Samba jako serwer udostępniania plików i drukarek w sieci LAN

Konfiguracja serwera
Samba w wersji 3 i 4

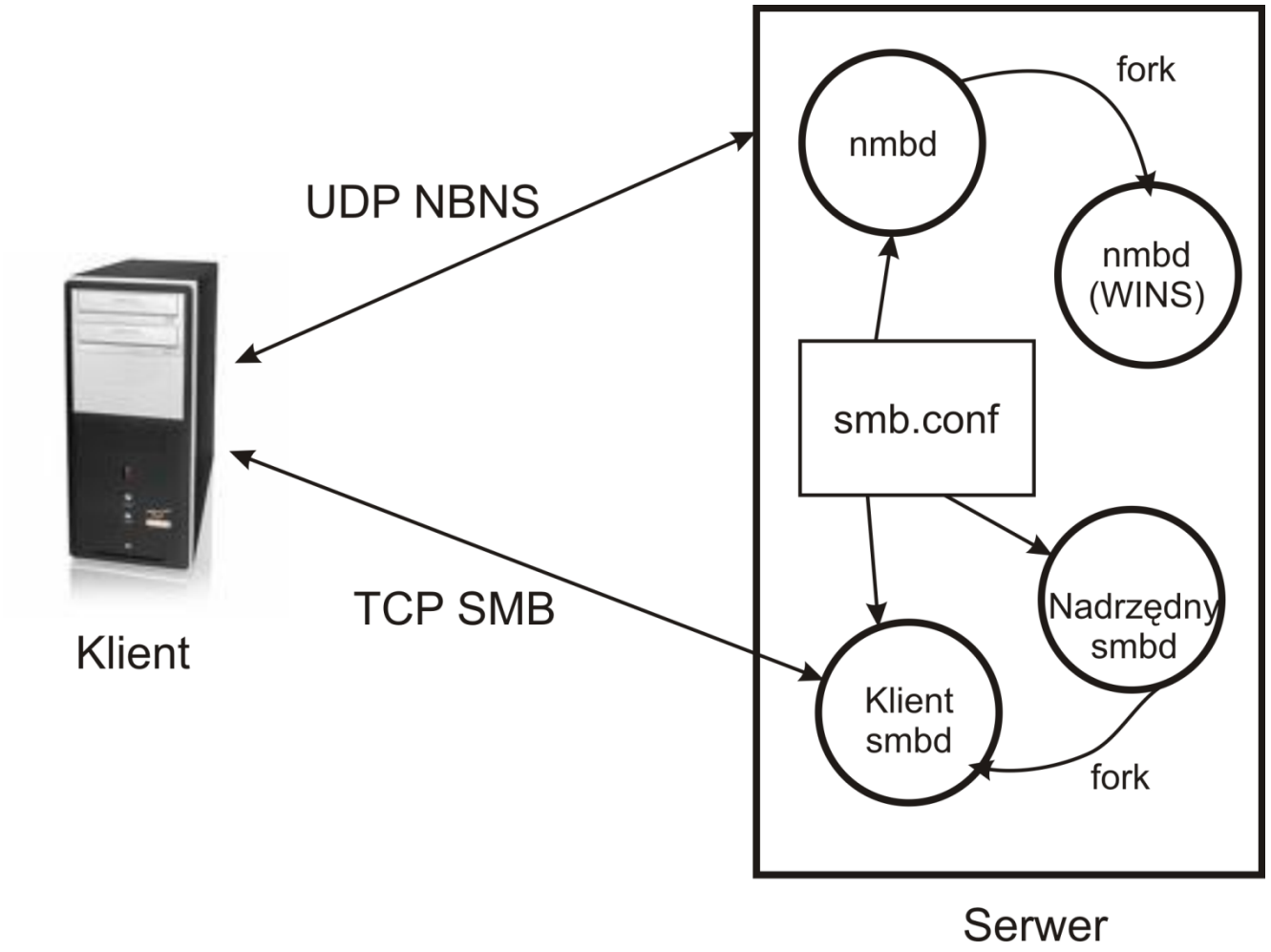
Cechy Samby w wersji 3

- *Samba* jest serwerem plików i drukarek, który zawiera implementację *protokołu SMB (Server Message Block).*
- *Samba* może wykorzystywać protokół *NetBIOS over TCP/IP (NetBT).*
- *Samba* może bezpośrednio pracować na protokole *TCP* (tak zwany *NetBIOS-less SMB*).
- Może pełnić rolę serwera rozwiązywania nazw *NetBIOS – NBNS (NetBIOS Name Server)*.
- Od wersji 3.5 eksperymentalna obsługa protokołu SMB2 (na dzień dzisiejszy – wersja 3.5.1 tak samo).

