

Samba - plik konfiguracyjny serwera

Położenie: `/etc/samba/smb.conf`

© 3bird Projects 2018, <http://edukacja.3bird.pl>

Uwaga: Plik dotyczy komputera, który pełni funkcję serwera (dla wielu usług). Jest m. in. kontrolerem domeny. Dostęp do zasobów mają tylko istniejący użytkownicy (potrzebne hasło).

Nazwa

[global]

```
# Nazwa serwera Samba
netbios name = server
netbios aliases = server
# Nazwa grupy roboczej lub domeny NT
workgroup = 3bird
# Komentarz, wyświetlany jako ekwiwalent "NT Description field".
server string = Samba Server (v %v) - %L wita!
```

Drukarki

```
# Automatyczne ładowanie listy wszystkich zainstalowanych drukarek. Pierwszy definiuje położenie pliku definicji drukarek, a drugi umożliwia udostępnienie wszystkich drukarek na serwerze.
; printcap name = lpstat
; printcap name = /etc/printcap
printcap name = cups
load printers = yes
# Może być konieczne wyszczególnienie systemu drukowania, chyba że twój system jest niestandardowy. Obecnie obsługiwane przez Sambę systemy to: bsd, sysv, plp, lpmg, aix, hpux, qnx.
printing = cups
```

Blokady dostępu

```
# Ta opcja jest ważna dla bezpieczeństwa. Pozwala ona ograniczyć połączenia do komputerów, które podłączone są do lokalnej sieci. Poniższy przykładowy wpis pozwala na dostęp do wszystkich komputerów w sieci lokalnej. Wpis można również zastosować do poszczególnych udziałów.
hosts allow = 192.168.10.1, 192.168.10.2, 192.168.10.3, 192.168.10.4, 192.168.10.5, 192.168.10.6, 192.168.10.7, 192.168.10.8, 192.168.10.9, 192.168.10.10, 192.168.10.11, 192.168.10.12, 192.168.10.13, 192.168.10.14, 192.168.10.15, 192.168.10.16
# Skonfiguruj Sambę do używania wielu interfejsów sieciowych. Jeśli posiadasz wiele interfejsów sieciowych, powinieneś wyszczególnić je tutaj. Możliwe jest wpisanie "eth*". Wpis staje się potrzebny, gdy serwer obsługuje wiele podsieci. Liczba 24 jest skróconą maską podsieci.
; interfaces = 192.168.12.2/24 192.168.13.2/24
# Niebezpieczna opcja, wskazuje na plik zawierający spis komputerów i użytkowników, którzy mogą logować się bez hasła.
; hosts equiv = /ścieżka/plik.txt
# Definiuje, czy pliki, których nazwa rozpoczyna się od kropki, mają mieć ustawiony atrybut DOS "ukryty".
hide dot files = yes
# Inne rodzaje plików ukrytych:
hide files = *.conf
# Ograniczenie dostępu do następujących rodzajów plików (oddzielamy je za pomocą znaku "/"):
veto files = *.conf
# Czy można usuwać pliki wyszczególnione w "veto files"?
delete veto files = no
# Wykaz katalogów (oddzielonych przecinkami), do których Samba nie powinna udzielać dostępu. Katalogi są wtedy widziane przez użytkowników jako puste.
dont descend = /proc, /dev, /var, /bin, /boot, /etc, /lib, /sbin, /usr
# Określa grupę, która podczas logowania do Samby otrzymuje uprawnienia administratora dla stacji roboczych.
domain admin group = @root
# Poniżej można określić konto GUEST. Aby to zadziałało należy je dodać (np. „anonim”) do pliku /etc/passwd, w przeciwnym razie zostanie użyty użytkownik "nobody".
; guest account = pcguest
# Zabronienie anonimowego dostępu do udziałów, gdy wartość jest "yes".
restrict anonymous = yes
```

