

Politechnika Krakowska

Katedra Automatyki i Technik Informatycznych

Laboratorium Sieci Komputerowych

2010/2011



SAMBA

1. Wprowadzenie

Celem tego ćwiczenia jest zapoznanie się z podstawowymi zagadnieniami dotyczącymi uruchamiania, konfiguracji i działania serwera protokołu SMB – Samba.

SMB

W sieci komputerowych SMB (Server Message Block) to protokół funkcjonujący w warstwie aplikacji modelu OSI. Stosowany głównie do współdzielenia dostępu do plików, drukarek, portów szeregowych oraz różnego rodzaju komunikacji między komputerami w sieci.

Pierwotna wersja tego protokołu została opracowana w roku 1984 przez pracownika firmy IBM. Protokół został pierwszy raz zastosowany w systemie MS-DOS 3.1, używano go do przesyłania zamówień wejścia-wyjścia przez sieć w programie IBM PC Network. Przez kolejne lata protokół ten ewoluował. Był wiele razy rozszerzany (głównie przez Microsoft) w sytuacjach, kiedy dostawcy potrzebowali nowych funkcji np. uwierzytelniania. W późniejszych latach SMB stał się podstawą „Otoczenia sieciowego” w systemach Windows. CIFS (*Common Internet File System*) to nowa wersja protokołu SMB opracowywana przez Microsoft i kilka innych firm, został on zaimplementowany m. in. w Windows 2000/XP/2003 oraz w Samba 3.0. W 2006 Microsoft wraz z Windows Vista wprowadził wersję SMB2.

SMB może pracować w oparciu o następujące protokoły warstwy niższej:

- NetBIOS w sieciach IPX i DECnet
- NetBEUI czyli implementacja NetBIOS w sieciach LLC(802.2)
- standard RFC NetBIOS w sieciach TCP/IP

Application	SMB			
Presentation				
Session	NetBIOS	NetBEUI	NetBIOS	NetBIOS
Transport	IPX		DECnet	TCP & UDP
Network			IP	

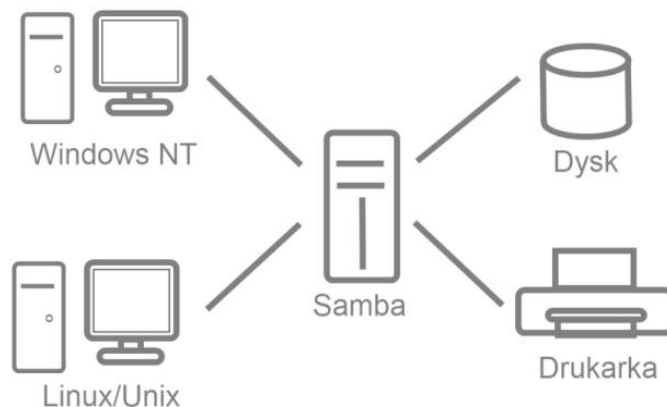
Lokalizacja protokołu SMB w modelu OSI

Samba

Samba to darmowy rozpowszechniany pod licencją GNU General Public License zbiór narzędzi umożliwiających przede wszystkim współdzielenie zasobów, takich jak drukarki i pliki, w sieci. Jest przeznaczona dla platformy Linux/Unix, ale współpracuje również z platformą Windows. Samba korzysta z protokołu SMB/CIFS.

Komputery-klienci Samby w czasie korzystania z serwera używają zarówno protokołu TCP, jak i UDP. Protokołu TCP używają w celu uzyskania dostępu do pliku lub drukarki oraz zalogowania się do

sieci. W tym celu ustanawiają połączenie TCP z demonem *smbd* na porcie 139. Komputery-klienty korzystają z protokołu UDP w celu zarejestrowania lub przekształcenia nazw NetBIOS, a także w czasie przeglądania sieci.



Serwer plików udostępniający pliki oraz drukarkę

Oto niektóre z funkcji Samby:

- Serwer logowania Sieci Windows. Identyfikacja oraz uwierzytelnianie komputerów i użytkowników poprzez Usługi Uwierzytelniające. Uwierzytelnianie logowania domeny Windows
- Serwer przeglądania Windows
- Serwer członkowski domeny – klient z użyciem Samby może zostać członkiem domeny
- Podstawowy kontroler domeny Windows NT (PDC)
- Wykonywanie skryptów logowania za każdym razem gdy użytkownik połączy lub rozłączy się z zasobem
- Scentralizowaną obsługę zasobów sieciowych, takich jak komputery czy użytkownicy, poprzez Usługi Katalogowe. Możliwość przyłączenia się do domeny Active Directory za pomocą LDAP i Kerberos
- Świadczenie usług nazewniczych (rozgłoszeniowych i WINS), może działać jako internetowy serwer nazw Windows dla klientów systemu Windows
- Obsługa OpLock – pozwala na buforowanie plików w komputerach-klientach
- Stosowanie aliasów NetBIOS, co pozwala działać pojedynczemu serwerowi Samby jak kilka oddzielnych serwerów
- Automatyczna instalacja sterowników drukarek w systemach Windows – umożliwia łatwą instalację sterowników drukarek w przypadku, gdy użytkownicy chcą skorzystać z nowych drukarek.
- Obsługa SSL – za pomocą serwerów proxy SSL można uzyskać bezpieczny dostęp do serwerów Samby w sieci Internet

Struktura Samby

Samby składa się z kilku komponentów. Funkcjonalnie składa się ona z demonów, plików programów, pliku konfiguracyjnego, oraz katalogu dla plików dzienników.

2. Konfiguracja serwera Samby

Instalacja Samby

Sambę możemy pozyskać z Internetu w wersji skompilowanej dla naszej wersji systemu operacyjnego (dla wielu odmian systemu UNIX, w szczególności dla systemu Linux), a w przypadku braku takiego pakietu lub w celu dostosowania Samby do specyficznych wymagań można także skompilować Sambę wykorzystując jej kod źródłowy do którego dostęp jest otwarty.

W wypadku dystrybucji Debian Linux, w celu zainstalowania lub uaktualnienia binarnej wersji Samby należy użyć programu apt i skorzystać z polecenia:

```
apt-get install samba samba-common samba-client swat
```

Powyższe polecenie zainstaluje także graficzne webowe narzędzie administracyjne Samby – SWAT.

Plik konfiguracyjny

Plikiem konfiguracyjnym serwera Samby jest plik o nazwie `smb.conf`, który w dystrybucji Debian znajduje się w katalogu `/etc/samba/`. Zawiera wszystkie informacje o konfiguracji demonów `smbd` i `nmbd`. Jest to zwykły plik tekstowy, a więc edycji możemy dokonać za pomocą dowolnego edytora tekstu. Plik ten podzielony jest na sekcje które posiadają swoje nagłówki. Nagłówki ujęte są w nawiasy kwadratowe `[]`. Kolejny nagłówek danej sekcji oznacza koniec sekcji poprzedniej. Komentarze umieszczone są w liniach rozpoczynających się od znaku `#` lub średnika.

