



Politechnika Wrocławska



Administrowanie sys. Windows

Robert Burduk
robert.burduk@pwr.wroc.pl
C4 p. 326



Win - historia

- Windows NT 3.1
- Windows NT 3.5
- Windows NT 3.51 (wersja Workstation oraz Server – był to pierwszy system Microsoftu dzielący się na edycje)
- Windows NT 4.0
- Windows NT 5.0 (Windows 2000)
- Windows NT 5.1 (Windows XP)
- Windows NT 5.2 (Windows Server 2003 i Windows XP Professional x64 Edition)
- Windows NT 6.0 (Windows Vista i Windows Server 2008)
- Windows NT 6.1 (Windows 7 i Windows Server 2008 R2)
- Windows NT 6.2 (Windows 8 i Windows Server 2012)
- Windows NT 6.3 (Windows 8.1 i Windows Server 2012 R2)



Win - historia

- Windows NT 3.1
- Windows NT 3.5
- Windows NT 3.51 (wersja Workstation oraz Server – był to pierwszy system Microsoftu dzielący się na edycje)
- Windows NT 4.0
- Windows NT 5.0 (Windows 2000)
- Windows NT 5.1 (Windows XP)
- Windows NT 5.2 (Windows Server 2003 i Windows XP Professional x64 Edition)
- Windows NT 6.0 (Windows Vista i Windows Server 2008)
- Windows NT 6.1 (Windows 7 i Windows Server 2008 R2)
- Windows NT 6.2 (Windows 8 i Windows Server 2012)
- Windows NT 6.3 (Windows 8.1 i Windows Server 2012 R2)



Grupa robocza

Grupa robocza jest grupą komputerów połączonych za pośrednictwem sieci nienależącej do domeny i współużytkujących zasoby, takie jak drukarki i pliki.

Podczas konfigurowania sieci system Windows automatycznie tworzy grupę roboczą i nadaje jej nazwę.

- Wszystkie komputery są równorzędne; żaden komputer nie ma kontroli nad innym.
- Każdy komputer ma zestaw kont użytkownika. Aby zalogować się na dowolnym komputerze należącym do grupy roboczej, trzeba mieć na tym komputerze konto.



Grupa robocza

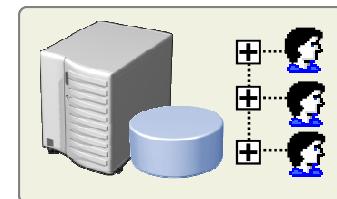
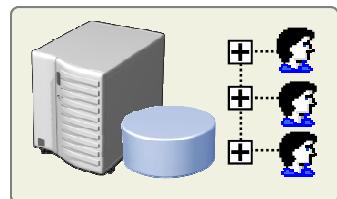
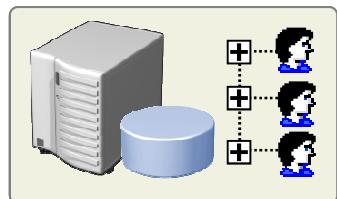
Grupa robocza jest grupą komputerów połączonych za pośrednictwem sieci nienależącej do domeny i współużytkujących zasoby, takie jak drukarki i pliki.

- Grupa robocza zawiera na ogół nie więcej niż dwadzieścia komputerów.
- Dostęp do grupy roboczej nie jest chroniony hasłem.
- Wszystkie komputery muszą się znajdować w tej samej sieci lub podsieci lokalnej.



Grupa robocza

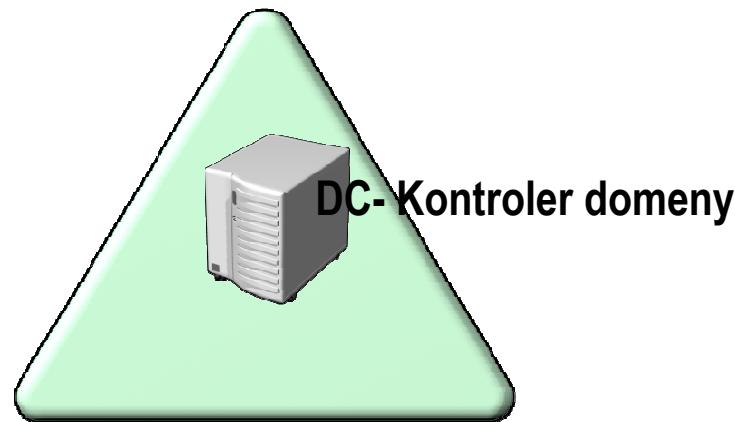
Każdy komputer posiada własną bazę kont użytkowników (*Security Accounts Manager – SAM*), dostęp tylko do zasobów komputera, na którym użytkownik został zalogowany.





Domena

Domena – logiczna grupa komputerów posiadająca wspólną bazę obiektów sieciowych. Baza przechowywana jest na „specjalnych” serwerach (tzw. kontrolerach domeny –DC)





Domena

Domena jest kolekcją komputerów w sieci korzystających ze wspólnej bazy danych i wspólnych zasad zabezpieczeń. Domena jest zarządzana jako jednostka ze wspólnymi prawami i procedurami. Każda domena ma unikatową nazwę.

- Co najmniej jeden komputer to serwer. Za pomocą serwerów administratorzy sieci kontrolują zabezpieczenia i uprawnienia dotyczące wszystkich komputerów w domenie. W ten sposób mogą łatwo wprowadzać zmiany, ponieważ są one automatycznie wdrażane na wszystkich komputerach. Gdy użytkownicy domeny uzyskują do niej dostęp, muszą zawsze podawać hasło lub inne informacje logowania.



Domena

Domena jest kolekcją komputerów w sieci korzystających ze wspólnej bazy danych i wspólnych zasad zabezpieczeń. Domena jest zarządzana jako jednostka ze wspólnymi prawami i procedurami. Każda domena ma unikatową nazwę.

- Jeśli masz konto użytkownika w domenie, możesz logować się na dowolnym komputerze w domenie bez konieczności posiadania konta na tym komputerze.
- Najczęściej wprowadzanie zmian ustawień na komputerze jest możliwe tylko w ograniczonym zakresie, ponieważ administratorom sieci zwykle zależy na zachowaniu spójności między wszystkimi komputerami w sieci.



Domena

Domena jest kolekcją komputerów w sieci korzystających ze wspólnej bazy danych i wspólnych zasad zabezpieczeń. Domena jest zarządzana jako jednostka ze wspólnymi prawami i procedurami. Każda domena ma unikatową nazwę.

- W domenie mogą być tysiące komputerów.
- Komputery mogą być w różnych sieciach lokalnych.



Domena - role komputerów



Serwer plików



Serwer wydruku



Serwer terminali

DC- Kontroler domeny

Zarządzanie tym serwerem

Zarządzanie tym serwerem Serwer: LONDON

Zarządzanie rolami serwera

Używaj znajdujących się tu narzędzi i informacji, aby dodawać lub usuwać role oraz wykonywać codzienne zadania administracyjne.

Twoj serwer został skonfigurowany dla następujących ролей:

- ▼ Serwer plików
- ▼ Serwer wydruku
- ▼ Kontroler domeny (Active Directory)
- ▼ Serwer DNS
- ▼ Serwer DHCP
- ▼ Serwer WINS

Nie wyświetlaj tej strony przy logowaniu

Narzędzia i aktualizacje

- Dodaj lub usuń role
- Przeczytaj na temat ról serwera
- Przeczytaj na temat administracji zdalnej

Zobacz też

- Pomoc i obsługa techniczna
- Microsoft TechNet
- Zestawy Deployment and Resource Kits
- Lista ogólnych zadań administracyjnych
- Współpracy Windows Server Communities
- Co nowego
- Program ochrony technologii strategicznej

Serwer DNS



Serwer aplikacji



Kontroler domeny



Serwer członkowski



Usługa katalogowa

Usługa katalogowa – baza danych o obiektach w sieci wraz z mechanizmami dostępu do tej bazy.

Apache Directory Project,
Apple Open Directory,
Fedora Directory Server,
IBM Tivoli Directory Server,
Novell eDirectory (dawniej NDS),
OpenLDAP



Usługa katalogowa - AD

Usługa *Active Directory* (usługa katalogowa) zawiera kartotekę przechowującą informację o zasobach sieciowych, a także wszystkie usługi czyniące je dostępnym i użytecznymi. Zasoby przechowywane w kartotece, takie jak dane o użytkownikach, drukarkach, serwerach, bazach danych, grupach, usługach, komputerach, czy też zasady zabezpieczeń, znane są jako *obiekty*.

OBIEKTY I ATRYBUTY

- Obiekty reprezentują coś konkretnego np. użytkownika, drukarkę, aplikację.
- Atrybuty zawierają dane, które opisują identyfikowany podmiot.
- Do atrybutów użytkownika mogą należeć: imię, nazwisko, adres poczty elektronicznej.

KLASY

- Klasy są to zgrupowane logicznie grupy obiektów.

KONTENER

- Kontener jest obiektem, który może zawierać inne obiekty.
- Jest pojemnikiem na obiekty katalogowe.



Usługa katalogowa (AD)

- Identyfikuje zasoby w sieci
- Zapewnia spójność:
 - Nazw
 - Opisów
 - Lokalizacji
 - Praw dostępu
 - Zarządzania
 - Zabezpieczeń