Hasła

```
# Użytkownik z hasłem o zerowej długości nie może zalogować się na Sambę. Aby umożliwić takie logowanie należy wpisać "yes". Domyślnie jest na "no".
null passwords = no
# Liczba znaków w hasle klienta, która nie jest rozróżniana na duże i małe. Stosowane, gdyż Windows nie jest wrażliwy na wiel-
```

kość znaków. Uaktywnienie powoduje jednak pewne opóźnienie w działaniu Samby. Nazwy kont w Linux powinny być z małej litery.

```
; password level = 8  
; username level = 12
```

Możesz użyć kodowania haseł. Opcja ta z reguły powinna być aktywna, jeśli klientami są Win98 i wyżej lub NT4 SP3 i wyżej (musi ona być zgodna z ustawieniami na kliencie). Jeśli występują różnice pomiędzy samymi klientami, zobacz: "encryption.txt", "Win95.txt", "WinNT.txt". Drugi z tych plików porównuje hasła z klienta z hasłami zakodowanymi w pliku "/etc/samba/smbpasswd". Kodowane hasła dodajemy za pomocą polecenia w terminalu: "smbpasswd -a użytkownik".

encrypt passwords = yes

smb passwd file = /etc/samba/private/smbpasswd

Poniższe wpisy pozwalają uaktualnić hasło na Linuxie pobrane z Windows. Należy uaktywnić poniższe wpisy, wtedy gdy uaktywnione są wpisy "encrypt password" and "smb passwd file".

unix password sync = yes

passwd program = /usr/bin/passwd %u

passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n *passwd:*all*authentication*tokens*updated*successfully*

Uaktywnienie poniższego wpisu powoduje, że zmiana hasła będzie odnotowana w dzienniku w postaci jawnego tekstu.

passwd chat debug = no

Możesz użyć flagi kontroli zmiany hasła PAM. Jeśli uaktywnisz wpis, wtedy PAM będzie używane do zmiany hasła podczas żądania klienta Samby zamiast użycia programu wpisanego do "passwd".

pam password change = yes

Użytkownicy Unixa mogą mapować inne nazwy użytkowników SMB. Przydatne wtedy, gdy użytkownik Windows ma inną nazwę w Windows niż w Linux.

username map = /etc/samba/smbusers

Odmowa dostępu, gdy użytkownik poda nieprawidłowe hasło. Gdy parametr będzie wynosił "Bad User" zostanie automatycznie zalogowany jako gość (bez ostrzeżenia). Parametr można stosować do poszczególnych udziałów.

map to guest = Never

Poniższy wpis umożliwia spersonalizowanie konfiguracji dla poszczególnego komputera. Znak "%m" zastępuje nazwę NETBIOS podłączonego komputera.

include = /etc/samba/smb.conf.%m

Kontrola tego, czy Samba powinna przestrzegać dyrektyw zarządzania kontem i sesją PAM. Domyślne zachowanie to użycie PAM do czyszczenia tekstu uwierzytelnienia i do ignorowania jakiegokolwiek zarządzania kontem i sesją. Zauważ, że Samba zawsze ignoruje PAM podczas uwierzytelniania, jeśli aktywny jest parametr "encrypt passwords = yes".

obey pam restrictions = yes

Kontroler domeny

Typ zabezpieczenia. Możliwy jest na poziomie użytkownika "user" (jeśli ta maszyna ma być kontrolerem domeny; dostęp do udziałów wymaga podania hasła i loginu). Aby podłączyć Sambę do innej domeny NT (sprawdzanie hasła przez inny komputer) można ustawić na "domain" (serwer musi być w tej samej domenie; musi być wypełniona opcja „Authentication Server”). Uwaga: od „Samby 4” zlikwidowana została opcja "share" (możliwy jest anonimowy dostęp do zasobu bez podania hasła lub samo hasło bez nazwy użytkownika; w definicji zasobu: „read only = Yes”, „guest only = Yes” lub gdy anonimowi mają mieć prawo zapisu: „force user = anonim”, „force group = users”, „read only = No”, „guest ok = Yes”) oraz opcja "server" (serwer Samba przekazuje hasła i loginy do sprawdzenia innemu serwerowi Samba; musi być wypełniona opcja „Authentication Server”). Zamiast opcji share, można zastosować opcję „security=user” oraz „map to guest = Bad User” (podanie jakiegokolwiek nazwy użytkownika traktowane jest jako użytkownik anonimowy).