Poniżej przedstawiono przykładowy plik `smb.conf`:

```
[global]
workgroup = GRUPAROBOCZA
server string = Serwer Samby
hosts allow = 192.168.0
printcap name = /etc/printcap
load printers = yes
printing = cups
log file = /var/log/samba/%m.log
max log size = 0
smb passwd file = /etc/samba/smbpasswd
```

```

security = user
encrypt passwords = Yes
pam password change = yes
obey pam restrictions = yes
dns proxy = no

[homes]
comment = Katalogi domowe
browseable = no
writeable = yes
valid users = %S
directory mode = 0775

[printers]
comment = Wszystkie drukarki
path = /var/spool/samba
browseable = no
quest ok = no
writable = no
printable = yes

```

Plik konfiguracyjny – sekcje

W poniższej tabeli zawarto sekcje które mogą znaleźć się w 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. Ustawiane są w niej domyślne parametry, które są brane pod uwagę jeżeli w tworzonym udziale nie wymienimy explicite jakiegoś parametru. Jest to jedyna sekcja, która jest potrzebna, aby komputer zaistniał w „otoczeniu sieciowym”. Sekcja <i>global</i> nie musi być oznaczona jako [global].
[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.

Ćwiczenie: SAMBA

[printers]	Trzecia sekcja specjalna. Definiuje ona specjalny udział, który pozwala użytkownikom Windows na podłączenie dowolnej drukarki zainstalowanej na serwerze Samby. Domyślnie lista drukarek do wyeksportowania jest pobierana z pliku /etc/printcap. Wszystkie parametry zdefiniowane w tej sekcji dotyczą wszystkich drukarek eksportowanych przez Sambę. Pozwala to na ustawienie parametrów bezpieczeństwa globalnie dla wszystkich drukarek.
[nazwa udziału]	Wszystkie pozostałe sekcje w pliku <code>smb.conf</code> określają pojedynczy udział o podanej nazwie. Komputery-klienci łączą się z udziałem, a następnie uzyskują dostęp do plików ramach tego udziału. Nazwy udziałów mogą zawierać makra polecenia. Pozwala to na automatyzację Samby.

Parametry podaje się w następującej formie:

`nazwa=wartosc`

gdzie:

nazwa określa nazwę parametru. Nazwa może zawierać spacje.

wartosc określa wartość przypisaną do parametru. Może to być ciąg znaków, liczba, słowo, wyrażenia regularne itp. Parametry mogą zajmować więcej niż jeden wiersz. W takim przypadku należy użyć standardowego uniksowego znaku kontynuacji \ Znak ten na końcu wiersza zmusza Sambę do traktowania następnego wiersza jako kontynuacji wiersza bieżącego.

Plik konfiguracyjny – parametry

Sekcja [global]

workgroup – kontroluje, jaka grupa sieciowa będzie przedstawiana na żądanie klienta, kontroluje także nazwę domeny użytą w ustawieniu `security = domain`. Domyślna wartość: ustawiana podczas kompilacji w zmiennej `workgroup`. Przykład: `workgroup = MOJAGRUPA`

server string – parametr ten określa, jaki ciąg znaków pojawia się w polu komentarza drukarki w menedżerze wydruku, a także jako opis serwera w otoczeniu sieciowym. Może to być dowolny ciąg znakowy, jaki wyświetli się użytkownikom. Określa także, co zostanie wyświetlone w liście przeglądania po nazwie komputera. Przykład `server string = Serwer Samby`.

wins support – boolowski parametr który kontroluje, czy proces `nmbd` w Sambie może występować w roli serwera WINS. Nie ustawia się tego parametru na `true` na więcej niż jednym komputerze w sieci lokalnej.

wins server – parametr ten określa adres IP (lub nazwę DNS: adres IP do wyboru) serwera WINS dla którego może się zarejestrować demon `nmbd`. Jeśli używamy w sieci serwer WINS parametr powinien mieć w wartości adres IP tego serwera.

dns proxy - gdy parametr ten jest ustawiony, to demon nmbd pracuje jako serwer WINS tj. gdy uzna nazwy NetBIOS jako niezarejestrowane, będzie interpretował te nazwy NetBIOS słowo w słowo tak jak w przypadku nazw DNS i będzie szukał ich za pomocą serwera DNS.

netbios name – parametr ten ustawia nazwę NetBIOS, pod którą przedstawiany będzie serwer Samby. Domyślnie jest ona taka sama, jak pierwszy składnik nazwy DNS tego komputera. Jeśli komputer ten jest serwerem przeglądania lub domen, nazwa ta będzie nazwą, pod którą ta usługa będzie widoczna.

status - włącza lub wyłącza logowanie (rejestrowanie) połączeń w pliku statusu który smbstatus(1) może czytać. Z tym parametrem wyłączonym smbstatus(1) nie będzie mógł powiedzieć ci, które połączenia są aktywne. Nie powinieneś nigdy potrzebować zmieniać tego parametru. Domyślnie: status = yes

log file – pozwala nadpisywać nazwę pliku dziennika zdarzeń Samby. Parametr ten używa standardowych podstawień, pozwalających na rozdzielanie plików dotyczących każdego z użytkowników lub komputerów.

max log size – opcja ta (liczba reprezentująca kilobajty) określa maksymalny rozmiar, do jakiego może urosnąć plik dziennika zdarzeń. Samba okresowo sprawdza rozmiar pliku i jeśli nastąpi przekroczenie zadanego rozmiaru, zmieniana jest nazwa pliku poprzez dodanie rozszerzenia .old. Przykład: max log size = 1000

security – opcja ta opisuje, w jaki sposób klienci odpowiadają Sambie i jest jednym z ważniejszych ustawień w pliku smb.conf. Opcja ta ustawia tryb bitu bezpieczeństwa, aby włączyć lub wyłączyć zabezpieczenie na poziomie udziału, w odpowiedzi na protokół wynegocjowany z demonem smbd. Dzięki temu bitowi klienci decydują czy (i jak) przesłać nazwę użytkownika i jego hasło do serwera. Parametr ten może przyjmować różne wartości: share, user, server, domain

security = share – gdy klienci łączą się na poziomie udziału zabezpieczeń serwera, to, dopóki nie spróbują połączyć się do zasobu udziału, nie muszą logować się do serwer z podaniem poprawnej nazwy oraz hasła. W zastępstwie klient wysyła informacje uwierzytelniające związane z udziałem, w czasie gdy użytkownik próbuje się połączyć z zasobem.

security = user – jest to domyślnie ustawienie parametru w Sambie. Dla zabezpieczeń na poziomie użytkownika, klient najpierw musi zalogować się przy użyciu poprawnej nazwy użytkownika i hasła. W trybie tym mogą być używane także hasła szyfrowane.

security = server – w tym trybie Samba próbuje stwierdzić poprawność nazwy użytkownika lub hasła przez przesłanie ich do innego serwer SMB takiego jak Windows NT. Jeśli się to nie powiedzie, powraca do trybu security = user. Tryby te różniąc się metodą, jaką postępuje serwer w celu autoryzacji użytkownika, co nie jest widoczne z zewnątrz dla klienta.

security = domain – tryb ten działa, tylko gdy przy dodawaniu tego komputera do domeny Windows NT wykorzystywany jest plik smbpasswd. Oczekuje on, że parametr encrypt passwords będzie ustawiony na true.

encrypt passwords – boolowski parametr kontroluje, czy z klientem będzie negocjowane szyfrowanie haseł. Aby szyfrowanie haseł działało poprawnie, demon smbd musi mieć dostęp do lokalnego pliku smbpasswd. Innym podejściem jest ustawienie parametru security server lub security domain, co wymusza uwierzytelnienie z innych serwerów.

