

Wprowadzenie do systemu NetWare 6 i usług eDirectory

mgr inż. Agata Skowrońska-
Kapusta, CNA, NAI

Novell Education

www.novell.com

PRESENTATION



Novell.

Tematyka wykładów

1. Wprowadzenie do systemu NetWare i usług eDirectory
2. Zarządzanie zabezpieczeniami eDirectory
3. Konfigurowanie dostępu użytkowników do sieci i zarządzanie nimi
4. Zarządzanie systemem plików
5. Zarządzanie zabezpieczeniami systemu plików
6. Tworzenie skryptów logowania i zarządzanie nimi
7. Drukowanie za pośrednictwem NDPS (Novell Distributed Print Services) i iPrint
8. Narzędzie iFolder
9. Zarządzanie e-mail - GroupWise
10. Zarządzanie bezpieczeństwem sieci NetWare

Literatura

1. „Foundations of Novell® Networking”, kurs 3001, Podręcznik uczestnika
2. „Novell NetWare. Poradnik administratora sieci”, red. W.Łabuda, Forum Media (poradnik aktualizowany)
3. PC WORLD KOMPUTER SPECIAL „Przewodnik po systemie NOVELL”, nr 2/2003
4. „NetWare 5”, J.E.Gaskin, EXIT 1998
5. „NetWare 5 nowa wersja systemu”, M.G.Moncur, J.Wm.Jenkins, J.Chellis, Mikom 1999
6. „Ćwiczenia z ... Novell NetWare 5”, M.Filocha, M.Trusiewicz, Mikom 2002
7. „Novell NetWare 5.x Ćwiczenia praktyczne”, W.Wrotek, HELION 2001
8. <http://www.novell.pl/products/netware/index.html>
9. <http://ptun.org.pl>, <ftp://ptun.org.pl>
10. <http://www.pckurier.pl/akademia/novell/>
11. <http://www.idg.pl/szukaj/szukaj.asp?qr=NetWare&sc=Rpix>
12. <http://nw65da2.digitalairlines.com>

Czym jest usługa katalogowa?

Usługi katalogowe są **specjalizowanym typem baz danych**, przeznaczonym przede wszystkim do szybkiego czytania, przeglądania i przeszukiwania - przy czym są to bazy nie-relacyjne, zazwyczaj **hierarchiczne**. Wykorzystywane są w rozmaity sposób:

- począwszy od prostych (w zastosowaniach) usług, typu samodzielna książka adresowa, czasem uwzględniająca podział na jednostki organizacyjne w przedsiębiorstwie,
- poprzez katalogi certyfikatów/kluczy publicznych w usługach PKI/X.509,
- proste aplikacje umożliwiające przechowywanie informacji o użytkownikach,
- ich ewentualne uwierzytelnianie w systemie,
- mechanizmy zarządzania użytkownikami, z których korzysta równolegle wiele usług,
- po rozbudowane bazy zarządzające pracą całej sieci: informacjami o użytkownikach, systemach, udostępnianych aplikacjach (z ewentualnym automatycznym mapowaniem tego na usługi, takie jak Service Location Protocol (SLP) w wypadku novellowego eDirectory lub rekordy SVR w wypadku Active Directory).

Definicja (wikipedia)

Usługa katalogowa - baza danych zawierająca następujące obiekty: użytkowników, aplikacje, urządzenia sieciowe i inne zasoby sieciowe. Usługa katalogowa musi być przynajmniej częściowo obiektową bazą danych reprezentującą użytkowników sieci i zasoby, co pomaga zarządzać relacjami między ludźmi a sieciami, urządzeniami sieciowymi, aplikacjami sieciowymi i zawartymi w sieci informacjami.

Usługa katalogowa zapewnia administratorom jeden, logiczny i precyzyjny sposób opisu wszystkich urządzeń i usług sieciowych. Oferuje ona dostęp za pośrednictwem bezpiecznego logowania się i hierarchicznie organizuje zasoby sieciowe (takie jak: użytkowników, drukarki, zespoły robocze, aplikacje, woluminy, serwery plików, serwery baz danych, obiekty itp.) na drzewie katalogowym. Usługa katalogowa zapewnia bezpieczeństwo, kontrolując dostęp i oferując pewien stopień odporności na błędy.

Typy serwisów katalogowych:

- zamknięte
- oparte na standardach (X.500, LDAP)
- hybrydowe
- usługi meta-katalogowe

Czym jest usługa katalogowa?

Usługi katalogowe stworzono do organizowania sieci komputerowych. Funkcjonują one tak jak książki telefoniczne.

Analogicznie do posługiwania się nazwiskiem do odszukania czyjegoś adresu i numeru telefonu, zadajemy usłudze katalogowej **znalezienie nazwy usługi** (na przykład nazwy folderu lub drukarki), a ona informuje nas, gdzie się mieści ta usługa.

Usługom katalogowym można zlecać **przeszukiwanie również według właściwości**. Przykładowo, jeśli zadamy znalezienie wszystkich elementów będących „drukarkami”, usługa katalogowa stworzy kompletną listę drukarek, niezależnie od tego, gdzie w sieci one się znajdują. Usługi katalogowe umożliwiają łatwe przeszukiwanie wszystkich zasobów sieci, za pomocą ujednoliconej listy zorganizowanej w strukturze drzewa.

Zasadniczą korzyścią płynącą z usług katalogowych jest **pozbycie się** za ich pomocą **potrzeby zarządzania duplikatami elementów sieci**. Przykładowo, nie trzeba posiadać oddzielnych list użytkowników na każdym serwerze. Zamiast tego zarządzają się jednym zestawem kont użytkowników, istniejącym w usłudze katalogowej, i przypisuje się im konkretne upoważnienia do różnych zasobów dostępnych na różnych serwerach. Inne zasoby działają w ten sam sposób i są centralnie zarządzane w usłudze katalogowej.

Rodzaje usług katalogowych - Novell

- **NDS - Novell Directory Services** jest usługą, która jest najdłużej w użyciu (oparta o protokół X.500). Usługa NDS jest uruchamiana na serwerach NetWare 4.x i nowszych, i jest również dostępna dla innych systemów operacyjnych (takich jak Windows NT/2000), co pozwala na wykorzystanie NDS jako pojedynczej usługi katalogowej do zarządzania siecią opartą na systemach wielu producentów.
- **eDirectory** - następca usługi NDS (od wersji 6.0) dostępny za pomocą protokołu LDAP, uruchamiany na serwerach NetWare 5.x i 6.x. NDS eDirectory działa także na systemach Linux, Solaris, Compaq Tru64 UNIX i Windows NT/2000.

Główne cechy charakteryzujące NDS / eDirectory to:

- możliwość podziału na partycje, czyli wyodrębnione części, które mogą być dystrybuowane na wybrane serwery (brak zbędnej replikacji);
- możliwość dowolnego sposobu kształtowania dostępu do danych w replice (kopii partycji) - repliki mogą mieć typ Master, Read/Write, Read Only i dodatkowo istnieje możliwość wprowadzenia filtrowania replikowanych atrybutów (oprócz Master);
- duża skalowalność - możliwe jest osiągnięcie katalogu o rozmiarze przekraczającym 1 miliard obiektów;
- wieloplatformowość.

Rodzaje usług katalogowych - Microsoft

• **Domeny Windows NT** nie są właściwie kompletnymi usługami katalogowymi, ale zapewniają kilka ich podstawowych funkcji. Domena posiada płaską strukturę pozbawioną podziału na kontenery - wszystkie obiekty położone są na jednym poziomie. Domena pozwala na przechowywanie informacji o ograniczonej stałej ilości typów obiektów (konto użytkownika lub komputera, grupa) z ograniczoną stałą ilością atrybutów. Domeny są technologicznie ograniczone ilością przechowywanych obiektów (do ok. 40 tys. obiektów w jednej domenie) oraz nie są oparte na żadnym otwartym protokole - nie ma możliwości dostępu z aplikacji innych producentów bez wykorzystania bibliotek firmy Microsoft.

• **Active Directory** to usługa katalogowa dla systemów Windows (Windows 2003 Server oraz Windows 2000), zgodna ze specyfikacją LDAP w wersji 3.0. Active Directory jako następcza domen systemu Windows NT usuwa największe wady domen, tj. wprowadzono:

- hierarchiczność przechowywania informacji
- dużo wyższe limity przechowywania informacji (powyżej 1 miliona obiektów w domenie Active Directory)
- rozszerzalność schematu zawierającego definicje obiektów.