security = user

Jeśli ustawiłeś zabezpieczenia na poziomie serwera lub domeny, to możesz użyć poniższej opcji. Wpis może wyglądać następująco: "password server = MójKontrolerDomeny" lub: "password server = *" aby automatycznie zlokalizować kontroler domeny.

password server = <NazwaSerweraNT>

Uaktywnij tę opcję jeśli chcesz, aby Samba była serwerem logowania do domeny dla stacji Windows.

domain logons = yes

Aktywacja wszystkich funkcjonalności z Windows Vista i wyższych wersji Windows:

max protocol = smb2

Ta maszyna staje się serwerem czasu dla klientów Windows.

time server = yes

Jeśli włączyłeś logowanie do domeny wtedy możesz określić plik skryptu logowania dla komputera lub dla poszczególnego użytkownika. Ustanawia to Sambę lokalnym serwerem dla klientów Win9x. Pierwszy z poniższych wpisów dotyczy komputera, zaś drugi dotyczy użytkownika. Skrypty powinny być utworzone w systemie Windows, a wszystkie wpisy zawierają lewy ukośnik "\" a nie prawy "/". Root powinien mieć wszystkie prawa do tego pliku, a użytkownicy prawo odczytu i uruchomienia.

logon script = %m.bat

logon script = scripts%\%U.bat

logon script = scripts\default.bat

Określenia położenia wędrującego profilu (tylko dla Win95 i WinNT). %L zastępuje nazwę NETBIOS serwera, zaś %U nazwę użytkownika. Należy przy tym uaktywnić udziały [profiles]. Wpis "logon path" dotyczy klientów WinNT, a "logon home" klientów Win9x. Polecenia tworzą w katalogu domowym użytkownika ukryty katalog ".profiles" i kopiują do niego profile.

logon path = \\%L%\%U\profiles

logon home = \\%L%\%U\profiles

Przeglądarka sieci

Ustaw na kliencie, gdy jest kilka podsieci. Synchronizacja zawartości ze zdalną przeglądarką sieci.

remote browse sync = 192.168.3.25 192.168.5.255

Spraw, aby ten komputer rozgłaszał się do lokalnej podsieci. Przeznaczony do zastosowania w grupach, które są rozproszone na kilka podsieci. Podsieci będą wtedy wciągnięte do przeglądania.

```

; remote announce = 192.168.1.255 192.168.2.44
# Samba będzie uczestniczyć w wyborach na lokalną przeglądarkę Twojej sieci LAN (zbiera informacje tylko z jednej sieci LAN).
local master = yes
# Samba staje się kontrolerem domeny (zbiera informacje z wielu podsieci LAN; nie używaj tego jeśli już masz kontroler domeny
Windows NT wykonujący tę czynność; włączenie opcji na yes czyni z Samby Primary Domain Controller; jeśli obecna samba ma
być zapasowym kontrolerem domeny, to ustaw opcję na "no"). Poniższą opcję ustawiamy na „yes” tylko wtedy, gdy aktywna jest
opcja „domain logons=yes”.
domain master = yes
# Im wyższy numer (do 64) tym większa szansa, że ten serwer zostanie wybrany na Nadrzędną Przeglądarkę sieci. Domyślna
wartość jest racjonalna.
os level = 65
# Samba może wymusić przy starcie wybór na lokalną przeglądarkę i dać trochę wyższe szanse wygrania wyboru.
preferred master = yes
# Wpis czyni z Samby serwer WINS.
wins support = yes
# Wpis czyni z Samby klienta WINS. Zauważ, że Samba może być albo serwerem albo klientem WINS, ale nie jednocześnie. Po-
wyższa opcja uaktywniona, gdy serwerem WINS jest inny komputer, np. WinNT.
; wins server = w.x.y.z
# Kolejność odczytywania informacji. Opcja "host" może oznaczać plik /etc/hosts, DNS lub NIS; zależy to od ustawień w /etc/
host.config, /etc/nsswitch.conf, /etc/resolv.conf.
name resolve order = hosts wins lmhosts bcst
# Spraw, aby Samba odpowiadała na zapytania dotyczące nazw w przypadku klientów nie zdolnych obsługiwać WINS. Musi być
przynajmniej jeden serwer WINS w sieci. Domyślnie jest "no".
wins proxy = no
# Określ czy Samba ma próbować znaleźć nazwy NETBIOS w DNS nslookup. Domyślnie w wersji 1.9.17 było "yes", ale w wersji
1.9.18 zmienione zostało na "no".
dns proxy = no

