Systemy Operacyjne

Zarządzanie/Administracja Systemem

“Zarządzanie użytkownikami”

autor: mgr inż. Andrzej Woźniak

Plan wykładu

- Pojęcia podstawowe
- Pojedynczy komputer
- Sieć komputerowa
- Usługi katalogowe
- Podstawowe zasady

Konto użytkownika

- konta bezosobowe (serwis, deamon)
- konta systemowe (system, root)
- konta administracyjne (admin, root, administrator, supervisor)
- konta gości (guest)
- konta lokalne (osobne na każdym komputerze)
- konta sieciowe (jedno dla wszystkich komputerów w sieci)

Grupy użytkowników

- grupy wbudowane
- grupy dynamiczne
- grupy lokalne
- grupy globalne

Profil / katalog domowy

- Profil – ustawienia systemowego środowiska pracy użytkownika
  - profil lokalny
  - profil mobilny
  - profil obowiązkowy (mandatory)
- Katalog domowy (Home dir) – domyślne miejsce przechowywania dokumentów, plików konfiguracyjnych aplikacji

Skrypty logowania

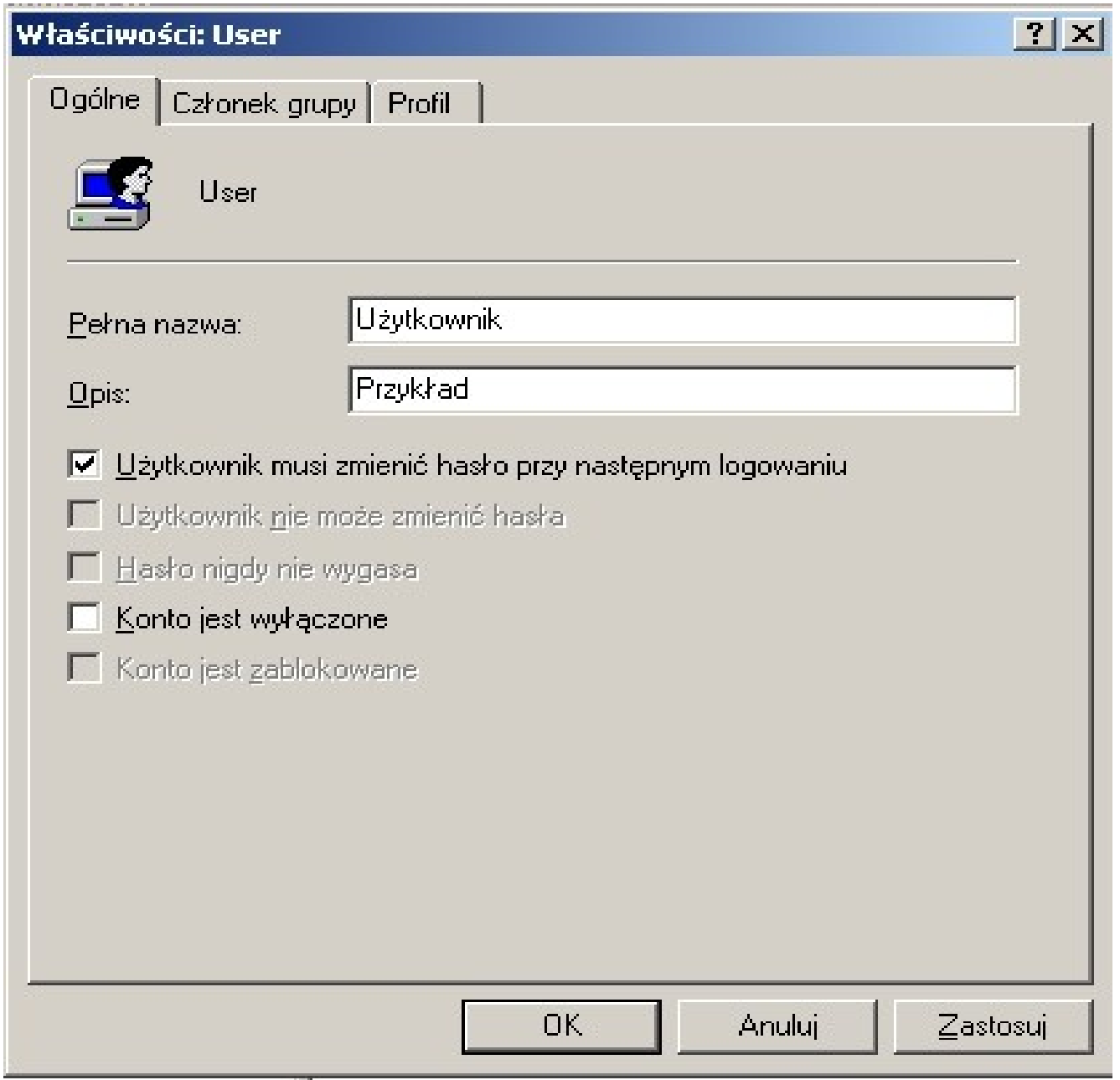
- Ciąg poleceń systemowych wykonywanych przez znakowy interpreter poleceń podczas logowania użytkownika
- Służy do ustawiania tych elementów środowiska pracy użytkownika, których nie zapamiętuje profil

Szablony użytkowników

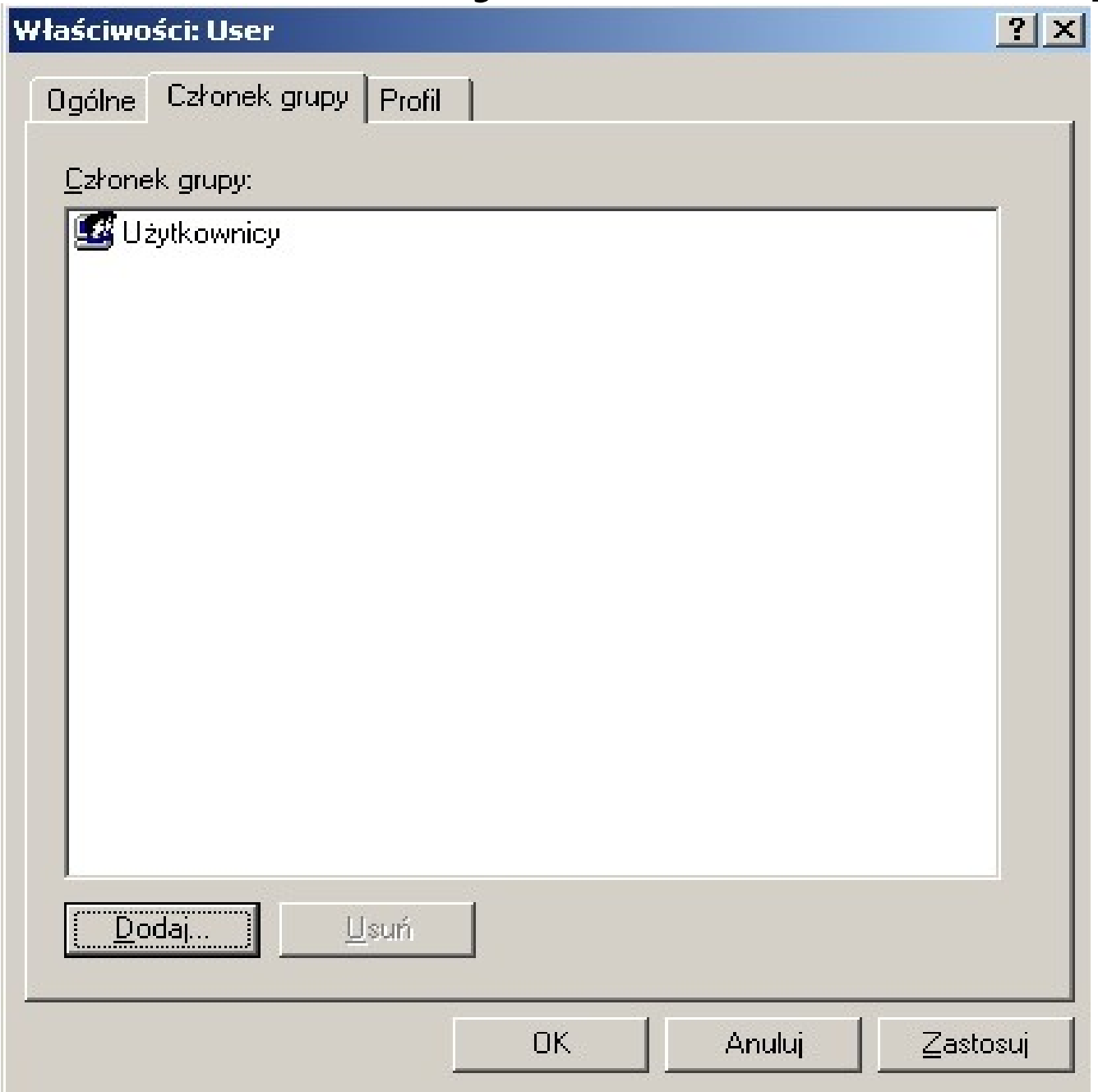
- Wzór ustawień dla konta użytkownika
- Pozwalają na szybkie zakładanie użytkowników

