



Usługi udostępniania plików i drukarek w sieci LAN

Oprogramowanie Samba

Cechy Samby

- *Samba* jest serwerem plików i drukarek, który zawiera implementację *protokołu SMB (Server Message Block)*.
- *Samba* realizuje cztery podstawowe rodzaje usług:
 1. Udostępnianie plików i drukarek,
 2. Uwierzytelnianie i Autoryzacja (w systemie Linux istnieją moduły PAM współpracujące s *Sambą*),
 3. Rozwiązywanie nazw w sieci lokalnej,
 4. Rozgłaszanie i lokalizacja usług (*browsing*).
- Strona domowa projektu, to: www.samba.org

Historia Samby

- Pierwsza implementacja to prosty programik, który umożliwiał dostęp z komputera *PC* z systemem *PATCHWORKS* firmy *Digital Equipment Corporation* dla *DOS* do plików znajdujących się na komputerze *Sun* (serwer dla systemu *SunOS*, który obsługiwał pakiety przesyłane przez klienta *PATCHWORKS*).
- Była to implementacja protokołów *NetBIOS* nad *TCP/IP* oraz *SMB* (RFC1001, RFC1002).
- Pierwsza nazwa, *SMB Server*, była jednak zastrzeżona. Stąd jej twórca Adrew Tridgell znalazł słowo *Samba*, jako najprostsze zawierające litery *s*, *m* oraz *b*.

Historia wersji

- 1991 r. – początki pracy nad oprogramowaniem,
- 1992 r. – wersja 1.0: a *Unix file server for Dos Pathworks*,
- 1993 r. – wersja 1.5 pod nazwą *Samba* współpracuje z *Windows LAN Manager*,
- 1999 r. – wersja 2.0; implementacja protokołów uwierzytelniania w *Domenie NT* (testy pokazują iż jest prawie 2 krotnie szybsza od Windows NT4,
- 2003 r. – wersja 3.0 umożliwia podłączanie klienta *Samby* do *Microsoft Active Directory*.
- 2006 r. – pierwsze wersje *Samby 4* mającej pracować jako kontroler domeny AD – wciąż nie ma wersji produkcyjnej.
- 2009 r. – wersja 3.4 zawiera kod źródłowy *Samby v3* i *v4*

Źródła popularności Samby

- Jest darmowa.
- Stanowi pakiet z otwartym dostępem do kodu źródłowego.
- Jest dostępna dla wielu platform: od UNIX, Linux po niszowe BeOS, OpenVMS. Może zatem integrować komputery PC z niemal każdym środowiskiem.
- Protokół *SMB/CIFS* leży u podstaw sieci Microsoft Windows, stąd Samba może zostać niskonakładowym i wysoko wydajnym substytutem serwera Windows.
- Posiada olbrzymią liczbę funkcji. Przykładowo *aliasy NetBIOS* czy serwery wirtualne.
- Pozwala na wykorzystywanie i integrację z innymi standardami (*NIS, LDAP*).

Instalacja z kodu źródłowego

- Kod źródłowy w skompresowanych archiwach, np. *samba-3.5.1.tar.gz*
- Kolejne kroki:

```
[root@dns1 ~]# tar -xzf samba-3.5.1.tar.gz
[root@dns1 ~]# cd samba-3.5.1/source3
[root@dns1 source3]# ./autogen.sh
[root@dns1 source3]# ./configure
[root@dns1 source3]# ./make
[root@dns1 source3]# ./make install
```

- Skrypt *autogen.sh* korzysta z programu narzędziowego *Autoconf*.

Instalacja apt-get install

- Samba
 - Serwer
 - apt-get install samba
 - Klient
 - apt-get install smbclient

Protokół SMB

- Protokół *SMB Server Message Block* stworzony został przez *IBM* w celu dostępu do systemu *DOS* z wykorzystaniem protokołu *NetBIOS*.
- Aktualnie umożliwia udostępnianie plików i drukarek z wykorzystaniem różnych protokołów niższych warstw.
- *SMB* pracuje w warstwie aplikacji modelu *ISO-OSI*.
- Protokół *SMB* może wykorzystywać z niższych warstw następujące protokoły:
 - *NetBIOS*, który posiada implementacje na wielu protokołach niższych warstw,
 - *TCP (port 445)* – co pozwala na integrację z nazwami *FQDN*.
- Jest to jeden z najbardziej zmieniających się i rozszerzanych protokołów w historii.

