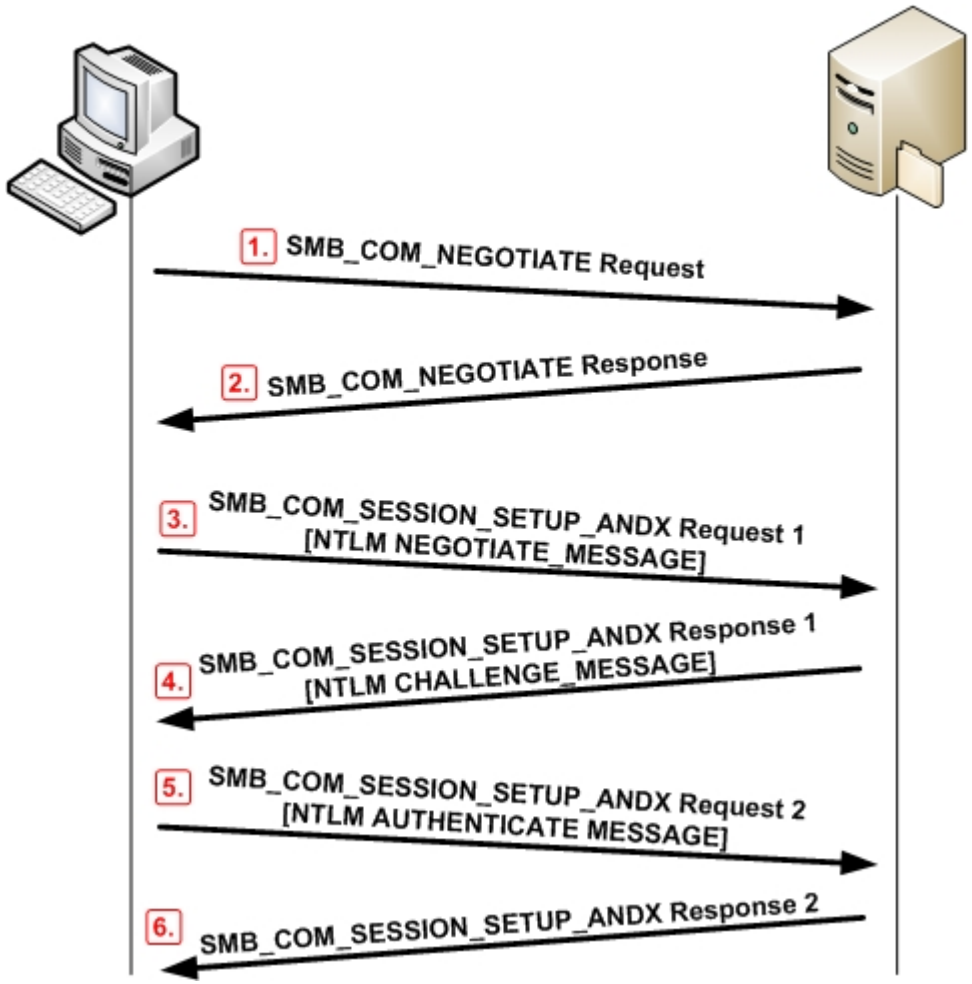
Serwer SMB

Udostępnienie zasobów systemowych w sieci

Jakub Stasiński, Jędrzej Chruściel, Michał Wojciechowski

Protokół SMB umożliwia

- udostępnianie plików
- udostępnianie drukarek



Protokół SMB

Samba - implementacja SMB

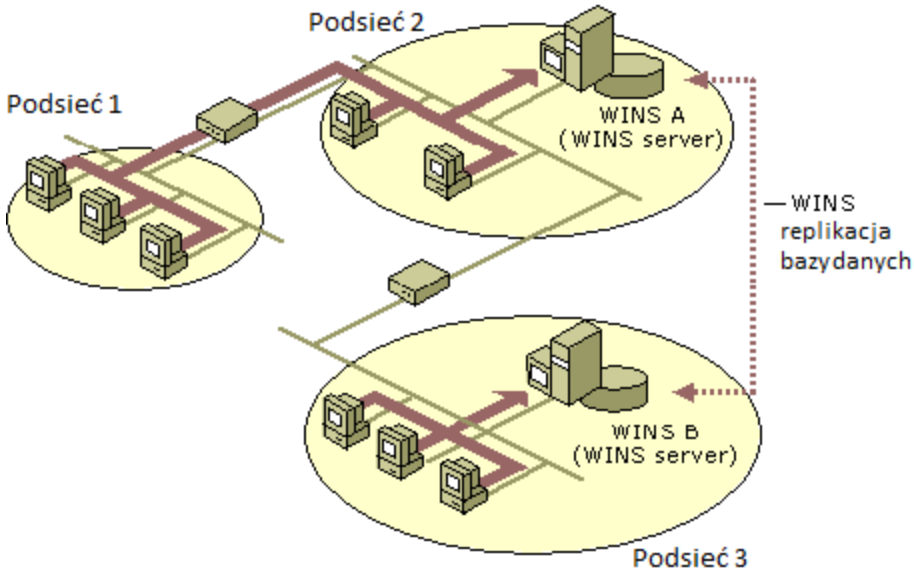
- smbd - odpowiada za współdzielenie plików i drukarek oraz uwierzytelnianie
- nmdb - świadczy usługi WINS wymagane do przeglądania zasobów sieci

Pozostałe pakiety Samby

- smbpasswd - zarządanie użytkownikami
- smbstatus - wyświetla obecny stan połączenia z sambą
- swat - interfejs webowy umożliwiający zarządanie Sambą

Serwery WINS

Serwer WINS przyjmuje od klientów żądania rejestracji nazw i adresów IP oraz odpowiada na wysyłane przez nie kwerendy o nazwy NetBIOS (sprawdzając w swojej bazie danych ich istnienie).
Ponadto serwery WINS są w stanie replikować między sobą bazy danych.



Rozpoznawanie nazw WINS

Mechanizm zamiany nazwy NetBIOS na adres IP zależy od skonfigurowanego rodzaju węzła NetBIOS.
W RFC 1001 węzły zdefiniowano jako:

- węzeł B: emituje kwerendy nazw NetBIOS do rejestracji i rozpoznawania nazw
- węzeł P (p2p): wykorzystuje serwer nazw NetBIOS (np. serwer WINS) do rozpoznawania nazw
- węzeł M: domyślnie działa jako węzeł B, w razie niepowodzenia jako P
- węzeł H: domyślnie działa jako węzeł P, w razie niepowodzenia jako B

Instalacja Samby

- apt-get install samba
- cała konfiguracja Samby znajduje się w pliku /etc/samba/smb.conf
- wszystkie komputery muszą być w tej samej domenie