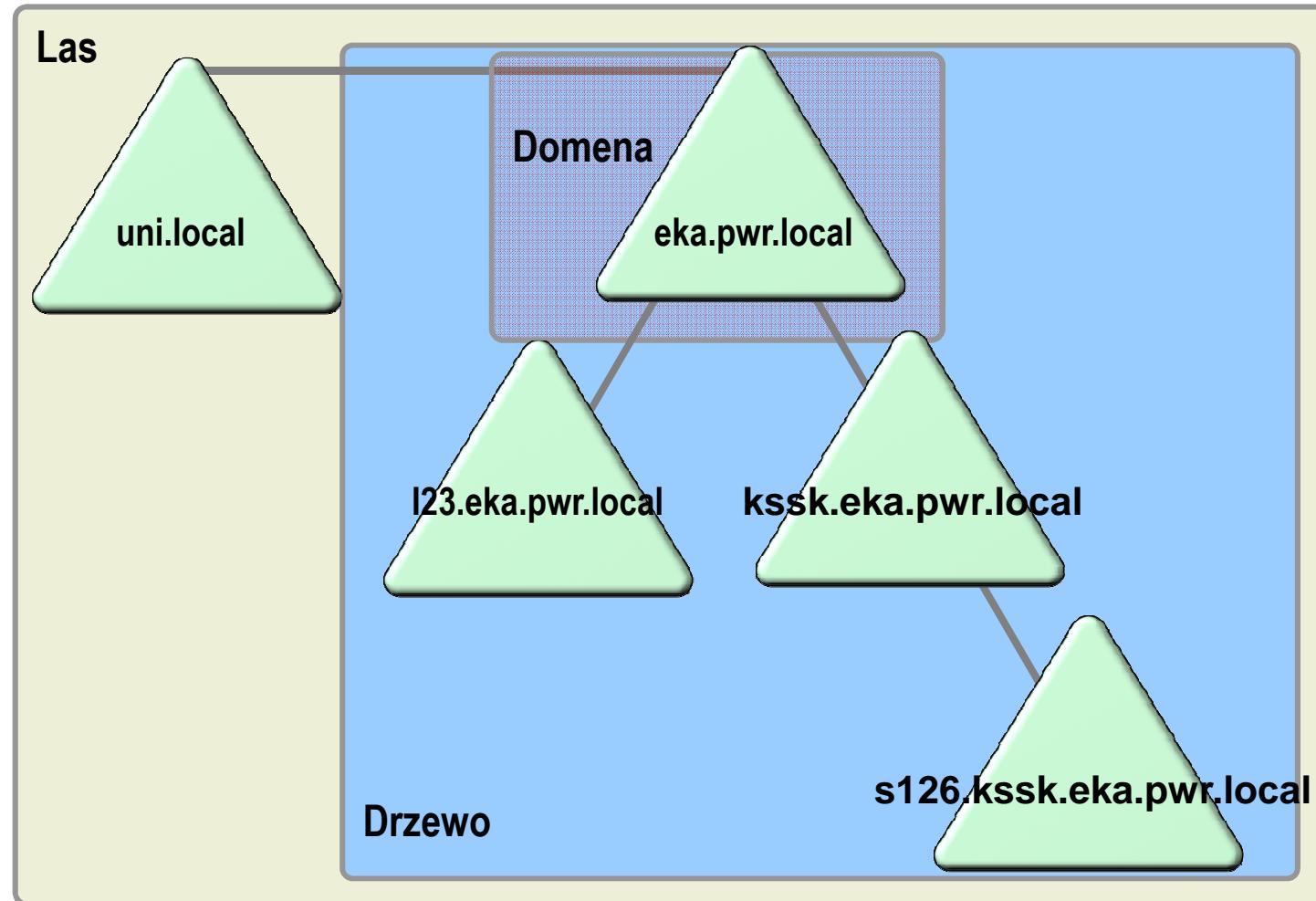


Usługa katalogowa (AD)

Domena typu NT4 pozwalała na przechowywanie informacji o ograniczonej stałej liczbie typów obiektów (konto użytkownika lub komputera, grupie) z ograniczoną stałą liczbą atrybutów przypisanych do konkretnych typów obiektów - nie istniała możliwość rozszerzenia schematu domeny o dodatkowe atrybuty lub typy obiektów, które można przechowywać. Domeny posiadały też technologiczne ograniczenie liczby obiektów, które mogłyby być przechowywane (do ok. 40 tys. obiektów w jednej domenie).



Podstawowe struktury AD





Podstawowe struktury AD

Drzewo

Domeny zorganizowane hierarchicznie mogą tworzyć strukturę drzewa (ang. ‘tree’). Drzewo posiada zawsze przynajmniej jedną domenę – domenę najwyższego poziomu (ang. ‘root’) – korzeń drzewa. Pozostałe domeny (o ile istnieją) mogą być umieszczone poniżej domeny najwyższego poziomu, tworząc drzewo. Niższe poziomy mogą się rozgałęziać.



Podstawowe struktury AD

Las

Każde drzewo znajduje się w jakimś lesie (ang. ‘forest’). Las składa się z przynajmniej jednego drzewa. Nie istnieje możliwość utrzymywania drzewa bez utrzymywania lasu. Uwaga ta odnosi się również do domeny Active Directory – domena nie może istnieć samodzielnie, musi istnieć w jakimś drzewie i jakimś lesie. Jeżeli jest to pierwsza domena, to tworzy pierwsze drzewo (którego korzeniem się staje) oraz pierwszy las. Las bierze nazwę od tej domeny.



Podstawowe struktury AD

Relacje zaufania

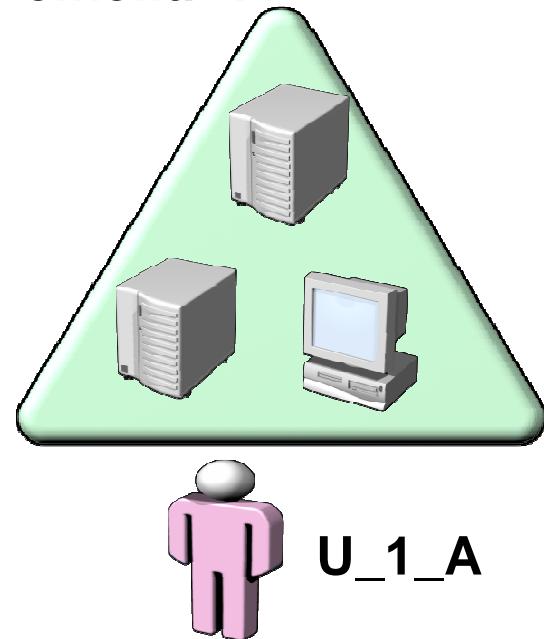
Głównym powodem istnienia Active Directory jest autoryzacja obiektów (np. użytkowników), którzy mają prawo lub nie dostępu do innych obiektów Active Directory oraz do zasobów innych, w tym dyskowych, sieciowych oraz aplikacji. Żeby była możliwa automatyczna autoryzacja użytkownika wobec innej usługi Active Directory lub zasobów korzystających z tej innej usługi, musi istnieć relacja zaufania (ang. ‘trust’) pomiędzy domenami Active Directory.

Domeny połączone relacją zaufania ufają sobie, o ile jest to relacja zaufania dwustronna, lub tylko jedna ufa drugiej, jeżeli jest to relacja jednostronna. Domeny w obrębie jednego lasu (w tym w obrębie tego samego drzewa) ufają sobie.



Podstawowe struktury AD

Domena "A"

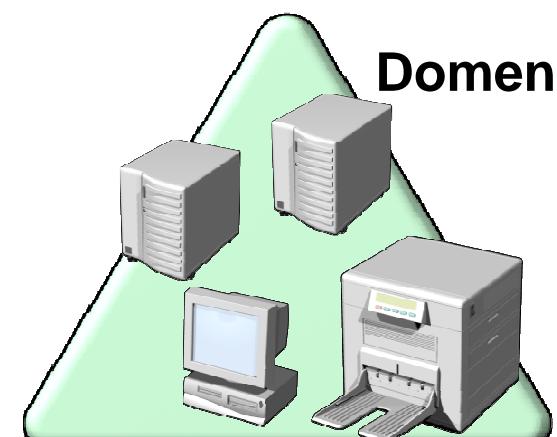


Domena zaufana (konto)

Czy jest możliwy dostęp do zasobów innej domeny, z wykorzystaniem jednego konta użytkownika?

Relacja zaufania
(pomiędzy domenami)

Domena "B"



Domena ufająca (zasób)



Poziom funkcjonalności Windows 2003

Poziom funkcjonalności domeny

Windows 2000 mieszany (domyślny)

Windows 2000 macierzysty

Windows Server 2003 tymczasowy

Windows Server 2003

Obsługiwane kontrolery domeny

**system Windows NT 4.0
Windows 2000
Systemy z rodziny
Windows Server 2003**

**Windows 2000
Systemy z rodziny
Windows Server 2003**

**Windows NT 4.0
Systemy z rodziny
Windows Server 2003**

**Systemy z rodziny
Windows Server 2003**



Poziom funkcjonalności Windows 2008

Poziom funkcjonalności domeny

Windows 2000 lokalny

Windows Server 2003

Windows Server 2008

Windows Server 2008 R2

Obsługiwane kontrolery domeny

Windows 2000 Server

Windows Server 2003

Windows Server 2008

Windows Server 2008 R2

Windows Server 2003

Windows Server 2008

Windows Server 2008 R2

Windows Server 2008

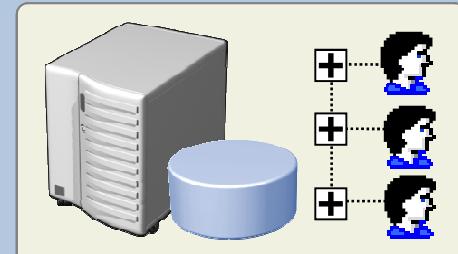
Windows Server 2008 R2

Windows Server 2008 R2

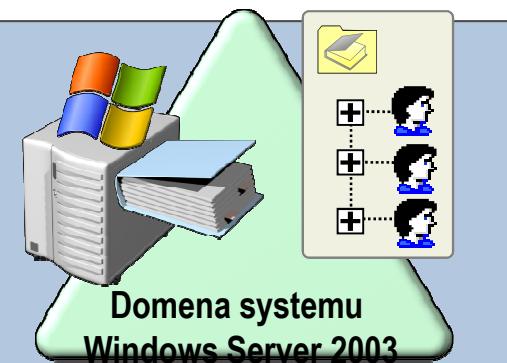


Konto użytkownika i grup

- Konta użytkowników i grup lokalnych
(przechowywane na komputerze lokalnym)



- Konta użytkowników i grup domeny
(przechowywane w usłudze Active Directory)





Grupy

Grupa jest zbiorem kont użytkowników, komputerów i innych grup, który może być zarządzany, jako pojedynczy element. Użytkownicy i komputery należący do danej grupy są nazywani członkami grupy.

Grupy w **Active Directory** są obiektami katalogu i mogą być umieszczane bezpośrednio w domenie lub kontenerze jednostki organizacyjnej. AD udostępnia zbiór domyślnych grup tworzonych podczas instalacji, oraz umożliwia tworzenie własnych.



Grupy

Grupy mogą być używane do:

- Uproszczenia administracji dzięki przypisywaniu uprawnień do współdzielonych zasobów grupie zamiast indywidualnym użytkownikom. Takie nadanie uprawnień daje taki sam dostęp do zasobu dla wszystkich członków grupy.
- Delegowania kontroli administracyjnej poprzez jednokrotne przypisanie praw użytkownika do grupy poprzez Zasady Grup (ang. **Group Policy**). Później wystarczy dodać członków do takiej grupy by uzyskali takie same prawa jak ta grupa.
- Tworzenie list dystrybucyjnych poczty elektronicznej



Grupy

Grupy są charakteryzowane poprzez zasięg (ang. scope) i typ.

