniem serwerów SMB takich jak Samba jest umożliwienie współdzielenia plików pomiędzy klientami. W jaki sposób odbywa się kontrola dostępu do tych plików? Spróbujemy odpowiedzieć na to pytanie, ale najpierw przyjrzymy się sposobowi łączenia klientów SMB z serwerami.

Kiedy klient żąda połączenia z udziałem, wykonuje czynności pokazane na rysunku 5.1. Opisano je w rozdziale 4., *Protokół SMB — wprowadzenie*, w podrozdziale *Przegląd protokołu SMB*.

Rysunek 5.1.
Uzyskiwanie dostępu do serwera Samby



Krok 5., należy wykonać tylko wtedy, gdy serwer pracuje w trybie kontroli dostępu na poziomie użytkownika.

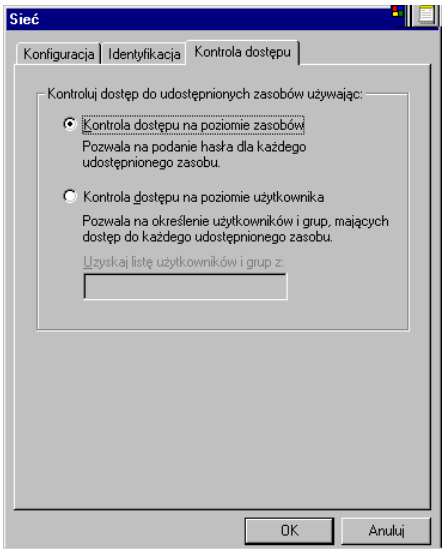
Pierwsze serwery SMB (jak np. *IBM PC Network Program*) „nie znały" pojęcia użytkowników, ponieważ korzystały z nich zwykłe komputery PC z systemem DOS 3.1. Klient uzyskujący dostęp do udziału mógł korzystać ze wszystkich plików w tym udziale. Pojęcie użytkowników zaimplementowano jednak w późniejszych serwerach takich jak LAN Manager oraz Lan Manager for UNIX. Tak więc programiści musieli znaleźć sposób na sprawne uwierzytelniania. Dodatkowo musieli znaleźć sposób na zgłaszanie przez serwery chęci uwierzytelniania. Osiągnięto to poprzez utworzenie nowego wariantu protokołu SMB, który dostarczał dodatkowych informacji w odpowiedzi na żądanie SMB *NEGPROT*.

W Sambie wiele uwagi poświęca się sprawom bezpieczeństwa. Oznacza to, że wszystkie operacje dostępu do plików wykonywane przez Sambę dla klienta są wykonywane w kontekście właściwego użytkownika serwera. Określony użytkownik może uzyskać dostęp tylko do określonych plików. Samba posiada kontrolę nad tym, które konto na serwerze jest wykorzystywane w celu uzyskania dostępu do plików.

Ze względów historycznych istnieją dwa modele poziomów bezpieczeństwa, na których może pracować serwer Samby (lub inny serwer SMB jak np. Win9x):

- Kontrola dostępu na poziomie zasobów — użytkownicy nie muszą przeprowadzać uwierzytelniania z serwerem. Czasem jednak przed uzyskaniem dostępu do zasobu może istnieć potrzeba podania hasła. W tym modelu bezpieczeństwa Samba nadal w celu uzyskania dostępu do plików wymaga właściwego użytkownika (i opcjonalnie hasła). Jednym ze sposobów rozwiązania tego problemu jest zdefiniowanie *konta gościa*.
- Kontrola dostępu na poziomie użytkowników — przed uzyskaniem dostępu do zasobu klient musi dostarczyć informacji o użytkowniku. Zwykle klient podaje nazwę użytkownika i hasło, które posłużyło do zalogowania się w systemie Windows.

Na rysunku 5.2 pokazano okno konfiguracji sieci systemu Windows 95, gdzie w celu udostępniania plików i drukarek ustawiono tryb kontroli dostępu na poziomie zasobów.

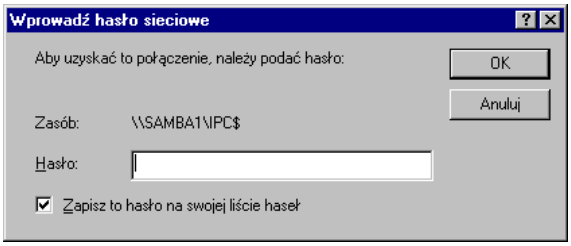


Rysunek 5.2. *Windows 95 może pracować w trybie bezpieczeństwa na poziomie zasobu oraz na poziomie użytkowników*

Przeglądając strony podręcznika *man* poświęcone plikowi *smb.conf*, zapewne zauważyliśmy, że w Sambie istnieją dwa dodatkowe tryby kontroli dostępu. Określa się je parametrami `security = server` oraz `security = domain`. Obydwa te tryby to ulepszenia trybu bezpieczeństwa na poziomie użytkowników. W modelach tych uwierzytelnianie na serwerze Samby odbywa się z wykorzystaniem innego serwera SMB. Bardziej szczegółowo tryby te opisano w rozdziale 8., *Zarządzanie hasłami w Sambie* oraz w rozdziale 17., *Samba a domeny Windows NT*.

Począwszy od wersji 2.0.0 zmienił się domyślny tryb działania Samby. We wcześniejszych wersjach (np. 1.9.18p10) domyślnym trybem była kontrola dostępu na poziomie zasobów. Od wersji 2.0.0 wzwyż domyślny tryb to kontrola dostępu na poziomie użytkowników.

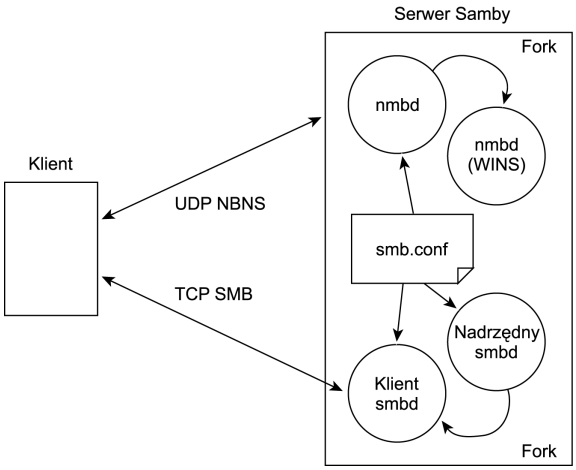
Dla początkujących użytkowników Samby zmiana ta stała się największym źródłem problemów. Najnowsze dystrybucje systemu Linux wyposażone są w wersję Samby 2.0.3 lub wyższej, a tryb kontroli dostępu na poziomie użytkowników, do połączenia z serwerem wymaga podania prawidłowego użytkownika i hasła. W wielu przypadkach, użytkownicy wykorzystują inne nazwy użytkowników dla klienta Windows, a inne dla serwera Linux. W takiej sytuacji, system Windows 95 wyświetla okno dialogowe jak na rysunku 5.3. We wcześniejszych wersjach Samby w takich sytuacjach można było wykorzystać konto gościa.



Rysunek 5.3. *Początkujący użytkownicy Samby często widzą to okno dialogowe*

Struktura Samby

Jak powiedziano w rozdziale 3., *Wprowadzenie do Samby*, Samba składa się z dwóch głównych komponentów *nmbd* oraz *smbd*, a także z kilku komponentów pomocniczych, które służą do wykonywania innych zadań. Są to *smbclient*, *nmblookup* oraz *smbstatus*. Strukturę Samby i jej demonów pokazano na rysunku 5.4.



Rysunek 5.4. *Struktura Samby*

Plik smb.conf

Sambą steruje plik *smb.conf*. Większość nowych dystrybucji Linuksa, instalując wersję Samby, umieszcza ten plik w katalogu */etc*. z systemem Caldera Open Linux plik ten umieszczono jednak w katalogu */etc/samba.d*[1].

Plik *smb.conf* składa się z ciągu sekcji. Każda z nich zawiera zestaw parametrów, które w określony sposób wpływają na sposób działania Samby. Oprócz trzech sekcji specjalnych `global`, `homes` oraz `printers` (patrz tabela 5.1) istnieje, sekcja opisująca pojedynczy udział (ang. *share*). Komputery-klienty łączą się z udziałem, a następnie uzyskują dostęp do plików w ramach tego udziału.

