Samba – informacje ogólne

Położenie: (nie dotyczy)

Informacje ogólne

Samba jest odpowiednikiem windowsowego „*Otoczenia sieciowego*” (Andrew Tridgell, 1991) i korzysta z implementacji protokołu **SMB** (*Server Message Block*) i jego rozszerzenia **CIFS** (*Common Internet File System*; port UDP/TCP 445) zasadzonego na protokołach TCP/IP (więc TCP/IP musi być aktywny!). W jądrze musi być aktywna opcja:

File Systems --->

[*] Network File Systems --->

[*] CIFS support (oraz podopcje)

Serwisy:

- **smbd** – udostępnia pliki, foldery i drukarki (otwarty port TCP 139 oraz 445), odpowiada także za weryfikację użytkownika;
- **nmbd** (*NetBIOS Name*) - wiąże nazwy *NetBIOS* z adresami IP (otwarty port UDP 137), transportuje dane (*NetBIOS Datagram*; otwarty port UDP 138; odpowiada za „*Master Browser*”) oraz tworzy sesje (*NetBIOS Session*; otwarty port TCP 139; *NetBIOS over TCP/IP*);
- **winbind** – pobiera nazwy użytkowników z Windows i odwzorowuje je na linuksowe numery ID.

Wersje protokołów:

- **SMB1** - zwane także NT1, 16-bitowe rozwiązanie zaprojektowane przez Barry Feigenbaum (IBM w 1983, bez zabezpieczeń). Wdrożony do systemu Windows (1990-1992) i obsługiwany przez aplikację *NetBIOS* (osadzona na *NetBEUI* oraz *Novell IPX/SPX*); porty biorące udział w komunikacji: TCP/UDP **137** (*NetBIOS name*), UDP **138** (*NetBIOS datagram*), TCP **139** (*NetBIOS session*). Aby aktywować tę wersję protokołu, należy w pliku konfiguracyjnym zdefiniować dwie opcje: „*disable netbios = no*”, „*smb ports = 139*”. Od wersji *Windows 2000* (już w 1996) wprowadzono „*NetBIOS over TCP/IP*” (Microsoft zaproponował wtedy zmianę nazwy na CIFS - *Common Internet File System*), który miał działać na porcie **445** bez konieczności korzystania z portu 139. Aby uaktywnić wersję CIFS, należy w pliku konfiguracyjnym zdefiniować: „*disable netbios = yes*”, „*smb ports = 445*”. W przypadku, gdy chcemy aktywować obie wersje protokołu: „*disable netbios = no*”, „*smb ports = 139 445*” (w tym przypadku priorytet dostaje komunikacja na porcie 445).
- **SMB2** - 32-bitowa wersja wprowadzona w 2006, funkcjonuje w systemie *Windows Vista / Windows 7, Windows Server 2008.* Linux obsługuje ten protokół od wersji Samba 3.6.
- **SMB3** - funkcjonuje w *Windows 8 / Windows Server 2012*. Dodana została m.in. funkcja „*SMB Direct*”.
- **SMB3.1.1** - wprowadzony w *Windows 10 / Windows Server 2016*, szyfrowanie AES-128.

Uwaga: W ramach danej wersji protokołu SMB, istnieją także „podwersje”.

Regułki do iptables będą mieć następującą postać:

 # iptables -I INPUT -s 192.168.0.0/24 -p udp --dport 137 -j ACCEPT
 # iptables -I INPUT -s 192.168.0.0/24 -p tcp --dport 137 -j ACCEPT
 # iptables -I INPUT -s 192.168.0.0/24 -p udp --dport 138 -j ACCEPT
 # iptables -I INPUT -s 192.168.0.0/24 -p tcp --dport 139 -j ACCEPT

 # iptables -I INPUT -s 192.168.0.0/24 -p udp --dport 445 -j ACCEPT
 # iptables -I INPUT -s 192.168.0.0/24 -p tcp --dport 445 -j ACCEPT

Operacje na serwerze

Serwer *standalone* nie jest członkiem domeny, w zasadzie jest stacją roboczą pełniącą w pewnym sensie rolę serwera (struktura sieci oparta o grupę roboczą, a nie o domenę).