```

Znaki

```

# Strona kodowa maszyn klienckich. Nazwy plików i komentarzy będą wyświetlane przy użyciu polskich znaków.
client code page = 852
charset = ISO8859-2
# Zauważ, że może to być ustawione na podstawie udziałów. Ma to coś wspólnego z profilami użytkowników. Określa, czy nowe
pliki są tworzone z nazwami plików, w których wielkość liter jest taka, jaką nadał ją użytkownik, czy też ma być automatycznie
dostosowana do wartości z parametru "default case".
preserve case = yes
# Jeśli parametr ma wartość "yes", nazwy plików w formacie DOS (8.3) będą przekształcane na wartość podaną w "default case".
short preserve case = yes
# Domyślnie ustawione jest na "upper" dla wszystkich plików DOS. Parametr ten określa domyślną wielkość liter dla nowych
nazw plików.
default case = lower
# Bądź bardzo ostrożny z czułością na wielkość liter - to może się źle skończyć. Jeśli poniższa wartość jest "no" Samba nie będzie
rozdzielać małych i wielkich liter w nazwach plików.
case sensitive = no

```

Logi

```

# Możesz określić położenie osobnego pliku dziennika dla każdego komputera, który się podłącza do Samby.
log file = /var/log/samba/%m.log
# Określ pojemność plików dziennika (w Kb):
max log size = 300
# Poziom "wielomówności" (verbosity)
; log level = 3
# Ustawienie szczegółowości informacji w pliku dziennika (od 1 do 10), im wyższa wartość, tym bardziej szczegółowe informacje.
debug level = 6

```

Inne

```

# Poniższy wpis jest potrzebny, aby uchronić klienta Samby przed sygnalizowaniem nieautentycznych błędów w przypadku, gdy
Samba była zainstalowana ze wsparciem dla SSL.
; ssl CA certFile = /usr/share/ssl/certs/ca-bundle.crt
# Większość ludzi sądzi, że ta opcja daje dobre efekty. Szczegóły w: pliku "speed.txt".
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
# Message command is run by samba when a "popup" message is sent to it. The example below is for use with LinPopUp:
; message command = /usr/bin/linpopup "%f" "%m" %s; rm %s

```

```

#===== Definicje udziałów =====

```

```

[homes]
comment = Katalog domowy
browseable = no
writable = yes

```

```
valid users = %S
create mode = 0600
directory mode = 0700
hosts allow = 192.168.10.1, 192.168.10.2, 192.168.10.3, 192.168.10.4, 192.168.10.5, 192.168.10.6, 192.168.10.7,
192.168.10.8, 192.168.10.9, 192.168.10.10, 192.168.10.11, 192.168.10.12, 192.168.10.13, 192.168.10.14, 192.168.10.15,
192.168.10.16
```

Katalog "netlogon" dla domeny logowania (tylko archiwalne: Windows95/98).