- Zasięg grupy określa czy jest ona widoczna tylko w domenie, w której została stworzona czy w też całym lesie.
- Typ grupy mówi nam, czy można ją użyć do przypisywania uprawnień (grupy zabezpieczeń), czy tylko jako listę dystrybucyjną poczty e-mail (grupy dystrybucyjne).



Grupy

Grupy są charakteryzowane poprzez zasięg (ang. scope) i typ.

- Zasięg grupy określa czy jest ona widoczna tylko w domenie, w której została stworzona czy w też całym lesie.
- Typ grupy mówi nam, czy można ją użyć do przypisywania uprawnień (grupy zabezpieczeń), czy tylko jako listę dystrybucyjną poczty e-mail (grupy dystrybucyjne).



Grupy

- Istnieją grupy, w których nie można modyfikować ani wyświetlić członkostwa. Są one nazywane grupami specjalnymi lub tożsamościami specjalnymi. Reprezentują one różnych użytkowników w różnym czasie w zależności od okoliczności. Np. grupa **Everyone** jest grupą specjalną reprezentującą wszystkich aktualnych użytkowników sieci włączając w to gości i konta użytkowników z innych domen.
- Grupy domyślne są predefiniowanymi grupami zabezpieczeń tworzonymi automatycznie podczas instalacji domeny Active Directory. Mogą być używane do ułatwienia kontroli dostępu do współdzielonych zasobów i delegowania peryficznych administracyjnych ról związanych z domeną.



Zasięg grup

Zasięg grupy określa czy może być ona użyta w domenie, w której istnieje czy w całym lesie. Wiąże się to również z tym, kto może być jej członkiem i czy ona sama może być zagnieżdżona w innej grupie. Dostępne są grupy o trzech zasięgach: domenowa grupa lokalna, globalna i uniwersalna.



Zasięg grup

Domenowe grupy lokalne

Członkami grup domenowych lokalnych mogą być inne grupy oraz konta z domen Windows Server 2003, Windows 2000, Windows NT i Windows Server 2008. Grupy te mogą mieć nadane uprawnienia tylko do zasobów znajdujących się w domenie.

Grupy o zasięgu domenowym lokalnym pomagają definiować i zarządzać dostępem do zasobów w pojedynczej domenie. Mogą posiadać następujących członków:

- Grupy o zasięgu globalnym
- Grupy o zasięgu uniwersalnym
- Konta
- Inne grupy o zasięgu domenowym lokalnym



Zasięg grup

Domenowe grupy globalne

Członkami grup globalnych mogą być inne grupy oraz konta, lecz tylko znajdujące się w domenie, w której grupa została zdefiniowana. Grupy te mogą mieć nadane uprawnienia w każdej domenie w lesie.

Wskazane jest, aby grup globalnych używać do codziennego zarządzania obiektami katalogu, takimi jak konta użytkowników i komputerów. Ponieważ grupy globalne nie są replikowane poza własną domeną, można często zmieniać listę ich członków bez generowania ruchu związanego z replikacją katalogu globalnego.



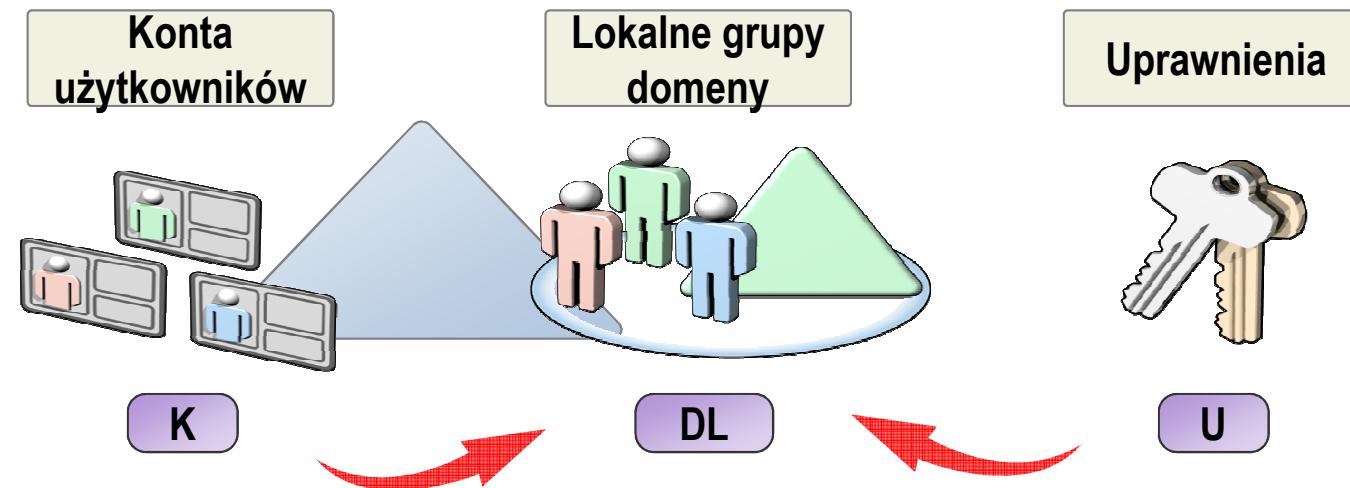
Zasięg grup

Domenowe grupy globalne

Członkami grup uniwersalnych mogą być inne grupy oraz konta z dowolnej domeny w lesie. Grupy te mogą mieć nadane uprawnienia w każdej domenie w lesie.