- Zalogować się jako root.
- Skopiować plik konfiguracyjny smb.conf. Muszą w nim być aktywne następujące opcje:
  - *security = user*
  - *domain master = yes*
  - *domain logons = yes*
  - *domain admin group = @root*
- **/etc/init.d/samba start** (w Fedorze będzie to: **/sbin/service smb start**)
- Tworzymy katalog na hasła Samby: **mkdir /etc/samba/private && chmod 700 /etc/samba/private**
- Tworzymy plik z hasłami Samby (tylko na serwerze): **touch /etc/samba/private/smbpasswd**
- Dodajemy maszynę (konta komputerów zaufania w Windows NT/2000 są po to, aby jakiś obcy komputer nie podszył się pod nazwę istniejącego w domenie hosta i nie autoryzował się w domenie): **/usr/sbin/useradd -g 100 -d /dev/null -c raven -s /bin/false raven$**
- **passwd -l raven$**
- **smbpasswd -a -m raven** (w obecnej wersji Samby jest **tdbsam**)
- Ustawiamy możliwość montowania udziałów (nie ustawiać suid na smbmount): **chmod 4755 /usr/sbin/smbmnt /usr/bin/smbumount**
- **/etc/init.d/samba reload**
- **smbpasswd -a użytkownik**
- Sprawdzamy konfigurację: **testparm /etc/samba/smb.conf**
- **/etc/init.d/samba reload**

Następnie wyłączamy protokół IPv6 (kliknij prawym przyciskiem myszy w ikonkę sieci obok zegara, zakładka *IPv6: Ignored*). Wyłączamy go także w systemie *Windows* (*Centrum sieci i udostępniania / Ethernet / Właściwości*).

Na **klientach windowsowych**, włączamy logowanie gości:

Uruchom: **gpedit.msc**

Konfiguracja komputera / Szablony administracyjne / Sieć / Stacja robocza LANman:

Włącz niezabezpieczone logowanie gościa: Włączone

Uwaga: Jest to równoważne włączeniu *Local Master Browser* (który umożliwia właśnie dostęp dla gości).

W systemie Windows należy także **wyłączyć** protokół SMB1 (jeśli jest włączony):

Panel sterowania: Duże ikony / Programy i funkcje / Włącz lub wyłącz funkcje systemu Windows /

- *Obsługa udostępniania plików SMB 1.0/CIFS* → Wyłącz*;*
- *SMB Direct* → Włącz.

Proste udostępnianie plików

Od wersji *Samba 4*, wartość „*security=share*” została wycofana. Jeśli jednak chcemy po prostu udostępnić jakieś pliki publicznie dla wszystkich (bez podawania hasła), należy umieścić w pliku konfiguracyjnym następujące wpisy:

[global]

server role = standalone server

netbios name = nazwaTwojegoKomputera *(np. linux14, nie więcej niż 15 znaków, bez odstępów)*

server string = Serwer plikow

workgroup = nazwaTwojejGrupyRoboczej

security = USER

map to guest = Bad User (co ma zrobić Samba, jeśli do udziału chce wejść użytkownik, który nie istnieje w systemie Linux („*Bad User*”); Samba mapuje takiego użytkownika do gościa i umożliwia dostęp do zasobów bez podawania loginu i hasła; wartość „*Bad Password*” powoduje, że po podaniu złego hasła przez istniejącego w Linuksie użytkownika, jest on mapowany do gościa, ale nie jest o tym informowany; wartość „*Bad Ids*” stosowana w domenach, gdy użytkownik jest utworzony w domenie, ale nie ma swojego konta w Linuksie – wtedy jest mapowany do gościa)

usershare allow guests = Yes (robi to samo co “guest ok”, ale domyślnie dla wszystkich zasobów)

disable netbios = Yes (wartość “no” uaktywnia SMB1)

protocol = SMB3 *(Windows 10 obsługuje tylko tę wersję protokołu, Windows 8 obsługuje SMB2)*