Sekcje są oznaczone, ujętą w nawiasy kwadratowe, nazwą sekcji. Poniższy przykład oznacza początek sekcji `homes`:

```
[homes]
```

Sekcja *global* nie musi być oznaczona przez `[global]`, ale zastosowanie takiego oznaczenia jest dobrym zwyczajem.

Parametry podaje się w następującej formie:

```
nazwa=wartość
```

gdzie:

- `nazwa` określa nazwę parametru. Nazwa może zawierać spacje. Poprawną nazwą parametru jest na przykład `os level`.

> Samba ignoruje spacje w nazwach parametrów. Tak więc, nazwa `os level` jest równoważna nazwie `osl evel`. Dobrze jest jednak ściśle trzymać się właściwych nazw parametrów (w tym przypadku `os level`).

- *`wartość`* określa wartość przypisaną do parametru. Może to być ciąg znaków, liczba, słowo takie jak `true`, `false`, `yes`, `no`, wyrażenie regularne itp.

W tabeli 5.1 wyszczególniono sekcje, które mogą znaleźć się w pliku *smb.conf*.

W pliku *smb.conf* można umieścić komentarze, które pozwolą zrozumieć innym znaczenie wprowadzonych parametrów. Istnieją dwa sposoby wprowadzania komentarzy. Jako pierwszy znak wiersza można wprowadzić znak średnika (`;`) albo znak hash (#). Generalnie, komentarze mogą znajdować się tylko w oddzielnych wierszach.

Parametry mogą zajmować więcej niż jeden wiersz. W takim przypadku należy użyć standardowego uniksowego znaku kontynuacji. Umieszczenie znaku `\` na końcu wiersza zmusza Sambę do traktowania następnego wiersza jako kontynuacji wiersza bieżącego.

---

[1] W najnowszym Slackwerze 8.0 ten plik jest w katalogu /etc/samba — *przyp. red.*

Tabela 5.1. *Sekcje pliku smb.conf*

Sekcja	Opis
`[global]`	Jedna z trzech sekcji specjalnych zawierająca parametry sterujące ogólnym działaniem Samby. Są to, na przykład, parametry dotyczące bezpieczeństwa oraz nazw NetBIOS. Sekcja `[global]` to jedyna sekcja, która nie definiuje udziału.
`[homes]`	Druga sekcja specjalna. Jest to skrócony sposób określenia faktu, że użytkownikom serwera Samby mają być udostępnione ich katalogi macierzyste. Potencjalnie, sekcja ta definiuje wiele udziałów.
`[printers]`	Trzecia sekcja specjalna. Skrócony sposób na zdefiniowanie faktu, że użytkownikom mają być udostępniane wszystkie drukarki podłączone do serwera Samby. Potencjalnie sekcja definiuje wiele udziałów.
`[nazwa udziału]`	Wszystkie pozostałe sekcje w pliku *smb.conf* określają pojedynczy udział o podanej nazwie. Nazwy udziałów mogą zawierać makraopolecenia. Więcej informacji na ten temat, znajduje się w podrozdziale *Dodatkowe zmienne* rozdziału 9., *Automatyzacja Samby*.

Spacje w wartościach parametrów można wstawiać dowolnie, tam gdzie są one potrzebne. Można także ująć tego typu łańcuchy w cudzysłowy, ale nie jest to wymagane.

Niektóre parametry mogą występować tylko w sekcji `global`, podczas gdy inne mogą znajdować się w dowolnej sekcji, włącznie z sekcją `global`. Parametry dla udziału, które znajdują się w sekcji `global` są wartościami domyślnymi dla tych udziałów, gdzie określonego parametru nie zdefiniowano.

W pliku *smb.conf* ma swoje miejsce inny bardzo ważny mechanizm: *makrodefinicje i zmienne*. Pozwalają one na pobieranie wartości z wbudowanych zmiennych Samby lub innych informacji, które Samba pobiera w czasie jej działania. Makrodefinicje i zmienne to jeden z kluczowych elementów automatyzacji Samby. Znaczenie niektórych z nich opisano w tabeli 5.2.

→ Aby dowiedzieć się więcej o makrodefinicjach i zmiennych, przeczytaj podrozdział *Makra Makrodefinicje i zmienne w Sambie* w rozdziale 9.

Tabela 5.2. *Niektóre zmienne Samby*

Zmienna	Znaczenie
`%S`	Nazwa bieżącej usługi.
`%h`	Nazwa serwera — pierwsza część FQDN serwera.
`%m`	Nazwa NetBIOS klienta podłączonego do tego procesu serwera.
`%L`	Nazwa NetBIOS serwera.

W czasie instalacji Samby w systemie, co często domyślnie towarzyszy instalacji Linuksa, na dysku pojawiają się także strony podręcznika *man* na temat Samby oraz domyślnego pliku *smb.conf*. Aby uzyskać informacje na temat określonego zasobu lub parametru, wystarczy sprawdzić stronę podręcznika *man* wpisując:

```
man smb.conf
```

Działający plik smb.conf

W rozdziale 3. stworzyliśmy prosty plik *smb.conf*. Teraz stworzymy nieco bardziej skomplikowany plik *smb.conf* i omówimy znaczenie wszystkich pól. Plik ten pokazano na listingu 5.1.

Listing 5.1. *Prosty plik smb.conf*

```
[global]
   workgroup = sambanet
   server string = Server Samby
   guest account = pcguest
   log file = /var/log/samba/log.%m
   password level = 8
[homes]
   comment = Katalogi macierzyste
   browseable = no
   writable = yes
```

Dodamy do niego kilka definicji udziałów. Można to zrobić, dokonując edycji pliku *smb.conf* za pomocą edytora *vi*:

```
vi /etc/smb.conf
```

Jeżeli nasza wersja Linuksa to Caldera OpenLinux, wpiszemy:

```
vi /etc/samba.d/smb.conf
```

Po otwarciu pliku *smb.conf* w edytorze *vi* dodamy następujące wiersze na końcu pliku (bezpośrednio po wierszu `writable = yes`):

```
[public]
   comment = Udział o dostępie publicznym
   path = /home/samba
   browsable = yes
   writable = yes
```

Użytkownicy Caldera Open Linux będą musieli ręcznie utworzyć katalog */home/samba*, ponieważ standardowy pakiet RPM nie zawiera tego katalogu. Możemy to zrobić za pomocą następującego polecenia:

```
mkdir /home/samba
```

Po wyjściu z edytora *vi* i ponownym uruchomieniu Samby,, w czasie przeglądania serwera powinniśmy zauważyć nowy zasób.

Ponowne uruchamianie Samby

W rozdziale 3. mówiliśmy o ponownym uruchamianiu Samby i poleceniu `samba`, które można zastosować do tego celu. W wielu przypadkach, po dokonaniu zmian w pliku *smb.conf* nie trzeba ponownie uruchamiać Samby. Często wystarczy, wysłać sygnał HUP do wszystkich demonów *smbd(8)*. Można to zrobić za pomocą następującego polecenia:

```
killall -HUP smbd
```

W opisanej sytuacji skorzystanie z tego polecenia wystarczy do ponownego uruchomienia Samby.

Stosując polecenie *restart*, proces *samba* kończy działanie wszystkich demonów *smbd(8)*. Mimo że w implementacji wszystkich klientów Microsoft zawarto obsługę funkcji ponownego połączenia, to niektóre aplikacje, jak np. Microsoft Word, niezbyt dobrze znoszą sytuacje odłączenia zasobu z otwartym plikiem.

Znaczenie poznanych parametrów

Plik *smb.conf* pokazany na listingu 5.1 jest dosyć prosty, ale zawiera pewną liczbę parametrów. Jaką funkcję spełniają te parametry? Ich znaczenie wyjaśniono w tabeli 5.3.