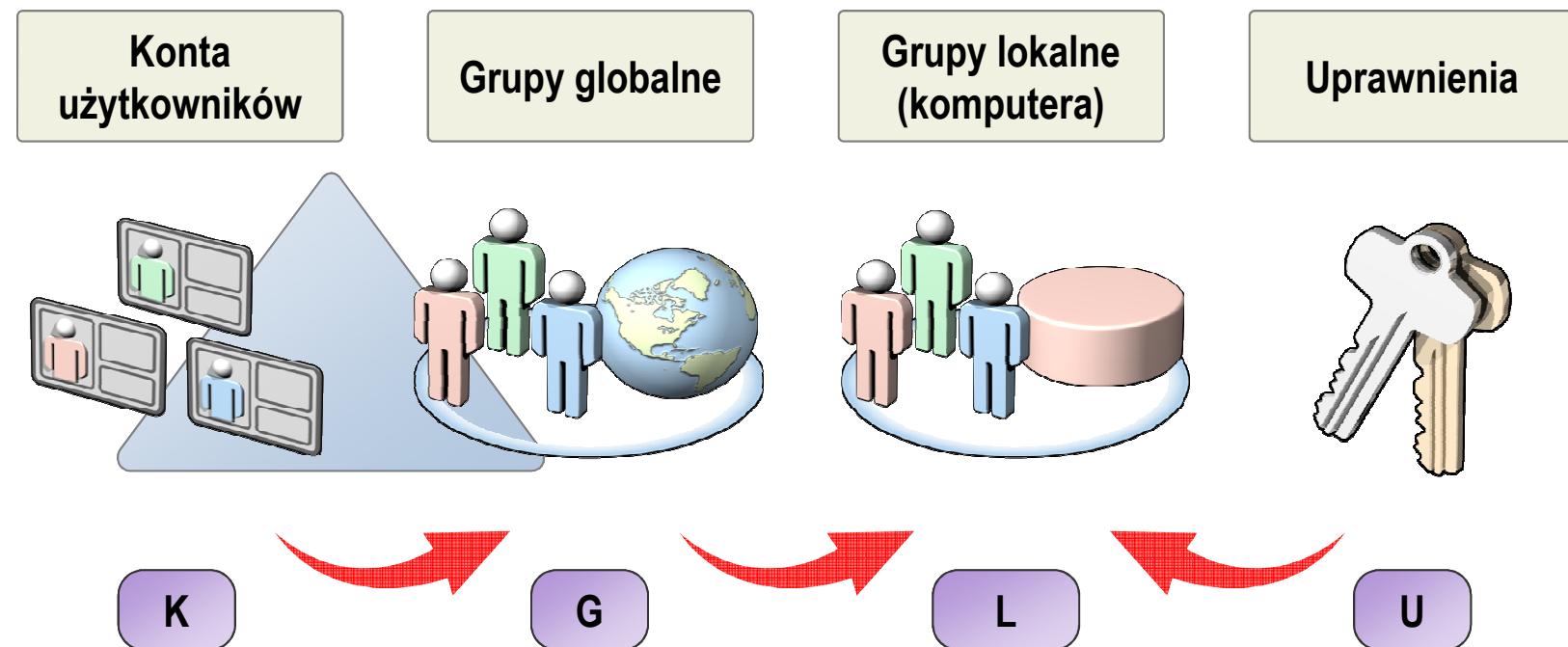


Strategia korzystania z grup



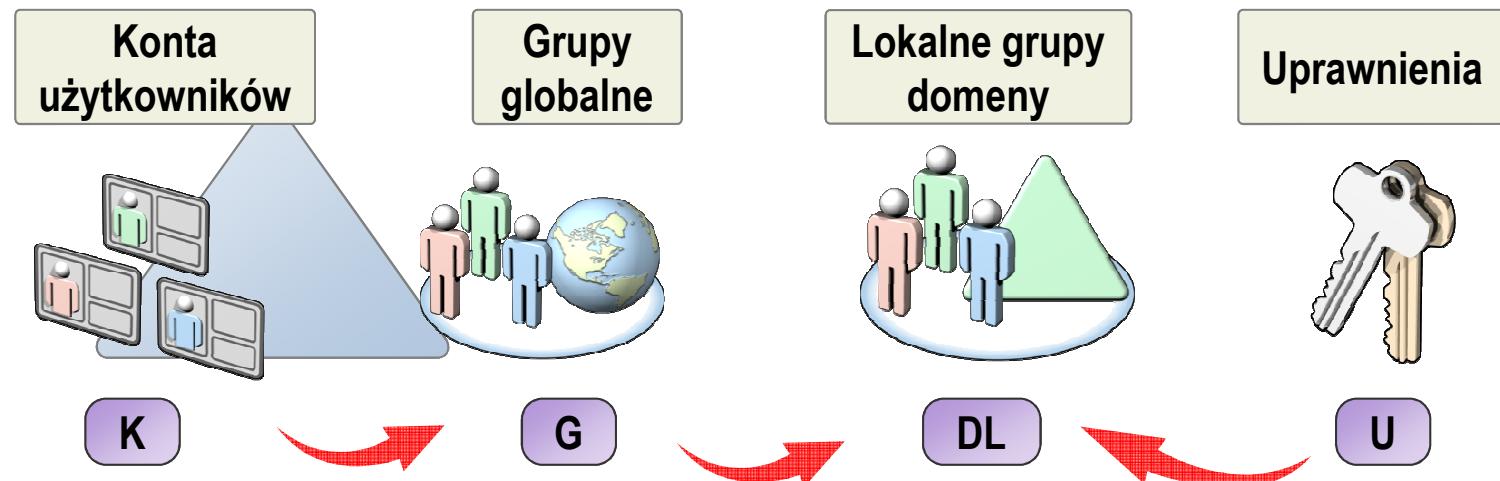


Strategia korzystania z grup



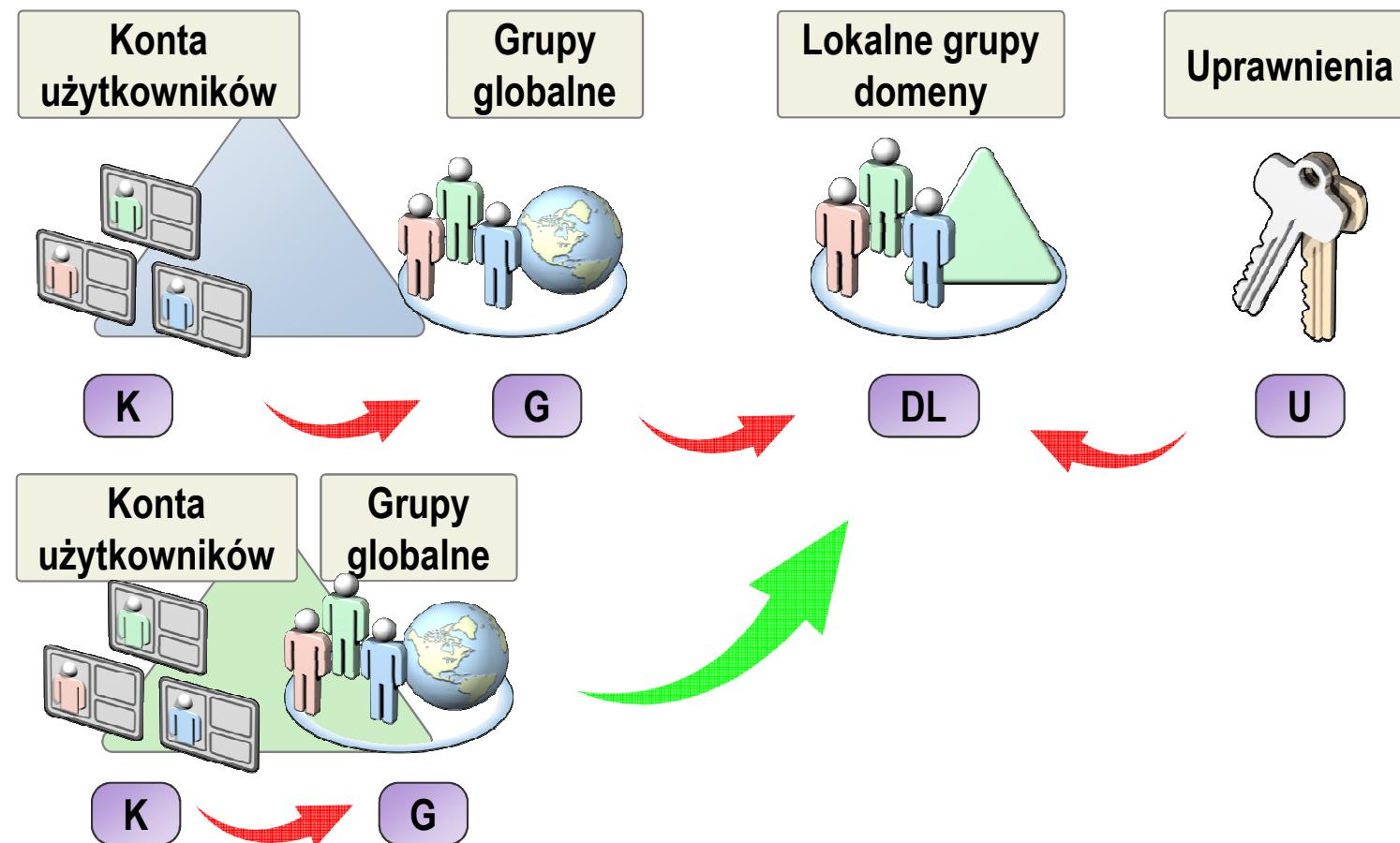


Strategia korzystania z grup





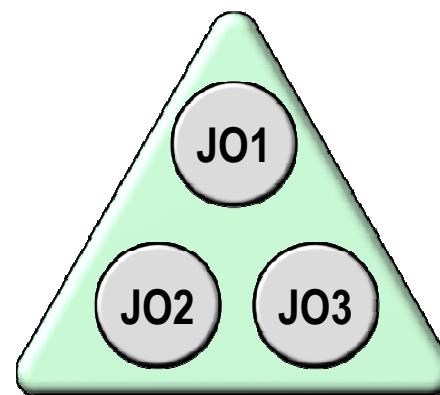
Strategia korzystania z grup





Jednostka organizacyjna

Jednostka organizacyjna (OU) jest kontenerem na poziomie administracyjnym i służy do logicznego organizowania obiektów w *Active Directory*.





Jednostka organizacyjna

Są to kontenery, w których mogą się znajdować użytkownicy, grupy, komputery, inne jednostki organizacyjne, a także opublikowane w usłudze AD zasoby plikowe i drukarki. Jednostki organizacyjne są najmniejszymi elementami, do których można przypisać zasady grup (GPO) lub delegować kontrolę administratorską. Wykorzystując je, można tworzyć kontenery w domenie reprezentujące hierarchiczną, logiczną strukturę organizacji. Zagnieżdżając jednostki organizacyjne w innych można modelować strukturę firmy minimalizując liczbę domen wymaganych w sieci.



Delegowanie kontroli

Delegowanie kontroli administracyjnej do jednostek organizacyjnych umożliwia przypisanie użytkownikom lub grupom uprawnień do zarządzania określonymi obiektami w usłudze Active Directory. Dzięki temu można ograniczyć grupę administratorów posiadających uprawnienia do całej struktury AD dając im możliwość zarządzania tylko jej pewną częścią, a także pozwala przydzielić podstawowe zadania administracyjne zwykłym użytkownikom (np. resetowanie haseł).



Delegowanie kontroli

Delegowanie uprawnień może polegać na:

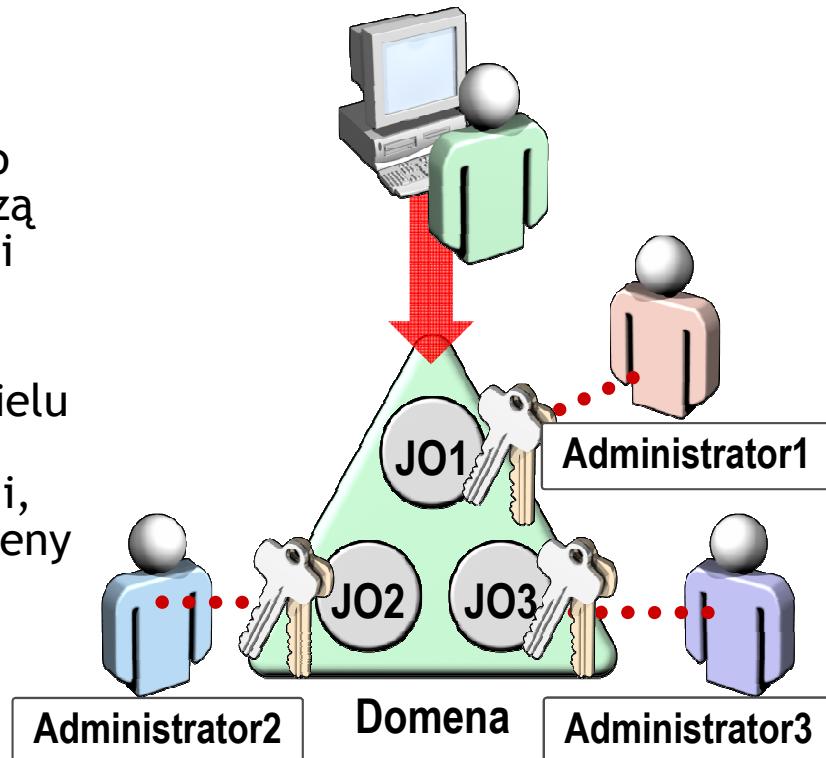
- zmianie atrybutów wszystkich obiektów w OU,
- tworzeniu, usuwaniu itp. obiektów potomnych określonego typu w OU,
- odczyt lub zapis określonych atrybutów dla określonego typu obiektów potomnych w OU.



Delegowanie kontroli

- Delegowanie administracji:

- Ułatwia ogólne administrowanie siecią przez rozdysytrybuowanie rutynowych zadań administracyjnych
- Oferuje użytkownikom lub grupom organizacji większą kontrolę nad ich lokalnymi zasobami sieciowymi
- Pomaga eliminować konieczność posiadania wielu kont administracyjnych z szerokimi uprawnieniami, na przykład dla całej domeny





Delegowanie kontroli

- Kontenery podrzędne i ich obiekty dziedziczą uprawnienia ustawione w kontenerze nadzędnym
- Uprawnienia podlegające dziedziczeniu są propagowane z obiektu nadzędnego do podrzędnego, gdy:
 - Tworzony jest obiekt podrzędny
 - Uprawnienia do obiektu nadzędnego są modyfikowane
- Przenoszone obiekty dziedziczą uprawnienia po nowej nadzędnej jednostce organizacyjnej
- Przenoszone obiekty nie dziedziczą już uprawnień po poprzedniej nadzędnej jednostce organizacyjnej
- Zapobieganie dziedziczeniu uprawnień



Różnice: OU a grupy

- OU widoczne są tylko dla administratorów, grupy mogą widzieć wszyscy użytkownicy w domenie (np. nadawanie uprawnień do folderu).
- Przynależność do jednej OU – przynależność do wielu grup.
- Grupa jest wystawcą zabezpieczeń (można przyznawać lub domawiać dostępu do obiektów na podstawie przynależności do grup, z wyjątkiem dystrybucyjnych).
- Funkcjonalność poczty elektronicznej dla grup – grupy dystrybucyjne.



Cechy systemu plików NTFS:

- Przypisanie praw dostępu do poszczególnych plików oraz folderów, które umożliwiają wyszczególnienie kto ma jakiego rodzaju prawo dostępu do danego pliku lub folderu.
- Odzyskiwanie oparte o koncepcję transakcji.
- Struktura drzew B powoduje, że dostęp do plików w folderach bardziej obszernych jest szybsza niż dostęp do plików w folderach o podobnej wielkości na woluminie FAT.
- Kompresja NTFS umożliwia odczyt oraz zapis plików podczas dokonywania kompresji, bez potrzeby uprzedniego użycia programu do dekompresji. To czy plik jest kompresowany czy nie ustala się za pomocą atrybutu. Warunkiem możliwości kompresji jest rozmiar klastra, który musi być większy niż 4K.