Smb.conf

- link podzielony jest na sekcje
  - **[global]** - konfiguracja globalna dla wszystkich udziałów
  - **[nazwaudzialu]** - konkretne konfiguracje udziałów
- zmiana pliku smb.conf wymaga przeładowania/restart samby
- samba automatycznie przeładowuje konfigurację co 1minutę

Smb.conf

```
[global]
workgroup = WORKGROUP
netbios name = bob
server string = Samba server %v
guest account = nobody
#security = share
security = user
local master = yes
log level = 2
log file = /var/log/samba/log.%m
map to guest = bad user
```

```
[public]
path = /home/samba/profiles/public
guest ok = yes
guest only = yes
read only = no
#valid user = nobody

[joe]
path = /home/joe
comment = katalog domowy
browseable = no
writable = yes
valid user = joe
public = no
```

Testowanie Samby

- Testowanie konfiguracji

testparm smb.conf

- Testowanie Samby

ps -A | grep smbd
ps -A | grep nmbd
smbclient -L localhost #próba połączenia

Podstawowa konfiguracja firewalla

#Akceptowanie połączeń na port tcp 139 z sieci lokalnej
iptables -A INPUT -p TCP -s 192.168.11.0/24 --destination-port 139 -j ACCEPT

#Akceptowanie połączeń na port udp 137 z sieci lokalnej
iptables -A INPUT -p UDP -s 192.168.11.0/24 --destination-port 137 -j ACCEPT

#Akceptowanie połączeń na port udp 138 z sieci lokalnej
iptables -A INPUT -p UDP -s 192.168.11.0/24 --destination-port 138 -j ACCEPT

Tryby działania samby

- Samba dla gości - bez autoryzacji
- Samba z autoryzacja użytkownika
- Samba jako kontroler domeny