Tabela 5.3. *Wyjaśnienie znaczenia parametrów wykorzystanych w przykładowym pliku smb.conf*

Parametr	Funkcja
`workgroup`	Ten parametr określa grupę roboczą lub domenę, której członkiem jest nasz serwer Samby. Grupy robocze oraz domeny opisano bardziej szczegółowo w rozdziale 10., *Wprowadzenie do sieci Microsoft Windows*.
`server string`	Parametr ten określa łańcuch znaków, który pojawi się jako opis naszego serwera w czasie przeglądania przez innych użytkowników sieci.
`guest account`	Parametr ten określa nazwę konta gościa, jeżeli jest ono potrzebne.
`log file`	Ten parametr określa położenie i nazwę pliku dziennika demona *smbd*. Ostatnim elementem nazwy pliku dziennika jest *log.%m*, co oznacza, że każdy klient będzie miał oddzielny plik dziennika z nazwą klienta w nazwie pliku.
`password level`	Parametr ten definiuje sposób działania w przypadku, gdy nazwa użytkownika i hasło nie są zgodne. Najpierw Samba próbuje zastosować hasło w taki sposób, w jaki zostało wprowadzone przez klienta. Jeżeli uwierzytelnianie się nie powiedzie, Samba zamienia wszystkie litery na małe. Jeżeli i to nie przyniesie skutku, Samba wypróbuje *n* kombinacji wielkich liter, gdzie *n* jest wartością określoną dla parametru `password level`.
`comment`	Komentarz dla udziału.
`browseable`	Parametr ten określa, czy udział można przeglądać. Udziały można przeglądać domyślnie, zatem parametr należy zdefiniować tylko dla tych udziałów, dla których chcemy zabronić prawa przeglądania.
`path`	Parametr określa miejsce w systemie plików Linuksa, od którego będą udostępniane pliki. Domyślną wartością dla tego parametru jest */tmp*, dlatego należy koniecznie go zdefiniować.
`public`	Ten parametr określa, czy goście mogą uzyskać dostęp do udziału.
`writable`	Ten parametr określa, czy istnieje prawo zapisu do zasobu. Domyślnie zasoby są *tylko do odczytu.*

Pełny opis wszystkich parametrów pliku *smb.conf* znajdziemy w dodatku A, *Wszystkie parametry Samby i ich znaczenie*. Ponadto, parametry bardziej szczegółowo opisano w każdym z rozdziałów, gdzie jest o nich mowa.

→ Aby dowiedzieć się więcej o konfigurowaniu udziałów-plików, przeczytaj rozdział 6., *Współdzielenie plików*.

→ Aby dowiedzieć się więcej o konfigurowaniu udziałów-drukarek, przeczytaj rozdział 7., *Współdzielenie drukarek*.

Pliki dziennika zdarzeń a usuwanie usterek

Samba zapisuje komunikaty o błędach oraz niektóre komunikaty informacyjne do dzienników zdarzeń. Wiele dystrybucji Linuksa włącznie z Red Hatem, Linux Mandrakiem, TurboLinuksem oraz Yellow Dog Linuksem tworzy swoje pliki dzienników zdarzeń w katalogu */var/log/samba*. W tabeli 5.4 pokazano utworzone tam pliki. W innych wersjach systemu UNIX pliki dzienników zdarzeń zwykle znajdują się w katalogu */usr/local/samba/var*.

Tabela 5.4. *Pliki dzienników zdarzeń tworzone przez Sambę w wielu wersjach Linuksa*

Plik	Zawartość
log.smb	W pliku tym rejestruje swoje informacje demon *smbd*. Jeżeli w pliku *smb.conf* określono parametr `log file`, każdy nowy egzemplarz demona *smbd* w czasie uruchamiania zapisze informacje w dzienniku zdarzeń. W innym przypadku, zapisze te informacje w pliku *log.smb*.
log.nmb	W tym pliku zapisuje swoje informacje demon *nmbd*.
log.nazwa	Jeżeli określiliśmy parametr `log file` tak, jak pokazano w przykładzie prostego pliku *smb.conf*, demon *smbd* zapisze informacje do pliku *log.nazwa* w momencie połączenia użytkownika. Argument *nazwa* jest nazwą NetBIOS klienta.

W przypadku Open Caldera Linux, Samba tworzy pliki dzienników w katalogu */var/log/samba.d*. Pliki te wyszczególniono w tabeli 5.5.

Tabela 5.5. *Pliki dzienników zdarzeń tworzone przez Sambę w systemie wielu wersji Open Caldera Linux*

Plik	Zawartość
Smbd	Informacje demona *smbd*.
Nmbd	Informacje demona *nmbd*.
smb.nazwa	Pliki dzienników dla każdego klienta, jeżeli w pliku *smb.conf* umieszczono zapis informujący o tym, że pliki te mają być zapisywane w katalogu */etc/samba.d*.

Inne dystrybucje, jak np. SuSE, przechowują pliki dzienników w katalogu */var/log*, ale wykorzystują tę samą strukturę plików dzienników, jak systemy wywodzące się z dystrybucji Red Hat.

Pliki dzienników są nieocenione w rozwiązywaniu problemów z Sambą. W plikach tych, Samba zapisuje bardzo dużą ilość informacji śledzących. Poziom szczegółowości definiuje się parametrem `debug level`. Domyślna wartość tego parametru to 0. W takim przypadku Samba jest bardzo lakoniczna i zapisuje tylko te błędy, które uniemożliwiają jej działanie. Poniżej pokazano przykładową zawartość pliku *smb.log* po starcie Samby. Ostatni komunikat jest wynikiem działania Samby w systemie Linux, który może mieć tylko 1024 otwarte pliki dla pojedynczego procesu.

```
[2000/02/08 14:42:16, 1] smbd/server.c:main(643)
   smbd version 2.0.6 started.
   Copyright Andrew Tidgell 1992 - 1998
[2000/02/08 14:42:16, 1] smbd/files.c:file_init(216)
   file_init: Information only: requested 10000 open files, 1014 are available.
```

Parametr `debug level` należy zwiększyć, aby móc śledzić informacje o problemach, na jakie napotyka Samba, próbując wykonać działania dla klientów. Problemy te obejmują między innymi błędy uwierzytelniania, brak możliwości transmisji pakietów, niepowodzenia przy otwieraniu lub tworzeniu plików itp.

Aby śledzić te informacje, dodamy do sekcji `global` poniższy zapis i ponownie uruchomimy Sambę:

```
debug level = 6
```

Zwykle wartość `6` dla parametru `debug level` jest wystarczająca. Wartość `10` spowoduje, że uzyskamy jeszcze więcej informacji włącznie ze zrzutem w postaci szesnastkowej każdego otrzymanego pakietu.

Jak już pisaliśmy w podrozdziałach omawiających plik *smb.conf*, Samba traktuje parametr *debug level* oraz *debuglevel* jako równoważne. W dokumentacji możemy spotkać pisownię *debuglevel*, ale osobiście wolę stosować go w formie *debug level*.

→ Aby dowiedzieć się więcej o rozwiązywaniu najczęściej spotykanych problemów, przeczytaj rozdział 21., *Identyfikowanie i usuwanie usterek w Sambie*.

Najczęstsze problemy podczas korzystania z Samby

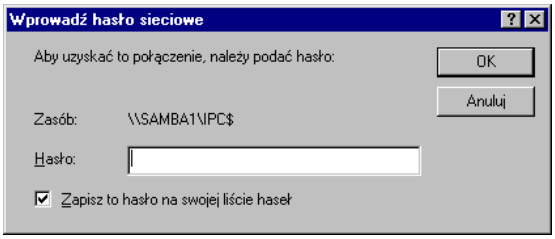
W tym rozdziale opiszemy problemy, na które często napotykają początkujący użytkownicy Samby. Niektóre z tych problemów wynikają ze zmian w sposobie działania Samby począwszy od wersji 2.0.0, podczas gdy inne wynikają ze zmian w sposobie działania systemów Windows 9x oraz NT. Jeszcze inne są po prostu wynikiem złej konfiguracji protokołu TCP/IP itp.

→ Aby dowiedzieć się więcej o rozwiązywaniu najczęściej spotykanych problemów, przeczytaj rozdział 21., *Identyfikowanie i usuwanie usterek w Sambie*, przeczytaj też podrozdziały *Główne problemy* w rozdziałach 12. i 14.