Cechy systemu plików NTFS:

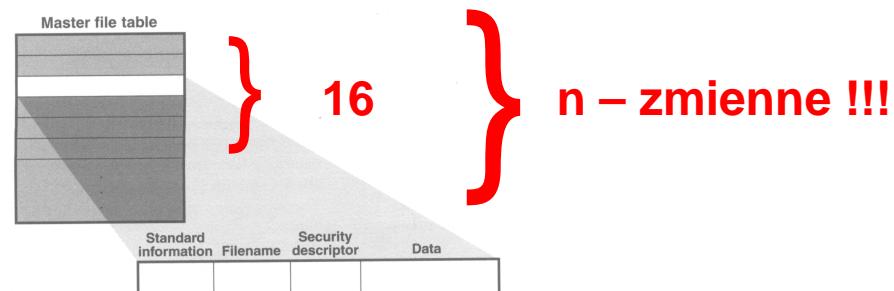
- Obsługa długich nazw plików.
- Przechowywanie informacji o ostatnim czasie dostępu (FAT przechowuje informacje tylko o dacie) .
- Obsługa do 2^{64} indeksów klastrów (16 miliar. GB dla 64kB klastra) - ograniczenie Win2000 128TB.
- Różnorodność atrybutów, dotyczą one danych w pliku, ochrony, itd.
- Zabezpieczenia plików i katalogów.
- NTFS nie może być stosowany na dyskietkach.
- System plików wykorzystywany tylko wraz z systemem Windows NT/2000.



Struktura wolumenu NTFS

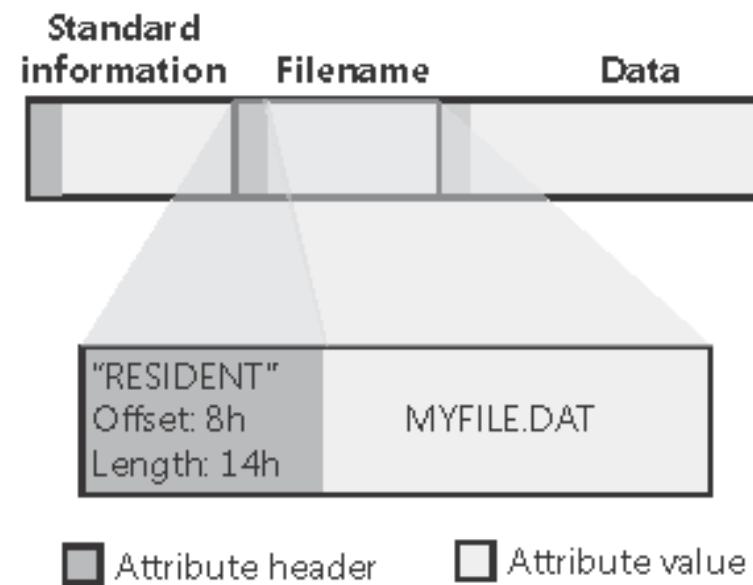
Po sektorze inicjującym występuje tzw. nadrzędna tabela plików (MFT - *Master File Table*), czyli po prostu tablica plików (indeks plików).

Wiersze o rozmiarze 1kB, jednoznacznie identyfikują pliki znajdujące się na wolumenie. Pierwsze 16 indeksów zarezerwowanych jest na pliki systemowe





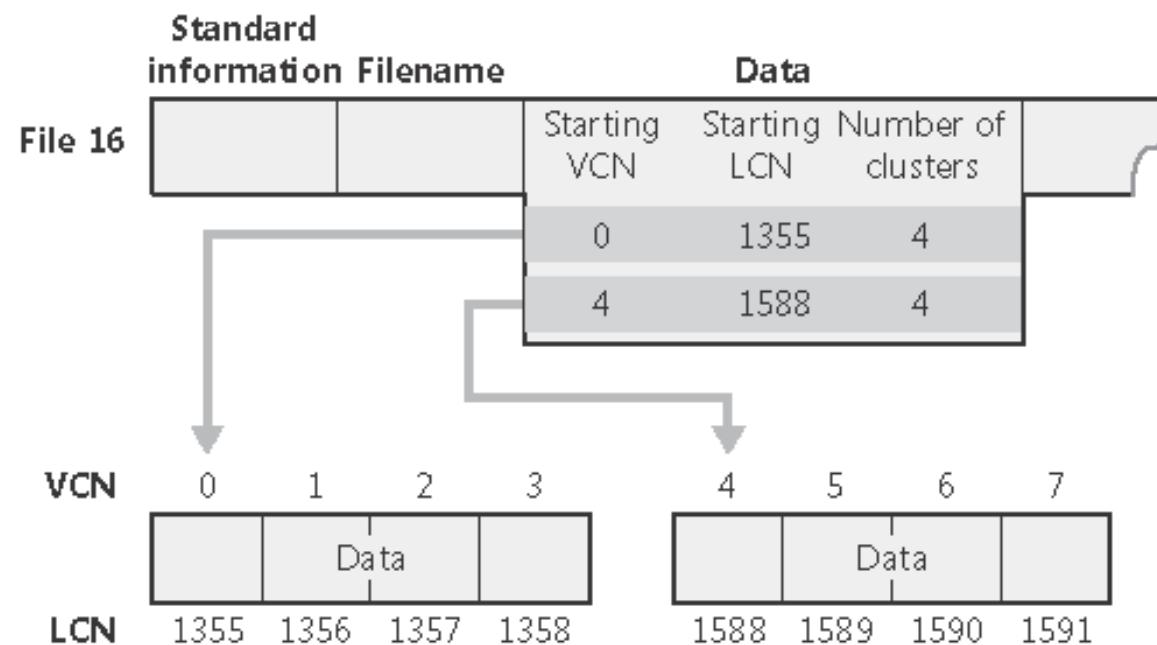
Przykład zawartości jednego rekordu MFT dla „małego” pliku



Atrybut *Informacje standardowe* zawiera między innymi:
atrybuty pliku, znaczniki czasowe.



Przykład zawartości jednego rekordu MFT dla „dużego” pliku





Przykład zawartości jednego rekordu MFT dla „małego” katalogu

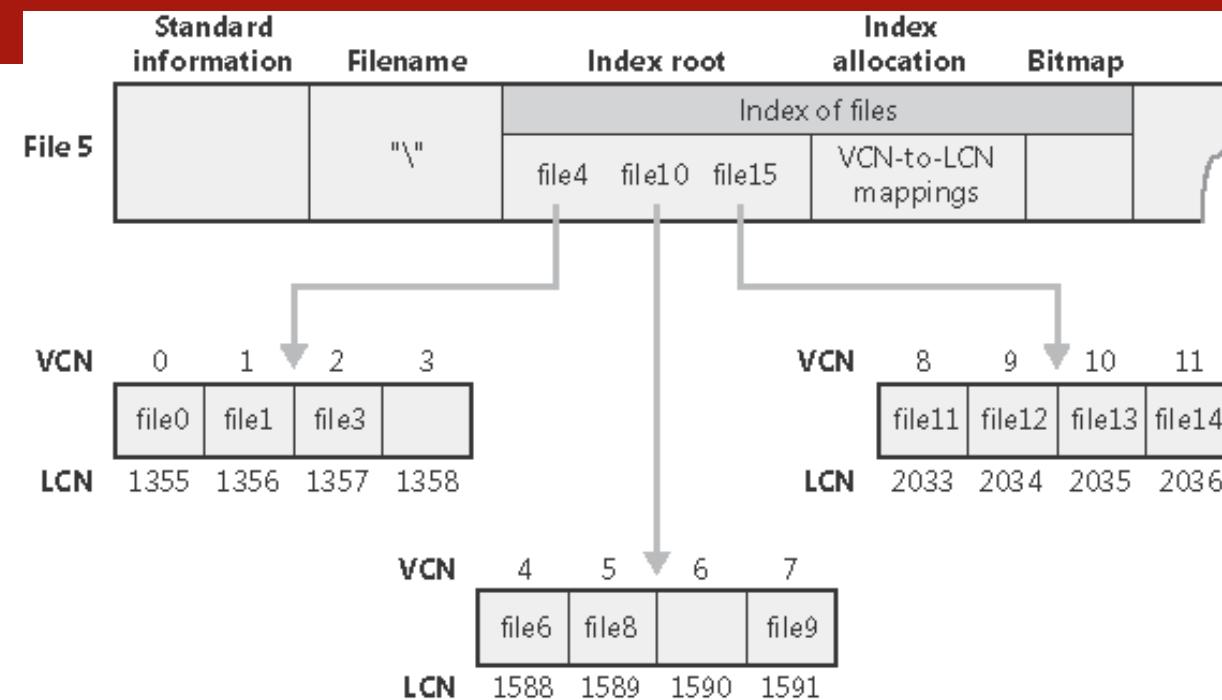
Standard information	Filename	Index root	
		Index of files	
		file1, file2, file3, ...	Empty

Wpis indeksu pliku jest bardzo uproszczony, ponieważ zawiera dodatkowo:

- odniesienie pliku w MFT,
- informacje o znaczniku czasowym,
- rozmiar pliku.