Sekcja [homes] oraz inne udziały

comment - Jest to pole tekstowe które jest widziane obok udziału, gdy klient wykonuje zapytania na serwerze albo poprzez otoczenie sieciowe, albo przez "net view" aby sprawdzić, które udziały są dostępne. Przykład comment = Pliki Samby

writeable - Jeśli ten parametr jest ustawiony na no, wtedy użytkownicy usługi nie mogą tworzyć lub modyfikować plików w jej katalogu. Parametry writeable=, writable= i write ok= są synonimami, co oznacza, że całkowicie się wzajemnie zastępują.

read only – jest odwróconym synonimem dla writeable=, writable= i write ok=, co oznacza, że read only=yes jest synonimem dla writeable=no, a read only=no jest synonimem dla writeable=yes.

browseable - Kontroluje czy ten współdział jest widziany na liście dostępnych współdziałów w net view i na liście przeglądania. Instruuje klienta SMB, czy wyświetlić udział w oknie klienta SMB (np. Eksploratora Windows). Jeżeli opcja ustawiona jest na yes, to fakt istnienia udziału jest obserwowalny nawet dla użytkownika bez prawa do niego. Jeżeli jest ustawiona na no, to udział nie jest widoczny nawet dla użytkowników umieszczonych na liście valid users. Jednak w przypadku klientów umożliwiających dostęp do udziału nie umieszczonego w spisie udziałów (np. smbclient), wpis browsable=no nie powstrzyma upoważnionego użytkownika przed otrzymaniem dostępu do udziału, tak długo, jak długo wpisuje on właściwe polecenie z właściwą nazwą udziałów.

hide files – w tym parametrze określa się listy plików ukrytych. Do plików tych można uzyskać dostęp znając nazwę (ścieżkę pliku) lub ustawiając przeglądanie plików ukrytych w przeglądarce

veto files – określa listę nazw plików, katalogów, które są oznaczone przez Sambę jako niewidoczne i nie można do nich uzyskać dostępu. Poszczególne wpisy listy są oddzielone znakiem /. Można stosować znaki specjalne ? i *.

volume – pozwala na zmianę nazwy woluminu dla udziału. Nazwa woluminu występuje w przypadku odwzorowania udziału jako dysku sieciowego.

path, directory – określa uniksową ścieżkę dostępu na serwerze Samby do udziału. Pliki i katalogi poniżej tego poziomu znajdują się w głównym katalogu udziału

guest ok – jeśli parametr ten jest ustawiony na yes, nie potrzebujemy hasła, aby zalogować się do udziału. Uprawnienia będą przejęte z definicji konta gościa.

guest account – nazwa użytkownika, która będzie używana podczas dostępu do usługi, przy włączonej opcji guest ok. Wszystkie uprawnienia przypisane temu użytkownikowi będą dostępne dla każdego, kto skorzysta z usługi gościa. W niektórych systemach domyślny użytkownik typu gość (zwany nobody) może nie posiadać uprawnień np. do drukowania.

read list – jest to lista użytkowników, którzy otrzymują prawa tylko do odczytu danej udziału. Jeśli podłączony użytkownik znajduje się na tej liście, to nie otrzyma prawa zapisywania bez względu na to, czy opcja read only jest ustawiona czy nie. Lista może zawierać nazwy grup. Parametr **write list** jest analogiczny.

valid users - jest to lista użytkowników którzy powinni mieć zezwolenie na logowanie się do tej usługi. Nazwy zaczynające się od '@', '+' i '&' są interpretowane przy użyciu tych samych reguł, co

Ćwiczenie: SAMBA

opisane w parametrze invalid users. Jeśli jest pusta (domyślnie), wtedy każdy użytkownik może się logować. Jeśli nazwa użytkownika jest zarówno na tej liście jak i invalid users, wtedy dostęp jest dla tego użytkownika zabroniony. Bieżąca nazwa usługi jest podstawiana za %S .

invalid users - jest to lista użytkowników, którzy nie mają dostępu do danego udziału. Ta lista nadpisuje wszystkie ustawienia z opcji valid users= dla tego udziału.

read list - określa listę użytkowników, którzy uzyskują dostęp „tylko do odczytu”. Parametr ten nadpisuje opcje read only=, writable= i podobne, ograniczając dostęp wymienionych użytkowników do prawa do odczytu danego udziału. Jeżeli dowolny użytkownik z listy read list= jest także na write list= dla danego udziału, to opcja read list= jest nadpisywana i dany użytkownik może także zapisywać do udziału.

path - Jest to ścieżka do katalogu reprezentowanego przez udział. W przypadku udziału drukarki jest to katalog [spool].

Sekcja [printers]

printable - jeśli ten parametr jest ustawiony na yes , wtedy klienci mogą otwierać, zapisywać do i wysyłać pliki wydruku do katalogu określonego dla usługi. Zauważ, że usługi drukowalne będą ZAWSZE pozwalać na zapis do ścieżki dostępu usługi (zgodnie z uprawnieniami użytkownika) poprzez kolejki danych do wydruku. Parametr writeable kontroluje tylko nie-drukowalny dostęp do zasobu. W sekcji [printers] opcja printable jest domyślnie ustawiona na yes. W pozostałych przypadkach jest ustawiona na no.

Plik konfiguracyjny – zmienne

W pliku smb.conf istnieją także bardzo ważna inne elementy funkcjonalne : *makrodefinicje i zmienne*. Pozwalają one na pobieranie wartości z wbudowanych zmiennych Samby lub innych informacji, które Samba pobiera w czasie jej działania.