Rodzaje usług katalogowych - standardy

- **X.500 DAP - Directory Access Protocol**, jest usługą katalogową o międzynarodowym standardzie wyposażoną w komplet funkcji. Jednak X.500 posiada ich aż tyle, że posługiwanie się i zarządzanie nimi staje się prawie niemożliwe, dodatkowo DAP funkcjonuje tylko w strukturach OSI.
- **LDAP - Lightweight Directory Access Protocol**, został opracowany jako podzestaw do X.500 w odpowiedzi na złożoność X.500 (dla struktur TCP/IP). Pokrewieństwo między LDAP i X.500 jest bardzo silne. LDAP został pomyślany jako metoda dostępu do katalogów X.500. Nie wymaga wprowadzić, ażeby to był konkretnie katalog X.500, ale używa jego terminów i definicji opisujących katalog.

Jest on implementowany w różnych produktach bądź jako system identyfikujący, bądź też system pocztowy albo aplikacja handlu elektronicznego. Do dziś pojawiło się na rynku ponad 60 serwerów LDAP. Przepuszczalnie ok. 90% tych produktów to samodzielne serwery LDAP, podczas gdy w pozostałych 10% jest sprzedawane jako składnik zintegrowany z innymi aplikacjami.

Dla systemu Linux dostępne są nieodpłatnie dwa serwery LDAP: U-Mich LDAP i OpenLDAP. To drugie rozwiązanie staje się powoli standardem dla Linuksa (i innych systemów UNIX).

Dokumenty: RFC-1777, RFC-1778, RFC 1823, RFC 2251-2256

Produkty LDAP

Tabela 1. Zalety i wady testowanych produktów LDAP

Producent	Nazwa produktu	Zalety	Wady
IPlanet (d. Netscape)	Directory Server	świetne operacje LDAP, wybitna dokumentacja	stosunkowo nieliczne usługi wspierające (<i>back-end</i>)
Innosoft	IDDS and Directory Portal 4.5	szerokie, wieloplatformowe wsparcie, łatwa instalacja, tworzenie łańcuchów wspierane przez LDAP	ręczne konfigurowanie za pośrednictwem plików konfiguracyjnych
Critical Path (Isocor)	Global Directory Server 3.0	dobre wsparcie X.500	niestaranna integracja LDAP-X.500, produkt zbyt skomplikowany
Novell	NDS eDirectory	integracja z wieloma platformami systemowymi	fragmentaryczne narzędzia zarządzające, serwer nie wytrzymuje większych obciążeń
Siemens	DirX 5.0	liczne i wydajne narzędzia zarządzania, dobra integracja X.500-LDAP	problemy z LDAP przy dużym obciążeniu, produkt skomplikowany
Computer Associates	eTrust Directory	mocne wsparcie X.500, wieloplatformowe narzędzia replikowania	trudny w użyciu interfejs zarządzający, produkt skomplikowany
Oracle	Oracle Internet Directory	bardzo dobry edytor schematów	brak możliwości bezpośredniej komunikacji z bazą danych

Drzewa katalogowe

Wspólnym elementem usług katalogowych jest ich organizacja, oparta na schemacie **drzewa**, w pewnym sensie podobna do organizacji katalogów na twardym dysku.

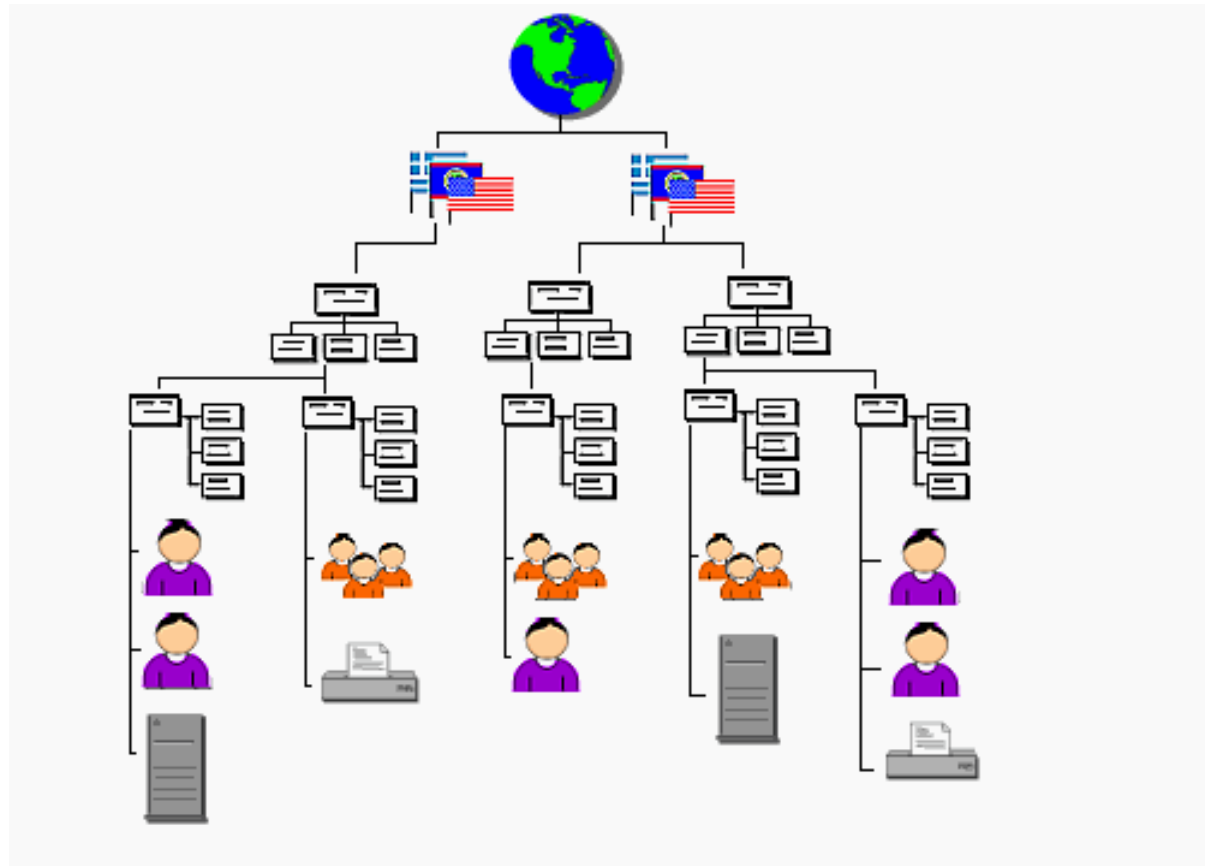
Na szczycie drzewa katalogowego znajduje się katalog główny (Root), od którego odchodzą pozostałe elementy. Są to albo „gałęzie” albo „liście”.

Liść reprezentuje faktyczny zasób w sieci, taki jak stacja robocza, drukarka, wspólny katalog, plik lub konto użytkownika.

Z kolei **gałąź** jest elementem, który zawiera w sobie kolejne elementy, które również mogą się dalej „rozgałęziać” - w przeciwieństwie do liścia, który nie może już w sobie zawierać innych obiektów.

Wszystkie obiekty drzewa katalogowego posiadają **atrybuty** (czasami zwane **właściviwościami**), które różnią się od siebie, w zależności od typu obiektu, do którego są przypisane.

Drzewa katalogowe

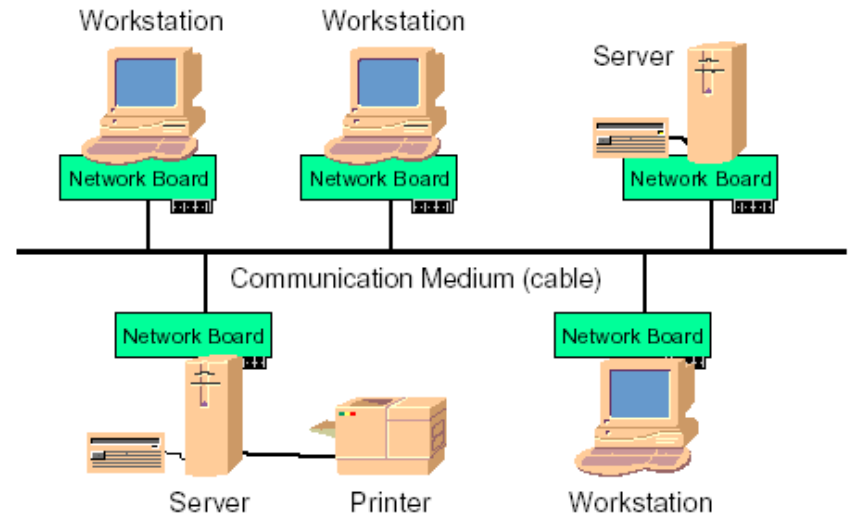


Wprowadzenie do systemu NetWare i usług eDirectory

1. Cechy systemu operacyjnego NetWare 6
2. Zarządzanie NetWare 6
3. Instalacja i zarządzanie klientem Novella
4. Katalog eDirectory i obiekty eDirectory
5. Rola usług eDirectory
6. Wpływ struktury drzewa eDirectory na sposób uzyskiwania dostępu do zasobów

Sieć i jej składniki

Jakie znane architektury sieciowych systemów operacyjnych?