Administracja użytkownikami na pojedynczym komputerem

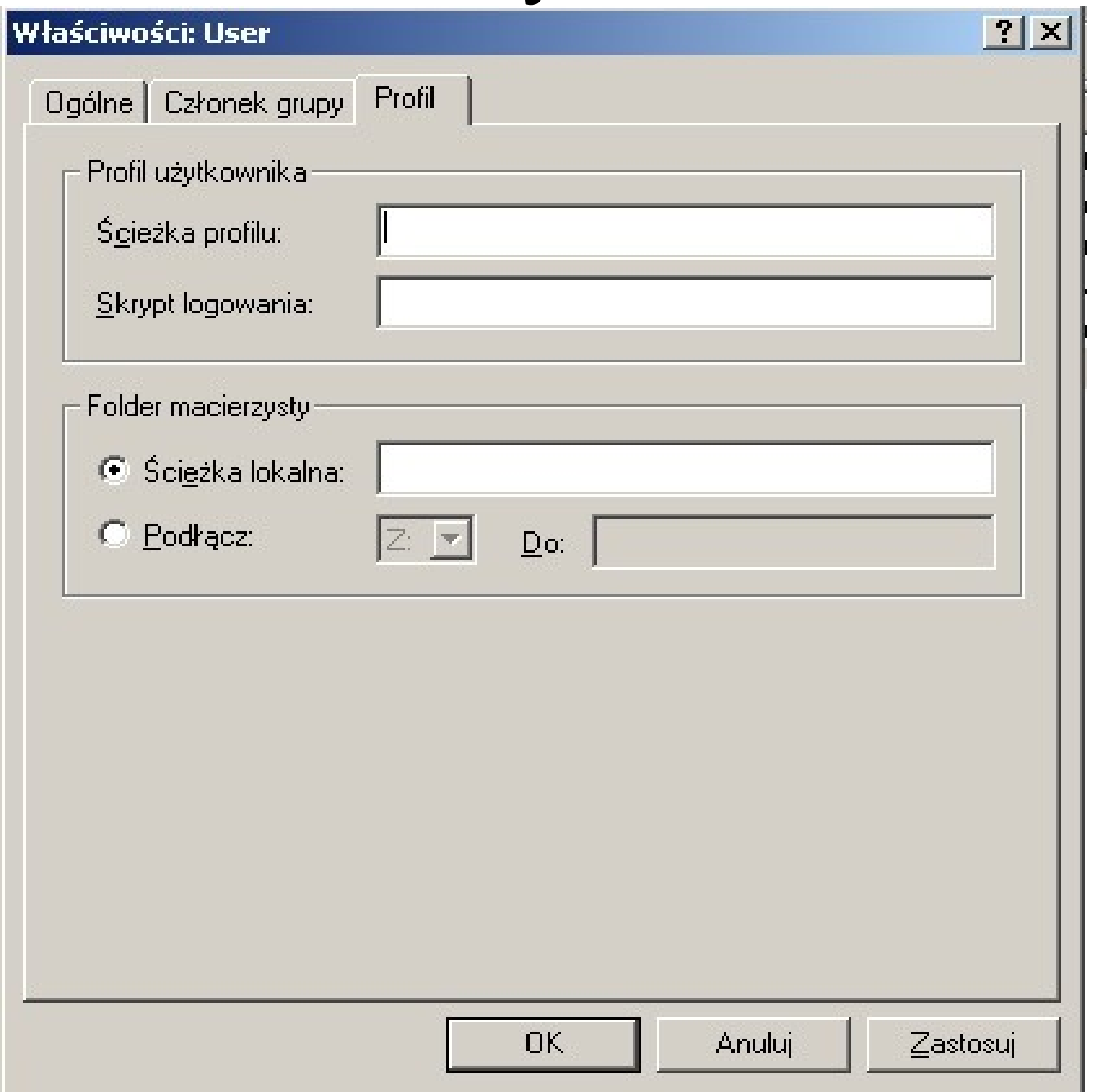
Windows Użytkownik - ogólne



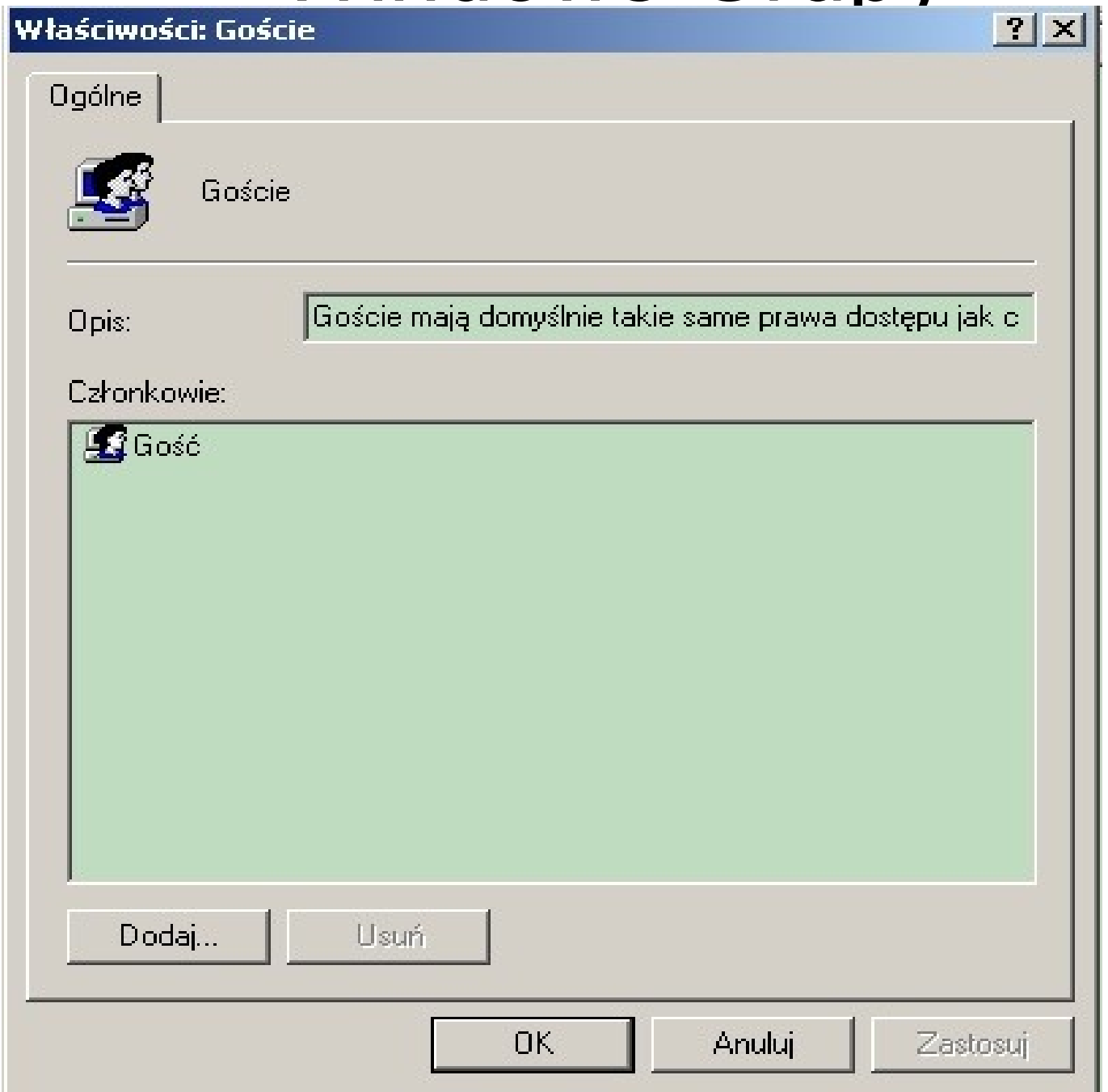
Windows Użytkownik - Grupy



Windows Użytkownik - Profil



Windows Grupy



Unix Użytkownik c.d.

- Pola oddzielane znakiem “:”
  - name- Nazwa użytkownika (login name)
  - passwd - hasło
  - uid - Identyfikator użytkownika
  - gid - Identyfikator podstawowej grupy
  - comment - Opis użytkownika
  - dir - Katalog domowy
  - shell - Interpreter poleceń

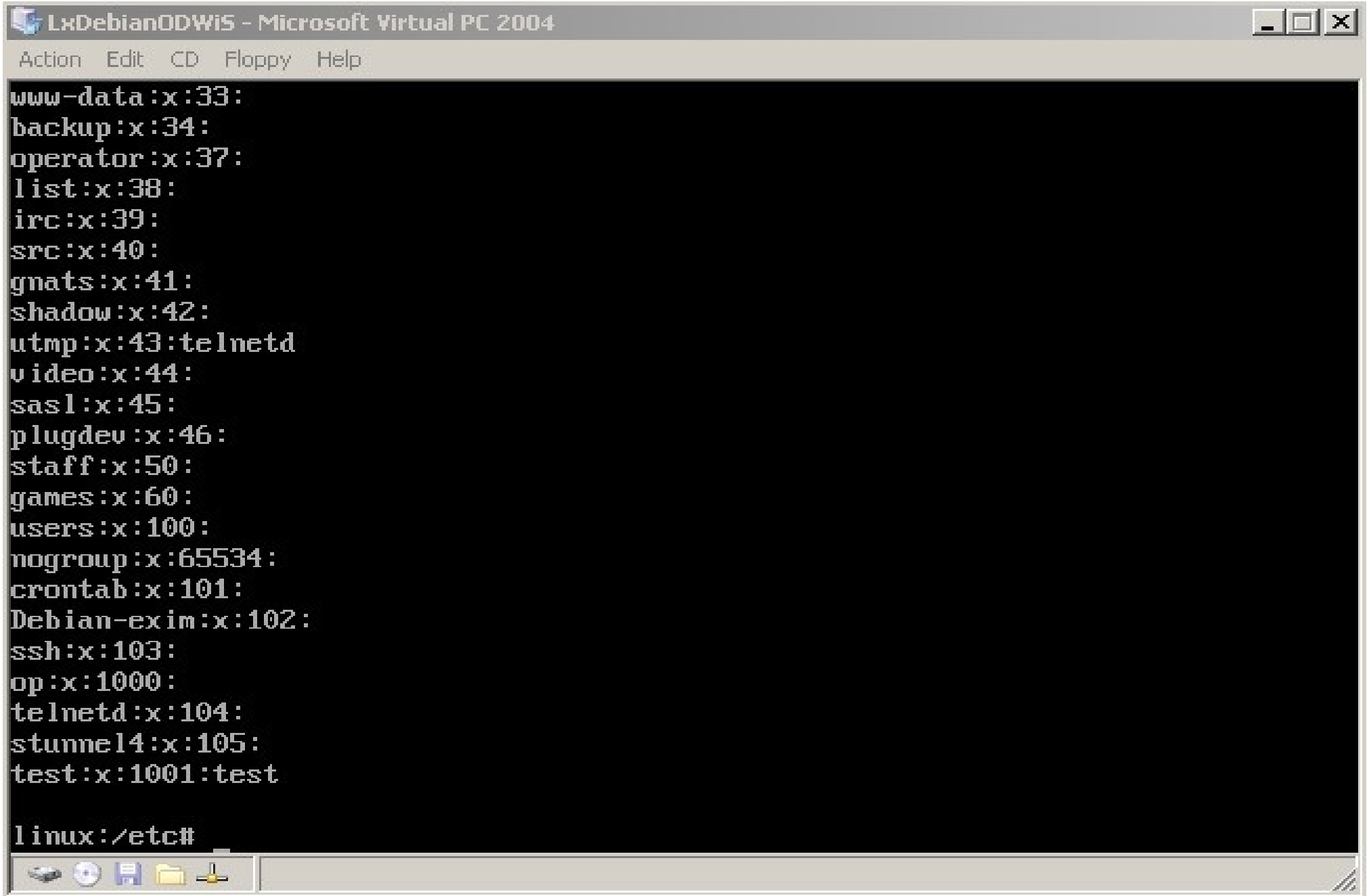
Unix Użytkownik

```
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
Debian-exim:x:102:102::/var/spool/exim4:/bin/false
identd:x:100:65534::/var/run/identd:/bin/false
sshd:x:101:65534::/var/run/sshd:/bin/false
op:x:1000:1000:Operator systemu:/home/op:/bin/bash
telnetd:x:104:104::/nonexistent:/bin/false
stunnel4:x:105:105::/var/run/stunnel4:/bin/false
test:x:1001:1001:Test TT,1,23,123,09?:/home/test:/bin/bash
linux:~#
```

Unix Grupy

- Pola oddzielane znakiem “:”
  - nazwa grupy
  - hasło
  - GID – Identyfikator grupy
  - Lista członków

Unix Grupy c.d.