Dostęp do udziałów / przykładowe ścieżki

\\nazwaLubAdresKomputera

\\adresIpSerwera\nazwaUdzialu

\\nazwaNetbiosowaSerwera\nazwaUdzialu

\\nazwaDnsSerwera\nazwaUdzialu

\\nazwaLubAdres\nazwaUdzialu\katalog

Samba dla gości - bez autoryzacji

- Tworzenie konta bez autoryzacji, bez dostępu do powłoki

addgroup nogroup

useradd -c "konto bez autoryzacji" -g nogroup -d /dev/null/ -s /bin/false nobody

[-c comment]
[-g initial_group]
[-d home_dir]
[-s shell]

Samba dla gości - bez autoryzacji

- Edycja pliku /etc/samba/smb.conf

```
[global]
workgroup = HOME                        #nazwa grupy roboczej
netbios name = serwer-sieci             #nazwa serwera w grupie roboczej
server string = Samba server %v         #oznaczenie, komentarz serwera
guest account = nobody                  #konto logujących się bez autoryzacji
security = share                        #usługa ma jedno hasło dla wszystkich
local master = yes                      #serwer będzie główną lokalna przeglądarką
```

Samba dla gości - bez autoryzacji

- Edycja pliku /etc/samba/smb.conf

```
[nazwaudzialu]
path = /home/samba/public                  #ścieżka do katalogu
guest ok = yes                              #dostęp także dla gości
guest only = yes                           #każdy użytkownik traktowany jako gość
read only = no                             #nie tylko do odczytu
valid user = nobody                        #jedynie uzytkownik nobody może widzieć zasób
force user = nobody                        #zapis w udziale z prawami usera nobody
```

Samba dla gości - bez autoryzacji

- Stworzenie odpowiedniego katalogu

```
mkdir /tmp/public
chown nobody /tmp/public
```

Samba z autoryzacją użytkownika

Wymagane jest założenia kont w systemie

- Dodanie grupy i użytkownika do systemu samby, bez dostępu do powłoki:

  addgroup smbgroup

  useradd -c "konto smb" -g smbgroup -d /dev/null -s /bin/false bob

- Dodanie użytkownika do bazy samby:

  smbpasswd -a bob

Samba z autoryzacją użytkownika

Konfiguracja smb.conf:

```
[global]
workgroup = siec                        #nazwa grupy roboczej
netbios name = serwer-sieci                 #nazwa serwera w grupie roboczej
server string = Samba server %v             #oznaczenie, komentarz serwera
guest account = nobody                      #konto logujących sie bez autoryzacji
security = user                             #zabezpieczenie na poziomie użytkownika
local master = yes                          #serwer będzie główną lokalna przeglądarką

[homes]
path = /home/samba/users
comment = katalog domowy                    #komentarz
browseable = no                             #udział nie rozgłaszany w listach przeglądania
writable = yes                              #udział nie jest przeznaczony tylko do odczytu
valid user = joe
```

Samba jako kontroler domeny

Tworzenie konta dla każdego użytkownika:

addgroup clients

useradd -c "konto maszyny" -g clients -d /dev/null -s /bin/false pc1$
#znak “$” jest konieczny przy nazwie komputera

smbpasswd -a -m pc1 #tutaj już bez symbolu $

Samba jako kontroler domeny

- Konfiguracja smb.conf

```
[global]
workgroup = siec                          #nazwa grupy roboczej
netbios name = serwer-sieci                    #nazwa serwera w grupie roboczej
server string = Samba server %v                #oznaczenie, komentarz serwera
guest account = nobody                         #konto logujących się bez autoryzacji
security = user                                #także konieczne w kontrolerze domeny
local master = yes                             #serwer będzie główną lokalna przeglądarką
domain master = yes                            #serwer będzie kontrolerem domeny
prefered master = yes                     #samba będzie główna przeglądarką
announce as =  NT server                       #samba będzie udawać serwer NT

encrypt passwords = yes                        #szyfrowanie haseł
smb passwd file = /etc/samba/smbpasswd         #ścieżka do pliku z kontami
```

Samba jako kontroler domeny

- Konfiguracja smb.conf

```
[homes]
path = /home/samba/users
comment = Katalog domowy
browseable = No                 #udział nie rozgłaszany w listach przeglądania
writable = Yes                  #udział nie jest przeznaczony tylko do odczytu
```

- Zmiana konfiguracji Windows XP

Local Group Policy - należy wyłączyć w *Security Options -> Domain Member* opcję *Digitally encrypt or sign secure channel data.*

Samba i profile mobilne (wędrujące)

- Jedną z podstawowych zalet logowania do domeny NT są tzw. profile wędrujące czy jak kto woli mobilne. Pozwalają one dla użytkowników systemów Windows używać swoich ustawień programów i systemu na rożnych komputerach w tej samej sieci pod warunkiem zalogowania się do tej samej domeny NT z tym samym użytkownikiem.
- Trzeba zaznaczyć że systemy Windows z rodziny 9x mają inna format profilu użytkownika od Windows z rodziny NT, dlatego miejsca składowania tych profili są kontrolowane przez dwa parametry wskazujące odpowiednie ścieżki UNC systemom Windows (czyli w stylu \\Serwer\Katalog\Użytkownik). Można próbować używać mieszanych profili ale może być tego różny skutek.