Współpraca Samby z Windows

- *Samba* może pełnić następujące role w odniesieniu do domen *Microsoft Windows:*
  - Klient domeny *WindowsNT*,
  - Klient domeny *Active Directory* – uwierzytelnianie i autoryzacja klientów – protokoły Kerberos i LDAP,
  - Podstawowy i zapasowy kontroler domeny *WindowsNT* dla wszystkich dystrybucji klienckich *Windows.*
- Może pracować również jako serwer *WINS* dla komputerów klienckich z rodziny *Microsoft.*
- *Samba* w wersji 3 nie może być w pełni funkcjonalnym kontrolerem domeny *Active Directory.*

Struktura Samby v.3



Opis struktury Samby v.3

- *Serwer Samba* składa się z dwóch demonów:

  SMBD – odpowiedzialny za:

  - Zarządzanie zasobami współdzielonymi przez serwer i jego klientów,
  - Zapewnia klientom (*Linux* i *Windows*) dostęp do udostępnionych zasobów plikowych i drukarek,
  - Dokonuje uwierzytelnienia i autoryzacji użytkowników,
  - Przekazuje wszystkie komunikaty pomiędzy serwerem *Samby*, a klientami.

  NMBD – odpowiedzialny za:

  - Rozwiązywanie nazw *NetBIOS* na adresy IP,
  - Obsługiwanie list przeglądarek *Grup roboczych* czy *domeny NT*
  - Pełnienie roli serwera *WINS* dla klientów *Microsoft.*

Instalacja Samby z pakietów

- Instalacja *samba-common* – pakietu potrzebnego praktycznie dla wszystkich pakietów *Samby*.
- Instalacja podstawowego pakietu serwera – *samba*
- Dodatkowo – instalacja pakietu *samba-winbind* – zawiera oprogramowanie związane z uwierzytelnianiem *Samby* w kontrolerach pracujących w systemie *Windows.*
- Oprogramowanie dla klienta zawierające także programy przydatne do testowania serwera – *samba-client.*
- Pakiet *samba-swat* umożliwa graficzne (z poziomu przeglądarki internetowej) zarządzania serwerem.
- Konfigurację serwera *Samba* można wykonywać:
  - Z poziomu przeglądarki i programu do zarządzania: *swat,*
  - Edytując bezpośrednio plik konfiguracyjny */etc/samba/smb.conf.*