Hasło dostępu do udziału

Prawdopodobnie największym problemem początkujących użytkowników jest właśnie ten. Zainstalowaliśmy Linuksa i Sambę. Przebrnęliśmy przez dokumentację i udało się nam utworzyć plik *smb.conf* (lub zmodyfikować plik oryginalnie dostarczony). Uruchamiamy Sambę. Następnie przechodzimy do Windows 9x lub Windows NT i przeglądamy sieć. Czujemy się szczęśliwi, widząc serwer Samby w otoczeniu sieciowym. Jednak, kiedy klikniemy ikonę serwera Samby uzyskamy okno jak na rysunku 5.5 z prośbą o hasło dostępu do udziału *IPC$* — udziału, o którym nawet nie wiedzieliśmy, że istnieje.

Rysunek 5.5. *Okno dialogowe z pytaniem o hasło sieciowe*



Powodem występowania tego problemu jest fakt, że w czasie przeglądania zasobów komputera (wykonując żądania *treecon*) potrzebny jest dostęp do wewnętrznego udziału *IPC$*. Więcej informacji o żądaniach *treecon* znajduje się w rozdziale 4. Problem mógł mieć jedną z poniższych przyczyn:

- Zalogowaliśmy się do Windows z nazwą użytkownika i hasłem, które nie jest poprawne dla serwera Linuksa. Możemy je przetestować próbując zalogować się do Linuksa. Być może będzie trzeba dodać nowe konto za pomocą polecenia `useradd` i ustawić odpowiednie hasło. Problem ten nasilił się od wydania Samby 2.0.0, ponieważ począwszy od tej wersji domyślnym trybem bezpieczeństwa jest kontrola dostępu na poziomie użytkowników (`security = user`). We wcześniejszych wersjach, domyślną wartością było `security = share` i można było liczyć na konto gościa dające dostęp do udziału *IPC$*.
- Klient wysyła do Samby zaszyfrowane hasło, ale Samba nie została skonfigurowana do obsługi haseł zaszyfrowanych. W systemach Windows 98, Windows NT SP3 i wyższych oraz Windows 95 OSR2 i wyższych obsługa szyfrowanych haseł jest domyślna. Jedna z uaktualnień wcześniejszej wersji Windows 95 również wprowadzała obsługę szyfrowanych haseł. Problem można rozwiązać na dwa sposoby: skonfigurować szyfrowane hasła w serwerze Samby albo wyłączyć je u klienta. Konfigurację Samby do obsługi szyfrowanych haseł omówimy w rozdziale 8.

W katalogu */usr/doc/samba-$wersja/docs* (gdzie parametr *$wersja* zastąpimy wersją Samby naszego systemu) znajduje się szereg plików, które wyłączają szyfrowanie haseł w systemach operacyjnych Windows. Pliki te opisano w tabeli 5.6.

Tabela 5.6. *Pliki umożliwiające wyłączenie szyfrowania haseł w Windows*

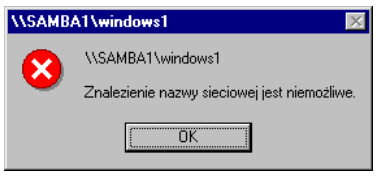
Plik	Funkcja
Win95_PlainPassword.reg	Wyłącza szyfrowanie haseł w systemie Windows 95.
Win98_PlainPassword.reg	Wyłącza szyfrowanie haseł w systemie Windows 98.
NT4_PlainPassword.reg	Wyłącza szyfrowanie haseł w systemie NT4 SP3 i wyższych.
Win2000_PlainPassword.reg	Wyłącza szyfrowanie haseł w systemie Windows 2000.

Należy po prostu skopiować odpowiedni plik do naszego klienta i dwukrotnie kliknąć jego ikonę w celu jego otwarcia. Do skopiowania tych plików na dyskietkę można wykorzystać polecenie *mcopy*.

Po zidentyfikowaniu, która z powyższych przyczyn była powodem problemu i jej usunięciu, powinniśmy bez problemu móc przeglądać serwer Samby.

Brak w sieci podanej nazwy

To prawdopodobnie, kolejny, zagadkowy błąd. Stworzyliśmy udział i możemy przeglądać serwer Samby, ale kiedy próbujemy uzyskać dostęp do nowego udziału, na ekranie pojawia się okno dialogowe jak na rysunku 5.6.



Rysunek 5.6. *Samba informuje, że w sieci nie występuje podana nazwa*

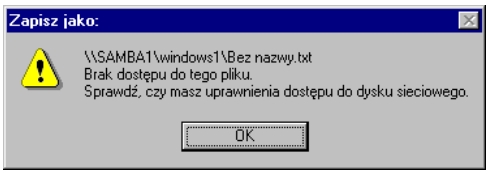
Komunikat ten nie pojawia się w przypadku błędu we wpisywaniu nazwy udziału lub dla udziału, który nie istnieje. Komunikat ten pojawia się tylko wtedy, gdy udział istnieje, ale nie istnieje udostępniany katalog albo użytkownik nie ma prawa do tego katalogu.

Aby rozwiązać ten problem, należy w przypadku, gdy katalog nie istnieje, po prostu go utworzyć, poprawić błędy w pisowni katalogu lub zmienić prawa dostępu tak, aby umożliwić dostęp określonym użytkownikom.

Brak dostępu

Inny znany problem dotyczy udziału z oznaczoną możliwością zapisu. W udziale tym powinno być możliwe dokonywanie zapisów. Niestety, zapomniano o prawach dostępu w systemie UNIX. Po prostu konto, którego używamy, nie posiada prawa do plików, które chcemy modyfikować.

Jeżeli coś takiego ma miejsce, na ekranie pojawi się okno dialogowe jak na rysunku 5.7.



Rysunek 5.7. *Samba nie pozwoli na utworzenie pliku lub katalogu*

Rozwiązanie tego problemu jest proste. Należy zmienić prawa dostępu do pliku lub katalogu, który jest przyczyną problemu.

Kłopoty z rozpoznaniem nazwy komputera

Jest to jeden z problemów, które uniemożliwiają uruchomienie serwera Samby. Demony *nmbd* oraz *smbd* poszukują nazwy hosta systemu, na którym pracują i próbują przekształcić tę nazwę na adres IP. W pliku dziennika *log.smb* zobaczymy taki zapis:

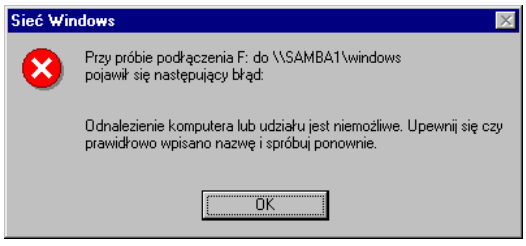
```
[1999/10/19 23:15:22, 1] smbd/server.c:main(626)
   smbd version 2.0.6-pre1 started.
   Copyright Andrew Tidgell 1992 - 1998
[1999/10/19 23:15:22, 1] smbd/files.c:file_init(216)
   file_init: Information only: requested 10000 open files, 1014 are available
[1999/10/19 23:15:22, 0] lib/util_sock.c:open_socket_in(854)
   Get_Hostbyname: Unknown host samba1.samba.com
```

Ostatni wiersz wyjaśnia problem. Funkcja `Get_Hostbyname` nie mogła przekształcić nazwy hosta na adres IP. Podobny komunikat znajdziemy w pliku *log.nmb*.

Jeżeli demony nie mogą przekształcić nazwy hosta na adres IP, nie uruchomią się. Aby rozwiązać problem, należy zapewnić, że nazwa naszego hosta może być przekształcona na adres IP. Pomocny okaże się plik */etc/hosts* albo system DNS.

Ogólne problemy podczas łączenia z serwerem

Możemy także napotkać na ogólne problemy z połączeniem. Często będzie się to objawiało komunikatem w postaci: „Nie można odnaleźć komputera lub udziału”. Przykład pokazano na rysunku 5.8.