Funkcje serwerów sieciowych

- **Serwer plików** służy do przechowywania i organizowania dostępu do danych zapisanych w pamięciach dyskowych.
- **Serwer drukowania** steruje współużytkowaniem drukarek i innych urządzeń peryferyjnych.
- **Serwer komunikacyjny** zapewnia łączność między oddalonymi od siebie sieciami lokalnymi lub samodzielnymi stacjami roboczymi.
- **Serwer baz danych** zajmuje się organizowaniem dostępu do dużej ilości danych zorganizowanych w bazy danych.
- **Serwer pocztowy** zapewnia obsługę poczty elektronicznej.
- **Serwer aplikacji** umożliwia uruchomienie aplikacji dla terminali.

Ogólna charakterystyka systemu Novell NetWare

System NetWare to sieciowy system operacyjny (opracowany przez firmę Novell) instalowany na dedykowanym komputerze, który pełni rolę tylko serwera.

Klientami systemu NetWare mogą być stacje robocze pracujące pod różnymi systemami (DOS, Windows, Linux, Macintosh, OS), na których instalowane jest dodatkowe oprogramowanie umożliwiające współpracę z serwerem NetWare. Oznacza to, że stacje robocze nie pracują pod kontrolą systemu NetWare - system operacyjny reprezentowany jest tylko przez oprogramowanie klienta.

System NetWare jest zestawem oprogramowania. Niektóre z jego składników działają wyłącznie na serwerze NetWare, inne - tylko na stacjach roboczych. Większość zadań administracyjnych jest wykonywana ze stacji roboczej.

System Novell NetWare jest sprzedawany na pewną liczbę licencji. Przez licencję (do wersji 5.x i dla rozwiązań edukacyjnych) rozumiemy możliwość aktywnego połączenia z serwerem. Dla wersji wyższych licencja = konto użytkownika w eDirectory.

Historia systemu Novell NetWare

1983r. - pierwsza wersja systemu NetWare dla komputerów opartych na procesorze Intel 8088.

1986r. - wersja 2.0 (procesor Intel 80286), która zapewniała większą funkcjonalność dzięki wprowadzeniu m.in. możliwości łączenia sieci.

1987r. - Novell wprowadził system SFT NetWare wyposażony w kilka poziomów ochrony danych.

1989r. - po kolejnych wersjach 2.x, pojawił się system oznaczony jako NetWare 386 (wersja 3.0) dla procesorów Intel 80386/80486.

1990r. - ulepszona wersja 3.1, a w lutym 3.11.

1993r. - wersja 4.0 - wprowadzała szereg nowych usług (DNS, protokół IP).

1996r. - kolejne wersje 4.x (do 1996), najdojrzalsza wersja 4.11.

1998r. - NetWare 5 (Moab), nakierowana głównie na Internet (IP).

1999r. - NetWare 5.1 (Cobra)

2001r. - NetWare 6.0

2003r. - NetWare 6.5 (Nakoma)

Sieciowe systemy operacyjne Novella - obecnie

Pod koniec grudnia 2004r. Novell udostępnił publiczną wersję beta systemu **Open Enterprise Server** (OES), a wersję pełną w marcu 2005r.

OES stanowi połączenie systemów **NetWare** i **SUSE LINUX Enterprise Server**. Udostępnia klientom ujednolicone narzędzia administracyjne, usługi oparte na technologii katalogowej oraz cały system pomocy technicznej stworzony przez firmę Novell.

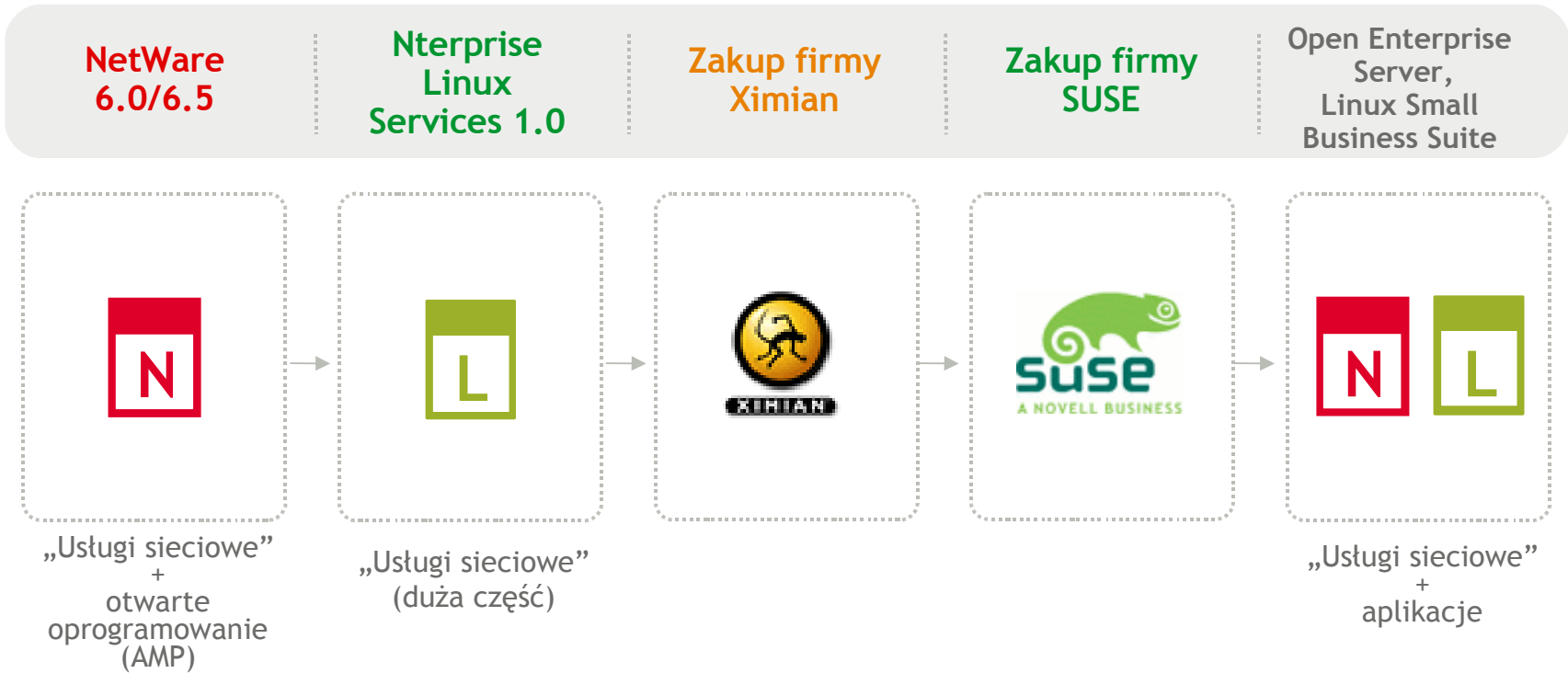
Udostępnia usługi sieciowe, które działają w oparciu o jądra systemów NetWare i Linux, m.in. zaawansowane usługi w dziedzinie plików i drukowania, usługi dotyczące tożsamości oraz usługi instalowania i poprawek / aktualizacji.