Zmienne Samby:

%a Architektura klienta (Samba, WfWg, WinNT, Win95/98 lub UNKNOWN)

%f Użytkownik, który przysłał komunikat (tylko komunikaty)

%G Nazwa podstawowej grupy %U (żądanego konta użytkownika)

%g Nazwa podstawowej grupy %u (rzeczywistego konta użytkownika)

%H Katalog macierzysty %u (rzeczywistego konta użytkownika)

%h Nazwa hosta (internetowego) serwera Samby

%I Adres IP klienta

%L Nazwa NetBIOS-owa serwera Samby (wirtualne serwery mają wiele nazw)

%M Nazwa hosta (internetowego) klienta

Ćwiczenie: SAMBA

%m Nazwa NetBIOS-owa klienta
%n Nowe hasło (tylko zmiana hasła)
%o Stare hasło (tylko zmiana hasła)
%P Katalog główny bieżącego udziału (rzeczywisty)
%S Nazwa bieżącego udziału
%T Bieżąca data i czas
%t Komputer docelowy (tylko komunikaty)
%u Nazwa użytkownika bieżącego udziału
%U Żądana nazwa użytkownika bieżącego udziału
%v Wersja Samby

Demony

Samba używa zwykle dwóch demonów:

nmbd – demon usługi nazw NetBIOS, w poprawnie skonfigurowanym serwerze Samby działa co najmniej jeden proces *nmbd*, a jeżeli skonfigurowano Sambę do pracy jako serwer WINS, będzie utworzona dodatkowa kopia demona *nmbd*. Trzecia kopia tego demona może działać w przypadku, gdy Samba korzysta z systemu DNS do przekształcania nazw NetBIOS. Obsługuje poszukiwanie nazw NetBIOS, a także żądania WINS. Spełnia ważną rolę w przeglądaniu.

smbd – demon protokołu SMB, w poprawnie skonfigurowanym serwerze Samby działa co najmniej jeden demon tego typu. Dla każdego klienta podłączonego do serwera Samby działa oddzielny demon *smbd*. Obsługuje dostęp do plików oraz drukarek, a także żądania API programu LAN Manager takie jak NetServerEnum, NetShareEnum, NetUserGetInfo itp.

Demon *nmbd* zwykle uruchamia się w czasie startu systemu, ale dodatkowo można też go uruchomić na trzy inne sposoby:

- ręcznie
- na życzenie administratora systemu
- z pomocą demona *inetd*

Pozostałe komponenty

- smbclient – klient protokołu SMB – program ten umożliwia użytkownikom korzystanie z poziomu systemu UNIX z innych serwerów SMB, także takich działających w oparciu o jądro Windows NT.
- nmblookup – program poszukiwania nazw NMB – program ten umożliwia użytkownikom zapytać do serwerów o zarejestrowane nazwy NetBIOS.
- smbstatus – polecenie statusu protokołu SMB – administratorzy wykorzystują je do uzyskania informacji na temat, tego kto korzysta z Samby i z jakich udziałów.
- smbprint – skrypt powłoki do drukowania w systemach Windows z poziomu systemu UNIX.
- smbtar – skrypt powłoki wykonywania kopii archiwalnych w systemach Windows z poziomu systemu UNIX.

Uruchamianie i zatrzymywanie

Aby Samba pracowała poprawnie, w systemie muszą działać procesy smbd i nmbd. Istnieją trzy sposoby ich uruchomienia: ręcznie - wykorzystując skrypt powłoki, jako demony autonomiczne lub za pośrednictwem inetd.

Sposób ręczny polega na uruchomieniu skryptu powłoki:

```
/etc/init.d/samba parametr
```

z odpowiednim parametrem, tj.:

start – uruchamia demony Samby (smbd i nmbd), jeżeli nie zostały jeszcze uruchomione do tej pory

stop – zatrzymuje demony Samby

restart – ponownie uruchamia demony Samby. Jest to po prostu dwukrotne uruchomienie skryptu: najpierw zatrzymanie demonów, a następnie ponowne ich uruchomienie.

Sambę można także uruchamiać wraz ze startem systemu.

W Debianie plikiem używanym przez system do uruchomienia Samby w czasie startu systemu jest `/etc/rc2.d/S20samba` który odwołuje się do skryptu powłoki uruchamiającego demony smbd i nmbd (`/etc/init.d/samba`). Po zainstalowaniu Samby przy pomocy programu `apt samba` uruchamia się automatycznie wraz ze startem systemu.

Zarządzanie dostępem do Samby

Każdy użytkownik, który uzyskuje dostęp do zasobów na serwerze Samby z klienta Windows czy UNIX musi posiadać konto na serwerze Samby. Aby dodać konto dla klienta należy najpierw dodać go w systemie operacyjnym na którym znajduje się serwer Samby, korzystając z polecenia:

```
useradd nowy_użytkownik
```

Kolejno trzeba wprowadzić hasła dla danego użytkownika w serwerze Samby, przez co hasło w systemie operacyjnym nie ulegnie zmianie. To hasło nie ma też nic wspólnego z hasłem, jakie użytkownik o tej nazwie, może mieć na komputerze Windows. Użytkownik łącząc się z Sambą będzie musiał podać to hasło. Do tego trzeba użyć polecenia:

```
smbpasswd -a użytkownik
```

Uwaga!

Systemy Windows od Windows NT 4.0 SP3 w górę odmawiają pracy z serwerami nie obsługującymi szyfrowanych haseł. Toteż należy dodać do pliku konfiguracyjnego kolejne wpisy:

```
encrypt passwords = yes  
smb passwd file = /etc/samba/smbpasswd
```

Można także ustawić serwer tak, aby użytkownik nie musiał wprowadzać hasła (puste hasło), podając dodatkowy parametr polecenia smbpasswd.

```
smbpasswd -n -a użytkownik
```

Wskazówka:

Przy łączeniu się do serwera Samby dla ułatwienia można zrezygnować z przeszukiwania otoczenia sieciowego (może to powodować problemy). Zamiast tego wpisujemy po prostu adres do naszego serwera. Aby dostać się bezpośrednio do udziału należy podać adres (lub nazwę) serwera oraz nazwę udziału. Format nazw jest następujący:

```
\\nazwaLubAdresKomputera  
\\adresIpSerwera\nazwaUdziału  
\\nazwaNetbiosowaSerwera\nazwaUdziału  
\\nazwaDnsSerwera\nazwaUdziału  
\\nazwaLubAdres\nazwaUdziału\katalog
```

Udziały plikowe – udostępnianie

W celu udostępnienia plików należy stworzyć nowy udział – dodać odpowiednie wpisy w pliku konfiguracyjnym. Oto przykład:

```
[pliki]  
comment = Udział plikowy  
path = /home/Udostępnione/  
browsable = yes  
writeable = yes
```

Taka konfiguracja udziału umożliwi nam przeglądanie i zapis plików w katalogu /home/Udostępnione/

Może zaistnieć potrzeba ograniczenia w przeglądaniu niektórych plików i katalogów. Samba umożliwia oznaczanie plików jako niedostępne lub ukryte za pomocą odpowiednich parametrów. Są to parametry hidefiles i vetofiles.

Aby ograniczyć dostęp do udziału ze względu na nazwę stacji roboczej należy użyć parametrów hosts allow oraz hosts deny. Hosty definiuje się wg następujących reguł:

- jeśli wymieniamy wiele hostów, nazwy oddzielamy przecinkami albo spacjami
- hosta określamy przez nazwę lub przez jego adres IP
- zakresy adresów IP mogą być definiowane za pomocą formatu *sieć/maska sieci* lub za pomocą częściowego adresu IP
- słowo kluczowe ALL odpowiada wszystkim adresom IP
- aby wykluczyć adresy z zakresu, można użyć słowa kluczowego EXCEPT

Kolejna kwestia to parametry ograniczające dostęp na podstawie nazwy użytkownika: readlist, writelist, validusers, invalidusers.