Instalacja Samby ze źródeł

- Pobranie źródeł ze strony projektu: *samba.org.*
- Kod źródłowy jest w skompresowanym archiwum.
- Kolejne kroki, to dekompresja, kompilacja i instalacja:

```
[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*.
- Źródła aktualnie zawierają również wersję 4, co umożliwia kompilację obydwu wersji jako *merged.*

Role pełnione przez Sambę

- Rola w jakiej *Samba* pracuje zdefiniowana jest przez wartość atrybutu *security* oraz związanych z nim innymi parametrami.
- Parametry te określają odpowiedni dla pełnionej roli sposób uwierzytelnienia i autoryzacji.
- Samba może pełnić następujące role w odniesieniu do domeny *Microsoft:*
  - *Serwer członkowski* w domenie NT,
  - *Serwer członkowski* w domenie AD,
  - *Podstawowy kontroler domeny (PDC)* w domenie NT,
  - *Autonomiczny (standalone) serwer.*

Serwer członkowski w domenie

- Samba może pełnić rolę serwera członkowskiego (*Domain Member Server*) zarówno w domenie *NT* jak i *AD*.
- Uczestniczy wtedy w bezpieczeństwie na poziomie domeny, co umożliwia stosowanie modelu *Single sign-on.*
- Użytkownicy otrzymują dostęp do udziałów *Samby* uwierzytelniając się za jej pośrednictwem w kontrolerze domeny (wykorzystanie programu *winbind*) stosując:
  - *Protokół NTLM* – uwierzytelnienie w domenie NT,
  - *Protokół Kerberos* – uwierzytelnienie w domene AD.
- Konieczne jest utworzenie *kont zaufania (Machine Trust Account)* dla komputerów pracujących w domenie.

Podstawowy kontroler domeny

- Samba w wersji 3 może jedynie być *PDC* dla domeny *NT*.
- Konta użytkowników przechowywane są:
  - Lokalnie w bazie kontrolera – dobre dla mniejszych domen,
  - W bazie dostępnej przez LDAP – lepsze dla większych wdrożeń (dobra skalowalność, łatwa replikacja, itp.).
- Stacjami klienckimi w domenie mogą być wszystkie klienckie systemy firmy *Microsoft*.
- Możliwość implementacji *profili migrujących* dla użytkowników pracujących na stacjach z *MS Windows.*
- Definiowanie skryptów startowych dla użytkowników w czasie ich logowania itp..
- Za pomocą *winbind* istnieje również możliwość uwierzytelniania użytkowników z systemów *Linux.*

Plik konfiguracyjny – *smb.conf*

- Plik konfiguracyjny */etc/samba/smb.conf* podzielony jest na sekcje.
- Każda sekcja zawiera definicje odpowiednich atrybutów.
- Definicje atrybutów są w postaci: *nazwa* = *wartości*
- W pliku mogą znaleźć się następujące sekcje
  - *[global]* – definicje parametrów globalnych dotyczących całej konfiguracji,
  - *[homes]* – definicje katalogów domowych użytkowników,
  - *[printers]* – ustawienia dotyczące udostępniania drukarek,
  - *[netlogon]* – udział związany z logowaniem do domeny,
  - *[profiles]* – ustawienia profili użytkowników,
  - *[swoja_nazwa]* – definicja własnego udziału.

Definicje globalne

- Sekcja *[global]* definiuje między innymi:
  - Nazwę serwera, jego opis i nazwę *grupy roboczej*,
  - Określenie pełnionej roli przez serwer: klient domeny NT lub AD, kontroler domeny NT czy wolnostojący serwer,
  - Ustawienia związane z pełnieniem roli serwera *WINS,*
  - Definicje dotyczącej ustawień przeglądarki w sieci lokalnej,
  - Opcje związane z udostępnianiem drukarek,
  - Ustawienia atrybutów związanych z systemem plików,
  - Definicje atrybutów związanych z raportowaniem (logowaniem),
  - Ustawienia dotyczące bezpieczeństwa – interfejsy na jakich nasłuchuje usługa, adresy sieci z których pochodzą klienci, lista użytkowników uprawnionych, domyślne uprawnienia plików, itp.,
  - Parametry związane z wydajnością.

Samba w roli klienta

- Wartości atrybutu *security* dla odpowiednich ról pełnionych przez sambę wraz z innymi potrzebnymi parametrami są następujące:

Samba jako członek *domeny NT*:

- security = domain,
- passdb backend = tdbsam,
- encrypt passwords = yes.

Samba jako członek domeny *Acitive Directory:*

- security = ads,
- realm = nazwa.twojego.królestwa,
- password server = adres.KDC,
- passdb backend = tdbsam,
- encrypt passwords = yes.

Samba jako kontroler

- W przypadku definiowania roli *Samby* jako podstawowego kontrolera domeny *NT* konieczne są do ustawienia:
  - security = user,
  - domain master = yes,
  - domain logons = yes,
  - passdb backend = tdbsam (lub ldapsam)
- Konieczne jest zdefiniowanie udziału *[netlogon]* służącego do przechowywania skryptów logowania, plików polityk grupowych (NTConfig.POL) i innych potrzebnych narzędzi wykorzystywanych w czasie logowania.
- Opcjonalne do zdefiniowania dla *PDC:*
  - Atrybuty: *logon path, logon home, logon drive, logon script,*
  - Udział *[profiles]* – przechowujący profile migrujące użytkowników.

Definiowanie udziału

- Najważniejsze atrybuty związane z definiowaniem udziału:
  - *[nazwa udziału]* – nazwa udziału widoczna w sieci,
  - *comment* – komentarz udziału widziany w sieci,
  - *path* – ścieżka bezwzględna do katalogu udziału,
  - *browseable* – określa widoczność w sieci – wartość logiczna,
  - *read only* – definiuje możliwość zapisu – wartość logiczna,
  - *valid users* – lista użytkowników w postaci *login* lub *@grupa* oddzilonych przecinkami; uprawnionych do korzystania z udziału,
  - guest ok – zezwolenie na dostęp użytkownikom nieuwierzytelnionym – wartość logiczna,
  - *create mask* – definiuje prawa tworzenia plików – podana wartość jest mnożona binarnie (AND) z prawami wynikającymi z *linuksa,*
  - *force create mode* – określenie praw jakie będą nadane plikom,
  - *directory mask* i *force directory mode* – analogiczne dla katalogów.

Przykłady udziałów

- Udział o nazwie *informacje* dostępny dla wszystkich z grupy *pracownicy* w trybie tylko do odczytu:

```
[informacje]
   comment = Informacje dla pracowników
   path = /usr/shares/informacje_do_odczytu
   browsable = yes
   read only = yes
   valid users = @pracownicy
```

- Udział *pub* dostępny nawet dla nieuwierzytelnionych:

```
[pub]
   comment = Pub – dla wszystkich
   path = /usr/shares/pub
   browsable = yes
   read only = no
   guest ok = yes
```

Przykłady udziałów c.d.

- Udział o nazwie *IT* posiadający następujące cechy:
  - Widoczny w sieci,
  - Dostęp dla członków grup *informatycy, it* i użytkownika *franio,*
  - Wymusza prawo tworzenia katalogów *2770* (prawo sgid),
  - Wymusza tworzenie plików z prawami 660 (zapis dla grupy),
  - Wymusza ustawienie właściciela grupowego plików na *it*

```
[IT]
   comment = Pliki działu IT
   path = /usr/shares/IT
   browsable = yes
   read only = no
   valid users = franio, @it, @pracownicy
   force directory mode = 2770
   force create mode = 0660
   force group = it
```

Udział [homes]

- Udział o *[homes]* definiujący katalog domowy użytkownika.
- Ma związek z następującymi globalnymi atrybutami:
  - *logon home* – adres udziału z katalogiem domowym użytkownika
  - *logon drive* – litera pod którą będzie mapowany katalog.

```
logon home = \\%L\%U
logon drive = H:
```

%L – nazwa NetBIOS serwera

%U – nazwa użytkownika żądana przez klienta

```
[homes]
   comment = Katalogi domowe
   browsable = no
   read only = no
   valid users = %S
```

%S – nazwa bieżącego użytkownika

Udział [Profiles]

- Udział o *[Profiles]* definiuje katalog dla przechowywania profili migurjących.
- Ma zastosowanie w konfiguracji *PDC.*
- Definiowany w parze z atrybutem *logon path* określającym adres udziału z profilem.

```
logon path = \\%L\Profiles\%U
```

```
[Profiles]
   comment = Profile migrujące użytkowników
   path = /usr/shares/profiles
   read only = no
   profile acls = yes
```

profile acls – ustawianie odpowiednich ACL związanych z profilem – sprawdzenie ACL wykonywane jest przez nowych klientów *Windows*

Udział [printers]

- Udział *[printers]* definiuje katalog kolejki wydruku.
- Ma związek z następującymi globalnymi atrybutami:
  - *printcap name* – nadpisanie domyślnego w systemie */etc/printcap*
  - *printing* – zdefiniowanie systemu wydruku.

```
printcap name = cups
printing = cups
```

- Udział *[printers]* powinien być następująco zdefiniowany:
  - Dostępny dla wszystkich,
  - Zadania zapisywane tylko z prawami dla właściciela,
  - Możliwość wydruku z tego udziału
  - Niewidoczny w sieci.

Udział [printers] – przykład

- Przykładowa definicja udziału *[printers]*:

```
[printers]
   comment = Udostępnione drukarki
   path = /var/spool/samba
   printer admin = franio
   create mask = 0600
   browsable = no
   printable = yes
   read only = no
   guest ok = yes
   use client driver = yes
```

Testowanie Samby

- Do wykonania testu poprawności pliku konfiguracyjnego */etc/samba/smb.conf* służy narzędzie *testparam.*
- Wyświetlenie aktualnego stanu zasobów – lista otwartych plików wraz z ich użytkownikami – polecenie *smbstatus*.
- Podłączenie się do serwera Samby – program smbclient:
  - Zażądanie i otrzymanie po poprawnym uwierzytelnieniu dostępu do udziału o adresie *dns1**franio* przez użytkownika *franio* będzie wyglądać następująco:

```
[root@fdns1 ~]# smbclient //DNS1/franio –U franio
Domain=[KRAKOW] OS=[Unix] Server=[Samba 3.4.7-0.50.fc11]
smb: \>
```

- W celu wypisania wszystkich udostępnionych udziałów można się podłączyć jako anonimowy użytkownik podając po opcji *–L* nazwę *NetBIOS* serwera.

Testowanie Samby c.d.

- Przykład podłączenia jako gość – program *smbclient:*

```
[root@fdns1 ~]# smbclient -L DNS1
Enter root's password:
Anonymous login successful
Domain=[KRAKOW] OS=[Unix] Server=[Samba 3.4.7-0.50.fc11]
        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server Version 3.4.7-
0.50.fc11)

        Server               Comment
        ---------            -------
        DNS1                 Samba Server Version 3.4.7-0.50.fc11

        Workgroup            Master
        ---------            -------
        KRAKOW               DNS1
```

Zarządzanie użytkownikami

- Do zarządzania użytkownikami służy polecenie *smbpasswd,* którego podstawowe zastosowania to:
  - *smbpasswd user* – zmiana hasła użytkownika *user,*
  - *smbpasswd -a user* – dodanie użytkownika *user,*
  - *smbpasswd -x user* – usunięcie użytkownika *user,*
  - *smbpasswd -m komputer* – utworzenie konta zaufania dla komputera o nazwie *komputer.*
- W wypadku wykorzystania protokołu *LDAP* jako dostępowego do informacji o użytkownikach, możliwe jest zarządzanie użytkownikami za pomocą poleceń umożliwiających zarządzanie bazą *LDAP.*

Samba w wersji 4

- Samba w wersji 4 może pełnić rolę kontrolera *Active Directory*.
- Umożliwia zarządzanie domeną *AD* z poziomu przystawek administracyjnych instalowanych na komputerze klienckim z systemem *MS Windows*.
- Daje możliwość zarządzania politykami *GPO.*
- Jest wciąż w wersji testowej i dlatego brak jej jeszcze pełnej produkcyjnej funkcjonalności.
- Używa natywnych protokołów Active Directory dla uwierzytelnienia i autoryzacji – kerberos i LDAP.

Zawartość Samby v.4

- Samba v.4 to jedna usługa o nazwie samba (nie ma już podziału na *smbd* i *nmbd*).
- Posiada wbudowane *KDC*
  - Implementacja *Heimdal,*
  - Uwzględnia rozszerzenie biletu *TGT* o pole *PAC* – dodane przez *Microsoft*,
- Posiada wbudowany serwer *LDAP*
  - Własna implementacja serwera *LDAP,*
  - Możliwa, poprzez odpowiednią zmianę konfiguracji, do zastąpienia przez serwer oparty o *OpenLDAP*

Pobranie Samby

- Sambę v.4 można pobrać ze strony projektu za pomocą:

wget http://www.samba.org/samba/ftp/samba4/samba-4.0.0alpha11.tar.gz

lub:

git clone git://git.samba.org/samba.git samba-master.

- W przypadku wykorzystania programu *git* zostaje pobrana pełniejsza wersja zawierająca również źródła dla wersji 3.
- Możliwa jest kompilacja w trybie *merged*, co umożliwia później uruchomienie Samby w dwóch wersji jednocześnie.
- Raczej nie występują pakiety binarne zawierające Sambę w tej wersji.

Kompilacja i instalacja Samby

- Przed przystąpieniem do kompilacji konieczne jest doinstalowanie odpowiednich pakietów*;* w przypadku RH są to:
  - Wersje deweloperskie pakietów: libacl-devel, gnutls-devel, readline-devel python-devel oraz e2fsprogs-devel
  - Pakiet autoconf – potrzebny do uruchomienia skryptu *autogen.sh* generującego plik *configure*.
- Kompilacja i instalacja *Samby:*