Rysunek 5.8. *Błąd spowodowany problemami z połączeniem*

Aby rozwiązać tego rodzaju problemy, należy skorzystać ze standardowych metod rozwiązywania problemów z siecią. Niektóre wskazówki, w formie pytań wymieniono poniżej:

- Czy w komputerze-kliencie zainstalowano i skonfigurowano protokół TCP/IP? Samba obsługuje wyłącznie protokół SMB w NetBIOS za pośrednictwem TCP/IP. Z tego powodu w komputerze-kliencie musi być zainstalowany i skonfigurowany protokół TCP/IP. Jeżeli tak nie jest, najpierw należy rozwiązać ten problem.
- Czy można wykonać polecenie *ping* z klienta do naszego serwera Samby za pomocą adresu IP? Jeżeli nie można, istnieje podstawowy problem z połączeniem., jak np. kable sieciowe nie są podłączone, niepoprawne są maski podsieci lub nie działa trasowanie. Należy rozwiązać te problemy i spróbować ponownie.
- Czy działają demony Samby (*smbd* i *nmbd*)? Można to sprawdzić za pomocą jednej z metod pokazanych w rozdziale 3. Jeżeli nie działają, spróbujmy je uruchomić, a jeśli w dalszym ciągu nie działają, sprawdźmy pliki dzienników, aby się dowiedzieć dlaczego. Rozwiążmy problem i spróbujmy ponownie.

Graficzne narzędzia konfiguracyjne

Przez długi czas jedynym sposobem konfiguracji Samby była konfiguracja ręczna. Należało dokonać edycji pliku *smb.conf* i ponownie uruchomić Sambę. Później pojawiło się kilka narzędzi pracujących w przeglądarce i kilka jeszcze innych. Wreszcie, wraz z pojawieniem się wersji 2.0.0, udostępniono narzędzie *SWAT* (ang. *Samba Web Administration Tool*).

SWAT

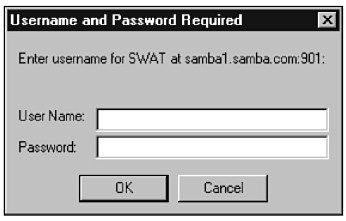
Narzędzie SWAT (*Samba Web Administration Tool*) pojawiło się wraz z Sambą 2.0.0. Jest to miniserwer WWW oraz aplikacja w postaci skryptu CGI zaprojektowana do pracy poprzez demona *inetd*. Aplikacja ta umożliwia dostęp do pliku *smb.conf* w systemie, w którym działa SWAT.

SWAT pozwala upoważnionemu użytkownikowi (z hasłem użytkownika *root*) na konfigurację wszystkich elementów Samby poprzez strony WWW. Na każdej stronie SWAT-a znajdują się pomocnicze linki do wszystkich konfigurowalnych opcji *smb.conf*, co pozwala administratorom łatwo zrozumieć efekty zmian.

SWAT instaluje się domyślnie. Wszystkie niezbędne czynności konfiguracyjne wykonywane są w czasie instalacji z Samby pakietu RPM w dowolnej dystrybucji Linuksa. Aby uruchomić SWAT-a, po prostu należy połączyć się przeglądarką z serwerem Samby na port 901. Na przykład, aby skonfigurować za pomocą programu SWAT-a serwer *samba1.samba.com*, należy użyć adresu *http://samba1.samba.com:901/*.

Po połączeniu przeglądarki ze SWAT-em, pojawi się okno dialogowe autoryzacji wyświetlające pytanie o nazwę użytkownika i hasło. W tym miejscu należy wprowadzić odpowiednie dane o użytkowniku, który posiada odpowiednie prawa jak np. *root*. Na rysunku 5.9. pokazano ekran autoryzacji SWAT w przeglądarce.

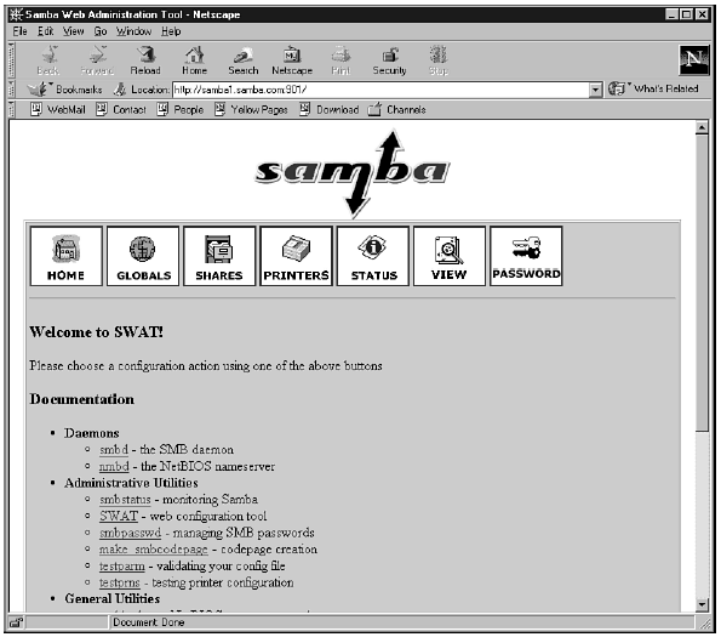
Rysunek 5.9.
Dostęp do programu SWAT przez przeglądarkę



Po zalogowaniu pojawi się główne okno SWAT-a, jak to pokazano na rysunku 5.10. Pozwala ono na wybór spośród:

- *Home* — powrót do głównej strony SWAT-a,
- *Globals* — zarządzanie sekcją `[global]` pliku *smb.conf*,
- *Shares* — zarządzanie udziałami plików dla serwera Samby,
- *Printers* — zarządzanie udziałami drukarek serwera Samby,
- *Status* — tu możemy uzyskać informacje na temat pracy serwera,
- *View* — podgląd pliku *smb.conf*,
- *Password* — zarządzanie hasłami serwera Samby lub w komputera zdalnego.

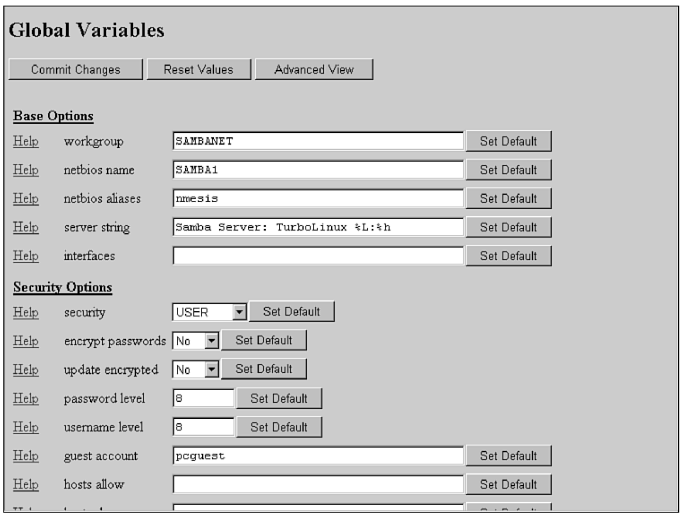
Rysunek 5.10.
Macierzysta strona SWAT-a



W każdej chwili możemy powrócić do macierzystej strony SWAT-a, poprzez kliknięcie ikony HOME. W poniższych podrozdziałach opiszemy każdą dostępną stronę konfiguracyjną.

Zarządzanie sekcją [global]

Jeżeli wybierzemy ikonę *GLOBALS*, program SWAT wyświetli stronę WWW, która pozwala na modyfikację wielu najważniejszych parametrów globalnych Samby. Tę stronę WWW pokazano na rysunku 5.11. Zmienne globalne Samby pogrupowano tematycznie.

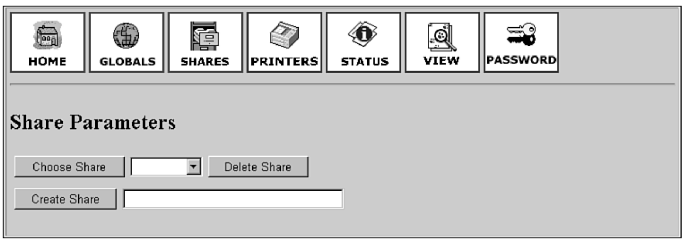


Rysunek 5.11. *Modyfikacja parametrów globalnych za pomocą programu SWAT jest łatwa*

Kliknięcie przycisku *Advanced View* powoduje wyświetlenie strony z tak samo pogrupowanymi opcjami, ale teraz możemy poprawiać wszystkie. Aby zmodyfikować parametr, wystarczy po prostu przewinąć ekran do określonego parametru, wprowadzić nową wartość i kliknąć przycisk *Commit*.

