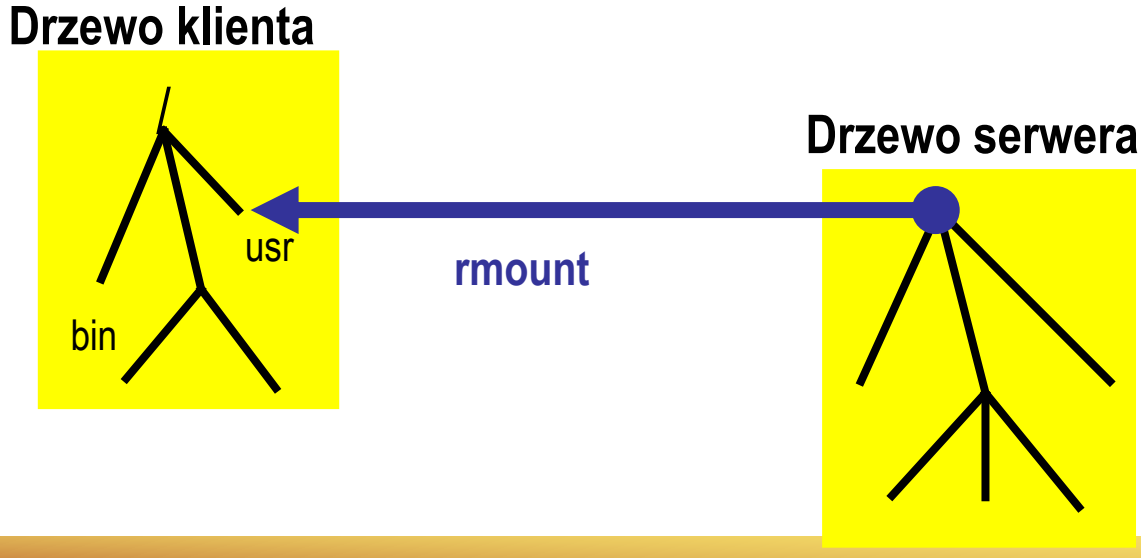
Udostępnianie zasobów – serwer SAMBA i NFS

Wprowadzenie do serwera Samba, NFS

- Wprowadzenie do serwera Samba, NFS
- Instalacja
- Konfiguracja
- Udostępnianie zasobów
- Uprawnienia do zasobów

Wprowadzenie do serwera Samba, NFS

- NFS
  - Bezpośrednie udostępniane
  - Udostępnione zasoby dostępne poprzez mount
  - NFS jest serwisem RPC więc wymaga portmap



Instalacja

- NFS
  - instalacja nfs-utils i portmap

    apt-get install nfs-kernel-server

Udostępnianie zasobów

- NFS
  - /etc/exports
  - ścieżka do zasobu
  - uprawniania i opcje

    $katalog $klient1($opcja1,$opcja2,...)
    $klient2($opcja1,$opcja2,...)

    /srv/pub 192.168.0.1(ro) 192.168.0.2(rw)
    /home 192.168.0.0/255.255.255.0(rw)

Uprawnienia do zasobów

- NFS
  - Bezpieczeństwo
    - iptables, portmap – odpowiednie porty
    - tcp_wraapers – portmap
  - Uprawnienia i opcje
    - ro – read only
    - rw – read/write
    - root_squah – zabrania dostępu jako root

Wprowadzenie do serwera Samba, NFS

- Samba
  - Samba to zbiór aplikacji funkcjonujących w systemie unix (linux) rozumiejących protokół SMB (*Server Message Block*). Udostępnione zasoby dostępne poprzez mount
  - Możliwa komunikacja protokołem Microsoft
  - Autentykacja i autoryzacja użytkowników
  - Udostępnienie drukarek i plików
  - rozwiązywanie nazw
- iptables
  - nmbd – 137/udp, 138/udp
  - smbd – 139/tcp, 445/tcp

Wprowadzenie do serwera Samba, NFS

- Samba

smbd – demon odpowiedzialny za zarządzanie zasobami współdzielonymi przez serwer i jego klientów.