Historia zmian protokołu SMB

- 1987 r. – Microsoft łączy go z *LAN Manager*,
- 1992 r. – Microsoft dodaje elementy by współpracował w środowisku *Windows for Workgroups*,
- 1996 r. – dodana jest obsługa protokołu *NTLM* dla Windows NT 4.0 i zmieniona nazwa na *Common Internet File System (CIFS)*,
- 2000 r. – Microsoft wprowadza *Direct hosting of SMB over TCP/IP*, co uniezależnia go od protokołu *NetBIOS* i umożliwia standaryzację nazw w oparciu o *DNS*,
- 2007 r. – Microsoft wprowadza wersję 2.0 *SMB*, która przede wszystkim go upraszcza – usuwając nieużywane komendy (z ponad 100 zostaje 19) oraz wprowadza wiele innych zmian.

Samba w modelu ISO-OSI

Aplikacji	SMB				Aplikacji
Prezentacji					
Sesji	NetBIOS	NetBEUI	NetBIOS	NetBIOS	TCP & UDP
Transportowa	IPX		DECnet	TCP & UDP	
Sieci		IP		IP	
Łącza	802.2 802.3 802.5	802.2 802.3 802.5	Ethernet V2	Ethernet V2	Ethernet
Fizyczna	Fizyczna	Fizyczna	Fizyczna	Fizyczna	Fizyczna

Obsługa nazw w NetBIOS

- Usługa nazw *NetBIOS* – *NetBIOS Naming Service* (*NBNS*) jest wykorzystywana do zarządzania nazwami *NetBIOS* w taki sposób, aby dostęp do serwerów mógł odbywać się w warstwie IP.
- Samba obsługuje usługę *NBNS*.
- *WINS* – implementacja Microsoft serwera usługi *NBNS*.
- Klasy nazw *NetBIOS* to:
 - *Nazwy unikatowe* – możliwość przypisania nazwie jednego adresu IP.
 - *Nazwy grupowe* – nazwa może mieć wiele adresów IP.
 - *Grupy Internetu* – WindowsNT i zarządzanie domenami.
 - *O wielu połączeniach* – nazwy unikatowe systemów z wieloma interfejsami.
 - *Domeny* – skojarzone z domenami Windows NT.

Cechy nazw NetBIOS

- Nazwy składają się z 16 znaków: 15 to nazwa, a ostatni określa typ nazwy.
Np. stacja robocza, kontroler domeny, główna przeglądarka, itp.
- Są zawsze uzupełniane spacjami do 15 znaków.
- W przypadku przesyłania nazw do innych systemów nazwy *NetBIOS* są przekształcane na duże litery.
- Mogą zawierać dowolne znaki za wyjątkiem:
 - Znaków o kodach niższych niż kod spacji (0x20) tj. znaków sterujących.
 - Znaków: .” / \ [] : | < > + = ; ,

Budowa pakietu SMB

- Pakiet *SMB* to blok danych przesyłany w połączeniu TCP.
- Składa się z nagłówka i opcjonalnie skojarzonych z nim danych.



Pola nagłówka pakietu SMB

- *0xFFSMB* – znacznik początku pakietu.
- *Polecenie* – jednobajtowe pole określające typ przesyłanego pakietu.
- *Klasa błędu* – pole jednobajtowe wskazujące klasę błędu odpowiedzi.
- *Kod błędu* – pole dwubajtowe wskazujące na typ błędu odpowiedzi.
- *Flagi* – 8 bitów, z których najstarszy wskazuje na to czy pakiet jest zapytaniem czy odpowiedzią. Pozostałe oznaczają funkcje obsługiwane przez klienta i serwer.
- *Flagi 2* – 16 bitów oznaczające pozostałe funkcje.

Pola nagłówka pakietu SMB

- *Pole zarezerwowane* – 12 bajtów.
- *Identyfikator drzewa* – pole dwubajtowe oznaczające drzewo na serwerze, do którego odnosi się polecenie lub odpowiedź.
- *Identyfikator procesu* – 16 bajtów oznaczających klienta.
- *Identyfikator użytkownika* – 16 bajtów zawierających zweryfikowany (po konfiguracji sesji i uwierzytelnieniu) identyfikator użytkownika. Pole generuje serwer.
- *MultiplexIS* – 16 bitów używane przez klienta kiedy przesyła wiele pakietów. Wykorzystywane do kojarzenia odpowiedzi z żądaniami.