```
[root@dns1 ~]# tar –xzf /samba-4.0.0alpha11.tar.gz
[root@dns1 ~]# cd samba-4.0.0alpha11/source4
[root@dns1 source4]# ./autogen.sh
[root@dns1 source4]# ./configure
[root@dns1 source4]# ./make
[root@dns1 source4]# ./make install
```

Provision Samba v.4

- Po wykonaniu instalacji domyślnie trafia ona do katalogu */usr/local/samba*
- Krok zwany *provision* powoduje wygenerowanie:
  - Bazy danych zawierających potrzebną strukturę dla *LDAP,*
  - Podstawowych użytkowników i wpisanie ich do *KDC,*
  - Pliku strefy dla domeny zawierającego rekordy *SRV* wskazujące na lokalizację usług w domenie *Active Directory* (Kerberos, LDAP),
  - Wygenerowanie pliku konfiguracyjnego *krb5.conf* dla klienta opisującego lokalizację *KDC.*
- Uruchomienie skryptu *provision* z katalogu instalacyjnego w celu utworzenia struktury kontrolera domeny *AD*

```
[root@dns1 source4]# ./setup/provision – –domain=KRAKOW \
– –realm=krakow.filemon.wszib.edu.pl – –adminpass=Ala1234 \
– –server-role=‘domain controller’
```

Uruchomienie Samby

- Wygenerowane przez *provision* pliki trafiły do */usr/local/samba/private.*
- Przed uruchomieniem *Samby* konieczne jest skonfigurowanie serwera *DNS* dla domeny *AD*

  Wygenerowany plik strefy zawiera rekordy srv lokalizujące usługi.
- Uruchomienie *Samby* tak by wypisywała komunikaty na ekranie i wykorzystywała pojedynczy proces:

```
[root@dns1 ~]# /usr/local/samba/sbin/samba –i –M single
```

- Uruchomienie *Samby* powoduje automatycznie uruchomienie wbudowanych serwerów usług *LDAP* i *Kerberos*; co można sprawdzić poleceniem *netstat.*

Testowanie Samby

- Oprócz standardowych programów do testowania *Samby* opisanych dla wersji trzeciej możliwe jest również:
  - Testowanie serwera *LDAP* poprzez wypisanie zawartości jego bazy za pomocą narzędzia *ldapsearch,*
  - Testowanie *KDC* poprzez pobranie biletu *TGT* dla *Administratora* domeny (zdefiniowanego przez skrypt *provision*) – program *kinit.*
- W celu usprawnienia funkcjonowania narzędzi klienckich dla *Kerberosa* i *LDAPa* konieczne jest zdefiniowanie odpowiednich atrybutów w plikach */etc/krb5.conf* oraz */etc/ldap.conf*

Zarządzanie użytkownikami

- Zarządzanie użytkownikami, politykami grupowymi itp. można wykonywać z komputera z systemem klienckim *Windows* za pomocą odpowiedniej przystawki; w tym celu:
  1. Ze strony *www.microsoft.com* należy pobrać *Remote Server Administration Tools* dla odpowiedniej wersji systemu (np. w7),
  2. Zainstalować na komputerze klienckim to oprogramowanie,
  3. W ustawieniach własności *menu Start* odblokować ukrywanie narzędzi administracyjnych,
  4. Zalogować się na komputerze klienckim (podłączonym uprzednio do domeny *AD*) jako *Administrator* domeny *AD*,
  5. Uruchomić odpowiednie narzędzie do zarządzania użytkownikami czy politykami grupowymi w domenie *AD*.

Współpraca Linuksa z Sambą

- Samba w wersji 4 obsługuje w pełni protokół *Kerberos* oraz *LDAP*, więc nic nie stoi na przeszkodzie aby użytkownicy systemu *Linux* mogli się w niej uwierzytelniać i autoryzować. W tym celu należy:
  1. Na komputerze klienckim skonfigurować odpowiednio pliki */etc/krb5.conf* i */etc/ldap.conf*, by wskazywały lokalizację serwerów
  2. Skonfigurować plik */etc/nsswitch.conf* by pobierać informację o użytkowniku z wykorzystaniem protokołu *LDAP*,
  3. Ustawić w *PAM* uwierzytelnianie użytkownika przy użyciu protokołu *Kerberos*,
  4. Dodać odpowiednie rekordy do bazy *LDAP* opisujące użytkownika linuksowego – wymagane pola dla obiektu klasy *PossixAccount*