[publiczny]

comment = Folder do uzytku publicznego

path = /home/nazwaUżytkownika/udostępnianyFolder

browseable = Yes *(dopuszczalne jest także “browsable” jako synonim)*

guest ok = Yes *(czy do tego konkretnego udziału mają dostęp goście, bez podawania hasła; synonimem jest “public=yes”; można ustawić nazwę gościa za pomocą parametru “guest account=nazwa” → musi być takie konto w systemie Linux; dodatkowo można ustawić “guest only=yes” gdy chcemy, aby dostęp do konta był tylko anonimowy, tylko dla gości)*

read only = Yes

hosts allow = all

create mask = 0755

directory mask = 0777

Zmiany w 2020

Windows 10 od wersji 1511 nie używa już domyślnie protokołu *SMBv1* ze względu bezpieczeństwa a od wersji 1709 nie pozwala na instalację *SMBv1* (a tym samym **nie używa już** *Przeglądarki Komputerów* vel *Otoczenie sieciowe [Network Neighborhood]* vel *NetBIOS*). Do wykrywania zasobów sieciowych używa protokołu *Web Services Dynamic Discovery* zwany *WS-Discovery* (wykrywanie *SMBv2/SMBv3*) korzystającego z *Pythona*. Linux ma implementację tego protokołu pod nazwą **WSD** *vel* **wsdd** (*Web Service Discovery host Daemon*), ale nie dotyczy to każdej dystrybucji.

Istnieją dwie możliwości przeglądania zasobów linuksowych na *Windows*:

1. Połączenie się z zasobem linuksowym przez numer IP (np. *\\192.168.6.**), po czym zmapowanie udostępnionego folderu do wirtualnego dysku (prawy przycisk myszy). Od tej pory zasób będzie dostępny jako dysk.

2. Instalacja na Linuksie WSDD (nie każda dystrybucja ma ten pakiet) przy jednoczesnej rezygnacji z SMB1. Poniżej wersja dla *Gentoo*:

https://github.com/christgau/wsdd-gentoo/blob/master/net-misc/wsdd/ (aby skompilować i zainstalować pakiet spoza *Portage*, należy zapoznać się z dokumentem „*Emerge*”).

Po instalacji:

\# **/etc/init.d/wsdd start**

rc-update add wsdd default

W systemie *Windows* usługi realizujące *WS-Discovery* to:

- *Functions Discovery Provider Host* (Host dostawcy odnajdywania funkcji);
- *Function Discovery Resource Publication* (Publikacja zasobów odnajdywania sieci);

WS-Discovery potrzebuje otwartych portów: 3702, 5351, 5357 (TCP).

Usługę możemy uruchamiać z różnymi parametrami:
nano /etc/conf.d/wsdd
WSDD_OPTS="--ipv4only"

Inne przykładowe opcje:
--interface eth0
--hostname nazwaHosta
--discovery (wyszukuje inne WSDD)

Regułki dla firewalla:

- udp/**3702** - incoming i outgoing (unicast);
- tcp/**5357** - incoming;

Uwaga: Niestety, wersja WSDD przeznaczona na *Gentoo* (0.6.2 / 0.6.4 / 0.7.0) przerywa rozgłaszanie po pierwszej minucie (na *openSUSE* nie ma tego problemu). Problem na razie nierozwiązany.