Cechy Open Enterprise Server

- usługi katalogowe eDirectory
- oprogramowania klastrowe (klastery do 32 serwerów)
- uaktualnianie (z NetWare do NetWare lub z NetWare do Linuksa)
- pakiet narzędzi wspomagających Virtual Office
- wirtualny dysk iFolder (Windows i Linux)
- system zdalnego druku - iPrint (NetWare, Linux)
- narzędzia zarządzania składowaniem danych Novell Storage Services (Linux)
- zintegrowany zestaw narzędzi administracyjnych iManager (NetWare, Linux)

Więcej informacji o tym produkcie oraz pakiet OES (ok. 4,6 GB) można znaleźć na stronie: - www.novell.com/products/openenterpriseserver

Ewolucja platform serwerowych



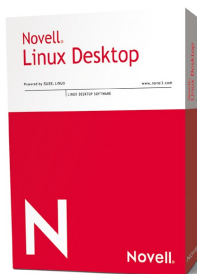
Podstawy rozwiązań linuksowych - rodzina produktów SUSE LINUX

Rozwiązania
serwerowe
**SUSE
LINUX
Enterprise
Server**



x86, AMD 64,
Itanium,
Opteron,
iSeries, p-Series,
z-Series

Rozwiązania
desktopowe
**NOVELL
LINUX
Desktop**



SUSE LINUX
Professional
(pudełka)



Rynek masowy

Rynek korporacyjny

Produkt na rynek masowy (retail)

SUSE LINUX Professional 10.1

Brak mechanizmu opieki nad oprogramowaniem

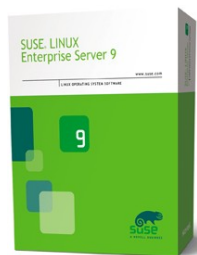
Brak profesjonalnej oferty pomocy technicznej

Co 6 miesięcy nowa wersja

Wprowadzane wszystkie nowości Linuksowe (nie zawsze do końca sprawdzone)

Potem nowości są wprowadzane do wersji korporacyjnych

Produkty na rynek korporacyjny



Opieka nad oprogramowaniem (Upgrade Protection)

Poprawki

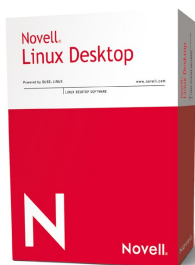
Testy integracyjne

Testy zgodności

Certyfikacje

Nowe funkcje

Nowe wersje



Pomoc techniczna

Zgłaszanie incydentów

Zróżnicowane pakiety

pomocy technicznej

Obsługa instalacja,

Konfiguracja, Tuning

Dostępna w Polsce -

Novell Professional

Services Poland



Gwarantowany 5 letni cykl życia i wspomagania produktu

SUSE LINUX Enterprise Server 9

Bezpieczna i stabilna platforma przetwarzania dla firm, oparta o otwarte oprogramowanie

Nieźródnana wydajność i skalowalność

Bogate narzędzia do zarządzania i administracji systemem

Wysoka dostępność (*High Availability*), klastry i przełączanie aplikacji (*fail-over*)

Szerokie wsparcie dla aplikacji

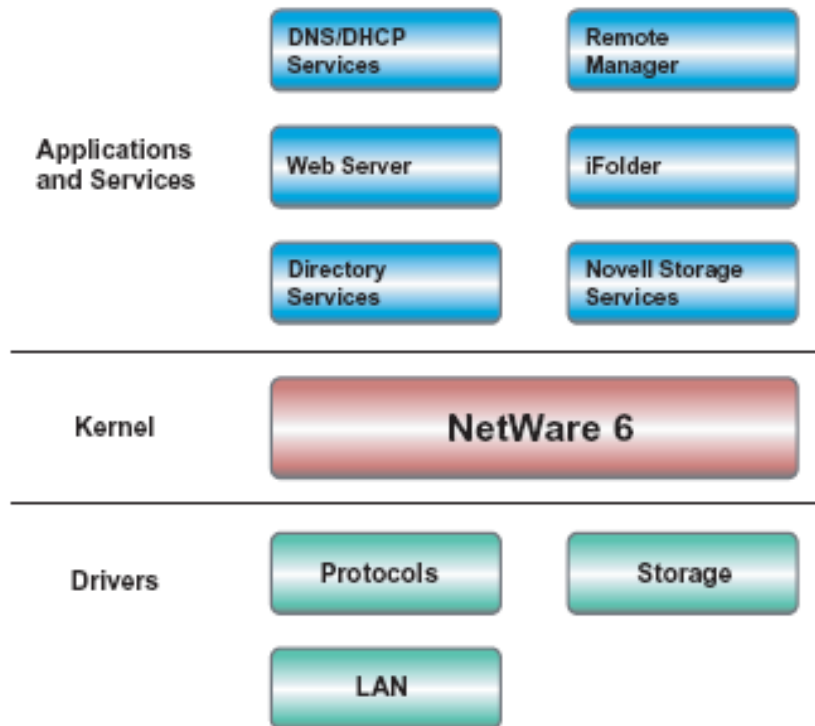
Zaplecze Novella największego ekosystemu wsparcia zorientowanego na Linuksa i otwarte oprogramowanie



Cechy systemu NetWare 6

- **eDirectory** - usługa niezależna od platformy, oparta na protokole LDAP. eDirectory zarządza obiektami, takimi jak użytkownicy, aplikacje, usługi sieciowe i dane.
- **iFolder** - umożliwia użytkownikom dostęp do ich danych z każdego miejsca, w dowolnym czasie.
- **iPrint** - zapewnia globalny dostęp do usług drukowania przez przeglądarkę internetową.
- **NetWare Web Access** - spersonalizowany interfejs, umożliwiający dostęp do ważnych zasobów sieciowych z każdego miejsca.
- **Novell Cluster Services** - niezawodny, odporny na błędy i nieprzerwany dostęp do sieci.
- **File protocols** - wsparcie dla protokołów plików dla Macintosh, UNIX, Windows NT/2000, i Linux.
- **Network management** - narzędzia do zdalnego zarządzania siecią, NetWare Remote Manager.
- **Novell Storage Services** - szybki dostęp do danych sieciowych, wsparcie dla dużych pojemności danych.
- **Multilingual support.**

Komponenty systemu NetWare 6



Architektura systemu NetWare składa się z trzech warstw:

- **aplikacji i usług**, odpowiedzialnej za funkcjonowanie wielu usług systemu NetWare,
- **jądra systemu (kernel)**, zarządzającej wszystkimi istotnymi mechanizmami systemu (m.in. bezpieczeństwem),
- **sterowników (drivers)**, odpowiedzialnej za komunikację z urządzeniami peryferyjnymi.

Sterowniki

LAN drivers. Są odpowiedzialne za komunikację pomiędzy systemem operacyjnym a kartą sieciową. Plik sterownika karty sieciowej musi mieć rozszerzenie LAN.

Storage drivers. Są odpowiedzialne za komunikację pomiędzy systemem operacyjnym a systemem pamięci masowej.

Kontroler urządzenia pamięci masowej (IDE czy SCSI) komunikuje się z komputerem za pomocą sterownika, zwanego modułem kontrolera głównego (**HAM - Host Adapter Module**).

Urządzenia pamięci masowej (dyski, CD-ROM, streamer) wymagają osobnego sterownika zwanego modułem urządzenia własnego (**CDM - Custom Device Module**).

Ponieważ pojedynczy kontroler może sterować kilkoma urządzeniami pamięci masowej różnych typów, komputer może wymagać obecności tylko jednego modułu HAM, nawet jeśli w komputerze zainstalowanych jest kilka różnych urządzeń, a co za tym idzie, kilka modułów CDM.

Protocols.

Kernel

Jądro systemu NetWare udostępnia podstawowe funkcje używane przez aplikacje uruchamiane na serwerze. Zarządza wieloma procesami, zwanymi wątkami i planuje zasoby procesora.

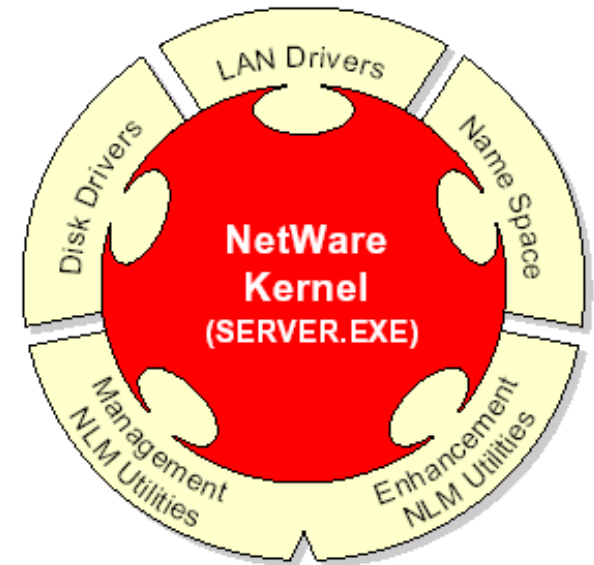
Moduł NLM (NetWare Loadable Module) jest programem serwera, który uzupełnia funkcje i usługi serwera NetWare. Zadaniem modułów NLM jest połączenie programów obsługi dysków, programów obsługi kart sieciowych, modułów przestrzeni nazewnicznej, programów narzędziowych i rozszerzeń serwera z systemem operacyjnym.

Moduł NLM może zostać wczytany i usunięty z pamięci serwera, co zazwyczaj nie ma wpływu na normalne funkcjonowanie serwera.