Zmienna część pakietu SMB

- Jest zdeterminowana przez polecenie zawarte w nagłówku.
- Może zawierać nazwy użytkowników, hasła lub nazwy plików do których żąda się dostępu.
- Istnieje 78 zdefiniowanych poleceń protokołu *SMB*.
- W celu zredukowania transmisji istnieje możliwość wysyłania wielu żądań w pojedynczym pakiecie.

Żądania wielokrotne

- Umożliwiają pakiety *SMB andX*.
- Możliwość ta dotyczy tylko niektórych żądań.
- Są czymś w stylu łączonych list (ang. *linked list*).
- W implementacjach stosuje się do 2 żądań.

Nagłówek stały 33 bajty	Nagłówek 1-go polecenia	Dane 1-go polecenia	Nagłówek 2-go polecenia	Dane 2-go polecenia
----------------------------	----------------------------	------------------------	----------------------------	------------------------

Nawiązanie sesji SMB po TCP

1. Przed połączeniem z serwerem klient wysyła zapytanie o nazwę *NetBIOS*.
2. Po tym jak klient otrzyma nazwę i skojarzony z nią adres IP serwera, ustanawiane jest połączenie TCP.
3. Klient rozpoczyna sesję *NetBIOS*. Istotne pola w komunikacie żądania sesji *NetBIOS* to:
 - *Nazwa wywoływana* – nazwa jednostki *NetBIOS*, do której kierowane jest żądanie.
 - *Nazwa wywołująca* – nazwa jednostki *NetBIOS* wysyłającej żądanie.
4. Po ustanowieniu sesji klient i serwer mogą wymieniać pakiety *SMB* – klient wysyła żądania dostępu do zasobów, a serwer na nie odpowiada.

Negocjacja wariantu protokołu SMB

5. Kolejną czynnością wykonywaną przez klienta jest wynegocjowanie wariantu protokołu.
 - Wynika ona z faktu, iż protokół *SMB* dopuszcza istnienie wariantów.
 - Do przykładowych wariantów należą:
 - *PC Network Protocol* – oryginalny opracowany przez IBM.
 - *LANMAN 1.0* – *LAN Manager* opracowany przez Microsoft.
 - *NT LM 0.12* – wariant dla Windows NT.

Uwierzytelnienie klienta

6. Kolejną czynnością wykonywaną przez klienta jest uwierzytelnienie lub zalogowanie się do serwera.
 - Klient wysyła pakiet *SMB* żądania konfiguracji sesji, który zawiera m.in. nazwę i hasło użytkownika.
 - Uwierzytelnianie może być na poziomie udziału – użytkownik uwierzytelnia się oddzielnie do każdego udziału, lub na poziomie użytkownika – uwierzytelnia się raz i dostaje odpowiedni dostęp do usług.
 - Hasło może być wysyłane w postaci jawnej lub zaszyfrowanej.
7. Po uwierzytelnieniu zakończonym sukcesem klient może rozpocząć korzystanie z zasobów serwera.

Dodatkowe funkcje protokołu SMB

- Prosty protokół *SMB* rozszerzyła firma Microsoft. Wszystkie zaawansowane funkcje sieci Microsoft Windows zaimplementowano za pomocą żądań. Obejmują one m.in.:
 - *Protokół przeglądania*, który korzysta ze szczelin pocztowych – jednokierunkowy transfer danych.
 - *Protokół LMRAP (Lan Manager Remote Administration Protocol)* – umożliwiający przesyłanie żądań API w sposób podobny do Remote Procedure Call (RPC).
 - *Protokół MS RPC* – pakiety RPC są pakowane jako żądania SMB *write* lub *writeX* i przesyłane między klientem a serwerem.
- W Sambie zostały one zaimplementowane. Stąd istnieje np. możliwość pracy jako kontroler domeny Windows NT.

Obsługa błędów w protokole SMB

- W protokole zaimplementowano strukturalne podejście do obsługi błędów.
- Każda odpowiedź posiada pole błędu z wartością równą zero w przypadku sukcesu.
- Kiedy serwer nie może obsłużyć klienta, zwraca w wyniku błąd, należący do jednej z czterech klas:
 1. *ERRDOS* – błędy w stylu DOS, np. nie znaleziono pliku.
 2. *ERRSRV* – błędy serwera, np. niepoprawne hasło.
 3. *ERRHRD* – błędy sprzętowe, np. błąd zapisu.
 4. *NT ERRORS* – błędy systemu NT.
- Klient jest odpowiedzialny za przekształcenie błędu na komunikat dla użytkownika.

Struktura Samby