nmbd - to prosty serwer odpowiadający za kontrolę mechanizmu nazw SMB. Jego rola polega na oczekiwaniu na żądania klientów i udzielania odpowiednich informacji.

smbclient – program uruchamiany z linii poleceń. Umożliwia połączenie z zasobami Samby.

smbstatus – wyświetla bieżące połączenia sieciowe z zasobami Samby.

smbtar - służy do tworzenia kopii zapasowych udziałów.

smbpasswd – pozwala na zmianę zaszyfrowanych haseł Samby.

nmblookiup – umożliwia sprawdzenie nazw NetBIOS-owych.

testparm – bardzo przydatny program sprawdzający poprawność pliku konfiguracyjnego.

testprns – program umożliwiający sprawdzenie czy drukarki są rozpoznawalne przez demona *smb*

Instalacja

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

Konfiguracja

- /etc/samba/smb.conf
  - sekcje
    - [global] – sekcja określająca ustawienia globalne
    - [homes] – dostęp do katalogu domowego dla danych użytkowników lub wszystkich
    - [printers] – definiuje drukarki
  - testparm – sprawdza poprawność wpisów (syntax)

Konfiguracja

- Użytkownicy
  - wymagane hasło
  - smbpasswd –a użytkownik
  - modyfikacja użytkowników smbpasswd

Udostępnianie zasobów

- Opcje udostępnienia plików i katalogów
  - path – ścieżka udostępnianego zasobu
  - public – zasób może być czytany przez guest
  - browsable – lista zasobów
  - writable – zasób do odczytu i zapisu
  - printable – drukarka nie dysk
  - group – wszystkie połączenia z określonej grupy

```
# udostępniony zasób
[test_share]
comment = plik test
path = /home/test
public = no
writable = yes
printable = no
```

Uprawnienia do zasobów

- Mechanizm zmiennych – określa charakterystykę klientów (% litera)
  - %I - adres IP klienta
  - %m - nazwa NetBIOS klienta
  - %M - nazwa DNS klienta
  - %H - katalog macierzysty zalogowanego użytkownika
  - (%u) %u - nazwa zalogowanego użytkownika
  - %S - nazwa bieżącego udziału
  - %L - nazwa NetBIOS serwera na którym uruchomiona jest Samba

  [pliki] path = /export/samba/%M

  katalog udostępniany przez udział pliki będzie zależał od wartości zmiennej %M a więc od nazwy DNS klienta.

Uprawnienia do zasobów

- Wskazanie konkretnych użytkowników

[finanse] path=/export/samba/finanse

writable = yes

guest ok = no

valid users = szef

Adam Dobrze

Uprawnienia do zasobów

- Strona klienta
  - Sprawdzenie połączenia
    - smbclient –L nazwa_serwera
    - smbclient://nazwa_serwera/zasób
  - mount lub /etc/fstab
    - mount –t smbfs –o guest //serwer/legal /mnt/smb

Metody autentykacji użytkowników

- Autoryzacja PAM
- autoryzacja użytkownika (login, hasło)
- autoryzacje użytkowników wielu domen
- serwer smb
- dostęp anonimowy

Konfiguracja list ACL

- Listy kontroli dostępu
- Konfiguracja w dwóch krokach
  - definicja elementu ACL

  składnia:

  acl nazwa_elementu typ_elementu argument_lub_argumenty

  acl lokalna src 192.168.192.0/255.255.255.0
  - dodanie elementu do listy

  składnia:

  nazwa_listy allow|deny element1 element2 ...

  http_access allow lokalna
- Sprawdzanie według kolejności lub łączone

  acl serwer dst 212.191.65.6/255.255.255.255

  acl lokalna src 192.168.192.0/255.255.255.0

  http_access deny serwer lokalna

Konfiguracja list ACL

- Typy elementów ACL
  - src – source klienta
  - dst – destination ip serwera
  - dstdomain – nazwa domenowa serwera
  - srcdom_regex – dopasowuje nazwę domenową klienta
  - dstdom_regex – dopasowuje nazwę domenową serwera
  - port – port docelowy
  - proto –protokół
  - method – metoda HTTP (post, get itp.)
  - maxconn – limit połączeń z jednego adresu IP