Miejsce przechowywania

- Windows
  - %SYSTEM_ROOT%\system32\config\Sam
- Unix
  - /etc/passwd
  - /etc/shadow
  - /etc/group

Katalog - Directory

- specyficzna baza danych przechowująca obiekty takie jak:
  - użytkownicy,
  - grupy,
  - komputery,
  - drukarki,
  - ....
- częściej czytana niż zapisywana

Usługi Katalogowe
Directory Services

- Katalog wraz z oprogramowaniem umożliwiającym:
  - lokalizowanie (wyszukiwanie),
  - zarządzanie,
  - administrowanie,
  - organizowanie w jednostki logiczne

X.500

- Pierwszy standard usług katalogowych opracowany przez ITU (International Telecommunication Union) i ISO (International Organization for Standardization)
- skomplikowany i restrykcyjny w implementacji

LDAP
Light-weight Directory Access Protocol

- Uproszczony standard usług katalogowych opracowany przez IETF (Internet Engineering Task Force):
- Bazuje na X.500, ale stosuje uproszczone protokoły
- używa protokołu komunikacyjnego TCP/IP

Kategoria Obiektu
Object Class

- Definiuje jakie informacje o obiekcie (atrybuty obiektu):
  - obowiązkowe, które muszą być zawarte w każdym wpisie tego typu w katalogu,
  - opcjonalne, które mogą być zawarte we wpisie tego typu w katalogu.

Plan Katalogu
Directory Schema

- Kompletny zbiór kategorii obiektów oraz ich atrybutów

Składnia Atrybutu
Attribute Syntax

- Każdy atrybut przechowuje dane określonego typu,
- Zakres danych może być ograniczany regułami weryfikacji zawartości (np. napis z cyfr),
- Drugi zestaw reguł określa jak operować wartością atrybutu przy porównaniach (np. porównuj jako tekst, ignoruj wielkość znaków).
- Typ danych jest jednoznacznie identyfikowany na podstawie identyfikatora ASN.1

Typy atrybutów

- CN - Common Name
- L - Locality Name
- ST - State or Province Name
- O - Organization Name
- OU - Organizational Unit Name
- C - Country Name
- STREET - Street Address
- DC - Domain Component
- UID - Userid

5 podstawowych cech LDAP

- Zoptymalizowane pod kątem odczytu,
- Struktura hierarchiczna,
- Informacja przechowywana jest jako wartość atrybutów,
- Tworzy jednolitą przestrzeń nazw dla wszystkich obiektów, dla których przechowuje informacje,
- Umożliwia replikację informacji

LDIF
LDAP Data Interchange Format

- Tekstowy format wymiany danych pomiędzy katalogami LDAP
- Umożliwia opisanie struktury katalogu oraz wpisów

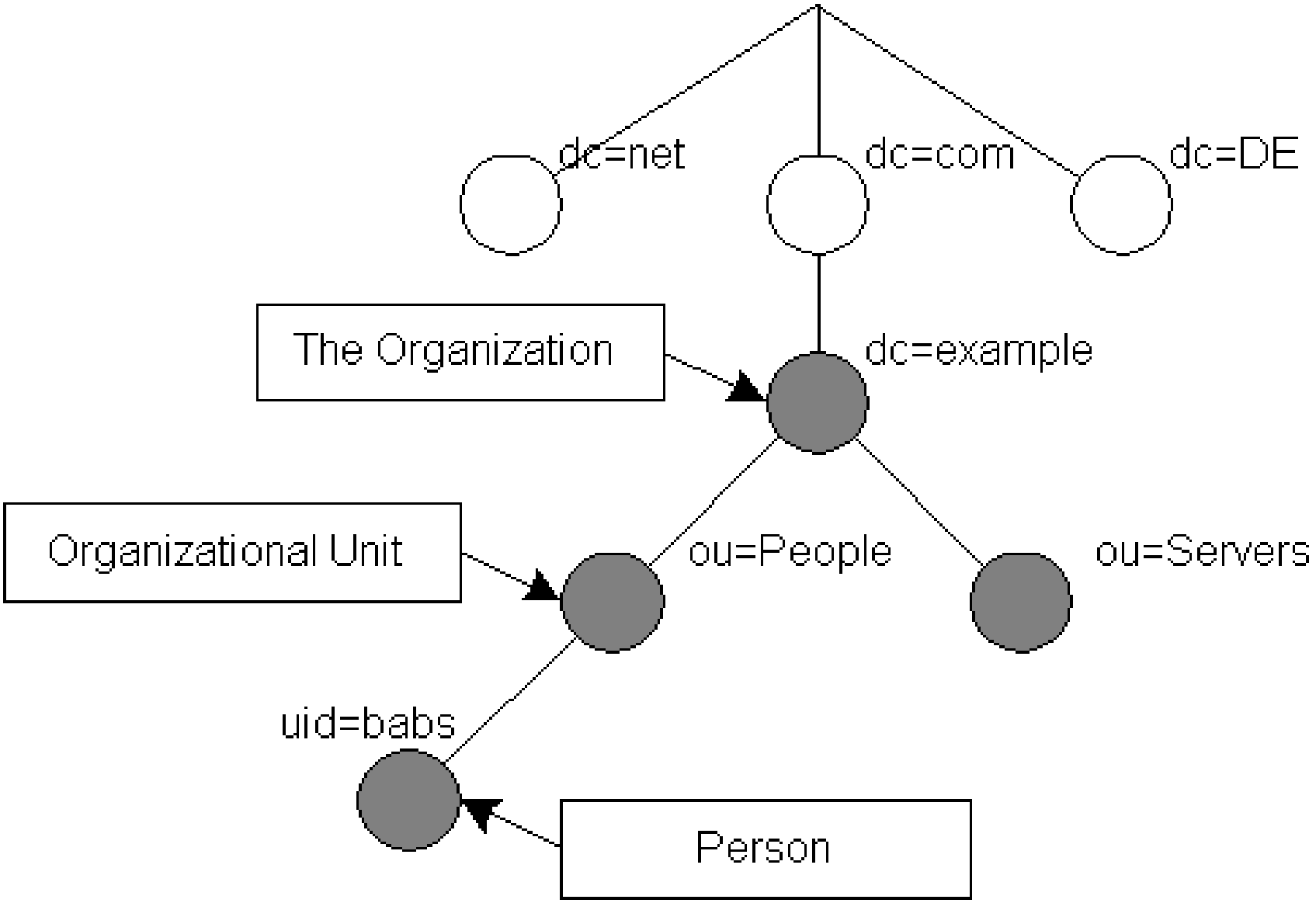
Model informacji LDAP
LDAP information model

- Definiuje rodzaj danych przechowywanych w katalogu
- Definiuje podstawową jednostkę informacji jako wpis (entry)
- Wpis to zbiór informacji o obiekcie, składa się z jednego lub więcej atrybutów
- Każdy atrybut ma typ i jedną lub więcej wartości

Model nazewnictwa LDAP
LDAP naming model

- Definiuje jak dane są zorganizowane w Katalogu i jak aplikacje odwołują się do katalogu
- Wpisy są zorganizowane w strukturze hierarchicznej odwróconego drzewa
- Korzeń drzewa nie jest przeznaczony do przechowywania danych
- Nazwy są uporządkowane w porządku odwrotnym