Katalogi domowe użytkowników

Użytkownicy posiadający konto w systemie UNIX o tej samej nazwie co na serwerze Samby mogą korzystać z automatycznego udostępniania ich katalogów domowych. Katalogi domowe ustawia się w sekcji [homes] używając takich samych parametrów jak dla zwykłych udziałów plikowych. Wymagane parametry zostały opisane w części „Plik konfiguracyjny – parametry”.

Graficzne narzędzie konfiguracyjne

Sambę można także skonfigurować przy użyciu specjalnych narzędzi takich jak SWAT (Samba Web Administration Tool) zamiast edytować plik smb.conf i ponownie uruchamiać Sambę. Narzędzie to udostępniono wraz z pojawieniem się wersji 2.0.0. Jest to mini serwer WWW oraz aplikacja w postaci skryptu CGI zaprojektowana do pracy poprzez demona inetd. Umożliwia konfigurację wszystkich elementów Samby poprzez strony WWW.

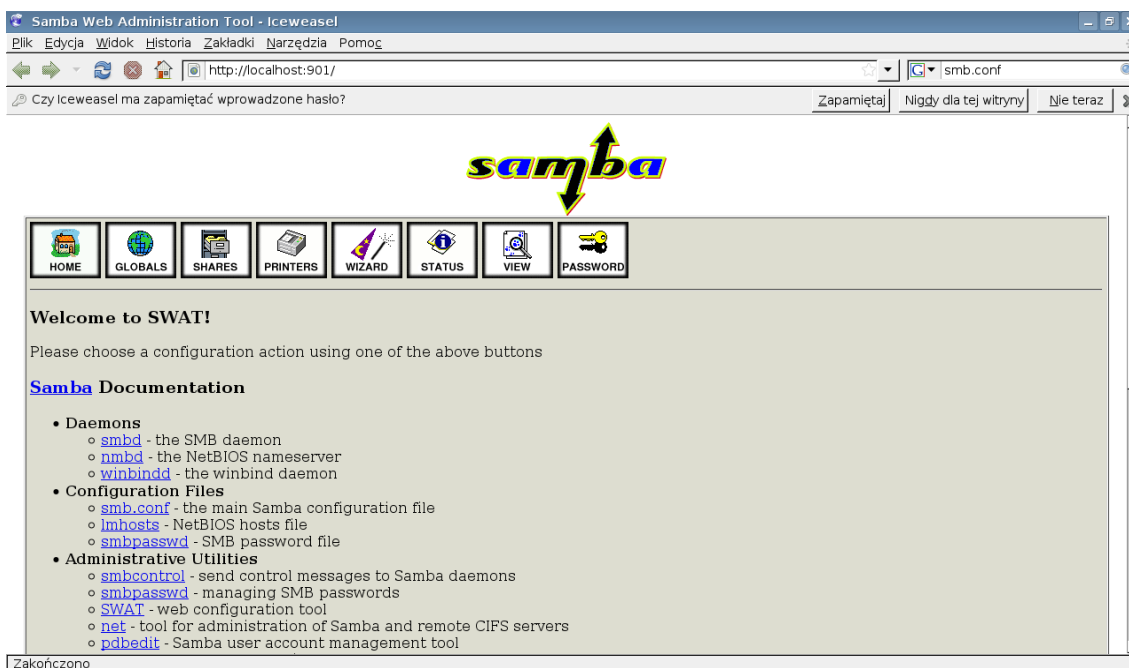
Dostęp do tej aplikacji uzyskujemy korzystając z przeglądarki internetowej pod adresem <http://localhost:901/> oraz zalogowaniu się jako użytkownik root. Po zalogowaniu pojawia się okno główne, jak pokazano na kolejnym rysunku.

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
- View – podgląd pliku smb.conf

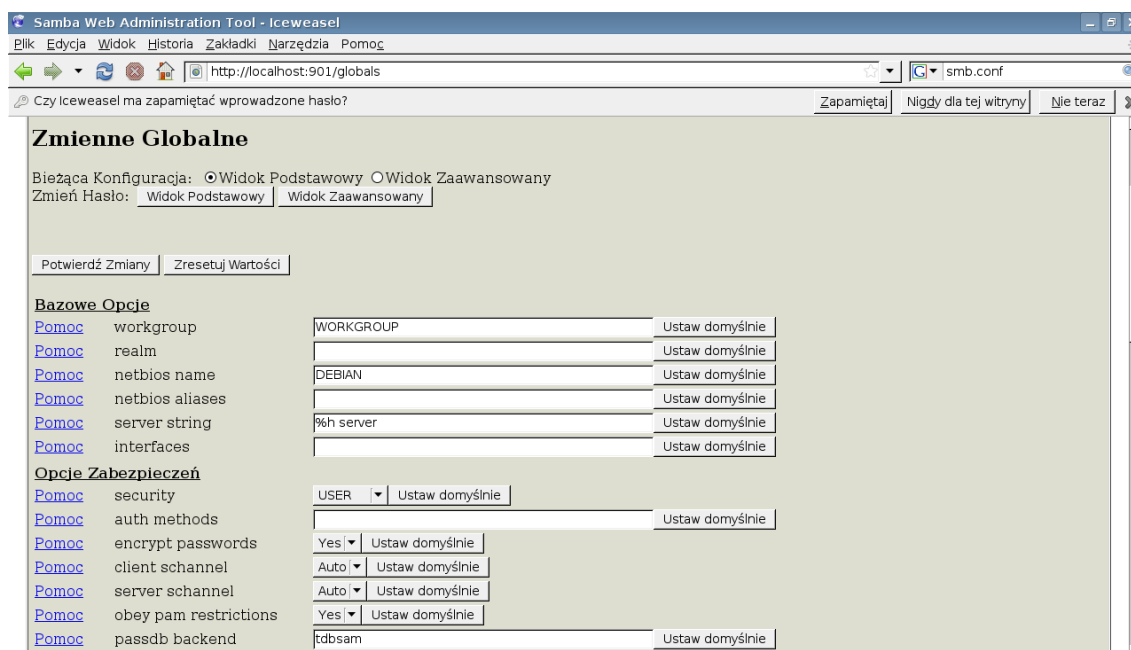
Ćwiczenie: SAMBA

- Password – zarządzanie hasłami serwera Samby, komputera zdalnego
- Wizard – kreator ustawień