Konfiguracja list ACL

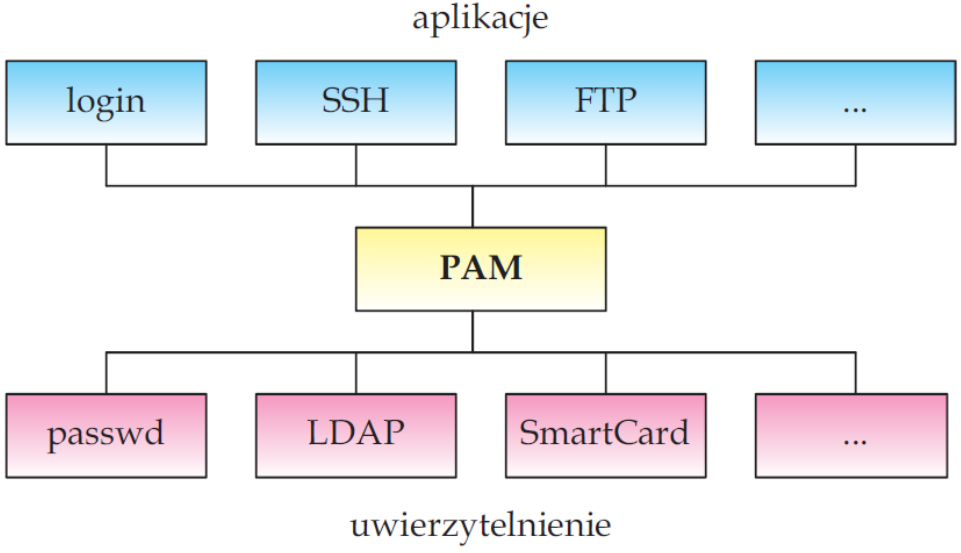
- Najważniejsze listy
  - http_access – lista zezwalająca na połączenia www
  - no_cache – co nie powinno być keszowane
  - redirector_access – co powinno być przekierowane
  - deny_info – strona błędu po zablokowaniu dostępu

Autentykacja PAM

- Wprowadzenie do PAM
- Instalacja i konfiguracja
- Moduły systemu PAM

Wprowadzenie do PAM

- **PAM** (*Pluggable Authentication Modules*) to system uwierzytelniania użytkowników



Wprowadzenie do PAM

- Oddzielna konfiguracja dla każdej usługi
- Kompilacja z użyciem bibliotek PAM
- Oddzielne pliki konfiguracyjne

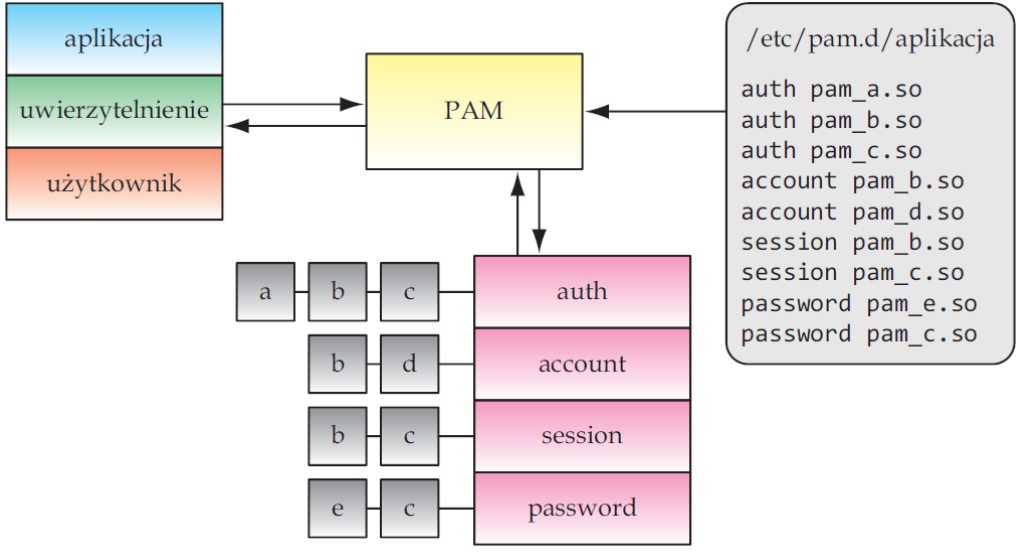
  /etc/pam.d/ login

  /etc/pam.d/ samba

  /etc/pam.d/ xscreensaver
- Wspólny system uwierzytelniania
- Równoległe korzystanie z innych sposobów