Przykład zawartości jednego rekordu MFT dla „dużego” katalogu



Każdy bufor indeksu o rozmiarze 4 kB może zawierać ok. 20 - 30 wpisów dotyczących plików

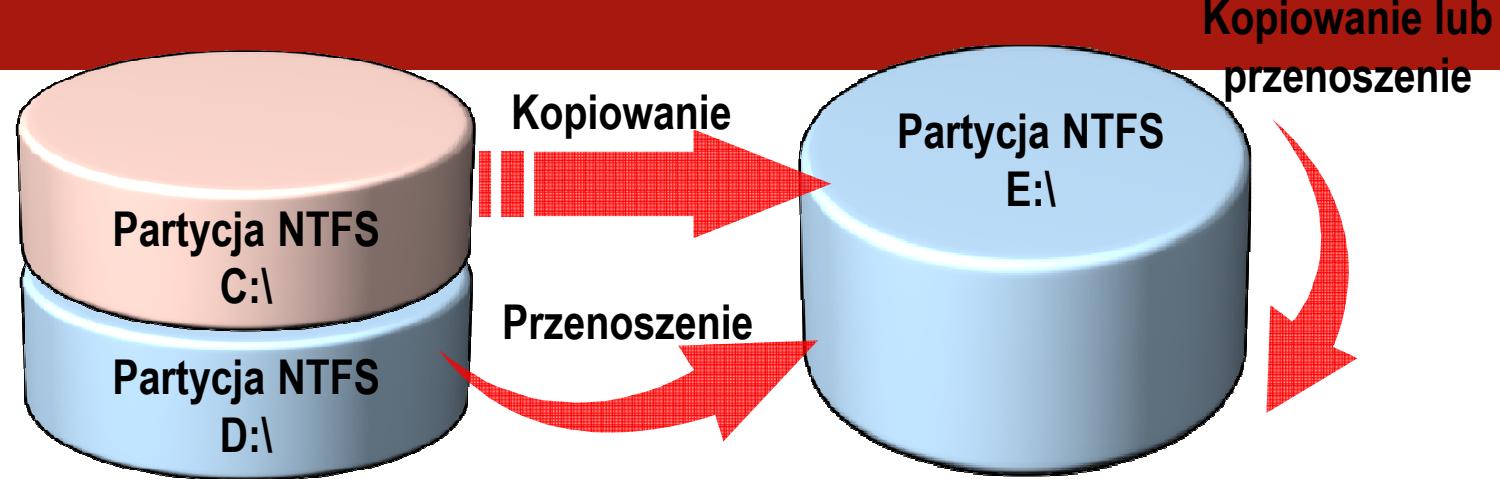


Pliki systemowe dla NTFS 5.0:

Plik systemowy	Nazwa pliku	Opis
Master File Table	\$Mft	Opisuje zawartość partycji NTFS
Master File Table #2	\$MftMirr	Jest to plik zawierający duplikat pierwszych rekordów z MFT.
Log File	\$LogFile	Plik logów służący do naprawy partycji w wyniku wystąpienia błędów (np. podczas wyłączenia napięcia)
Volume	\$Volume	informacje o wolumenie (w tym etykieta wolumenu i numer wersji NTFS)
Attribute Definition	\$AttrDef	tablica definicji atrybutów (nazwy, numery identyfikacyjne, objaśnienia)
Root Filename Index	\$.	katalog główny
Cluster Bitmap	\$Bitmap	mapa bitowa klastrów (opis zajętości partycji)
Partition Boot Sector	\$Boot	Sektor startowy
Bad Cluster File	\$BadClus	Lista uszkodzonych klastrów
Secure	\$Secure	Plik konfiguracji zabezpieczeń
Upcase Table	\$Upcase	tabela konwersji małych liter na duże odpowiedniki Unicode
Extendent	\$Extend	Katalog rozszerzonych metadanych



Wpływ kopiowania i przenoszenia plików i folderów na uprawnienia NTFS



- Gdy pliki i foldery są kopiowane, dziedziczą uprawnienia folderu docelowego
- Gdy pliki i foldery są przenoszone w obrębie tej samej partycji, zachowują swoje uprawnienia
- Gdy pliki i foldery są przenoszone do innej partycji, dziedziczą uprawnienia folderu docelowego



Strumienie

- Atrybut *Data* w rekordzie MFT jest strumieniem nienazwanym, w systemie plików NTFS można dodawać do pliku i folderu inne nazwane strumienie.

```
C:\test>echo dane w pliku > test.txt
```

```
C:\test>more < test.txt
```

dane w pliku

```
C:\test>echo strumien1 > test.txt:s1
```

```
C:\test>more < test.txt:s1
```

strumien1



Strumienie

- Program taki jak Notatnik nie otworzy takiego strumienia - należy nadać rozszerzenie (strumieniowi !!!)

```
C:\test>echo strumien2 > test.txt:s2.txt
```

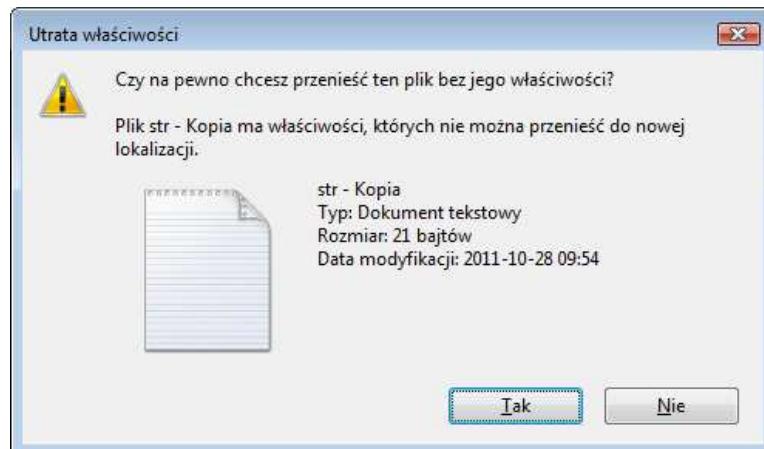
- Teraz można edytować strumień pisząc

```
C:\test> notepad test.txt:s2.txt
```



Cechy strumieni

- nie pokazują ich standardowe narzędzia Windows
np. www.heysoft.de/nt/lads.zip
- edytując zakładkę *Podsumowanie* z menu *Właściwości* edytujemy odpowiednie strumienie (XP i 2003)
- nie są wliczane do miejsca jakie zajmuje plik (folder !!!)
- dzięki nim można omijać Quotę





Zasady Grupowe

- **Zasady grupowe** umożliwiają centralne określenie wielu cech oraz ograniczeń dotyczących systemu operacyjnego (ok. 450 możliwych ustawień dla Windows 2000 i ponad 600 dla Windows 2003) takich jak konfiguracji pulpitu, aplikacji, przeadresowywania folderów, ustawień językowych, zabezpieczeń itp.



Ustawienia Zasad grupowych:

- Mogą być powiązane z lokacjami, domenami i jednostkami organizacyjnymi,
- Dotyczą wszystkich użytkowników i komputerów należących do danej lokacji, domeny lub jednostki organizacyjnej,
- Mogą ulec dalszemu przystosowywaniu opierającemu się na przynależności użytkowników lub komputerów do grup zabezpieczenia.

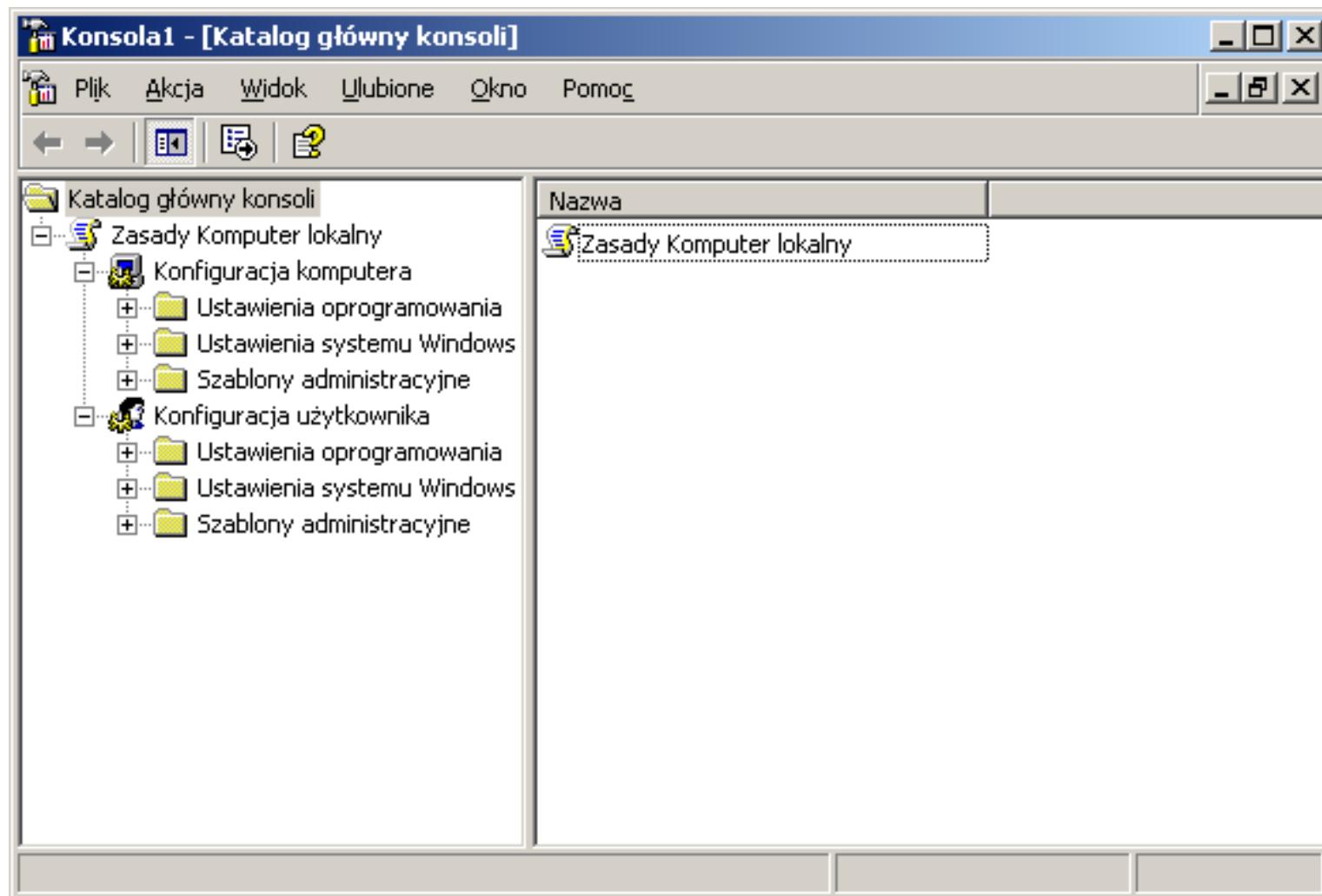


Zasady grupowe obejmują:

- **Ustawienia zasad komputera** znajdują się w węźle **Konfiguracja komputera** i są uzyskiwane, gdy dokonywany jest rozruch komputera (lub podczas okresowego cyklu odświeżania - 90 min. +/- 30 mim.),
- **Zasady użytkownika** (ustawienia znajdujące się w węźle **Konfiguracja użytkownika**) są uzyskiwane, gdy użytkownik loguje się (lub podczas okresowego cyklu odświeżania).



