

# SMB jako rozproszony system plików

## Prezentacja na SO

Sławomir Zatorski

21 stycznia 2003

# Spis treści

<b>1</b>	<b>Pakiet Samba</b>	<b>3</b>
<b>2</b>	<b>Implementacje Microsoftu</b>	<b>3</b>
<b>3</b>	<b>Dostęp do plików na innym komputerze</b>	<b>3</b>
<b>4</b>	<b>Różnice w systemach plików Windows i Unix</b>	<b>4</b>
4.1	Ukrywanie plików . . . . .	4
4.2	Dowiązania . . . . .	4
4.3	Prawa dostępu i atrybuty plików . . . . .	5
<b>5</b>	<b>Współbieżny dostęp do plików</b>	<b>5</b>
5.1	Blokady oportunistyczne . . . . .	5
5.2	Buforowanie . . . . .	5
<b>6</b>	<b>Uwierzytelnianie, kontrola dostępu</b>	<b>6</b>
6.1	Zabezpieczenia na poziomie udziału . . . . .	6
6.2	Zabezpieczenia na poziomie użytkownika . . . . .	6
6.3	Zabezpieczenia na poziomie serwera . . . . .	6
6.4	Zabezpieczenia na poziomie domeny . . . . .	6
<b>7</b>	<b>Odporność na awarie</b>	<b>6</b>

# 1 Pakiet Samba

Samba to pakiet narzędzi umożliwiających współdzielenie zasobów, takich jak drukarki i pliki, w sieci. Samba korzysta z protokołu Server Message Block (SMB), wspólnego produktu Microsoftu i IBM, w celu przesyłania danych między klientami Windows i serwerami uniksowymi w sieci TCP/IP.

Samba jest darmową implementacją tego protokołu dostępną na maszyny unixowe i nie tylko. Samba jest szczególnie atrakcyjna z następujących powodów:

- Używa tego samego protokołu, z którego standardowo korzystają systemy operacyjne IBM i Microsoftu, począwszy od DOS-a 3.0. Oznacza to, że rozumieją go niemal wszystkie komputery Windows i nie ma potrzeby instalowania w nich dodatkowego oprogramowania klienckiego.
- Działa na różnych platformach, w tym w większości odmian Uniksa.
- Jest bezpłatna.
- Administrowanie Sambą jest scentralizowane.

Prezentacja ta dotyczy używania protokołu SMB jako rozproszonego systemu plików. Samba oferuje ponadto :

- Współdzielenie drukarek.
- Wysyłanie wiadomości WinPopup do użytkowników.
- Usługi nazewnicze.

Opisywanie ich wykracza jednak poza temat prezentacji. Prezentacja ta będzie opierała się na Sambie jako podstawowej implementacji SMB. Wiele cech dotyczy jednak także innych implementacji. Czytając należy brać poprawkę na utożsamianie niektórych cech Samba z cechami protokołu SMB.

## 2 Implementacje Microsoftu

Implementacja SMB jest wbudowana we wszystkie Windowsy. Jest ich częścią. Dostęp do systemu plików znajdującego się na innym komputerze uzyskujemy poprzez kliknięcie na ikonę „Otoczenie Sieciowe”.

## 3 Dostęp do plików na innym komputerze

Do identyfikacji komputerów w SMB używa się nazw NetBios. Nazwa taka składa się maksymalnie z 15 liter. Każdy komputer w segmencie sieciowym jest identyfikowany poprzez unikatową nazwę. Korzystanie z nazw NetBios nie jest koniecznością do uzyskania dostępu do

zasobu.