Opis niektórych parametrów

Prawa systemu Linux do pliku są ważniejsze niż prawa Samby. Jeśli chcemy ustawiać prawa za pomocą Samby, to trzeba udostępnić plik wszystkim do odczytu (777 lub 666).

valid/invalid users - wybór jednego z tych poleceń podyktowany jest naszą decyzją, czy udział ma być dla większości niedostępny czy dostępny. Pokazuje zawartość udziału lub nie. Jeśli nie ma kogoś na VALID to automatycznie jest na INVALID, i odwrotnie.

read list - udział *tylko-do-odczytu* dla osób umieszczonych w tej sekcji.

writeable - domyślnie udostępnienie do zapisu wszystkim. Jest słabsze niż *read list* i *write list* (one są bardziej szczegółowe).

hosts deny = ALL - zabrania dostępu wszystkim komputerom, oprócz tych wyszczególnionych w hosts allow.

Operacje na kliencie linuksowym

Aby klient Samby logował się do serwera, nie może posiadać u siebie pliku smbpasswd (tylko na serwerze), nie może być nadrzędną przeglądarką.

- Zalogować się jako *root*.
- Skopiować plik konfiguracyjny smb.conf. Muszą w nim być aktywne następujące opcje:
  - *security = domain*
  - *password servers = 192.168.0.1*
- Wyłączyć demony Samby.
- **smbpasswd -j nazwaDomeny -r nazwaSerweraPDC -U root%hasłoRoota**
- **/etc/init.d/samba start**
- Ustawiamy możliwość montowania udziałów (nie ustawiać suid na smbmount): **chmod 4755 /usr/sbin/smbmnt /usr/bin/smbumount**
- Sprawdzamy konfigurację: **testparm.**

Przeglądanie zasobów na kliencie linuksowym

Uwaga: pamiętaj o wyłączeniu (lub odpowiedniej konfiguracji) firewalla!

- Wyświetlenie udziałów konkretnej maszyny: **smbclient -NL 192.168.7.40**
- Połączenie się z udziałem: **smbclient //192.168.7.40/homes -U nazwaUżytkownika** lub **smbclient //raven/Pobierz** (zapyta o hasło)
- Połączenie się i zamontowanie udziału chronionego hasłem:

mount -t cifs -o
user=*właścicielUdziału***,pass=***hasłoWłaściciela***,dom=***nazwaGrupyRoboczej*
//nazwaSerwera/nazwaUdziału /mnt/*jakiśFolder*

lub niechronionego hasłem:

mount.cifs //nazwaSerwera/nazwaUdzialu /mnt/*jakiśFolder* **-o guest**

Uwaga: W sytuacji, gdy nie ma wpisu w */etc/fstab* - kopiować do tego folderu może tylko osoba, która go zamontowała, czyli root.

- Przeglądarka graficzna: **smb4k** (ale obsługuje tylko protokół NT1). Przykład konfiguracji: *Sieć / Przeszukaj grupę roboczą* (jest to nakładka na program *nmblookup*, który przeszukuje za pomocą *broadcastu* lub pyta się nadrzędnej przeglądarki sieci, a ona dostarcza mu wykaz maszyn w grupie roboczej; trzeba odczekać 2-3 minuty, aby program pobrał informacje);

  lub

  Sieć / Skanuj obszary rozgłaszania: 192.168.0.255

  Samba / Montowanie / Tryb bezpieczeństwa → Protokół NTLMSSP

W oknie „Podpięcie zasobu”:

Położenie: *smb://192.168.7.40/nazwaUdziału*

Adres IP: *192.168.7.40*

Grupa robocza: *3bird*

Problemy

Udział linuksowej Samby po prostu nie pojawia się w otoczeniu sieciowym

1. Upewnij się, że Samba jest w tej samej grupie roboczej, co reszta sieci i jest w tej samej puli adresów IP.

2. Wydaj poniższe polecenie, aby wykryć ewentualne błędy w pliku konfiguracyjnym:

testparm

3. Wyłącz firewall w Linuksie i w Windowsie.

4. W przypadku Ubuntu, doinstaluj:

apt-get install cifs-utils

Spróbuj także uruchomić serwer w następującej kolejności:

/etc/init.d/nmbd start (lub: **systemctl restart nmb**)

/etc/init.d/smbd start (lub: **systemctl restart smb**)