Zarządzanie udziałami plików

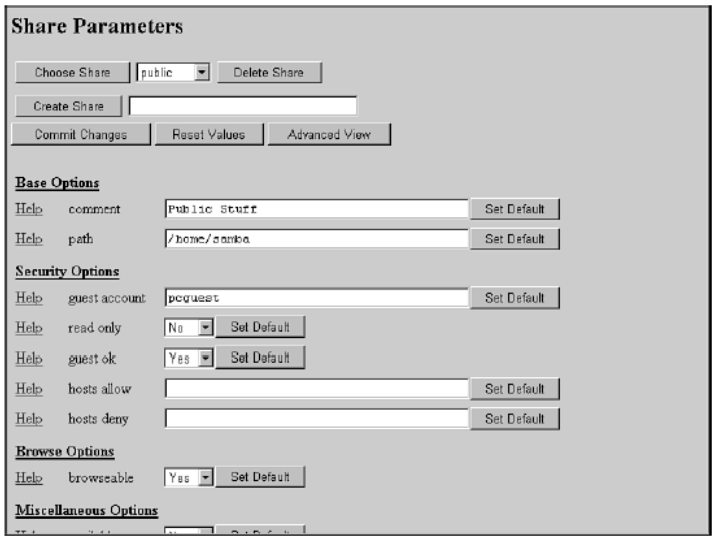
Kiedy wybierzemy ikonę *SHARES*, SWAT wyświetli stronę WWW, która pozwala na tworzenie nowych udziałów i modyfikowanie istniejących. Stronę tę pokazano na rysunku 5.12.



Rysunek 5.12. *Za pomocą SWAT-a można tworzyć i modyfikować udziały*

Aby zmodyfikować dowolny z parametrów dla istniejącego udziału, należy wybrać ten udział z listy rozwijanej położonej obok przycisku *Choose Share*, a następnie kliknąć ten przycisk. Na ekranie pojawi się strona pokazana na rysunku 5.13.

Znów, aby utworzyć nowy udział, należy wprowadzić jego nazwę w polu obok przycisku *Create Share*, a następnie kliknąć ten przycisk. Na ekranie pojawi się strona podobna do przedstawionej na rysunku 5.13 z nazwą nowego udziału wpisaną w pierwsze pole.



Rysunek 5.13. *Modyfikacja lub tworzenie nowego udziału za pomocą SWAT-a*

Na tej stronie można wykonać następujące operacje:

- Wybrać inny udział poprzez wybranie go z listy i kliknięcie przycisku *Choose Share*.
- Utworzyć nowy udział poprzez wprowadzenie jego nazwy w odpowiednim polu i kliknięcie przycisku *New Share*.
- Zatwierdzić wprowadzone zmiany poprzez kliknięcie przycisku *Commit Changes*.
- Usunąć udział poprzez kliknięcie przycisku *Delete Share*.

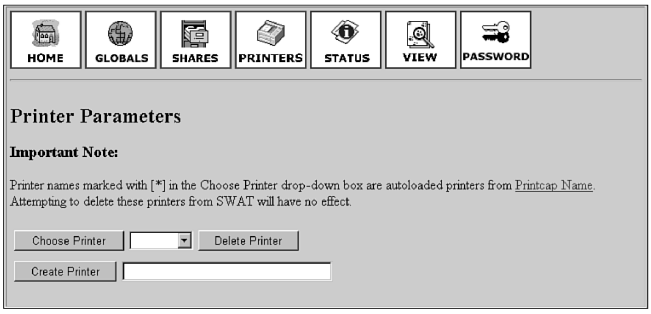
Aby zmodyfikować parametry, których nie ma na tej stronie, należy kliknąć przycisk *Advanced View* i dokonać odpowiednich zmian.

Po dokonaniu wszystkich zmian należy kliknąć przycisk *Commit Changes*, a zostaną one uwzględnione dla określonego udziału. Zmiany są uwzględniane przez Sambę natychmiast.

Zarządzanie udziałami drukarek

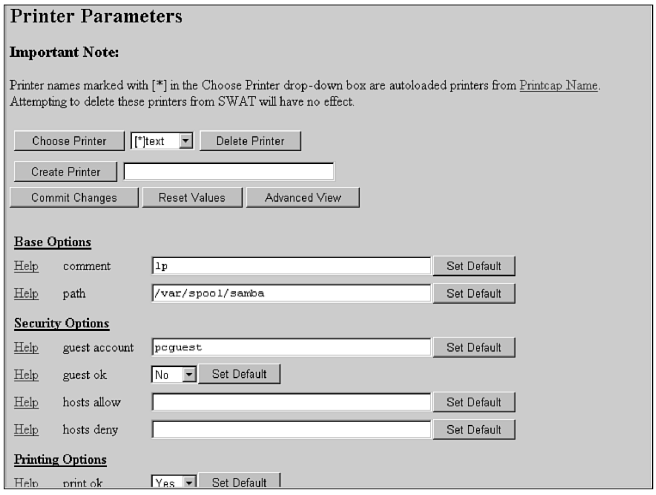
Po wybraniu ikony *PRINTERS* z dowolnej strony SWAT-a na ekranie pojawi się strona WWW umożliwiająca tworzenie nowych drukarek i modyfikację istniejących. Stronę tę pokazano na rysunku 5.14.

Rysunek 5.14. *Tworzenie i modyfikacja drukarek za pomocą SWAT-a*



Aby zmodyfikować istniejącą drukarkę, należy wybrać ją z listy rozwijanej położonej obok przycisku *Choose Printer*, a następnie kliknąć ten przycisk. Na ekranie pojawi się strona jak na rysunku 5.15.

Rysunek 5.15. *Modyfikacja lub tworzenie drukarek za pomocą SWAT-a*



Ponownie, aby utworzyć nową drukarkę, należy wprowadzić jej nazwę w polu obok przycisku *Create Printer* i kliknąć ten przycisk. Na ekranie pojawi się strona podobna do przedstawionej na rysunku 5.15 z nazwą nowej drukarki w pierwszym polu.

Na tej stronie można wykonać następujące operacje:

- Wybrać inną drukarkę poprzez wybranie jej i kliknięcie przycisku *Choose Share*.
- Utworzyć nową drukarkę poprzez wprowadzenie jej nazwy w odpowiednim polu i kliknięcie przycisku *New Share*.

- Zatwierdzić wszystkie wykonane zmiany poprzez kliknięcie przycisku *Commit Changes*.
- Usunąć drukarkę poprzez kliknięcie przycisku *Delete Share*.

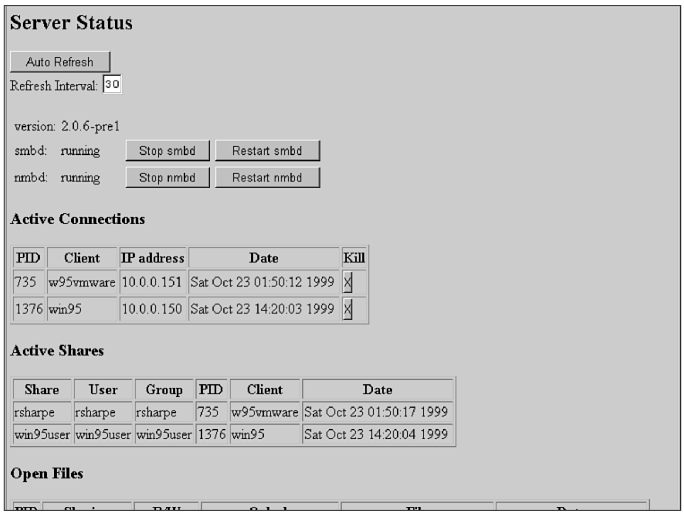
Aby zmodyfikować parametry, których nie ma na tej stronie, należy kliknąć przycisk *Advanced View* i dokonać odpowiednich zmian.