Zasady grupowe obejmują:



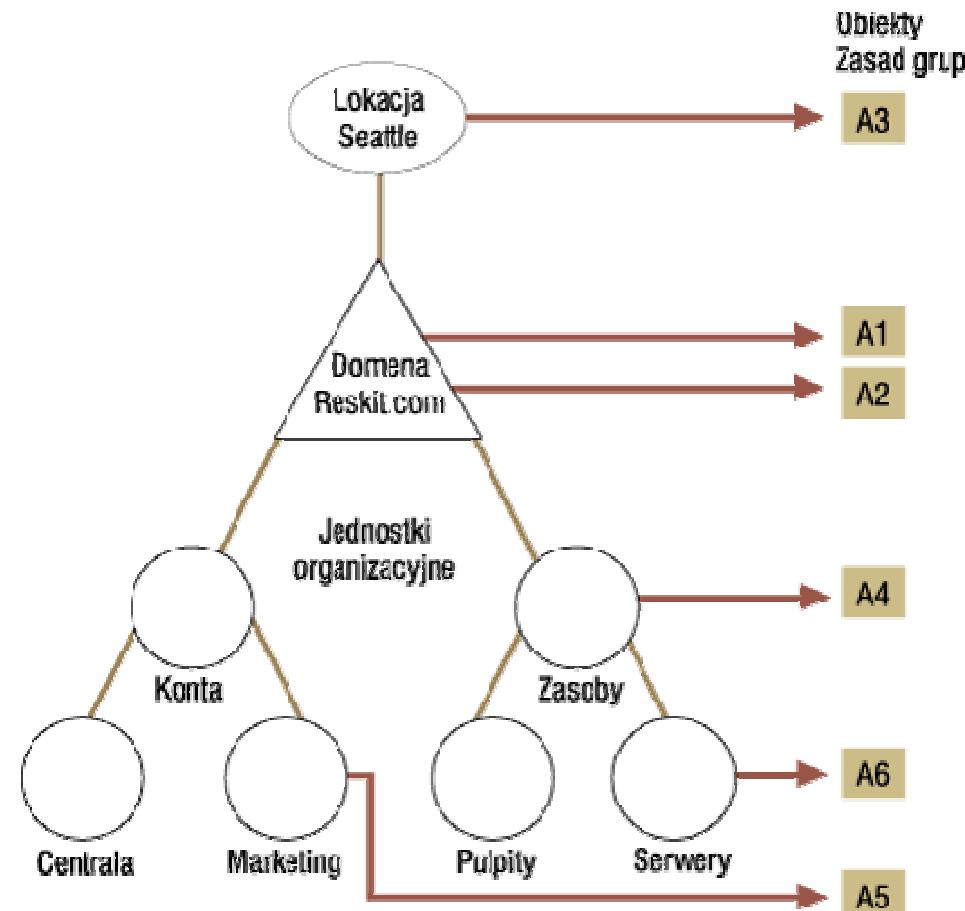


Zasady są stosowane w następującej kolejności:

- Unikatowy, lokalny obiekt Zasad grup,
- Obiekty Zasad grup lokalizacji, w kolejności określonej administracyjnie,
- Obiekty Zasad grup domeny, w kolejności określonej administracyjne,
- Obiekty Zasad grup jednostek organizacyjnych, od nadzędnej do podzędnej jednostki organizacyjnej i w kolejności określonej administracyjne na poziomie każdej jednostki organizacyjnej.



Przykład przydziału zasad grupowych

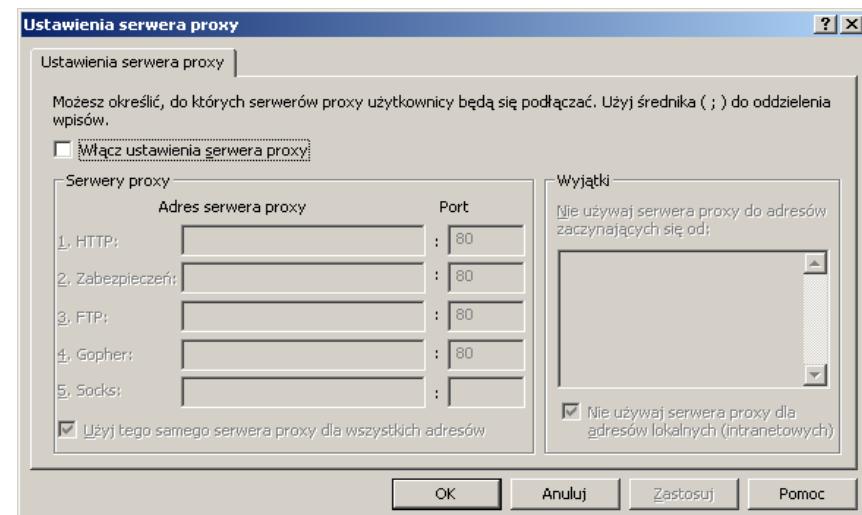
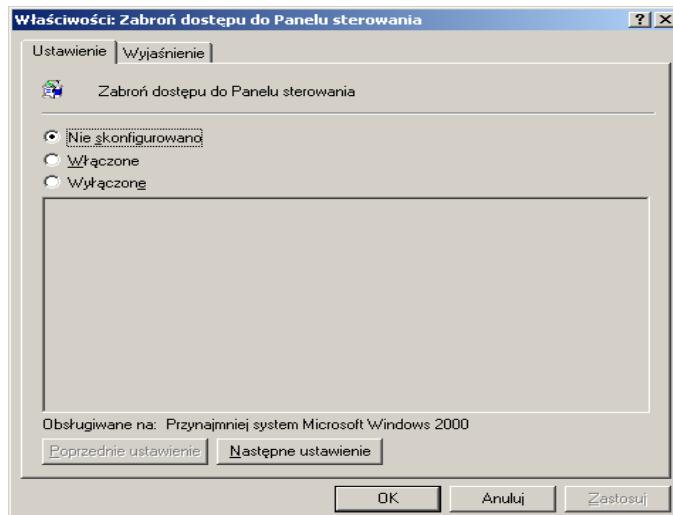


Rys .1 Przykładowy schemat przydziału zasad grupowych



Zasady przetwarzania

- Domyślnie, zasady zastosowane później zastępują zasady zastosowane wcześniej, o ile ustawienia są *Włączone* lub *Wyłączone*. Ustawienia *Nie skonfigurowane* nie mają wpływu na wcześniej zastosowane ustawienia.



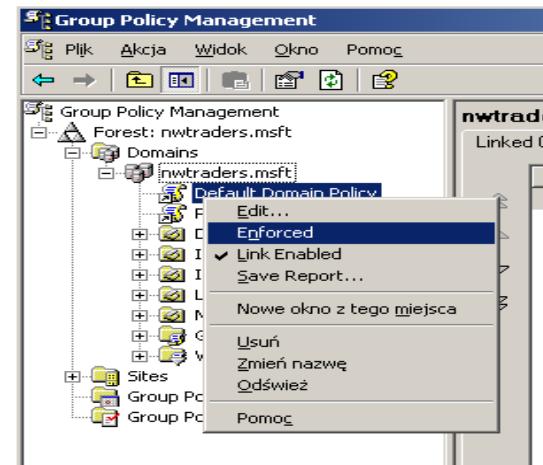


Zasady przetwarzania

Istnieją także mechanizmy pozwalające zmienić domyślne zachowanie omówione powyżej.

Należą do nich są ustawienia:

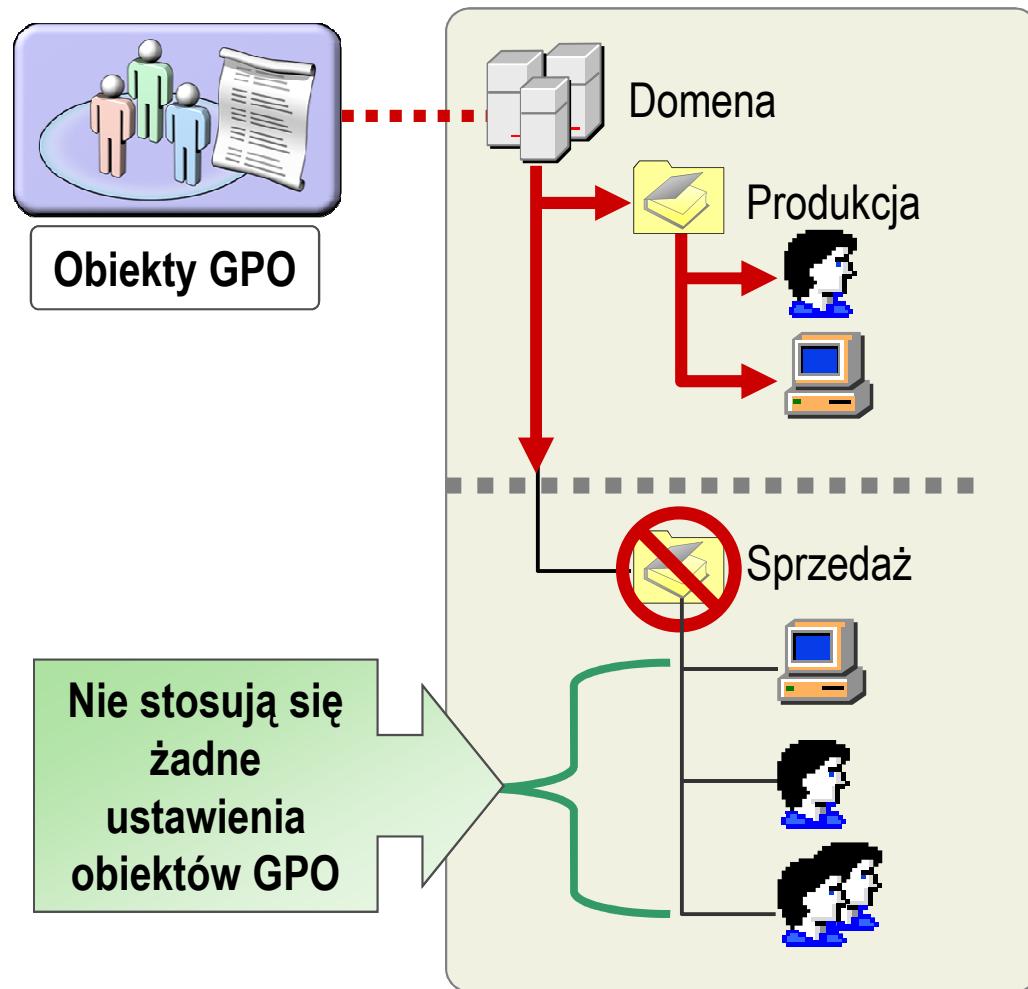
- *Nie zastępuj*
- *Wymuszaj* (gdy stosujemy *Group Policy Management*)





Zasady przetwarzania

- Zablokuj dziedziczenie zasad (nie istnieje dla lokacji)





Identyfikator bezpieczeństwa SID

- Identyfikator bezpieczeństwa (SID) jest unikalną wartością o zmiennej długości, stosowaną do identyfikowania podmiotu zabezpieczeń (użytkownika lub grup zabezpieczeń).
- Identyfikator SID wskazujący określone konto lub grupę, jest generowany przez system w czasie tworzenia tego konta lub grupy.