Samba i profile mobilne (wędrujące)

Standardowo profile mobilne są włączone w Sambie,
wartości domyślne dla tych opcji to:

logon home = \\%N\%U << domyślna ścieżka dla profili dla Windows 95/98/98SE/Me

logon path = \\%N\%U\profile << domyślna ścieżka dla profili dla Windows NT4/2000/XP/2003

Zmienna %N oznacza nazwę serwera NIS katalogu domowego.

Zmienna %U oznacza nazwę użytkownika sesji, nazwę którą klient chciał, niekoniecznie taka sama jaką otrzymał.

Samba i profile mobilne

- By stworzyć udział do przechowywania profili należy dodać do sekcji udziałów w smb.conf:

```
[profiles]
comment = Network Profiles Share
path = /srv/samba/profiles                  #ścieżka udziału profili
read only = No
create mask = 0600
directory mask = 0700
browseable = no
guest ok = no
printable = no                              #nie jest do drukarka
profile acls = yes                          #lista kontroli dostępu
```

acl- Umożliwia bardziej rozbudowana i dokładną kontrolę dostępu do plików

Netlogon

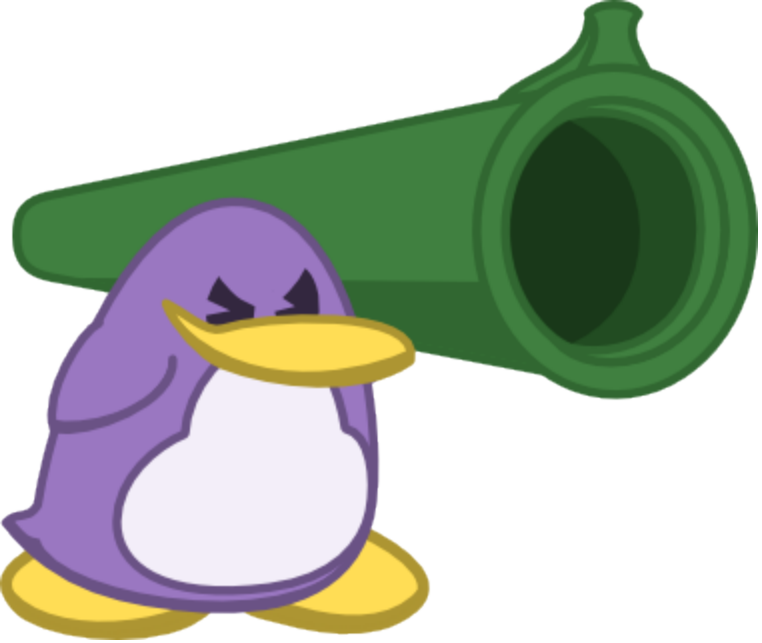
- Konfiguracja udziału netlogon:

```
[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon
guest ok = no
writable = no
browseable = no
```

Klient Samby

Windows: net use P: \\server\share /USER:user

Linux: smbclient //server/share -U joe



Bezpieczeństwo Samby

allow hosts = 192.168.0.100/24	#wymienia komputery które mogą się łączyć z sambą
available = true/tes	#zabrania dostępu do udziału
deny hosts = lista hostów	
dont descent = lista przecinkowa katalogów	#nie pozwala przeglądać ani przejść do katalogów.
invalid users = lista użytkowników	# lista userów którzy nie mogą korzystać z udziału.
max connections = liczba	#określa max. liczbę połączeń z udziałem
read only = wartość logiczna	#mówi o trybie udziału tylko do odczytu
revalidate = wartość logiczna	#jeśli jest ustawiona na YES użytkownicy będą za #każdym razem musieli wprowadzać hasło #przeglądając udział.
veto files = lista ukośnikowa	#lista plików które nie będą pokazywane klientowi