Po dokonaniu wszystkich zmian należy kliknąć przycisk *Commit Changes*, a zostaną one uwzględnione dla określonego udziału. Zmiany są uwzględniane przez Sambę natychmiast.

Uzyskiwanie informacji o pracy serwera

Po wybraniu ikony *STATUS* z dowolnej strony SWAT-a na ekranie pojawi się strona WWW wyświetlająca informacje na temat pracy Samby. Strona ta pozwala także na zatrzymanie i ponowne uruchomienie demonów Samby. Pozwala także na rozłączenie aktywnych użytkowników. Stronę WWW, jaką wyświetla SWAT, pokazano na rysunku 5.16.

Rysunek 5.16. *Strona statusu systemu SWAT*



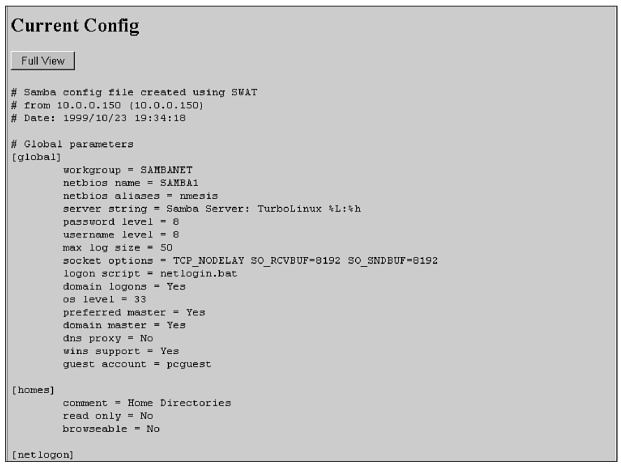
Strona statusu posiada także mechanizmy pozwalające na ciągłe odświeżanie. Należy wprowadzić czas odświeżania w polu *Refresh Interval* i kliknąć przycisk *Auto Refresh*.

Przeglądanie pliku smb.conf

Po wybraniu ikony *VIEW* na ekranie pojawi się strona WWW wyświetlająca kompletny plik *smb.conf*. Stronę tę pokazano na rysunku 5.17.

Aby uzyskać listing zawierający wartości wszystkich parametrów utrzymywanych przez Sambę, wystarczy kliknąć przycisk *Full View*.

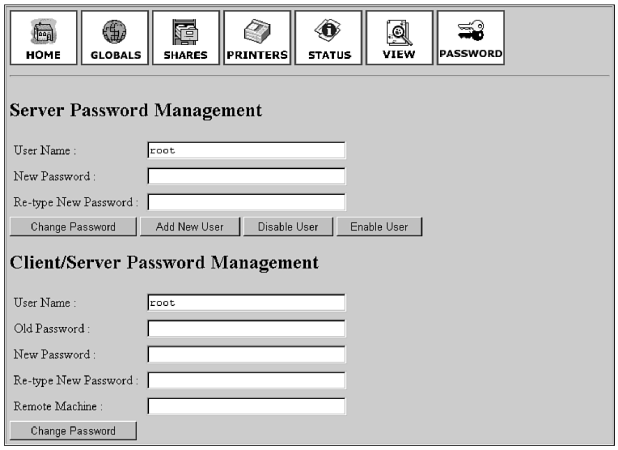
Rysunek 5.17. *Plik smb.conf utworzony za pomocą systemu SWAT-a*



Zmiana hasła

Kliknięcie ikony *PASSWORD* powoduje wyświetlenie strony WWW umożliwiającej modyfikację hasła na serwerze Samby albo na zmianę hasła na innym serwerze CIFS/SMB w innym miejscu sieci. Można także dodać, wyłączyć lub włączyć konta użytkowników. Stronę tę pokazano na rysunku 5.18.

Rysunek 5.18. *Zmiana hasła za pomocą SWAT-a*



Samba wykonuje operacje wyłącznie z plikiem *smbpasswd*, a nie z plikiem haseł systemu UNIX.

WEBMIN

Webmin to pakiet administracji systemów UNIX w przeglądarce WWW. Zawiera funkcje zarządzania Sambą oraz konfiguracji kont, DNS, serwera Apache, sendmail oraz wielu innych zadań administracyjnych. W tej książce skupimy się na funkcjach systemu Webmin pomagających w konfiguracji Samby.

Webmin składa się z miniaturowego serwera WWW napisanego w Perlu oraz zbioru programów CGI implementujących funkcje konfiguracji systemu z poziomu przeglądarki WWW. Aby móc korzystać z Webmina, należy go zdobyć i zainstalować.

Program Webmin można pobrać pod adresem *www.webmin.com/webmin/*. Następnie należy go rozpakować ze skompresowanego archiwum *tar*[2]. Można to zrobić za pomocą następującego polecenia:

```
tar -zxvf webmin-${VERSION}_tar.gz
```

W systemach, w których nie ma programu *tar* z licencją GNU, najpierw trzeba będzie rozpakować plik. Można to zarobić za pomocą polecenia `gzip -d webmin-${VERSION}_tar.gz` (w niektórych systemach można skorzystać z programu *gunzip*). W każdym poleceniu z poprzedniego ciągu wyrażenie `${VERSION}` należy zamienić na bieżącą wersję programu Webmin. W czasie pisania tej książki najnowszą wersją była 0.78[3].

Po rozpakowaniu i wydobyciu plików z archiwum dystrybucji należy przejść do nowo utworzonego katalogu — zwykle *webmin-VER*, gdzie *VER* jest numerem wersji Webmina. Następnie należy przeczytać plik *README* zawierający instrukcje instalacyjne. Na cały proces instalacji składają się: z etap uruchomienia odpowiedniego polecenia oraz etap udzielania odpowiedzi na zadawane pytania:

```
./setup.sh
```

Podczas instalacji system zada nam pytanie o hasło pierwszego użytkownika systemu Webmin — *admin*. Hasło to będzie potrzebne do połączenia ze stroną Webmin.

W czasie pisania tej książki program Webmin obsługiwały następujące dystrybucje Linuksa:

- Red Hat Linux 4.0 do 6.1;
- Caldera OpenLinux 2.3 i 3.0 oraz OpenLinux Server 2.3e;
- Slackware Linux 3.2 do 4.0 oraz 7.0;
- Debian Linux 1.3 do 2.2;
- Linux Mandrake 5.3, 6.0, 6.1 oraz 7.0;
- SuSE Linux 5.1 do 6.3;
- Colel Linux 1.0;
- DELIX DLD 5.2 do 6.0;
- MkLinux DR2.1 i 3.0;
- TurboLinux 4.0.

[2] Dostępne są również wersje gotowe do zainstalowania menedżerami pakietów popularnych dystrybucji — *przyp. red.*

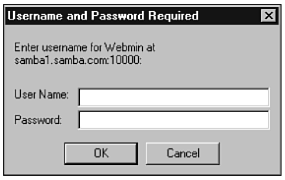
[3] W tej chwili (listopad 2001 r.) ukazała się wersja 0.90 — *przyp. red.*

Webmin działa także w innych dystrybucjach podobnych do Red Hata. Na przykład działa poprawnie w systemie TurboLinux 3.4.0 i wyższych, włącznie z TurboLinux 6.0. Obsługuje także kilka innych systemów operacyjnych UNIX takich jak FreeBSD, OpenBSD, Sun Solaris, BSDI, HP-UX, SGI Irix, Tru64 UNIX (poprzednio Digital UNIX), AIX oraz SCO UNIXWARE.

Informacje o pełniejszej liście systemów operacyjnych obsługiwanych przez Webmin można znaleźć na stronie WWW systemu Webmin (*http://www.webmin.com/webmin*) oraz w skrypcie instalacyjnym.