Każdy komputer może udostępniać fragmenty swojego systemu plików. Fragmenty te nazywamy zasobami. Inny komputer może uzyskać dostęp do zasobu znając nazwę komputera udostępniającego oraz nazwę tego zasobu. W przypadku Windowsa uzyskujemy do niego dostęp poprzez wywołanie `\\<nazwa komputera>\<nazwa zasobu>`. Jest on widziany jako zwykły katalog systemu Windows. `<nazwa komputera>` może być nazwą NetBios, ale może być także jego nazwą DNS'owa czy choćby po prostu adresem IP. W implementacji unixowej Samby mamy do dyspozycji polecenie „`smbmount`”. Wymaga ono nazwy komputera, nazwy zasobu oraz punktu montowania. Działa podobnie do polecenia „`mount`”. Po zamontowaniu możemy korzystać z udostępnionych plików w sposób przezroczysty dla użytkownika traktując je jako lokalne.

Czasami do uzyskania zasobu lub dostępu do konkretnych plików stosuje się mechanizmy kontroli dostępu, o których mowa będzie w dalszej części.

Jak można zauważyć, SMB jako rozproszony system plików zapewnia przezroczystość dostępu oraz położenia. Nie pozwala on na zwielokrotnianie pliku. Przezroczystość zmiany położenia można uzyskać podobnie jak w NFS za pomocą edycji tablic montowania u każdego klienta.

## 4 Różnice w systemach plików Windows i Unix

### 4.1 Ukrywanie plików

Czasami chcemy ukryć plik przed użytkownikiem, kiedy ten przegląda zawartość katalogu. Nie chodzi tu o odebranie praw dostępu do pliku. W systemach Windows pliki mają atrybut, który pozwala na ich ukrycie podczas wyświetlania zawartości katalogu. W Uniksie tradycyjnie metodą ukrywania plików w katalogu jest nadanie im nazw zaczynających się od kropki (.). Dzięki temu podczas wykonywania zwykłego polecenia `ls` nie są wyświetlane pliki konfiguracyjne lub pliki z parametrami domyślnymi. Jeśli jednak chcemy w ogóle pozbawić użytkownika możliwości dostępu do pliku, musimy posługiwać się zezwoleniami plikowymi i katalogowymi.

Sposobem rozwiązania tego problemu w przypadku Samby jest ustawienie odpowiedniej opcji w jej pliku konfiguracyjnym. Samba zacznie wtedy automatycznie nadawać plikom z korpką na początku atrybut „ukryty”.

### 4.2 Dowiązania

W systemach plików DOS-a i Windows NT nie ma dowiązań symbolicznych. Systemy Windows 95/98/NT używają zamiast nich „skrótów”. Kiedy więc klient spróbuje otworzyć dowiązanie symboliczne w udziale serwera Samby, Samba podąża za dowiązaniem, aby znaleźć prawdziwy plik i umożliwić klientowi jego otworzenie, zupełnie tak, jakby użytkownik pracował na komputerze uniksowym. Można to wyłączyć ustawiając odpowiednią opcję w konfiguracji Samby.

### 4.3 Prawa dostępu i atrybuty plików

Dos nigdy nie miał być wielodostępowym, sieciowym systemem operacyjnym, natomiast Unix był zaprojektowany w ten sposób od samego początku. Jedną z największych różnic między Uniksem i Dosem jest obsługa praw dostępu do plików. Wszystkie pliki Uniksa mają zezwolenia na odczyt, zapis i wykonywanie dla trzech kategorii użytkowników: właściciela, grupy i „reszty świata”. DOS/Windows (Windows z serii NT ma atrybuty jak unix) używa dla pliku atrybutów : Archiwalny, Systemowy, Ukryty, Tylko do odczytu. System plików DOS-a i Windows identyfikują pliki wykonywalne na podstawie rozszerzeń .exe, .com, .cmd, .bat.

Z tego wynika, że trzy uniksowe bity wykonywalności nie mają żadnego zastosowania w odniesieniu do pliku przechowywanego w udziale dyskowym Samby. Samba może przechować atrybuty Archiwalny, Systemowy i Ukryty wykorzystując bity wykonywalności pliku uniksowego - jeśli się od niej zażąda. Odwzorowanie bitów wiąże się jednak z niepożądanym efektem ubocznym - Unix może źle interpretować niektóre bity wykonywalności plików pochodzących od Windows.