5. Upewnij się, że jest otwarty port 139 (polecenie **nmap** *twojeIP* lub windowsowe polecenie w Power Shell: PS C:\WINDOWS\system32> **Test-NetConnection 192.168.6.122 -port 139**)

6. Sprawdź logi:

cat /var/log/samba/log.nmbd

cat /var/log/samba/log.smbd

7. Upewnij się, że klienty *Windows* znajdują się w sieci o profilu "*Prywatna*" (lub "*Dom*"), a nie "*Publiczna*" (lub "*Firma*"). Tylko sieć "*Prywatna*" ("*Dom*") bierze udział w Sambie. W przypadku sieci Wi-Fi kliknij w ikonę połączeń (obok zegara), wybierz obecne połączenie, a następnie "*Właściwości*".

8. Upewnij się, że są włączone w systemie *Windows* następujące usługi w trybie automatycznego opóźnionego uruchamiania (*Win+R: services.msc*):

- *Grupowanie sieci równorzędnej;*
- *Host dostawcy odnajdowania funkcji (to jest WSDD);*
- *Host urządzenia UPnP;*
- *Menedżer tożsamości sieci równorzędnej;*
- *Odnajdywanie SSDP (SSDP Discovery);*
- *Połączenia sieciowe;*
- *Protokół rozpoznawania nazw równorzędnych;*
- *Publikacja zasobów odnajdywania funkcji (to jest WSDD);*
- *Przeglądarka komputera (usługa pojawia się po aktywacji funkcji SMB1… zalecane tylko w ostateczności);*

9. Jeśli Samba znajduje się na *VirtualBox*, upewnij się, że we właściwościach protokołu IPv4 masz aktywną opcję „*VirtualBox Bridged Networking Driver*” lub „*Sterownik filtru sieciowego programu VirtualPC*”.

10. Włącz w systemie Windows opcję „*NetBIOS over TCP/IP*”.

W otoczeniu sieciowym znajdują się nieaktualne informacje

Należy dowiedzieć się, który komputer w sieci jest „*Lokalną Przeglądarką Sieci*” (wygrał elekcję)[1], gdyż to on przetrzymuje listę komputerów w sieci i odświeża ją co 12 minut[2]:

nmblookup -M "-"

lub:

nmblookup -M -- -

lub:

nmblookup -M nazwaGrupyRoboczej

Maszyna o identyfikatorze *<1d>*[3] jest *Lokalną Przeglądarką Sieci*.

W systemie Windows należy użyć polecenia:

C:\WINDOWS\system32> **nbtstat -c**

Aby na podstawie IP uzyskać nazwę komputera w sieci, wydaj polecenie:

C:\> **nbtstat -A 192.168.0.38** (w *Windows*)

nmblookup -A 192.168.0.38 (w *Linux*)

Aby na podstawie nazwy komputera uzyskać jego IP, należy przełączyć w otoczeniu sieciowym widok na „*Szczegóły*” oraz „*PPM/Sortuj jako...*” (widoczny będzie także MAC i metoda odnajdywania).

[1] Lokalna Przeglądarka Sieci wybierana jest w demokratycznych wyborach przez komputery. Natomiast Nadrzędna Przeglądarka **Domeny** (*Domain Master Browser*) musi być ustanowiona przez administratora sieci.

[2] Jeśli klient nie został prawidłowo zamknięty (np. brak prądu), to jego usunięcie z listy zajmie jeszcze więcej czasu: 36 minut. System przy prawidłowym zamykaniu wysyła informację do nadrzędnej przeglądarki, która odświeży stan po 12 minutach.