Przykład drzewa



Nazwy wpisu

- RDN – Relatywna Nazwa Identyfikująca (Relative Distinguished Name)
- DN – Unikalna Nazwa Identyfikująca (Distinguished Name)
- Przykład
- RDN wpisu uid=babs
- DN wpisu uid=babs,ou=People,dc=example,dc=com

Przykłady Usług Katalogowych LDAP

- Netscape Directory Server
- SUN ONE Directory Server
- Microsoft Active Directory
- IBM Directory Server
- Novell eDirectory (NDS)
- Oracle Internet Directory
- OpenLDAP

Active Directory (AD)

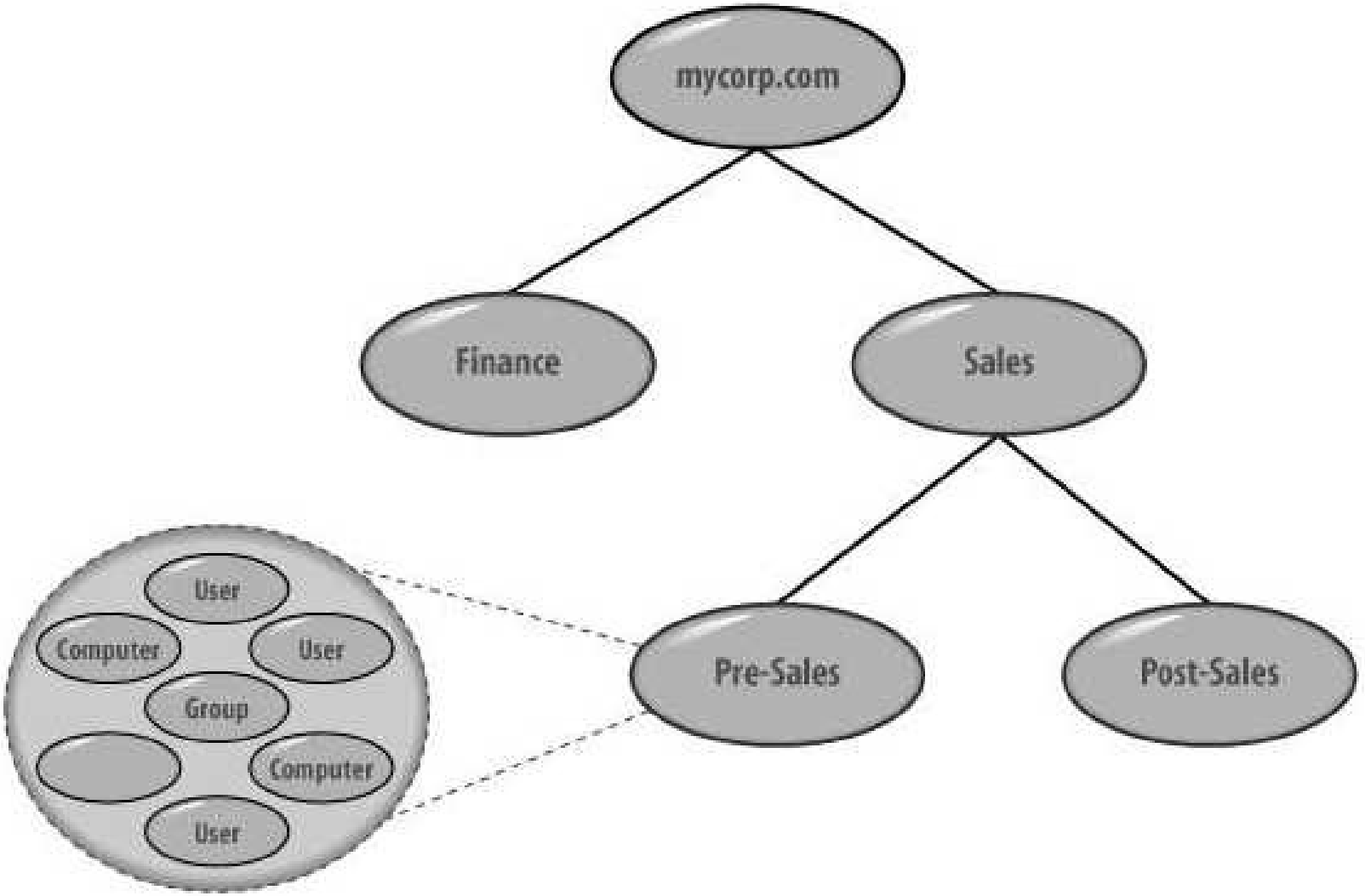
- Implementacja LDAP w systemie operacyjnym Microsoft Windows 2000 i 2003.
- Bazuje na bazie danych ESE (Extensible Storage Engine) o pojemności milionów obiektów i maksymalnej wielkości 16 TB.

Obiekty w AD

Dwa rodzaje obiektów:

- kontener (container node)
- niekontener (liść - leaf node)

Hierarchia obiektów



Identyfikacja Obiektów w AD

- Każdy obiekt w AD posiada GUID - Globalnie Unikalny Identyfikator (Globally Unique Identifier)
- GUID to 128 bitowa liczba
- GUID obiektu nie zmienia się
- GUID jest trudny do zapamiętania
- ADsPaths zgdony z LDAP

ADsPaths Przykład

- ADsPaths

LDAP://cn=Woźniak Andrzej, cn=Wykładowcy, ou=WEiI, dc=tu, dc=koszalin, dc=pl

- DN
- cn=Woźniak Andrzej, cn=Wykładowcy, ou=WEiI, dc=tu, dc=koszalin, dc=pl
- RDN
- cn=Woźniak Andrzej