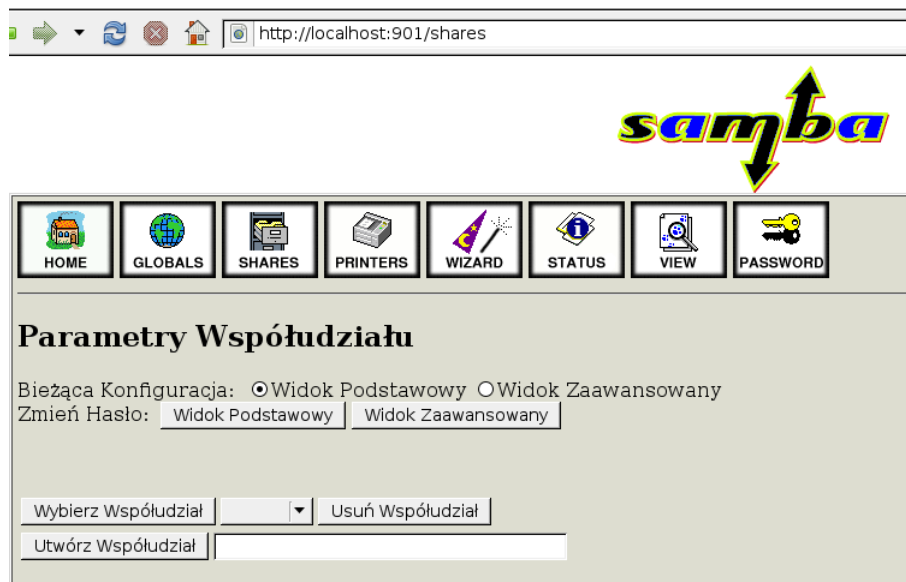
SWAT – zarządzanie sekcją [global]

W stronie głównej po wybraniu ikony GLOBALS, program SWAT przenosi nas na stronę WWW pozwalającą na modyfikację wielu najważniejszych parametrów globalnych Samby.



SWAT – zarządzanie udziałami plików

Po wybraniu ikony SHARES, wyświetli stronę WWW, która pozwoli na tworzenie nowych udziałów i modyfikowanie istniejących. Aby zmodyfikować dowolny z parametrów dla istniejącego udziału.



Należy wybrać ten udział z listy rozwijanej położonej obok przycisku „Utwórz Współudział”, a następnie kliknąć na ten przycisk. Pojawi się podstrona:

Na tej stronie można wykonać następujące operacje:

- Wybrać inny udział poprzez wybranie go z listy i kliknięcie przycisku „Wybierz Współudział”

- Utworzyć nowy udział poprzez wprowadzenie jego nazwy w odpowiednim polu i kliknięcie przycisku „Utwórz Współudział”
- Zmodyfikować parametry udziału (aby zmodyfikować parametry których nie ma na tej stronie, należy kliknąć przycisk „Widok Zaawansowany” i dokonać odpowiednich zmian)

Po wykonaniu zmian należy kliknąć przycisk „Potwierdź zmiany”. Zmiany są uwzględniane przez Sambę natychmiast.

Zarządzanie udziałami drukarek jest tożsame z zarządzaniem udziałami plików.

Narzędzie SWAT posiada także funkcjonalności takie jak monitorowanie statusu Samby, zarządzanie hasłami, kreator i podgląd pliku smb.conf. Ich obsługa jest stosunkowo intuicyjna.

Konfiguracja Samby jako głównego kontrolera domeny

Główny kontroler domeny (ang. Primary domain controller – PDC) jest zazwyczaj komputerem z systemem operacyjnym z serii Windows NT. Jest on skonfigurowany do pracy jako kontroler domeny i jest odpowiedzialny za zadania wewnątrz domeny. Czyli uwierzytelnianie logowania użytkowników i stacji roboczych będących członkami domeny oraz spełnianie roli centralnego punktu zarządzania informacjami o kontach użytkowników oraz grupach w domenie. Użytkownik zalogowany jako administrator domeny może dodawać, usuwać lub modyfikować informacje o kontach na dowolnym komputerze, który jest częścią domeny.

Aby Samba jako PDC mogła uwierzytelniać logowania użytkowników z komputerów, które są członkami domeny, trzeba ustawić parametr **domain logons** na wartość **true**, co pozwoli na włączenie obsługi logowania dla domeny Windows NT określonej parametrem **workgroup**.

Należy także dodać odpowiednie wpisy powodujące konfigurację serwera Samby jako lokalnego głównego serwera przeglądania domeny - zabieg ten ma na celu jedynie przyspieszenie pobierania list przeglądania dla domeny.

```
domain master = true
```

```
preferred master = true
```

```
local master = true
```

Samba jako serwer logowania

Serwer logowania umożliwia centralizację uwierzytelniania użytkowników oraz eliminuje obciążenie związane z utrzymywaniem kont użytkowników i haseł w każdej stacji roboczej. Można go używać także do przetwarzania skryptów logowania oraz przechowywania profili mobilnych. Serwer taki może także realizować odwzorowania dysków sieciowych oraz pamiętać ustawienia pulpitu każdego użytkownika.

Głównym zadaniem serwera logowania jest uwierzytelnianie użytkowników w sieci. Składa się z weryfikacji przynależności użytkownika do konkretnej domeny oraz sprawdzenia poprawności wprowadzonego przez użytkownika hasła sieciowego. Po zalogowaniu się na serwer logowania domeny klient wykorzystuje te same informacje uwierzytelniania – nazwę użytkownika i hasło. Wykorzystanie serwera logowania w sieci pozwala na pojedyncze logowanie do sieci, bez względu na

to, czy klient żąda dostępu do zasobów sieciowych na samym serwerze logowania czy też na innych serwerach w ramach tej samej domeny sieciowej. Klienci Windows NT wymagają, aby serwer logowania spełniał funkcje PDC – kontrolera domeny. Oznacza to że serwer Samby musi być skonfigurowany jako główny kontroler domeny.

Aby Samba obsługiwała logowanie do domeny, należy do sekcji [global] pliku konfiguracyjnego dodać następujący wpis:

```
domain logons = yes
```

Od tej pory serwer Samby będzie obsługiwał żądania logowania do domeny tożsamej z adresem rozgłoszeniowym grupy roboczej, której jest członkiem.

Kolejno należy dodać do domeny stację roboczą z której będziemy się logować i korzystać z zasobów jako członek domeny. Członkiem domeny może być: serwer Windows NT, stacja robocza Windows NT lub stacja robocza z systemem UNIX. Wykonuje się to w następujący sposób:

- dodać użytkownika UNIX z tą samą nazwą NetBIOS, co członek domeny ale zakończoną znakiem \$. Np.

```
useradd -c "konto" -d /dev/null -s /bin/false NazwaNetBIOS$
```

- dodać użytkownika do serwera Samby, tym razem bez użycia znaku \$.

```
smbpasswd -a -m NazwaNetBIOS
```

- dodać komputer do domeny po stronie klienta. W Windows XP: Właściwości systemu->Nazwa komputera->Zmień...

W polu Domena wprowadzić wartość parametru `workgroup` pliku konfiguracyjnego Samby

- uruchomić ponownie komputer klienta, aby zatwierdzić zmiany

Serwer logowania – skrypty logowania

Skrypty logowania to skrypty uruchamiane podczas logowania. Jest to bardzo ważna funkcja serwera logowania. Klient wykonuje je natychmiast po pomyślnym wykonaniu procedury logowania. Dla klientów Windows skrypty te składają się z plików sadowych. Typowe zastosowanie skryptów logowania:

- konfiguracja napędu sieciowego i połączeń z drukarką
- synchronizacja czasu komputera PC klienta z serwerem
- wyświetlanie ważnych informacji (np. informacji od administratora serwera)

Aby skrypty logowania mogły być wykonywane, serwer Samby oraz komputer-klient muszą posiadać skonfigurowaną obsługę logowania do domeny.