Kernel

W systemie NetWare występują cztery rodzaje wczytywanych modułów:

- **Programy obsługi dysków** - sterują komunikacją między systemem operacyjnym serwera a urządzeniami pamięci masowej. Ponieważ programy obsługi dysków są modułami NLM, w trakcie pracy serwera jest możliwe wczytywanie i usuwanie programów obsługi dysków.
- **Programy obsługi kart sieciowych** - sterują komunikacją między systemem operacyjnym serwera a kartami sieciowymi. W trakcie pracy serwera można usunąć jeden program obsługi karty sieciowej z pamięci i wczytać nowy. Moduły te mają rozszerzenie LAN.
- **Moduły przestrzeni nazwicznej** - pozwalają na przechowywanie na woluminach NetWare nazw plików niezgodnych z formatem DOS-u. Moduły te mają rozszerzenie NAM.
- **Programy narzędziowe NLM.** Większość modułów NLM stanowią programy narzędziowe oraz moduły aplikacji serwera. Pozwalają one na uruchamianie usług nie wbudowanych w rdzeń systemu operacyjnego. Te moduły mają rozszerzenie NLM.



Aplikacje i usługi

- **Directory Services.**
- **DNS/DHCP Services.**
- **Remote Manager Service.**
- **Web Services:** Enterprise Web Server i NetWare Web Search Server.
- **Novell iFolder Service.**
- **Novell Storage Services (NSS).**

Współpraca systemu NetWare z innymi systemami operacyjnymi

- NetWare nie posiada własnego systemu bootującego - korzysta z plików systemowych DOS (IO.SYS, MSDOS.SYS, i COMMAND.COM). Po starcie systemu DOS uruchamiany jest plik SERVER.EXE (z katalogu C:\NWSERVER), odpowiedzialny za uruchomienie systemu operacyjnego NetWare.
- NetWare 6 może współpracować ze stacjami roboczymi pracującymi po różnych systemami operacyjnymi takimi jak np. DOS, Macintosh, Linux, Windows NT, Windows 2000, czy Windows XP.

Klient Novella

Klient Novella odgrywa zasadniczą rolę w procesie komunikowania się stacji roboczej z siecią. Współpracuje z innymi elementami oprogramowania stacji roboczej, zwłaszcza z systemem operacyjnym, zapewniając:

- **Dostęp do usług NetWare**, które obejmują: drukowanie na drukarce sieciowej, zapisywanie plików na serwerze plików, wyszukiwanie i otwieranie plików w sieci.
- **Wdrożenie zabezpieczeń sieciowych** w celu umożliwienia korzystania z sieci tylko uprawnionym osobom.
- **Zarządzanie przesyłaniem danych** w poprawnym formacie, tak aby inne urządzenia pracujące w sieci mogły rozumieć i odbierać dane.

Klient Novella wykonuje te zadania działając jako program na stacji roboczej. Udostępnia okno, w którym użytkownik - aby uzyskać dostęp do sieci - podaje swój identyfikator i hasło.

Instalowanie oprogramowania klienta Novella

Oprogramowanie klienta Novella wchodzi w skład pakietu NetWare 6 - znajduje się na jednym z CD-ROMów; lub można je pobrać ze stron:

<http://support.novell.com/> - *oficjalna strona Novella*

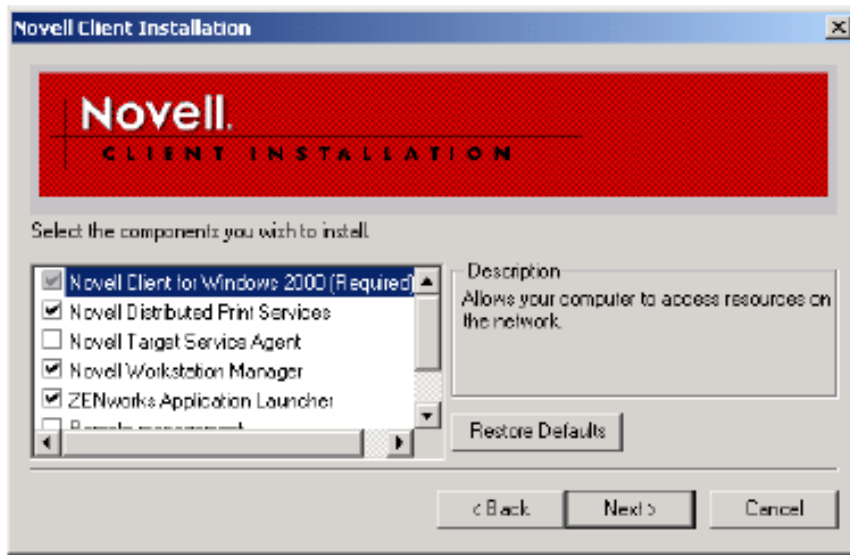
<ftp://ftp.ptun.org.pl/> - *ftp Polskiego Towarzystwa Użytkowników Novella*

Oprogramowanie klienta instalujemy na stacji roboczej. W zależności od tego, czy stacja robocza działa pod kontrolą systemu operacyjnego Windows 9.x czy Windows NT/2000/XP potrzebna jest inna wersja oprogramowania klienta Novella.

Klient Novella nie może jednak pracować samodzielnie. Do jego funkcjonowania niezbędna jest ścisła współpraca z osprzętem stacji roboczej i z jej systemami operacyjnymi.

Po zainstalowaniu klienta stacja robocza zostanie zaopatrzona w nową ikonę logowania się za pomocą klienta Novella. Dwukrotne kliknięcie na tej ikonie uruchomi proces logowania, umożliwiając użytkownikowi zalogowanie się do sieci i korzystanie z niej.

Opcje konfiguracyjne oprogramowania klienta Novella



- Novell Client for Windows 2000
- Novell Distributed Print Services
- Novell Target Service Agent
- Novell Workstation Manager
- ZENworks Application Launcher
- Remote Management
- ZENworks Imaging Service

Protokoły sieciowe:

- IP (*Internet Protocol*)
- IPX (*Internetwork Packet Exchange*)

Procedura logowania

Dostęp do sieci uzyskuje się za pomocą procedury logowania. Aby się zalogować użytkownik musi:

- Używać stacji roboczej z zainstalowanym oprogramowaniem klienta Novella;
- Mieć aktywne połączenia z siecią NetWare;
- Mieć nadane poprawny identyfikator i hasło.

Identyfikator, którym użytkownik posługuje się przy logowaniu, jest **identyczny z nazwą** przypisanego mu **obiektu typu User**.

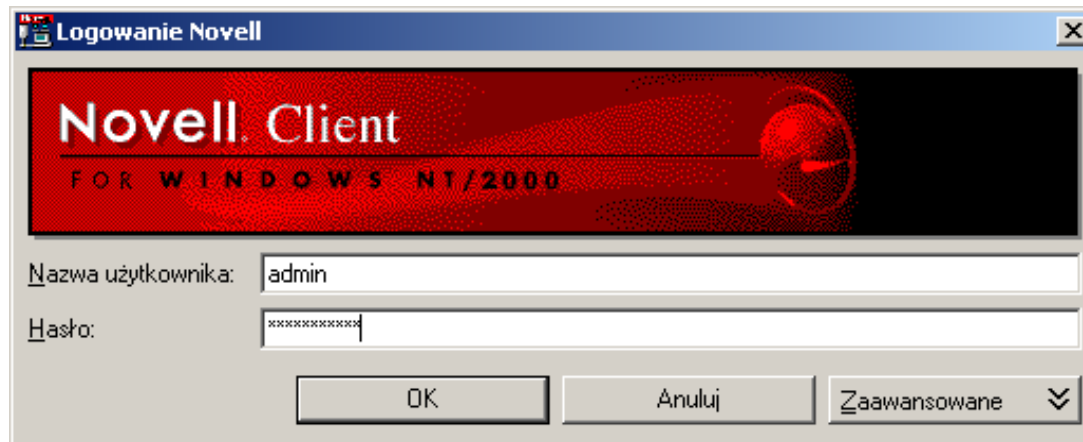
Użytkownik, który się wyloguje, zostaje odłączony od sieci. Rozwiązanie takie ma na celu ochronę plików sieciowych przed niepowołanymi osobami.

Procedura logowania

Po zainstalowaniu klienta Novella można logować się do sieci na różne sposoby:

- Użyć okna logowania klienta Novella, pojawiającego się przy uruchomieniu stacji roboczej;
- W systemie Windows za pomocą przycisku **START** i polecenia logowania;
- Kliknąć na ikonie **N** widocznej na pasku poleceń Windowsa, po czym wybrać polecenie *Logowanie NetWare*.