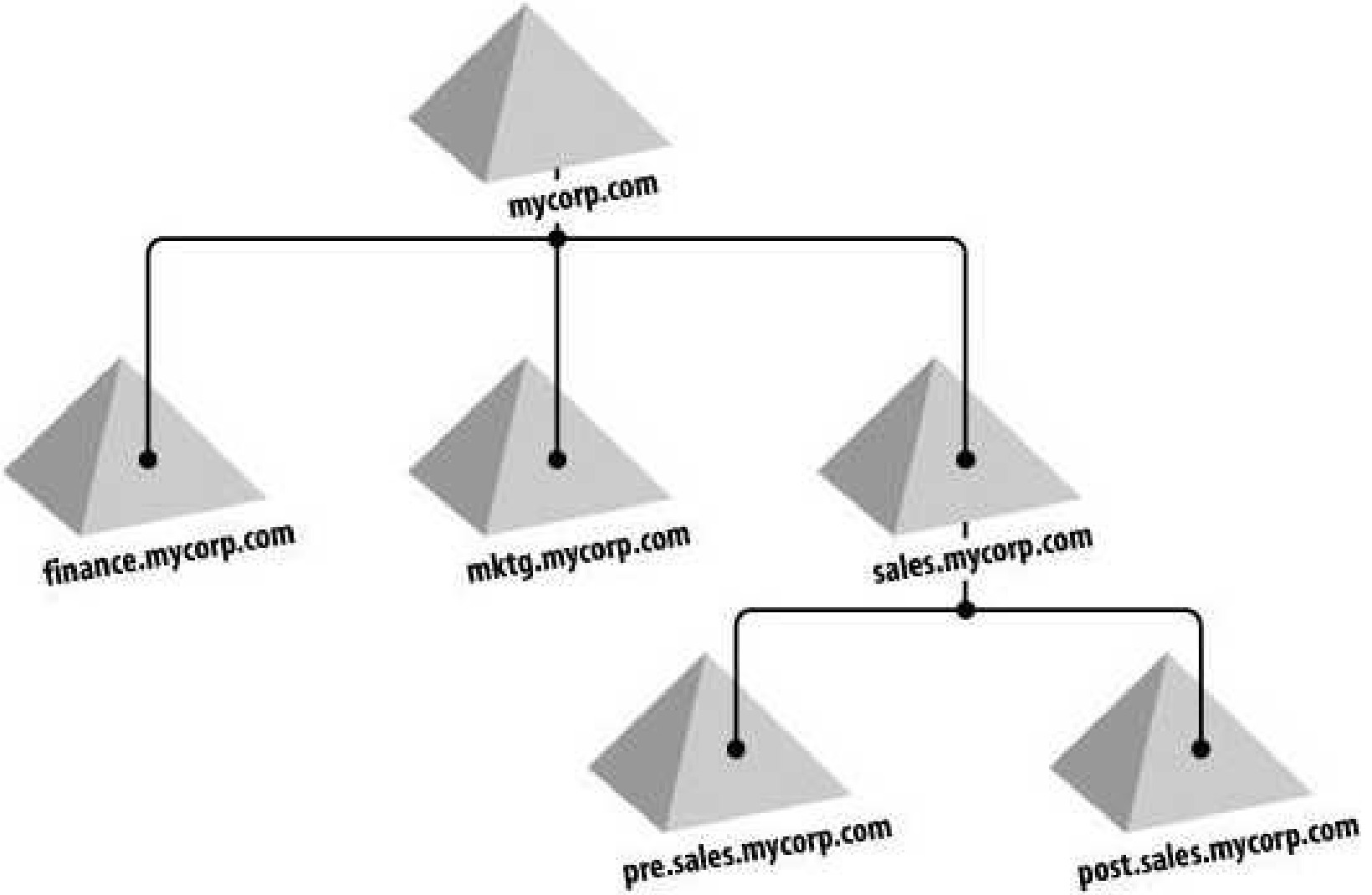
Typy atrybutów w AD

- CN – Common Name
- L – Locality Name
- ~~ST – State or Province Name~~
- O – Organization Name
- OU – Organizational Unit Name
- C – Country Name
- ~~STREET – Street Address~~
- DC – Domain Component
- ~~UID – Userid~~

Składniki Domeny

- Hierarchiczna struktura obiektów oparta na X.500
- Nazwa DNS domeny jest jej unikalnym identyfikatorem
- Dostęp do zasobów tylko poprzez konta w domenie lub zaufanie do innych domen
- Polisy regulujące funkcjonalność w ramach domeny

Drzewo Domen
Domain Tree



Las
Forest

- Zbiór drzew domen, które współdzielą konfigurację i schemat
- Drzewa w lesie ufają sobie
- Las jest związany z pierwszą domeną utworzoną w Lesie (Forest Root Domain)
- Usunięcie Głównej Domeny Lasu niszczy Las

Jednostka Organizacyjna
OU - Oraganizational Unit

- Podstawowy obiekt hierarchii w domenie
- Określa zakres stosowania polis
- Określa granice delegowania uprawnień administracyjnych

Domyślne kontenery

W Domenie:

- Users
- Computers
- Domain Controller OU

W Lesie:

- Configuration
- Schema

Katalog Globalny
Global Catalog

- Zawiera wszystkie obiekty lasu
- Umożliwia poszukiwanie obiektów w ramach całego lasu
- Tylko do odczytu
- Dla każde obiektu zawiera atrybuty zdefiniowane w częściowym zbiorze atrybutów PAS (Partial Attribut Set)

FSMO
Flexible Single Master Operation

- FSMO jest terminem odnoszącym się do operacji Active Directory, które są pojedyncze-główne, to znaczy, że nie mogą wystąpić w różnych miejscach sieci w tym samym czasie.
- Przykłady takich operacji:
  - Modyfikację schematu
  - Nazywanie domeny
  - Wybór PDC
  - Przydział RID
  - Pewne zmiany infrastruktury

Tryby Domeny Windows 2000

- mixed mode
- native mode

Poziomy Serwera Windows 2003

- Dotyczą zarówno domeny jak i lasu
- Poziomy Domeny:
  - Windows 2000 mixed
  - Windows 2000 native
  - Windows Server 2003 Interim
  - Windows Server 2003

Poziomy Serwera Windows 2003 c.d.

- Poziomy lasu:
  - Windows 2000
  - Windows Server 2003 Interim
  - Windows Server 2003

Grupy

- Trzy rodzaje grup:
  - domenowe lokalne
  - domenowe globalne
  - uniwersalne
- Zachowanie grup rożni się w zależności od poziomu domeny lub lasu
- Dwa zakresy stosowania grup:
  - dystrybucja
  - bezpieczeństwo

Naming Context Application Partitions

- Configuration Naming Context – Kontekst Nazewniczy lasu
- Schema Naming Context – Kontekst Nazewniczy Schematu lasu
- Domain Naming Context – Kontekst Nazewniczy dla każdej domeny
- Application Partitions - Partycje aplikacji

Typowe Zastosowanie Application Partitions

Przechowywanie dynamicznych danych usług sieciowych np.:

- DNS - Domain Name Service
- DHCP - Dynamic Host Configuration Protocol
- COPS - Common Open Polisy Service
- RAS - Remote Access Service
- RADIUS - Remote Authentication Dial In Users Service

Topologia AD
Site Topology

- Mapa opisująca połączenia sieciowe
- Składniki:
  - Lokalizacje
  - Podsieci
  - Połączenia pomiędzy lokalizacjami
  - Obiekty połączeniowe

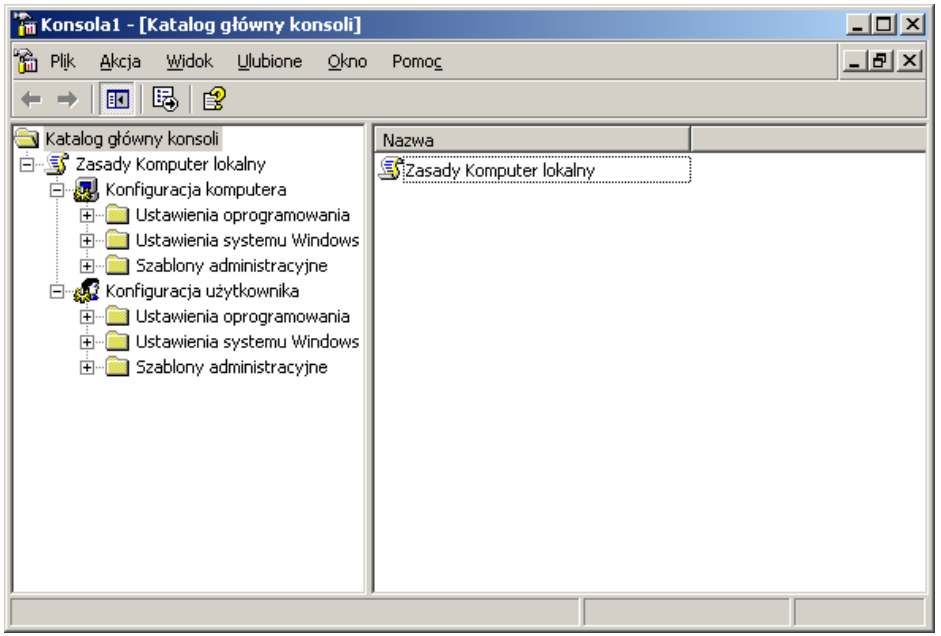
Zasady Grup
Group Policy Object (GPO)