Wprowadzenie do PAM

- Komunikacja z PAM
- Określenie sposobu autentykacji
- Określenie modułów w procesie

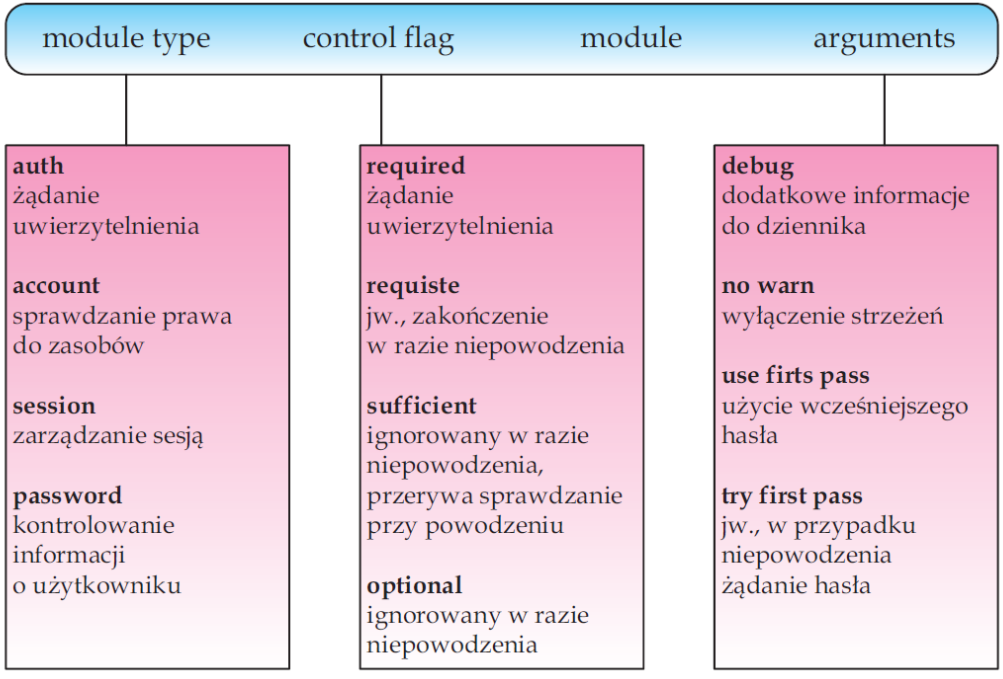


Instalacja i konfiguracja

- Konfiguracja PAM
  - /etc/pam.d – plik konfiguracyjny
- testy są podzielone na grupy
  - auth – autentykacja użytkownika
  - account – autoryzowane konta, które mogą być używane
  - password – kontrola zmiany hasła
  - session – otwieranie, zamykanie i logowanie sesji
- Każda grupa jest wywoływana w razie potrzeby i dostarcza oddzielny rezultat do serwisu

Instalacja i konfiguracja

- Wartości kontrolne



Instalacja i konfiguracja

- Przykładowy plik : /etc/pam.d/login

```
auth       optional   pam_faildelay.so  delay=3000000
auth [success=ok new_authtok_reqd=ok ignore=ignore user_unknown=bad default=die] pam_securetty.so
auth       requisite  pam_nologin.so
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so close
session       required   pam_env.so readenv=1
session       required   pam_env.so readenv=1 envfile=/etc/default/locale
@include common-auth
auth       optional   pam_group.so
session    required   pam_limits.so
session    optional   pam_lastlog.so
session    optional   pam_exec.so type=open_session stdout /bin/uname -snrvm
session    optional   pam_motd.so
session    optional   pam_mail.so standard
session    required     pam_loginuid.so
@include common-account
@include common-session
@include common-password
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so open
```

Moduły systemu PAM

- Moduły PAM
  - **auth** – uwierzytelnianie użytkownika (czy jest tym za kogo się podaje, ewentualnie przyznanie członkostwa innej grupy),
  - **account** – sprawdzanie uprawnień do zasobów i usług (ważne konto, dostęp w czasowy, lokalizacja),
  - **session** – zarządzanie sesją, zadania które należy wykonać dla użytkownika zanim będzie mógł uzyskać dostęp do usługi (montownie zasobów i urządzeń, otwieranie i zamykanie plików, zmienne środowiskowe),
  - **password** – uaktualnianie baz danych o użytkownikach (hasła, listy uprawnień).