[3] Inne oznaczenia:

<00> - stacja klienta

<1b> - nadrzędna przeglądarka **domeny**

<20> - serwer plików

Otwierając udział Samby pojawia się pytanie o hasło

Przyczyną może być zbyt długa nazwa użytkownika, który próbuje otworzyć lub udostępnić udział. Jeśli to nie pomoże, należy także sprawdzić (w *Windows*): *Narzędzia administratora / Zasady Zabezpieczeń Lokalnych / Zasady Lokalne / Opcje zabezpieczeń / Zabezpieczenia sieci -->*

- *Poziom uwierzytelniania LAN Manager / Wyślij odpowiedzi LM i NTLM*
- *Minimalne zabezpieczenia sesji dla klientów opartych na NTLM SSP / [ ] Wymagaj szyfrowania 128-bitowego* (powinno być nieaktywne)
- *Minimalne zabezpieczenia sesji dla serwerów opartych na NTLM SSP / [ ] Wymagaj szyfrowania 128-bitowego* (powinno być nieaktywne)

Inna przyczyna: Udostępniony folder znajduje się na koncie *root*.

Windows nie może uzyskać dostępu do udziału //NazwaUdziału (0x80070035)

1. Należy sprawdzić, czy wszystkie maszyny przeprowadziły aktualizację systemu do najnowszej wersji (od wersji Windows 10 v.1709, protokół SMB1 nie jest instalowany i nie jest zalecany).

2. Jeśli to nie pomoże, należy w rejestrze *Windows* uaktywnić następującą opcję:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters/ AllowInsecureGuestAuth 1
To samo można wykonać w Zasadach grupy. Uruchom: **gpedit.msc**
Konfiguracja komputera / Szablony administracyjne / Sieć / Stacja robocza LANman:
Włącz niezabezpieczone logowanie gościa: Włączone

3. Można także ręcznie zainstalować protokół SMB1: *Panel sterowania / Programy i funkcje / Włącz lub wyłącz funkcje systemu Windows / Obsługa udostępniania plików SMB 1.0/CIFS (w przypadku systemu Windows Server: Server Manager / Dashboard / Remove Roles and Features Wizard / SMB 1.0/CIFS).* Nie jest to jednak zalecane ze względów bezpieczeństwa.

4. Przydatne może być także polecenie czyszczące lokalną tablicę DNS, gdy adres IP klienta lub serwera zmienił się:
C:\> **ipconfig /flushdns**

5. Pomocne mogą być także polecenia resetujące sieć („*Wiersz polecenia*” należy uruchomić jako administrator):
C:\WINDOWS\system32> **netsh winsock reset**
C:\WINDOWS\system32> **netsh int ip reset**

6. Upewnij się, że nazwa *hostname* serwera i klienta jest krótsza niż 15 znaków.

Otwierając udział pojawia się komunikat „Lokalizacja jest już niedostępna” (ERROR_NETNAME_DELETED)

1. Jeśli Samba jest uruchomiona na maszynie wirtualnej, przydziel jej więcej mocy procesora i więcej pamięci RAM.

2. Odinstaluj lub wyłącz niepotrzebne programy w Windows, w szczególności *Himachi*, *Steam*, itp.

3. Włącz do komunikacji Samby protokół „*NetBIOS over TCP/IP*”[4] (zwany *NetBT* lub *NBT*) na Windows. Zwykły *NetBIOS* używa *broadcastu (wysyła NAME_QUERY_REQUEST)*, co powoduje spore natężenie ruchu sieciowego (gdy jakaś maszyna posiada szukaną nazwę, odsyła *NAME_QUERY_RESPONSE*). A może pójść krok dalej i zrezygnować z protokołu NetBIOS, a w

[4] Aktywacja „*NetBIOS over TCP/IP*” ma swoje negatywne konsekwencje związane z bezpieczeństwem (dostęp do Samby z zewnętrznej sieci), dlatego należy zablokować taki ruch z zewnątrz na routerze.

zamian zastosować „*SMB over TCP/IP*” (czyli *de facto – CIFS*), co ustawiamy za pomocą wpisów w pliku konfiguracyjnym:

disable netbios = yes

smb ports = 445 *(będzie używany tylko serwis smbd, a nie nmbd; ten sam efekt w Windows daje wyłączenie protokołu NetBIOS; musimy korzystać w tym przypadku z serwera WINS, aby widzieć nazwy komputerów w otoczeniu sieciowym; ale zawsze można połączyć się z danym zasobem w eksploratorze plików: \\IP_komputera lub – w przypadku Windows 10, który obsługuje DNS-SD – poprzez \\nazwaKomputera.local)*

Jeśli chcemy używać obu protokołów:

disable netbios = no

smb ports = 139 445

W powyższym przykładzie, najpierw system spróbuje komunikacji na porcie 445, a jeśli będzie to niemożliwe, to na porcie 139.