Należy udostępnić same skrypty logowania za pośrednictwem specjalnego udziału na serwerze Samby. Będzie to udział o nazwie [netlogon], a prawo do odczytu tego udziału powinni posiadać wszyscy użytkownicy. Udział należy skonfigurować jak na listingu:

```
[netlogon]
comment = udział Netlogon
path = /home/netlogon
writeable = no
guest ok = no
browseable = no
```

W sekcji [global] pliku konfiguracyjnego należy wprowadzić wpis:

```
logon script = logon.bat
```

Dzięki temu każdy użytkownik wykona skrypt logon.bat. Plik wsadowy powinien być umieszczony w odpowiednim miejscu w serwerze (w tym przykładzie /home/netlogon/logon.bat)

Udostępnianie drukarek w Sambie

Samba ma służyć w celu ułatwienia dostępu do drukarek zainstalowanych na serwerach UNIX. Jeśli drukarki pracują poprawnie w systemie UNIX, udostępnienie ich przez Sambę jest sprawą prostą. Do ich udostępniania służy sekcja [printers]. Sekcja ta definiuje specjalny udział pozwalający użytkownikom Windows na podłączenie dowolnej drukarki zainstalowanej na serwerze Samby. Domyślnie lista drukarek do wyeksportowania jest pobierana z pliku /etc/printcap. Do zmiany tej ścieżki służy parametr printcap name. Podstawową kwestią jest ustawienie w tym udziale parametru printable na yes. Należy także podać ścieżkę gdzie drukowane dane będą kolejgowane przed przekazaniem ich do komputera bezpośrednio zajmującego się drukowaniem jako wartość zmiennej path. Jeśli potrzebne są ustawienia dla każdej drukarki z osobna należy utworzyć osobny udział o nazwie drukarki zgodnej z tą z pliku printcap.

Styl drukowania określony jest wartością parametru printing. Styl drukowania określa w jaki sposób wykonywane są następujące działania: buforowanie zadań dla drukarki, usuwanie zadania z kolejki wydruku, wyświetlanie postępu, zatrzymanie i wznowianie zadań wydruku, zatrzymanie i wznowianie kolejki wydruku. Parametr ten w zależności od systemu UNIX może przyjąć jedną z następujących wartości:

- BSD dla komputerów z UNIX opartym na UNIX BSD
- SYSV dla komputerów z UNIX opartym na System V
- HPUX, QNX, AIX dla konkretnych odmian UNIX
- CUPS (Common UNIX Printing System) dla systemów UNIX

Automatyczna instalacja sterownika drukarki

W czasie instalowania drukarki udostępnionej przez serwer Windows NT instalacja sterownika może odbywać się przez sieć. Może to przy dużej ilości komputerów-klientów zaoszczędzić sporo czasu. Samba obsługuje automatyczną instalację sterownika drukarki dla klientów Windows. Do tego trzeba wykorzystać program **make_printerdef**. Wcześniej trzeba uzyskać nazwę pod jaką drukarka występuje w systemie Windows oraz pliki z komputera z systemem Windows, gdzie zainstalowano już tą drukarkę. Te pliki to **MSPRINT.INF** oraz **MSPRINTx.INF**, gdzie x jest liczbą zwykle od 2 do 4. Zazwyczaj pliki te znajdują się w katalogu C:\Windows\Inf. Potrzebujemy też listę plików generowaną przez program **make_printerdef**. Pliki te należy skopiować do udziału **PRINTER\$**. Należy także przenieść definicję drukarki którą generuje również program **make_printerdef**.

Aby wygenerować tę informację należy wywołać ten program w następujący sposób:

```
make_printerdef plik_inf nazwa_drukarki_w_Windows > /tmp/printers.def
```

gdzie plik_inf to jeden z plików: MSPRINT.INF, MSPRINTx.INF (możliwe że trzeba będzie wywołać program ponownie z innym plikiem w przypadku gdy program nie znajdzie w pliku informacji o drukarce). Nazwa drukarki musi także odpowiadać tej w plikach .INF. Jeśli nazwa drukarki posiada spację należy ująć ją w cudzysłów przekazując ją przy wywołaniu programu make_printerdef.

Wynik działania programu jest zapisywany do pliku /tmp/printers.def

Program wyświetli pliki potrzebne do zainstalowania drukarki. Pliki te można znaleźć w katalogu C:\Windows\System. Pliki należy skopiować do katalogu /usr/local/samba/lib/drivers gdzie ten katalog jest lokalizacją udziału PRINTER\$ (określoną parametrem path).

Plik wygenerowany przez program make_printers należy skopiować do katalogu:

```
/usr/local/samba/lib
```

Kolejno trzeba stworzyć udziału printer\$

```
[printer$]
comment = Sterowniki drukarki
path = /usr/local/samba/lib/drivers
public = yes
writeable = no
```

oraz dodać następujący wpis do sekcji global

```
printer driver file = path = /usr/local/samba/lib/printers.def
```

Na końcu musimy utworzyć udział drukarki, który będzie mógł być zainstalowany w komputerach-klientach. Wartość parametru printer driver musi dokładnie odpowiadać nazwie drukarki użytej w czasie wykonywania programu make_printerdef. Przykładowo:

```
[lj3]
comment = HP LaserJet III
```

```
browseable = yes
printable = yes
public = yes
printer driver = HP LaserJet III
```

3. Realizacja ćwiczenia

Narzędzia

Do realizacji ćwiczenia przygotowano system operacyjny Linux Debian 5.04 (wariant stable – lenny). Wykorzystywane środowisko graficzne to KDE w wersji 3.5.10. Użytkownik loguje się do systemu za pomocą konta

```
root
```

do którego hasło to:

```
samba
```

Do wirtualizacji użyto programu VirtualBox 3.2.0 firmy Oracle. Na maszynie wirtualnej zainstalowano system Windows XP wraz z przeglądarką Mozilla Firefox 3.6.3, który służy jako komputer klienta. Nazwa tego komputera to:

```
winxp
```

a dostęp do konta administratora na tym komputerze można uzyskać używając pustego hasła i konta **Administrator**. Na komputerze macierzystym (Debian) sieć skonfigurowana jest domyślnie, adres IP przydzielony zostaje przez dhcp.

Maszyna wirtualna (Windows XP) łączy się z komp. macierzystym poprzez NAT:

```
Ethernet adapter Local Area Connection:
```

```
IP Address . . . . . : 10.0.2.15
```

```
Subnet Mask . . . . . : 255.255.255.0
```

```
Default Gateway . . . . . : 10.0.2
```

Zadanie 1

Proszę zatrzymać Sambę, która uruchamia się automatycznie wraz ze startem systemu. Następnie sprawdzić czy, aby na pewno nie działa żaden z demonów Samby. Kolejno uruchomić Sambę i sprawdzić jej status. Ile demonów samby jest uruchomionych? Od czego może zależeć liczba ich kopii? W wykonaniu tego zadania należy się posłużyć poleceniami powłoki przedstawianymi w części 2.