- Pozwalają na łatwe centralne ustawienie środowiska pracy użytkowników i komputerów
- Umożliwiają dystrybucję aplikacji dla użytkowników i komputerów
- Stosowane dynamicznie
- Działają bez restartu komputera

GPO – klasy zasad

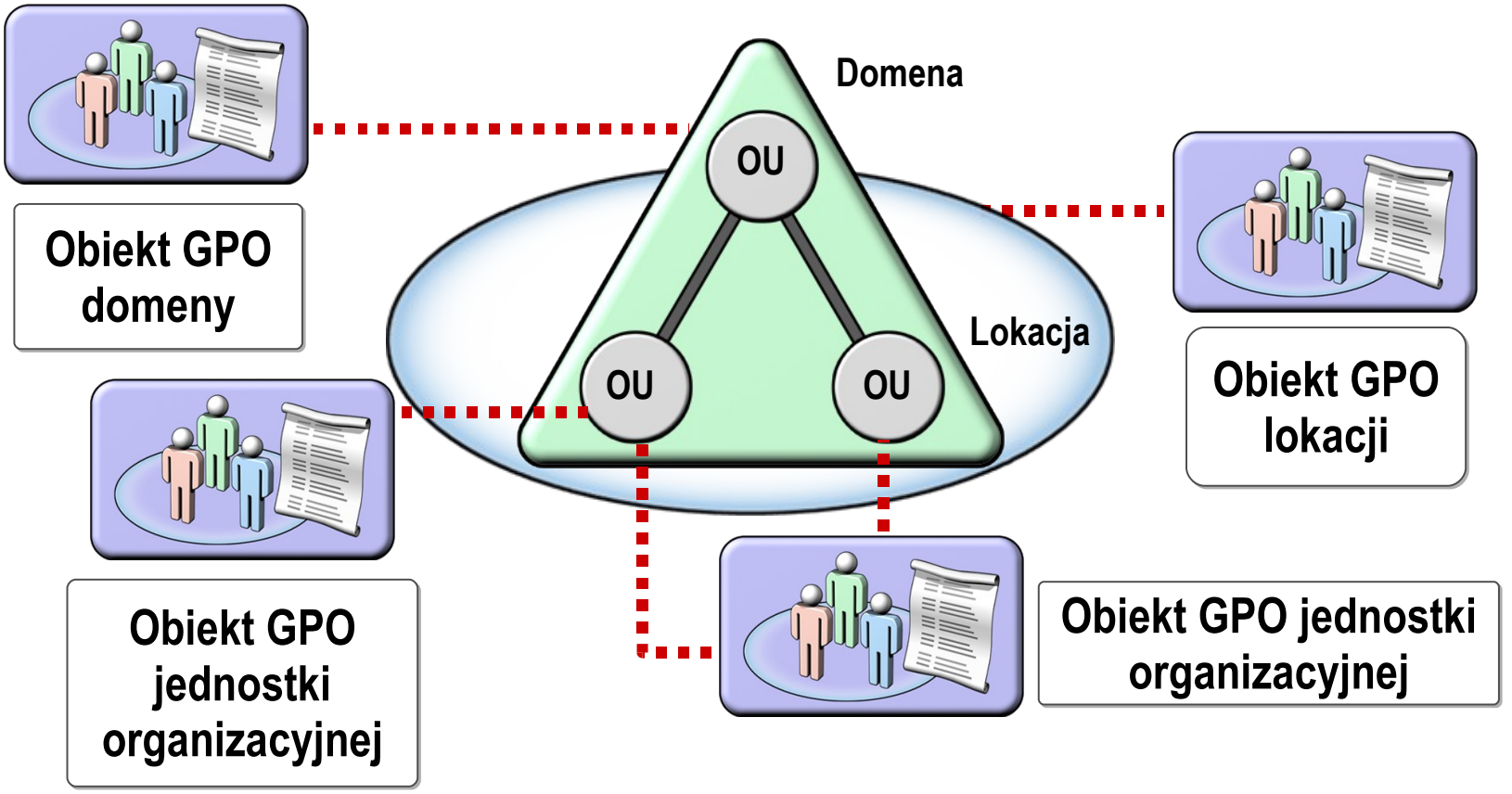
- Zasady dotyczące komputera
- Zasady dotyczące użytkownika

GPO - Zasady lokalne



- W konfiguracji domyślnej stosowane na każdym komputerze z systemem Windows 2000 lub XP

GPO - Połączenia



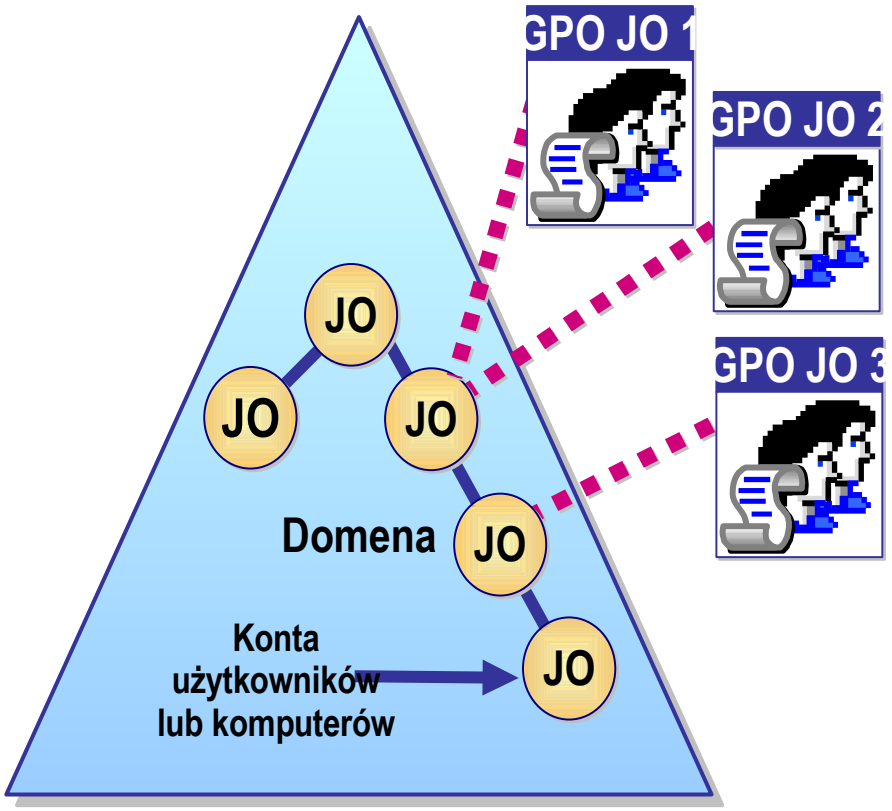
GPO – zakres stosowania

- GPO przyłączone do lokacji stosuje się do wszystkich komputerów i użytkowników w tej lokacji niezależnie od domeny, do której należą.
- GPO przyłączone do domeny stosuje się do wszystkich komputerów i użytkowników domeny. Domeny podrzędne nie dziedziczą GPO.
- GPO przyłączony do jednostki organizacyjnej stosuje się do wszystkich komputerów i użytkowników tej jednostki i jednostek podrzędnych.