[netlogon]

```
comment = Usługa logowania do sieci
path = /home/.netlogon
browsable = no
guest ok = no
writable = no
write list = root
share modes = no
```

Specyfikacja wędrujących profili użytkowników. Domyślnie używane są domowe katalogi użytkowników (bardzo niewygodne). Zauważ, że poniższy wpis udostępnia tylko zwykły katalog o nazwie "profiles" widoczny w otoczeniu sieciowym jako "\\%L\profiles". Nie robi nic więcej. Polecenie wczytywania i zapisywania profili znajduje się w sekcji "global".

[profiles]

```
comment = Profile użytkowników
path = %H/.profiles
browseable = no
guest ok = no
writable = yes
create mode = 0600
directory mode = 0700
```

Publicznie udostępniony katalog tylko-do-odczytu, za wyjątkiem użytkowników należących do grupy "root", którzy mają pełny dostęp.

[Pobierz]

```
comment = Materiały do pobrania
path = /home/ftp
public = no
writable = no
write list = @root
read list = @users
valid users = %U
hosts allow = 192.168.10.1, 192.168.10.2, 192.168.10.3, 192.168.10.4, 192.168.10.5, 192.168.10.6, 192.168.10.7,
192.168.10.8, 192.168.10.9, 192.168.10.10, 192.168.10.11, 192.168.10.12, 192.168.10.13, 192.168.10.14, 192.168.10.15,
192.168.10.16
```

Inne przykłady udziałów

Zauważ, że jeśli posiadasz system drukowania BSD, to nie ma żadnej potrzeby definiowania drukarek każdej z osobna. Poniższy wpis określa wszystkie drukarki dostępne dla wszystkich. Zauważ, że nie ma wpisu "printer name", gdyż nazwy drukarek pobierane są z pliku "printcap".

```
:[printers]
```

```
; comment = Wszystkie drukarki
; path = /var/spool/samba
; browseable = no
# Ustaw "public = yes", aby pozwolić użytkownikowi "guest" drukować.
; public = yes
; guest ok = no
; writable = no
; printable = yes
# Poniższy wpis oznacza, że wszystkie pliki są tworzone z przypisanymi wszystkimi prawami dla danego użytkownika, lecz dla nikogo innego.
; create mode = 0700
```

Ta opcja jest użyteczna dla ludzi dla udostępniania plików

```
:[tmp]
```

```
; comment = Katalog dla plików tymczasowych
; path = /tmp
; writable = yes
; write list = @users, @root
; public = no
; valid users = %U
; create mode = 0666
; force create mode = 0666
; directory mode = 0777
; force directory mode = 0777
# Poniżej: 0 = nie można zmieniać, a 7 = można zmieniać w pełnym zakresie
; directory security mask = 0777
```

Dedykowany udział drukarki (poszczególne drukarki dla wybranych użytkowników). Wartość "path" obowiązkowo musi wynosić "/var/spool/samba", gdyż klient nie rozpoznaje wartości "/home/%U", np. dla użytkownika "root", który nie mieści się w "home".

```
;  
; [HPLaser6]  
; comment = Drukarka laserowa  
; browsable = no  
; writable = yes  
; printable = yes  
; printer name = HPLaser6  
; path = /var/spool/samba  
; public = no  
; write list = root, robert, lilka, student  
; valid users = root, robert, lilka, student  
; create mode = 0700  
; print command = lpr -P %p -o raw %s -r # użycie sterowników klienta
```

Dostęp do CD-ROM i dyskietek.

```
;  
; [DVD]  
; comment = CD-ROM  
; path = /mnt/cdrom  
; public = yes  
; browsable = yes  
; writable = no  
; valid users = %U  
; hosts allow = 192.168. EXCEPT 192.168.0.2
```

```
;  
; [CD-RW]  
; comment = CD-RW  
; path = /mnt/cd-rw  
; public = yes  
; browsable = yes  
; writable = yes  
; valid users = %U  
; hosts allow = 192.168.0.2
```

Ostatnia aktualizacja: 10 sierpnia 2018.