Identyfikator bezpieczeństwa SID

Notacja SID:

S-R-X-Y1-Y2 . . . -Yn-1-Yn

S - oznacza, że łańcuch znaków jest identyfikatorem SID.

R - stanowi wersję korekty.

X - jest wartością wydawcy identyfikatora.

Y - jest kolekcją wartości podwydawców, gdzie *n* jest liczbą podwydawcy.

Przykłady

S-1-1-0

Wszyscy

S-1-5-<domena>-501

Gość

S-1-5-<domena>-512

Administratorzy domeny

S-1-5-32-544

Administratorzy (konto wbudowane)

S-1-5-32-550

Operatorzy wydruku (wbudowane)

S-1-5-21-1004336348-1177238915-682003330-512

Ostatnia wartość w kolekcji względnie identyfikuje określone konto lub grupę w domenie. Wartością tą jest *identyfikator względny (RID)*

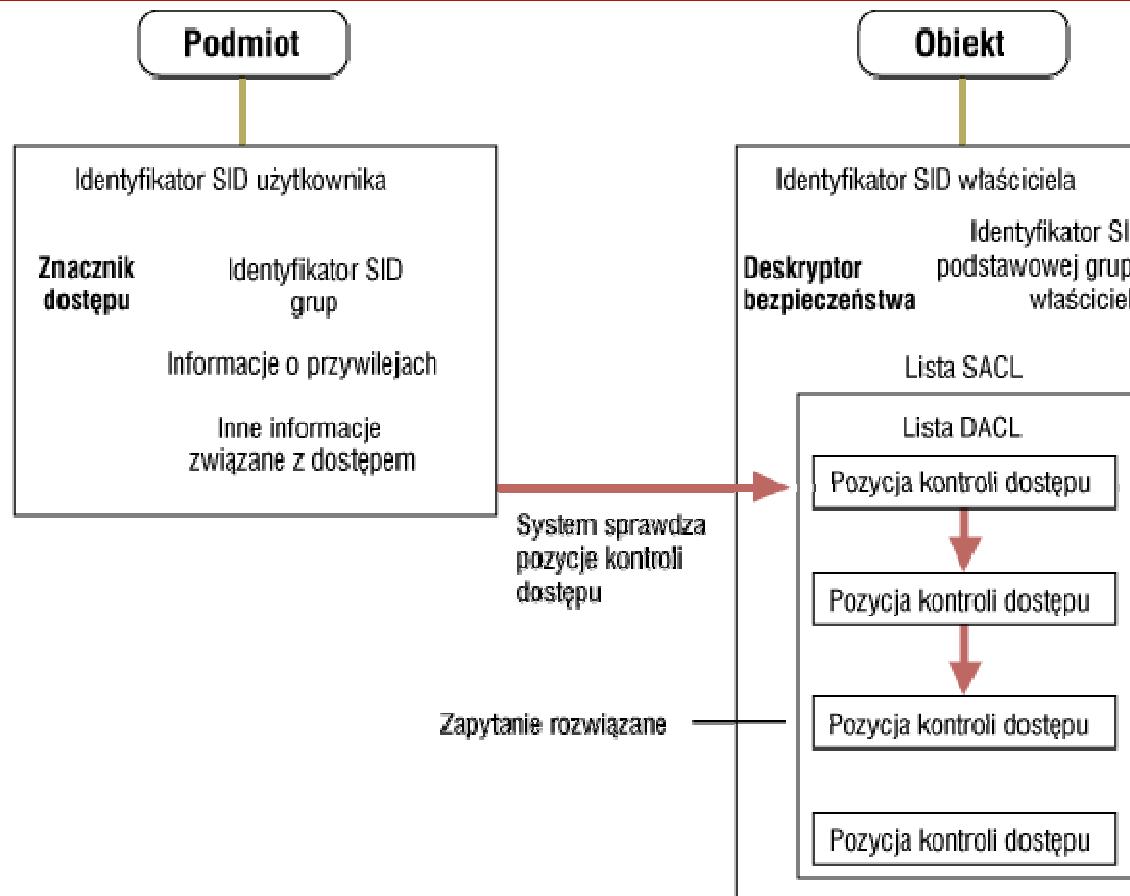


Deskryptory bezpieczeństwa

- **Deskryptor bezpieczeństwa** stanowi strukturę danych binarnych o zmiennej długości, która zawiera informacje bezpieczeństwa związane z obiektem chronionym.



Deskryptory bezpieczeństwa



Rys. 3 Sprawdzanie poprawności żądania dostępu
http://www.microsoft.com/poland/windows2000/win2000serv/SYS_ROZ/roz12.mspx



Lista kontroli dostępu

- Lista kontroli dostępu (ACL) jest uporządkowaną listą złożoną z pozycji kontroli dostępu (ACE) definiujących zabezpieczenia, jakie są stosowane do obiektu i jego właściwości.
- Poszczególne elementy listy ACL są następujące:
 - **Rozmiar listy ACL** Liczba bajtów pamięci przydzielonych dla listy ACL. Rozmiar listy ACL może się ważyć w zależności od liczby i rozmiaru pozycji ACE.
 - **Wersja ACL** Numer wersji korekty struktury danych listy ACL. Numer wersji korekty dla większości obiektów wynosi 2, a dla obiektów Active Directory 4.
 - **Liczba pozycji ACE** Liczba pozycji ACE w liście ACL. Wartość zerowa oznacza, że lista ACL nie posiada żadnej pozycji ACE - jest pusta, dlatego też proces sprawdzania praw dostępu może się skończyć.
 - **Pozycje ACE** Uporządkowana lista zawierająca zero lub więcej pozycji ACE. W trakcie sprawdzania praw dostępu, pozycje ACE są przetwarzane w kolejności wynikającej z ich występowania na liście.



Deskryptory bezpieczeństwa

Rozmiar listy ACL	Wersja listy ACE
Liczba pozycji ACE	
ACE: odmowa dostępu	Jawne pozycje ACE
ACE: zezwolenie dostępu	
ACE: odmowa dostępu	Dziedziczone pozycje ACE
ACE: zezwolenie dostępu	

Rys. 1 Porządek wpisów ACE w liście ACL
http://www.microsoft.com/poland/windows2000/win2000serv/SYS_ROZ/roz12.mspx

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
G R	G W	G E	G A	Zarezerwowane	A S	Standardowe prawa dostępu																								Prawa dostępu specyficzne dla obiektu	

Key	Opis
GR	Ogólne prawo odczytu
GW	Ogólne prawo zapisu
GE	Ogólne prawo uruchomienia
GA	Zbiór wszystkich praw ogólnych
AS	Prawo dostępu do listy SACL

Rys. 2 Maska dostępu dla jednej pozycji ACE
http://www.microsoft.com/poland/windows2000/win2000serv/SYS_ROZ/roz12.mspx



Lista kontroli dostępu

- Wszystkie pozycje ACE zawierają następujące informacje kontroli dostępu:
 - **Identyfikator SID** określa jednoznacznie użytkownika lub grupę
 - **Maska dostępu** 32-bitowa wartość binarna, której bity odpowiadają prawom dostępu do obiektu. Bity można ustawiać lub wyłączać, ale znaczenie ustawienia jest uzależnione od typu pozycji ACE. Jeśli na przykład jest ustawiony bit odpowiadający prawu umożliwiającemu odczyt uprawnień, a typem pozycji ACE jest Odmawiaj, to wtedy pozycja ACE odmawia prawa czytania uprawnień obiektu. Jeżeli ten sam bit jest ustawiony w pozycji ACE typu Zezwalaj, to wtedy pozycja ta uprawnia do czytania uprawnień obiektu.



Kolejność pozycji ACE w liście DACL

- Wszystkie jawne pozycje ACE są umieszczone przed jakimkolwiek dziedzicznymi pozycjami ACE.
- W grupie jawnego pozycji ACE, pozycje odmawiające dostępu są umieszczone przed pozycjami zezwalającymi.
- Dziedziczne pozycje ACE są umieszczone w porządku, w którym były dziedziczone. Pozycje ACE obiektu nadzawanego dziedziczone przez obiekt podzawodny występują w pierwszej kolejności. Następnie występują pozycje ACE dziedziczone z obiektu nadzawanego ponad obiektem nadzawanym i tak dalej w górę drzewa obiektów.



Prawa użytkownika

- Prawo użytkownika jest pełnomocnictwem wykonania operacji dotyczącej całego komputera, a nie tylko określonego obiektu na tym komputerze. Prawa użytkownika dzielone są na dwie kategorie: *prawa logowania i przywileje*.
- Przywileje nadawane użytkownikom upoważniają ich do manipulowania zasobami systemowymi



Konflikty praw użytkownika i uprawnień

- Prawa użytkownika i uprawnienia są konflikcie przeważnie tylko w przypadkach, gdy żądane prawa do administrowania systemem pokrywają się z prawami własności zasobów. W przypadku konfliktu praw, przywilej uchyla uprawnienie (np. przejęcie na własność).



Przykładowe pytania testowe

1. Konto użytkownika może należeć do:

- (a) wielu grup globalnych w domenie
- (b) do wielu JO w domenie
- (c) tylko do jednej JO
- (d) do wielu grup globalnych w drzewie

2. Kolejność wpisów w liście kontroli dostępu ACL jest:

- (a) przypadkowa
- (b) wg wzrastającego identyfikatora SID
- (c) wg malejącego identyfikatora SID
- (d) brak prawidłowej odpowiedzi



Przykładowe pytania testowe

3. Administrator może przejąć folder/plik na własność:

- (a) nigdy
- (b) jeśli ma odpowiednie przywileje
- (c) tylko na DC
- (d) zawsze na stacji członkowskiej

4. Indeks pliku zawarty w rekordzie katalogu z MFT zawiera :

- (a) nazwę pliku
- (b) indeks pliku w MFT
- (c) rozmiar pliku
- (d) informacje o czasie utworzenia pliku



Przykładowe pytania testowe

5. Grupy lokalne komputera mogą być członkami grup:

- (a) globalnych
- (b) lokalnych w domenie, w której istnieją
- (c) uniwersalnych
- (d) brak prawidłowej odpowiedzi

6. „Filtrowanie” obiektu GPO polega na:

- (a) wybraniu opcji aktywnych
- (b) edycji prawa „zastosuj Zasady Grupy”
- (c) wybraniu opcji nie aktywnych
- (d) brak prawidłowej odpowiedzi