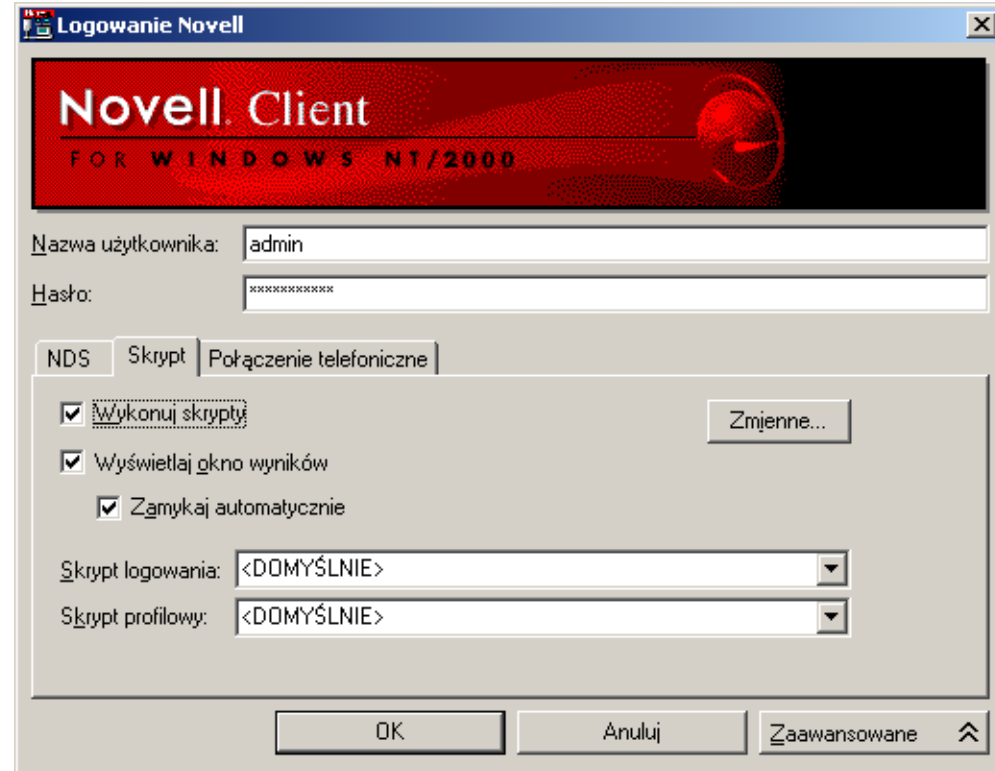
Z logowaniem do sieci wiąże się pojęcie kontekstu. Kontekst obiektu opisuje jego położenie w drzewie katalogu. Drzewo katalogu jest utworzone w taki sposób, aby odzwierciedlało strukturę organizacji.



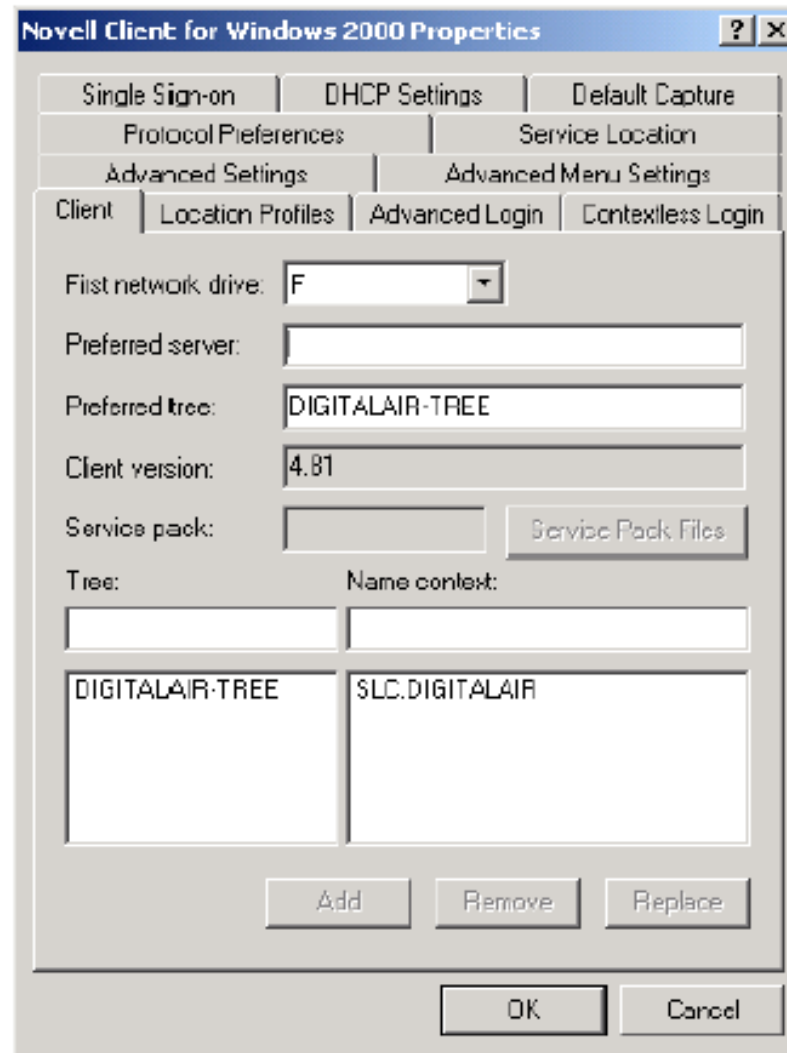
Skrypty logowania

Podczas logowania klient Novella umożliwia wykonywanie specjalnych poleceń, które zapewniają użytkownikowi dostęp do określonych zasobów sieciowych (np. drukarek lub plików).

Polecenia te zapisywane są w postaci **skryptów logowania**. W oknie logowania, na zakładce *Skrypt* wyświetlane są parametry skryptu logowania, z których korzysta klient Novella, gdy zostanie zapoczątkowany proces logowania.



Konfiguracja Klienta Novella



Katalog i obiekty eDirectory

Usługi eDirectory są usługami katalogowymi udostępniającymi bazę danych o wszystkich zasobach sieciowych. Baza ta nazywana jest **Katalogiem**.

Wszystkie serwery NetWare znajdujące się w tej samej sieci mają informacje o wszelkich zasobach sieciowych, ponieważ używają tego samego Katalogu.

Każdy zasób sieciowy ma swój własny wpis w Katalogu identyfikowany przez unikatową nazwę. Użytkownik żąda dostępu do zasobu podając właśnie tę nazwę.

Schemat (schema) eDirectory

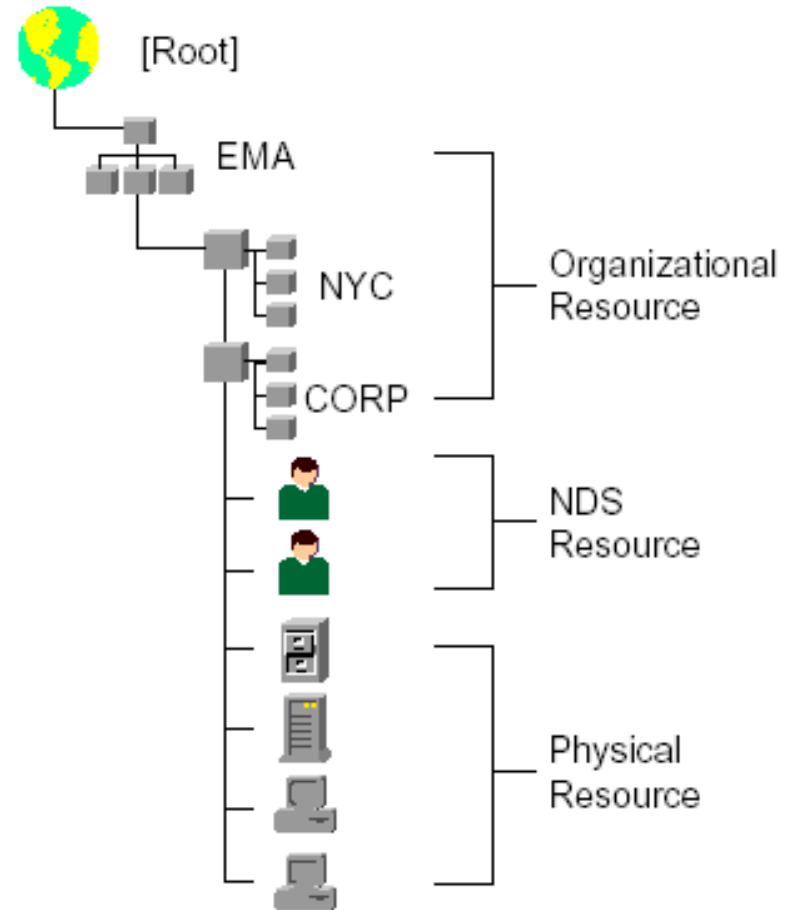
Schemat opisuje zależności podrzędności i nadrzędności między obiektami. Definiuje każdy obiekt jako **element pewnej klasy** (oznacza to, że są obiekty mające pewne wspólne cechy), **która może dziedziczyć atrybuty po innych klasach schematu.**

Schemat opisuje i definiuje **dozwolone klasy obiektów eDirectory**, ich **właściwości** oraz reguły tworzenia i istnienia. Określa też, w jaki sposób obiekty mogą dziedziczyć właściwości i prawa nadrzędnych obiektów. Ponadto definiuje strukturę drzewa eDirectory oraz sposób nazywania występujących w nim obiektów.