Control flag wskazuje jak PAM będzie reagować rezultat pracy modułu

Moduły systemu PAM

- Przykładowe moduły PAM
  - **pam_cracklib** eliminuje słabe hasła
  - **pam_deny** realizuje odmowę dostępu
  - **pam_ftp** obsługuje anonimowe ftp
  - **pam_group** przydziela do grup użytkowników
  - **pam_limits** ogranicza dostęp na podstawie dostępnych zasobów
  - **pam_listfile** reguluje dostęp na podstawie list użytkowników
  - **pam_tally** realizuje odmowę dostępu w zależności od liczby nieudanych logowań
  - **pam_unix** realizuje standardowe uniksowe zarządzanie uwierzytelnieni
  - **pam_warn** moduł logujący informacje do dziennika
  - **mod_auth** pam moduł uwierzytelnienia dla serwera Apache,
  - **pam_smb** grupa modułów współpracujących z serwerem Samba
  - **pam_mysql** uwierzytelnienie na podstawie bazy danych MySQL
  - **pam_ldap** współpraca z serwisem LDAP
  - **pam_proftpd** uwierzytelnienie dla serwera ProFtpd

Klient LDAP

Klient LDAP

- Wprowadzenie do LDAP
- Użycie klienta LDAP

Klient LDAP - Wprowadzenie do LDAP

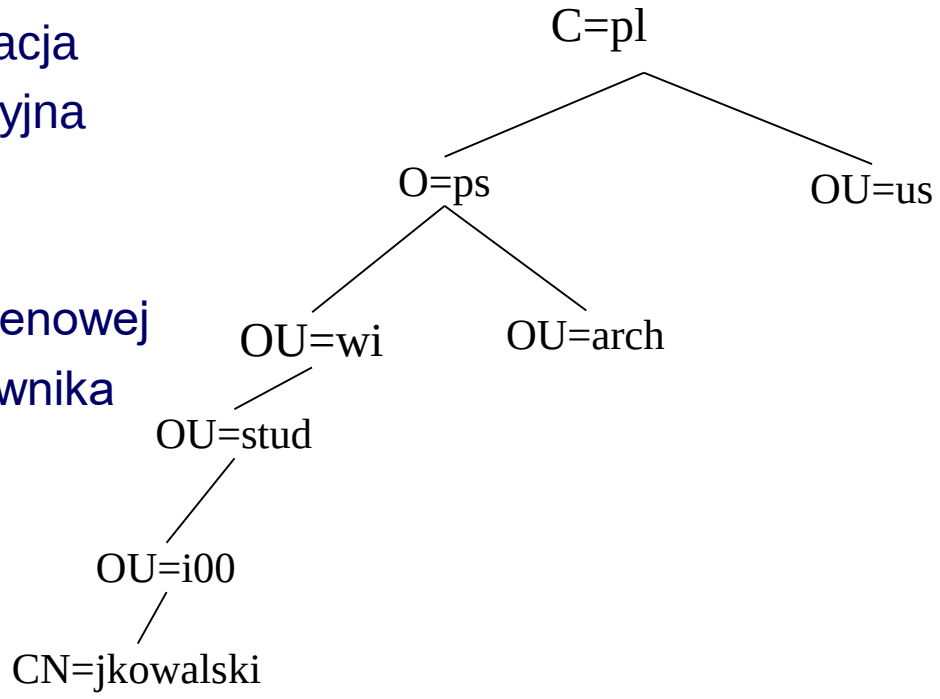
- **Lightweight Directory Access Protocol** (**LDAP**) – protokół przeznaczony do korzystania z usług katalogowych, bazujący na standardzie X.500
- Dane w strukturze drzewa
- Funkcje protokołu
  - bind – uwierzytelnianie
  - unbind – zakończenie sesji
  - serch - zgłoszenie żądania poszukiwanego zasobu,
  - *add* – daje klientowi możliwość zgłoszenia żądania dodania wpisów do katalogu
  - *delete* – umożliwia klientowi żądanie usunięcia wpisów z katalogu