GPO – kolejność stosowania

- Zasady lokalnego GPO (LGPO)
- GPO połączone z lokacją
- GPO połączone z domeną
- GPO połączone z jednostkami organizacyjnymi zgodnie z ich hierarchą

GPO- Kumulacja i konflikty



- Kumulacja – uaktywniane są wszystkie zasady ze wszystkich kolejno stosowanych GPO.
- Konflikty:
  - przy GPO tej samej klasy ważne jest ustawienie zasady z ostatnio zastosowanego GPO,
  - przy GPO różnych klas stosowane są zasady z GPO komputera.

GPO - komputera

- Ustawienia oprogramowania – Software installation
- Ustawienia systemu – Windows Settings
- Szablony administracyjne – Administrative templates

GPO - Użytkownika

- Ustawienia oprogramowania – Software installation
- Ustawienia systemu – Windows Settings
- Szablony administracyjne – Administrative templates

GPO – Przekierowanie folderów

Foldery, które można przekierować:

- Moje dokumenty
- Dane aplikacji
- Pulpit
- Menu Start

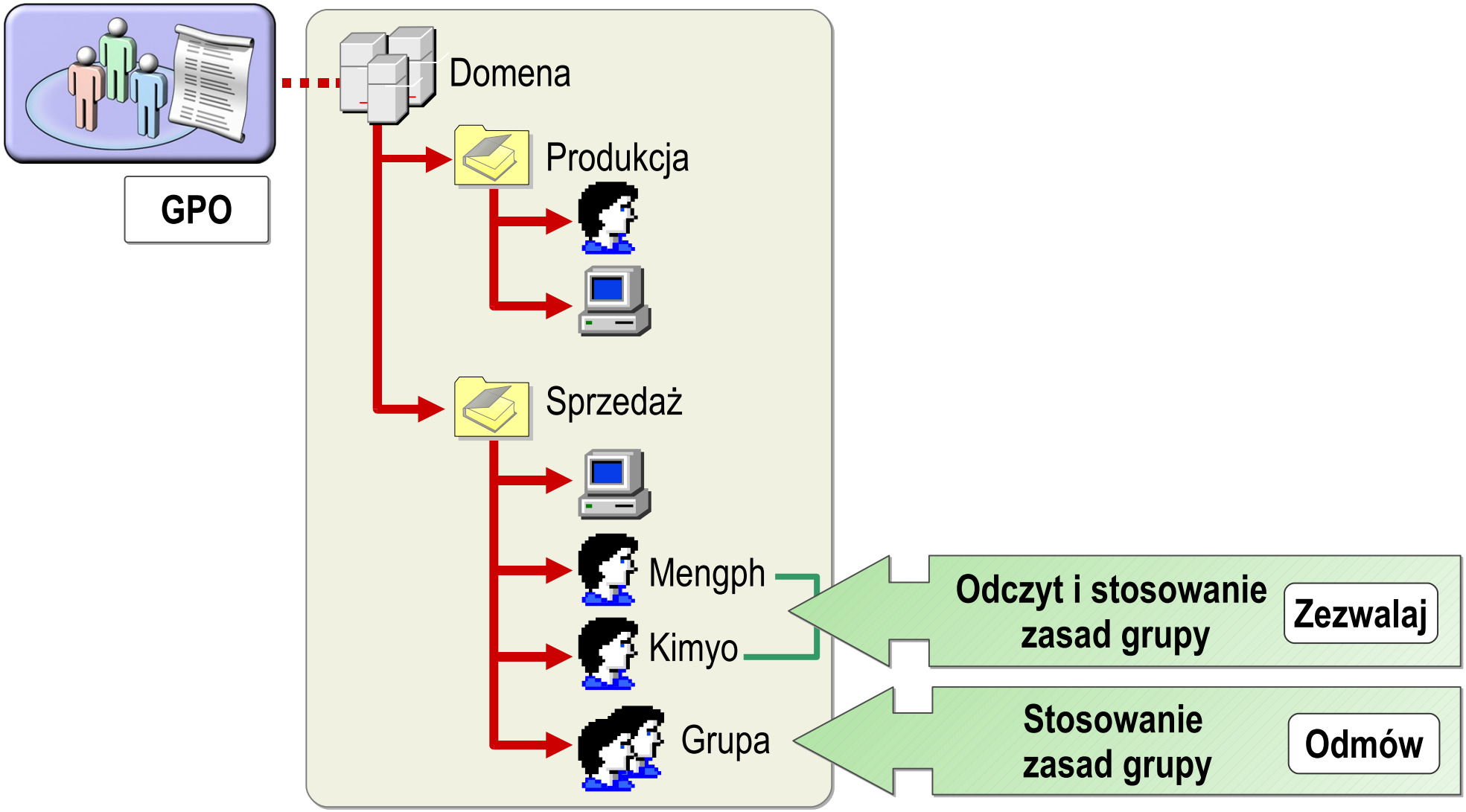
GPO - Odświerzanie

- Komputery co 90 minut ± 30 minut
- Kontrolery domen co 5 minut
- Wyjątki:
  - GPO komputera typu ustawienia oprogramowania – po restarcie,
  - GPO użytkownika typu ustawienia oprogramowania – przy następnym logowaniu,
  - GPO użytkownika typu przekierowanie folderu – przy następnym logowaniu,
  - Ustawienia zabezpieczeń w GPO komputera - co 16 godzin.

GPO – Zmiana domyślnego przetwarzania

- Blokowanie dziedziczenia (Block Inheritance)
- Wyłączenie zastępowania (no override)
- Filtrowanie obiektów
- Tryb przetwarzania zwrotnego

GPO - Filtrowanie



GPO – sprzężenie zwrotne

- Konto komputera i użytkownika w różnych kontenerach,
- Dwa tryby:
  - Zamień (replace) – GPO użytkownika nie jest przetwarzane,
  - Scal (merge) – po przetworzeniu GPO użytkownika z jego własnego kontenera przetwarzane jest GPO użytkownika z kontenera komputera

Szablony zabezpieczeń

- Pliki zawierające ustawienia bezpieczeństwa
- Stosowane lokalnie lub importowane do GPO
- Szybkie ustawienie identycznych zabezpieczeń dla dużych grup komputerów
- Stosowane, gdy ustawień nie można wprowadzić za pomocą samych zasad

Domyślne szablony zabezpieczeń

- Basic
- Optional Component File Security
- Compatible
- Secure
- High Secure
- No Terminal User ID
- System Root Security
- Setup Security

Zasady Bezpiecznej pracy

- zawsze z minimalnymi uprawnieniami
- ograniczony dostęp do konsoli serwera
- uprawnienia przez grupy
- używaj predefiniowanych grup
- włączone wykrywanie włamań
- blokowanie użytkowników
- twórz nowe obiekty zamiast modyfikować standardowe
- Definiuj zasady grup na jak najwyższym poziomie