4. Przyczyną może być także przedwczesne wygaszenie sesji przez serwer Samby. Należy wtedy wprowadzić do rejestru klienta następujący wpis (oznaczający 30 sekund, co jest maksymalną wartością):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:
InvalidFileServerCacheLifeTime REG_DWORD 30

5. Sprawdź, czy Samby używają tej samej wersji protokołu:

- *SMBv1 (Windows 95/98/Me)* – składnik domyślnie usunięty w *Windows 10* (od wersji 1709) i jego ponowna instalacja nie jest zalecana przez Microsoft (duże ryzyko zarażenia się robakami);
- *SMBv2 (Windows Vista / 7 / 8, Windows Server 2008)*
- *SMBv3 (Windows 8/10, Windows Server 2012/2016)* – zawiera funkcję *SMB Direct*

Włączanie i wyłączanie protokołów w Windows zarówno na serwerze jak i kliencie znajduje się w rejestrze, w adresie:

HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters *(wpisy: SMB1, SMB2 o wartości „1” lub „0”)*

HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters *(wpisy: SMB1, SMB2 o wartości „1” lub „0”)*

Można również do tego celu wykorzystać *PowerShell*:

PS C:\WINDOWS\system32> **Get-WindowsOptionalFeature –Online –FeatureName SMB1Protocol** *(sprawdzamy status SMB1 / SMB2 / SMB3)*

PS C:\WINDOWS\system32> **Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart** *(włączamy SMB1 / SMB2 / SMB3)*

PS C:\WINDOWS\system32> **Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol** *(wyłączenie SMB1 / SMB2 / SMB3)*

PS C:\WINDOWS\system32> **Get-SmbServerConfiguration | Select EnableSMB2Protocol** *(czy SMB2 jest włączona?)*

PS C:\WINDOWS\system32> **Set-SmbServerConfiguration -EnableSMB2Protocol $true** *(włączanie SMB2/SMB3; jeśli chcemy wyłączyć, należy na końcu podać wartość $false)*

Uwaga: Protokóły SMB2 i SMB3 są na stałe powiązane ze sobą.

6. Spróbuj uzyskać dostęp do udziału poprzez wpisanie do przeglądarki internetowej:

smb://192.168.0.* *(zamiast gwiazdki wpisz IP serwera Samby)*

7. Jeśli nie pomogą powyższe zabiegi, przyczyną prawdopodobnie może być sama wersja Samby lub wersja dystrybucji Linuksa (zdarzały się takie sytuacje np. w przypadku *Ubuntu*). Zainstaluj nową wersję dystrybucji lub inną dystrybucję.

Przy starcie Samby pojawia się: relocation error: /usr/lib64/samba/libauthkrb5-samba4.so

Dokładna treść błędu: „*relocation error: /usr/lib64/samba/libauthkrb5-samba4.so: symbol tevent_req_is_unix_error, version TEVENT_UTIL_0.0.1 not defined in file libtevent-util.so.0 with link time reference*". Należy zrobić update całego systemu.

Wymuszenie komunikacji klienta z serwerem za pomocą IPv4

Należy wyłączyć na obu maszynach protokół IPv6 (w przypadku DHCP - wyłączyć na routerze). Dodatkowo (alternatywnie) można określić w pliku konfiguracyjnym:

interfaces = „192.168.1.10" „192.168.1.11" lo (*loopback* jest tutaj konieczny)

bind interfaces only = yes

Ostatnia aktualizacja: 31 stycznia 2023.