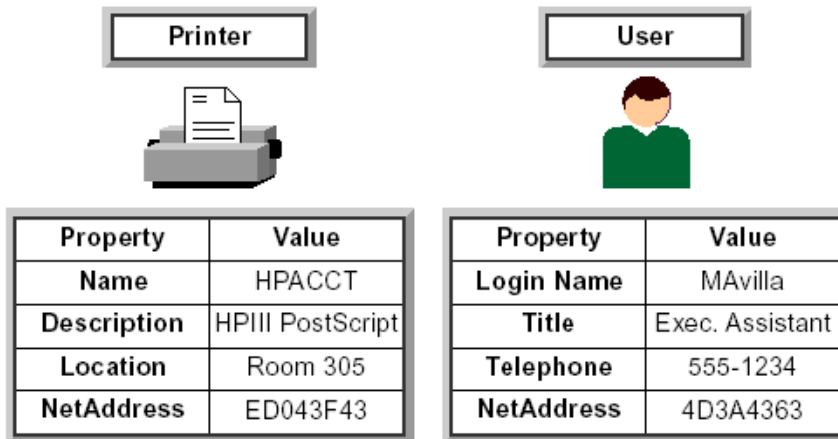
Struktura Katalogu

Katalog składa się z obiektów, cech i wartości:

- **Obiekt** - zawiera informacje o konkretnym zasobie (odpowiednik rekordu w tradycyjnej bazie danych). Usługi eDirectory przedstawiają poszczególne zasoby sieciowe jako obiekty w Katalogu. Obiekt może być zasobem fizycznym (stacja robocza), zasobem eDirectory (grupa) lub zasobem organizacyjnym (kontener).
- **Cecha** - to jednostkowa informacja charakteryzująca dany obiekt.
- **Wartość** - to dana przypisana do cechy. Obiekty tego samego typu mają takie same cechy; różne typy obiektów mogą mieć takie same cechy.



Struktura Katalogu



Część atrybutów obiektu jest niezbędna do jego utworzenia, inne bywają opcjonalne.

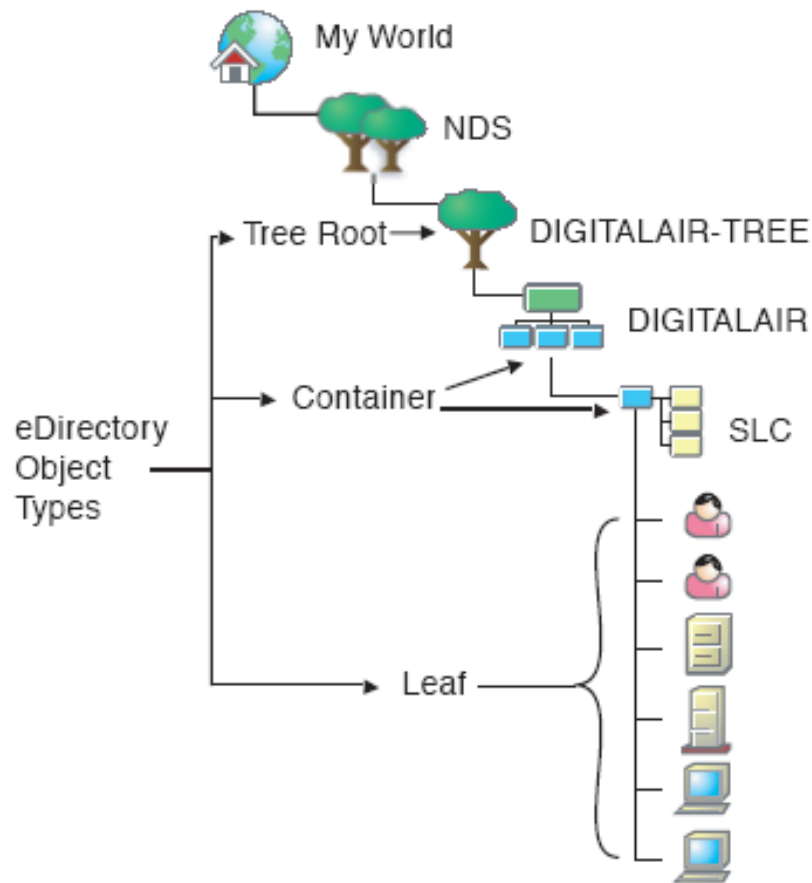
Dla przykładu, dla obiektu User należy podać wartość atrybutu Login Name. Inne atrybuty obiektu User, np. numer telefonu czy funkcja, są opcjonalne.

Każdy atrybut obiektu może mieć określony typ wartości. Niektóre atrybuty mogą zawierać więcej niż jedną wartość (**atrybut wielowartościowy**), np. numer telefonu obiektu User może mieć wiele wartości dla każdego użytkownika.

Rodzaje obiektów

Obiekty eDirectory można podzielić na trzy klasy, czyli rodzaje:

- Tree [Root] - korzeń struktury;
- Container - kontener;
- Leaf - liść.



Obiekt Tree - Tree [Root]

Obiekt Tree reprezentuje najwyższy poziom w drzewie Katalogu. Zapewnia dostęp do obiektów różnych typów, takich jak Country i Organization.

Obiekt Tree określa miejsce, nie zawiera żadnych informacji (oprócz cechy Name). Obiekty typu Country, Organization, Security i Alias mogą być tworzone bezpośrednio pod obiektem Tree.

Obiekt Tree jest czasami definiowany jako obiekt klasy Container, jednak różni się on od rzeczywistych obiektów tej klasy:

- Może zostać utworzony tylko podczas instalowania pierwszego serwera w sieci;
- Nie może zostać usunięty ani przeniesiony,
- Używa nazwy drzewa eDirectory, która może być zmieniona.

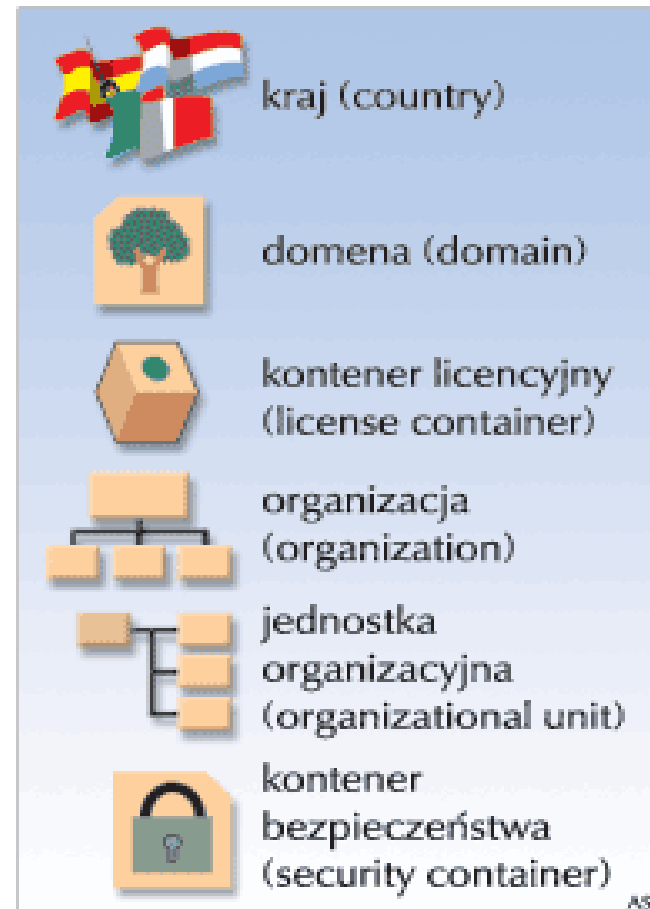
Obiekt Tree [Root] może mieć dysponentów, może też sam zostać uczyniony dysponentem. Każdy Katalog może mieć tylko jeden obiekt Tree.

Obiekty klasy Container (kontener)

Obiekty typu kontener nie reprezentują bezpośrednio zasobu sieciowego. Służą do organizowania i porządkowania struktury katalogu. Mogą zawierać obiekty typu liść (użytkownicy czy drukarki) lub inne kontenery.

Mogą reprezentować kraje, lokalizacje w kraju, firmy, działy, grupy robocze czy wspólne zasoby.