## 5 Współbieżny dostęp do plików

Samba obsługuje standardowe żądania blokady DOS-a i systemu plików NT, które pozwalają na pisanie w całym pliku tylko jendemu procesowi w danej chwili. Samba nakłada także blokady zakresów bajtów. Ponadto Samba obsługuje nowy mechanizm blokowania, w terminologii Windows NT nazywany „blokadą oportunistyczną.

### 5.1 Blokada oportunistyczne

Dzięki tym blokadom klient może poinformować serwer Samby, że nie tylko będzie jedynym uprawnionym do pisania w pliku, ale że będzie buforował wszystkie zmiany lokalnie w celu przyspieszenia dostępu do pliku. Kiedy Samba wie, że plik został zablokowany oportunistycznie przez klienta, zaznacza swoją wersję tego pliku jako obłożoną blokadą i czeka, aż klient zakończy operacje na pliku i odeśle jego ostateczną wersję w celu wzajemnej synchronizacji.

Jeśli inny klient zażąda dostępu do tego pliku, zanim pierwszy klient zakończy pracę, Samba może wysłać żądanie „przerwania blokady” do pierwszego klienta. Jest to informacja dla klienta, że powinien zaprzestać lokalnego buforowania i zwrócić informacje o bieżącym stanie pliku, aby nowy klient mógł użyć go wedle swego uznania.

### 5.2 Buforowanie

Dostęp do pliku nie jest buforowany za wyjątkiem przypadku założenia blokady oportunistycznej. Starsze wersje Uniksa nie obsługiwały tego mechanizmu. Korzystać mogą one jedynie z trybu odmowy. Samba może nie dopuszczać do zakładania blokad oportunistycznych w celu zgodności ze starszymi uniksami. Niekiedy trzeba ponieść koszt nieefektywnego zapisu do plików z jakiegoś zasobu dla zapewnienia zgodności ze starszymi uniksami korzystającymi z niego.

## **6 Uwierzytelnianie, kontrola dostępu**

Dostęp do zasobów może być swobodny. Jednak czasami zachodzi potrzeba ograniczania go dla wybranych użytkowników. Mamy do dyspozycji następujące sposoby uwierzytelniania użytkownika:

### **6.1 Zabezpieczenia na poziomie udziału**

Każdy udział w grupie roboczej jest chroniony oddzielnym hasłem. Każdy, kto zna hasło dostępu do udziału, może z tego udziału korzystać.

### **6.2 Zabezpieczenia na poziomie użytkownika**

Każdy udział w grupie roboczej jest skonfigurowany tak, aby pozwalał na dostęp tylko określonym użytkownikom. Po wstępnym nawiązaniu połączenia z zasobem, serwer Samby weryfikuje użytkowników i ich hasła, zanim przyzna im dostęp do udziału.

### **6.3 Zabezpieczenia na poziomie serwera**

Podobne do zabezpieczeń na poziomie użytkownika, ale Samba używa oddzielnego serwera SMB, który zatwierdza użytkowników i ich hasła przed przyznaniem dostępu do udziału.

### **6.4 Zabezpieczenia na poziomie domeny**

Samba staje się członkiem domeny Windows i uwierzytelnia klientów za pośrednictwem podstawowego kontrolera domeny (PDC). Po uwierzytelnieniu użytkownik otrzymuje specjalny żeton, który umożliwia mu korzystanie ze wszystkich udziałów, do których ma odpowiednie uprawnienia. Dzięki temu żetonowi, PDC nie będzie musiał ponownie weryfikować hasła użytkownika za każdym razem, kiedy ten spróbuje połączyć się z innym udziałem w domenie.

## **7 Odporność na awarie**

Protokół SMB używa prawie wyłącznie TCP. Dzięki temu jest odporny na chwilowe niedyspozycje sieci - dba o to TCP. System plików oparty na SMB jest stanowy. Między klientem a serwerem jest ustanawiana sesja. Awaria serwera powoduje utratę dostępu do danych.