Klient LDAP - Wprowadzenie do LDAP

- Jasno określone API (umożliwiające korzystanie z usług z poziomu dowolnego języka)
- Łatwość użycia
- Dużo dostępnych narzędzi
- Dobra integracja z innymi produktami

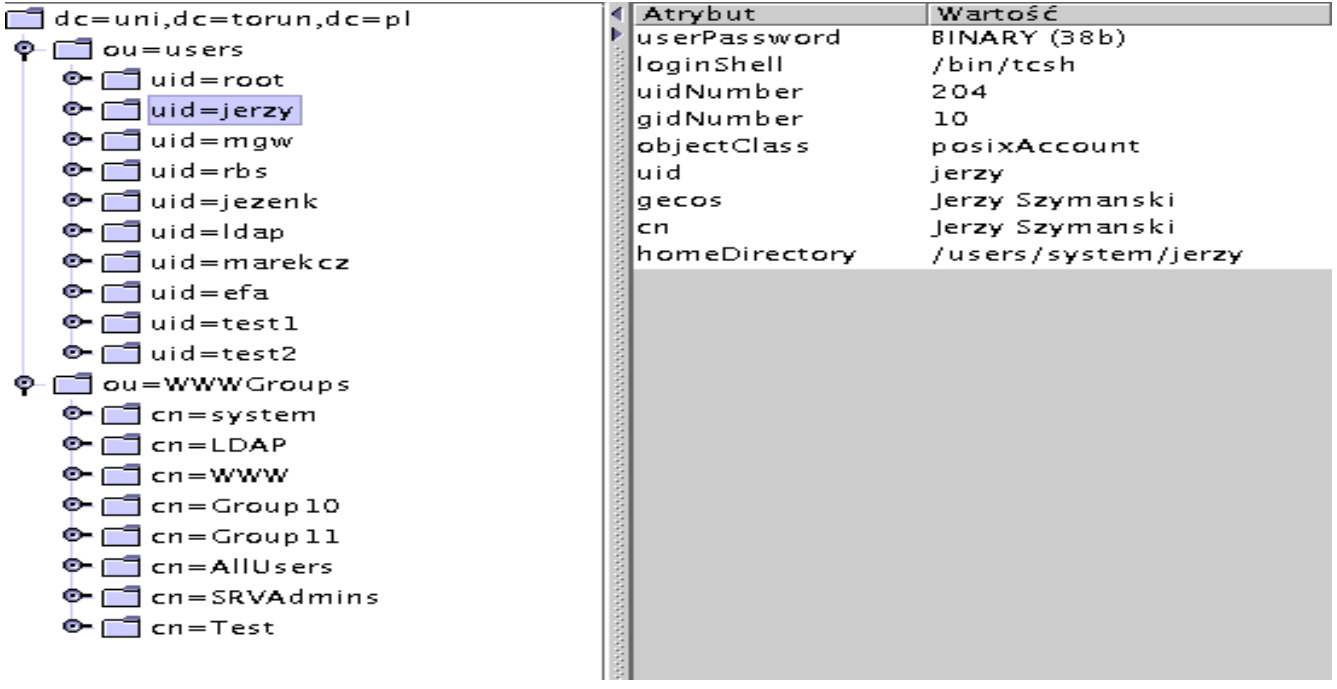
Klient LDAP - Wprowadzenie do LDAP

- C – Kraj
- O – jednostka lub organizacja
- OU – jednostka organizacyjna
- CN – imię
- SN - nazwisko
- DC – składnik nazwy domenowej
- UID – identyfikator użytkownika