Status Samby można sprawdzić korzystając także z poleceń powłoki takich jak: `testparm` (który także umożliwia podgląd pliku konfiguracyjnego `smb.conf`), `testprns` (sprawdza czy drukarki są rozpoznawane przez

Ćwiczenie: SAMBA

Sambę). Zaś polecenie `smbstatus` wyświetla komputery podłączone do udziałów Samby. Polecenie `nmblookup` służy do wyszukiwania nazw NetBIOS. Aby sprawdzić wyszukać uruchomione procesy `nmbd` oraz `smbd` można użyć polecenia: `ps -ax | grep mbd`.

Zadanie 2

Zadanie polega na podstawowej konfiguracji serwera Samby. Proszę usunąć całą zawartość pliku `smb.conf` następnie wprowadzić odpowiednie wpisy w następujących sekcjach tak aby:

Global

- nazwą grupy roboczej była „WORKINF-[INICJAŁY STUDENTÓW-4 litery]”
- nazwą NetBIOS była „ [Dowolne_Słowo]”
- opisem serwera było „Samba INF_[liczba w przedziale 1-6]”
- szyfrowanie haseł było aktywne
- ścieżka do pliku `smbpasswd` zawierającego szyfrowane hasła była następująca: „/etc/samba/smbpasswd”
- ustawić kontrolę dostępu na poziomie użytkownika
- pliki dzienników były przechowywane w katalogu `/var/log/samba/dzienniki/`

oraz aby każdy klient miał oddzielny plik dziennika z nazwą klienta w nazwie pliku (należy użyć zmiennej `%m`, czyli `../dzienniki/log.%m`)

Homes

- udział posiadał komentarz „Katalogi macierzyste”
- zabronić prawo do przeglądania zasobu
- umożliwić zapis w tym udziale

Printers

- umożliwić dostęp do zasobu tak aby mógł przyjmować polecenia wydruku

Następnie proszę stworzyć nowego użytkownika serwera Samby o nazwie **studentinf** i ustawić mu hasło (ewentualnie jedynie to drugie-można skorzystać z narzędzi graficznych). Kolejno proszę się zalogować do serwera z poziomu klienta – Windows XP.

Jakie udziały udostępnia serwer? Dlaczego udział Homes jest niewidoczny?

Zadanie 3.

W tym zadaniu proszę stworzyć udział plikowy o nazwie [Moje pliki]. Zablokować dostęp dla hostów spoza maszyny klienta (proszę sprawdzić czy jest możliwość połączenia z innego komputera w laboratorium). Umożliwić dostęp bez uwierzytelniania. Ustawić nazwę woluminu dla udziału na „Dysk sieciowy” a także dowolny komentarz dla udziału. Umożliwić użytkownikom zapis w udziale. Utworzyć dwa katalogi: `/tmp/Dane` , `/tmp/Dane/Katalog1`. Nadać im atrybuty za pomocą polecenia `chmod 777`. Określić ścieżkę do katalogu `/tmp/Dane`. Następnie połączyć się z serwerem przez maszynę wirtualną

Ćwiczenie: SAMBA

Windows XP. Wejść do katalogu /tmp/Dane/Katalog1 i utworzyć tam dowolny plik tekstowy. Sprawdzić z poziomu serwera czy pliki znajdują się na serwerze.

Zadanie 4.

Proszę skonfigurować Sambę jako serwer logowania. Utworzyć użytkownika w celu umożliwienia logowania się klienta (maszyna wirtualna – Windows XP). Sprawdzić poprawność logowania. Gdzie przechowywane są ustawienia pulpitu każdego użytkownika?

Zadanie 5.

Stworzyć skrypt logowania który uruchomi się po zalogowaniu do domeny który będzie wyświetlał opis „Witaj w domenie” następnie wykona mapowanie udziału jaki dysk Z oraz zsynchronizuje czas z serwerem.

Synchronizacji dokonuje się poleceniem:

```
NET TIME \\NazwaNetBIOSserwera /SET /YES
```

a mapowanie:

```
NET USE X: \\NazwaNetBIOSserwera\Udział
```

Logując się do domeny sprawdzić poprawność wykonania skryptu.

Zadanie 6 (opcjonalne)

Proszę skonfigurować udział drukarki oraz automatyczną instalację sterowników do tej drukarki dla klientów Windows. Uwaga: może być to drukarka wirtualna. Do testowania najlepiej skorzystać z komputera połączony do sieci lokalnej w której znajduje się serwer Samby.

4. Wnioski i zakończenie

Samba odnosi sukcesy z wielu powodów. Są to między innymi:

- Cena – użytkownicy nie muszą wносить opłat licencyjnych. Samba to niezwykle ekonomiczny sposób na udostępnianie usług serwera plików i drukarek dla dużej liczby komputerów.
- Otwarty dostęp do kodu źródłowego – Sambę może usprawniać każdy. Oznacza to, że w przypadku wykrycia błędów są one szybko usuwane.
- Dostępność dla wielu platform – Samba może działać na wielu platformach, począwszy od wszystkich rodzajów systemu UNIX (włącznie z systemem Linux) do BeOS, OpenVMS, a nawet MVS. Oznacza to że można zintegrować komputery PC z każdym niemal środowiskiem programowym.

Ćwiczenie: SAMBA

- Olbrzymia liczba funkcji – Samba w czasie pracy jako serwer plików i drukarek umożliwia tak łatwe wykonywanie przeróżnych zadań, że znajduje one zasłużone uznanie u administratorów systemów. Przykłady obejmują funkcje aliasów NetBIOS oraz serwerów wirtualnych, których implementacje znajdują się w Sambie. W łatwy sposób umożliwiają one połączenie kilku serwerów w jeden.
- Obsługuje szeroki zakres technologii - pozwala to na łatwą integrację PC z istniejącymi już środowiskami. Przykładem może być NIS oraz LDAP dla uwierzytelniania.

W sprawozdaniu należy przedstawić tok wykonywania ćwiczenia, własne wnioski i obserwacje a także jedno zadania związanego z Serwerem Samby lub samym protokołem SMB. Należy także wymienić słabe strony/błędy w instrukcji co pozwoli dopracować ją na przyszłość.

Literatura dodatkowa

- „Samba dla każdego : serwer plików i drukarek dla wielu systemów operacyjnych” Richard Sharpe, Tim Potter, Morris Jim
- „Sieci Linux. Receptury”, Carla Schroder
- „Linux Bible 2009 Edition”, Negus Christopher
- [Dokumentacja Samby: http://samba.org/samba/docs/](http://samba.org/samba/docs/)

Instrukcja opracowana przez:

Tomasz Osiniak
Mateusz Popek

Opieka merytoryczna:

dr inż. Piotr Andrzej Kowalski, dr inż. Szymon Łukasik, mgr inż. Sławomir Żak