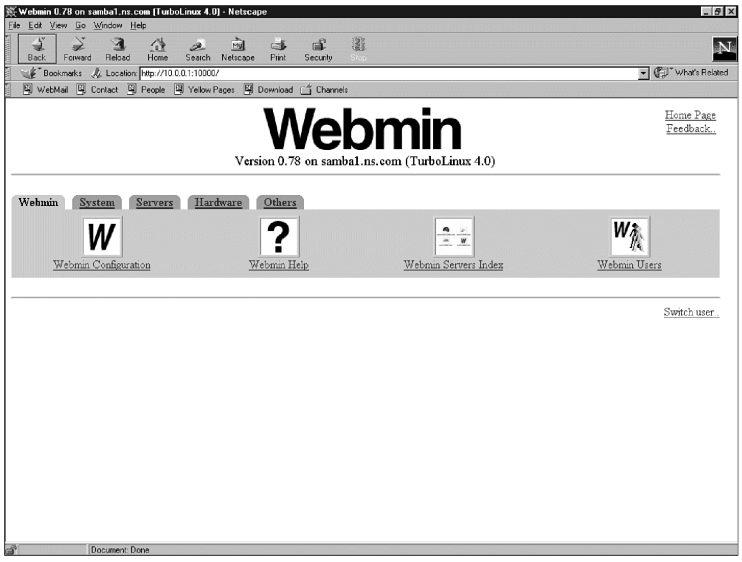
Po wykonaniu instalacji i uruchomieniu systemu Webmin można uzyskać do niego dostęp z dowolnej przeglądarki łącząc się na port 10000 serwera(maszyny), gdzie zainstalowana jest Samba. W przypadku zmiany numeru portu przypisanego do systemu Webmin powinniśmy użyć go zamiast domyślnego portu 10000.

Rysunek 5.19.
Połączenie z Webminem



Po wprowadzeniu poprawnej nazwy użytkownika i hasła na ekranie pojawi się macierzysta strona Webmin, jak to pokazano na rysunku 5.20.

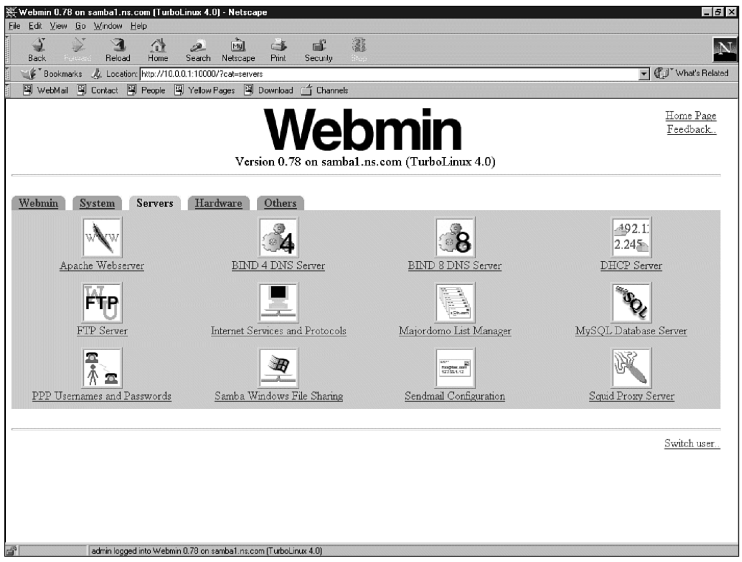
Rysunek 5.20.
Główna strona Webmina; należy wybrać kartę Servers



Za pomocą systemu Webmin można administrować wieloma elementami systemów UNIX, ale nas interesują tylko możliwości administrowania Sambą. Aby zmienić konfigurację Samby, należy wybrać zakładkę *Servers* na głównej stronie Webmin. Na ekranie pojawi się strona jak na rysunku 5.21.

Na tym ekranie wybieramy ikonę *Samba Windows File Sharing*.

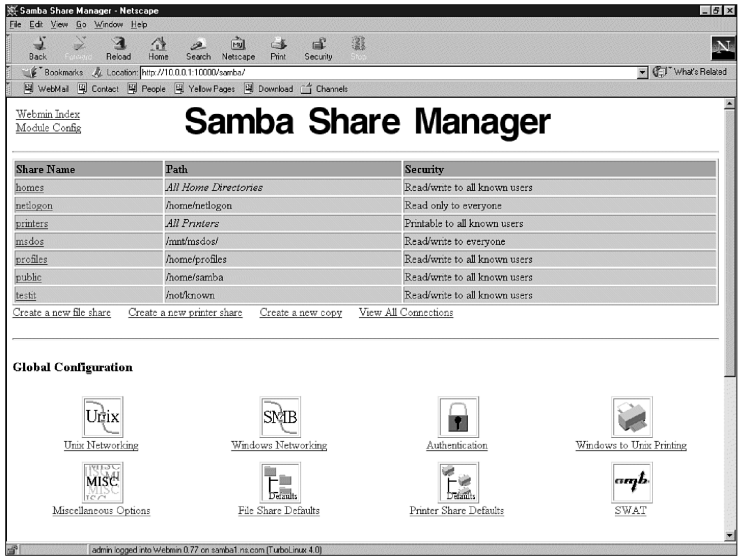
Rysunek 5.21. *Strona Webmin karty Servers na stronie Webmina wyświetla wszystkie obsługiwane przez system serwery*



We wcześniejszych wersjach Webmina wszystkie ikony administracyjne znajdowały się na stronie głównej. Jeżeli posiadamy wersję starszą niż 0.78 lub dużo nowszą niż 0.78, powinniśmy odpowiednio dostosować przedstawione tu instrukcje do naszych potrzeb.

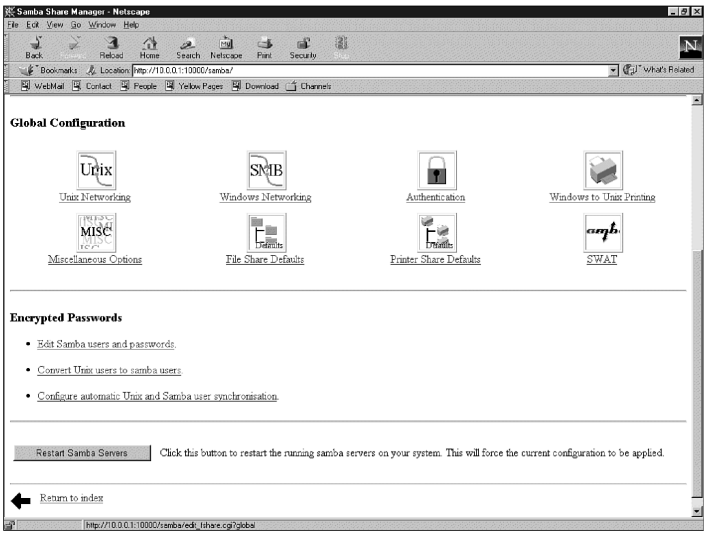
Po wybraniu ikony *Samba Windows File Sharing* na ekranie pojawi się strona menedżera Samby (*Samba Share Manager*), jak to pokazano na rysunku 5.22.

Rysunek 5.22. *Strona menedżera Samby w Webmin*



Z tej strony można zarządzać udziałami plików i drukarek oraz innymi elementami parametrów globalnych Samby. Sekcję parametrów globalnych można wybrać, klikając ikony pokazane u dołu ekranu na rysunku 5.22. Przewijając stronę pokazaną na

rysunku 5.22, zorientujemy się, że znajduje się na niej także obsługa zaszyfrowanych haseł oraz że można z jej poziomu ponownie uruchomić serwer Samby. Na rysunku 5.23 pokazano drugą połowę strony menedżera Samby w Webminie.



Rysunek 5.23. *Webmin pozwala także na ponowne uruchomienie Samby i zarządzanie zaszyfrowanymi hasłami*

Z tych stron można wykonać te same funkcje działania, jak na stronach systemu SWAT.

System Webmin nie obsługuje nazw plików zawierających w nazwie znak myślnika (-) oraz nie obsługuje pliku *smb.conf* zawierającego parametry `config` lub `include`.

Dodatkowe informacje

Aby uzyskać więcej informacji o diagnozowaniu problemów z Sambą, przeczytaj plik *DIAGNOSIS.txt*, który znajdziesz w katalogu *docs/textdocs*.

O wszystkich parametrach Samby przeczytasz na stronach podręcznika *man* (należy skorzystać z polecenia `man smb.conf` na serwerze z zainstalowaną Sambą).