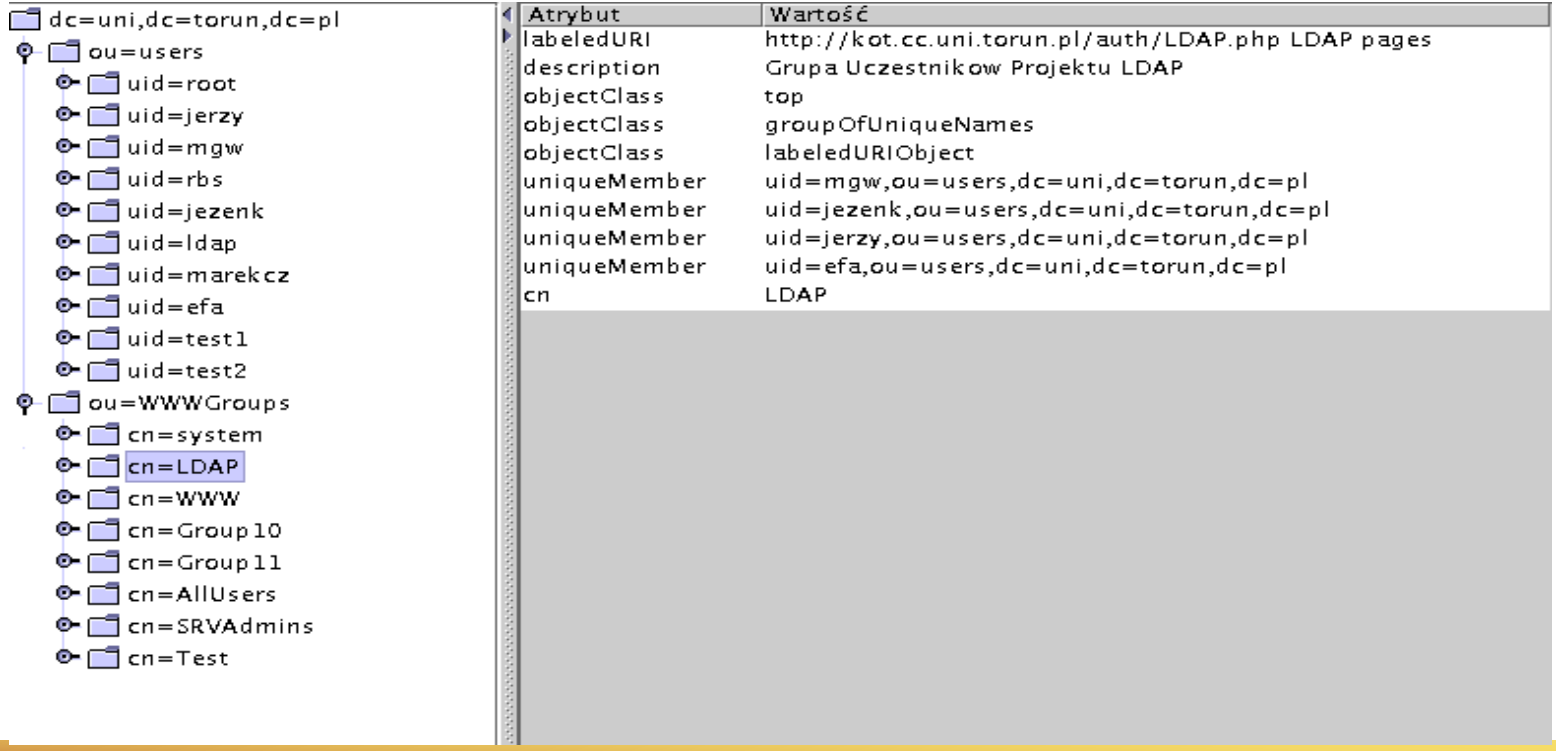
Klient LDAP

- Schemat bazy LDAP użytkownicy



Klient LDAP

- Schemat bazy LDAP grupy



Klient LDAP – użycie klienta

- **Uwierzytelnianie**
  - **anonimowe** – wbudowany użytkownik guest
  - **hasło** – DN, hasło
  - **SSL** – wymiana certyfikatów
  - **PROXY** - wykorzystywane przez aplikację, która uwierzytelnia się na hasło użytkownika PROXY,

KONIEC