Obiektami typu kontener są np. **kraj** (country), **domena** (domain), **kontener licencyjny** (license container), **organizacja** (organization), **jednostka organizacyjna** (organizational unit), **kontener bezpieczeństwa** (security container).



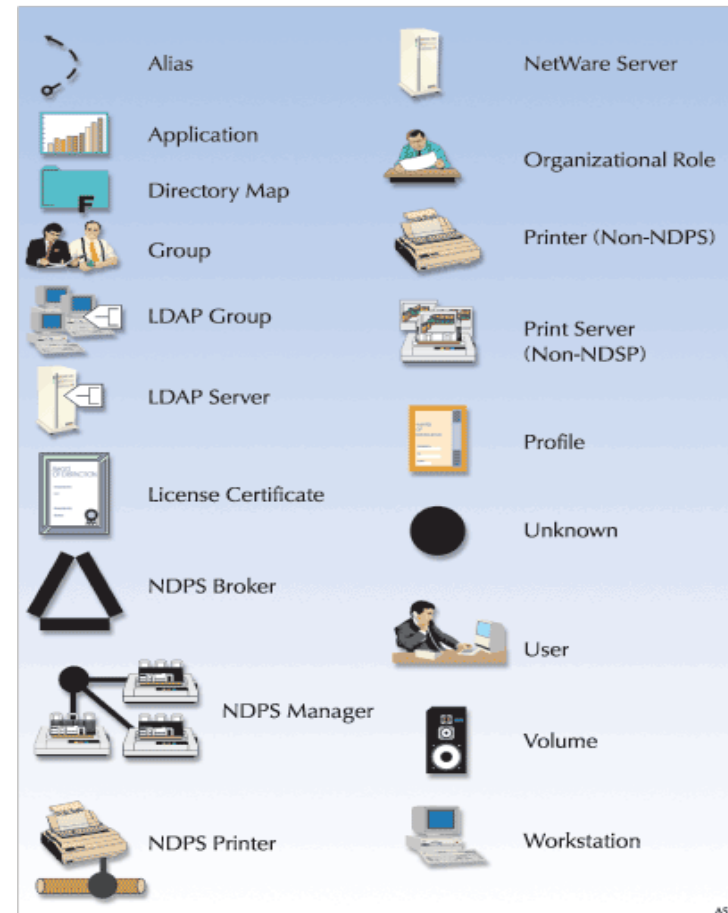
Obiekty klasy Container (kontener)

- **Obiekt kraj (country - C)** jest tworzony poniżej obiektu drzewa [root], pozwala wprowadzić w strukturze sieci korporacji podział międzynarodowy. Obiekt typu kraj jest częścią standardu X.500, który definiuje dwuliterowe oznaczenia dla każdego kraju (np. PL, DE).
- **Obiekt typu domena (domain - DC)** reprezentuje składniki usługi DNS. Zwykle jest tworzony poniżej kontenerów organizacji, jednostki organizacyjnej, kraju.
- **Kontener licencji (license container - LC)** jest specjalnym kontenerem wykorzystywanym przez usługi licencyjne (Novell Licensing Services) do lokalizacji informacji o dostępnych licencjach. Zawiera dwa obiekty reprezentujące licencję serwera i użytkowników.
- **Obiekty typu organizacja (organization - O)** służą do dzielenia opisu sieci na struktury, np. przedsiębiorstwo, uniwersytet lub dział. Drzewo katalogu musi zawierać minimum jeden obiekt typu organizacja. Organizacja może zawierać kolejne obiekty organizacji lub obiekty podrzędne typu liść.
- **Obiekt typu jednostka organizacyjna (organizational unit - OU)** opisuje istniejące w strukturze grupy organizacyjne, np. działy, departamenty czy zespoły projektowe. Jest obiektem opcjonalnym, lokalizowanym poniżej obiektu kraj lub organizacji.
- **Obiekt typu kontener bezpieczeństwa (security - S)** jest położony poniżej obiektu drzewa lub obiektu kraj. Jego zadaniem jest przechowywanie globalnych ustawień dla systemu autoryzacji i systemu kluczy publicznych.

Obiekty klasy Leaf (liść)

Wszystkie obiekty kontenerowe tworzące strukturę zawierają obiekty typu liść.

Cechą charakterystyczną obiektów typu liść jest to, iż nie mogą zawierać innych obiektów.



Obiekty klasy Leaf (liść)

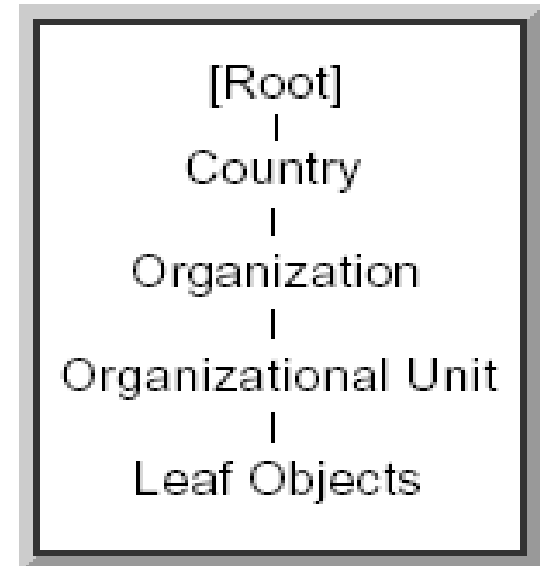
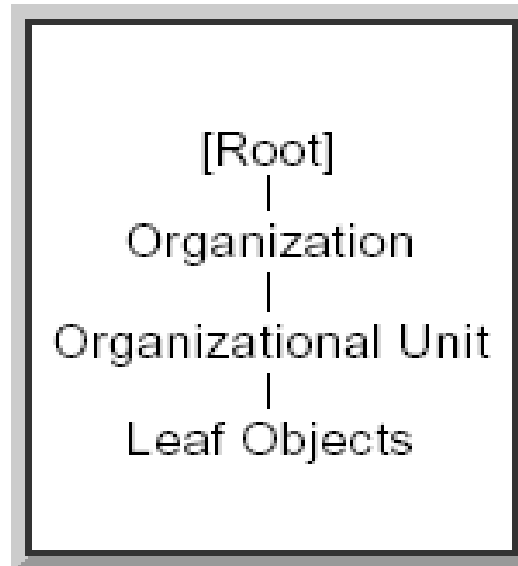
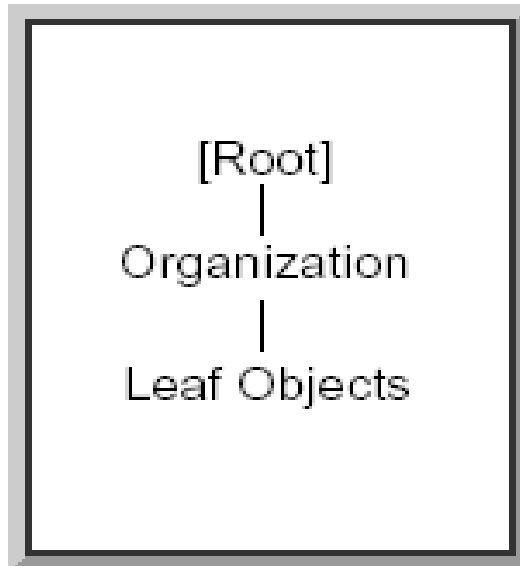
Obiekty typu liść reprezentują fizyczne i programowe zasoby sieciowe.

- **grupa** (group) - umożliwia sprawne administrowanie prawami dostępu do zasobów sieciowych; prawa przyznawane dla grupy dziedziczone są przez wszystkich jej członków,
- **rola organizacyjna** (organizational role) - definiuje pozycję w organizacji. Pozostaje ona zawsze taka sama, a przypisywane do niej prawa są niezmiennie. Zmiana osoby pełniącej daną rolę polega na zmianie skojarzenia obiektu z odpowiednim obiektem użytkownika,
- **wolumin** (volume) - reprezentuje wolumin dyskowy na serwerze, zawierający pliki i katalogi. Dane te można przeglądać np. w ConsoleOne, nie są one obiektami eDirectory. Ich opis i uprawnienia przechowuje system plików,
- **alias** - umożliwia wskazywanie innych obiektów, które mogą być kontenerem, obiektem użytkownika lub innym obiektem w katalogu,
- **zamapowany katalog** (directory map) - reprezentuje folder zlokalizowany na serwerze, funkcjonujący jako obiekt systemu plików na komputerze użytkownika. Mapowanie katalogów pozwala uprościć dostęp do przypisanych użytkownikom zasobów serwera,
- **zasoby opisujące system wydruku NDPS** (NDPS printer, manager i broker) oraz systemu kolejkowego (printer, print queue, print server).

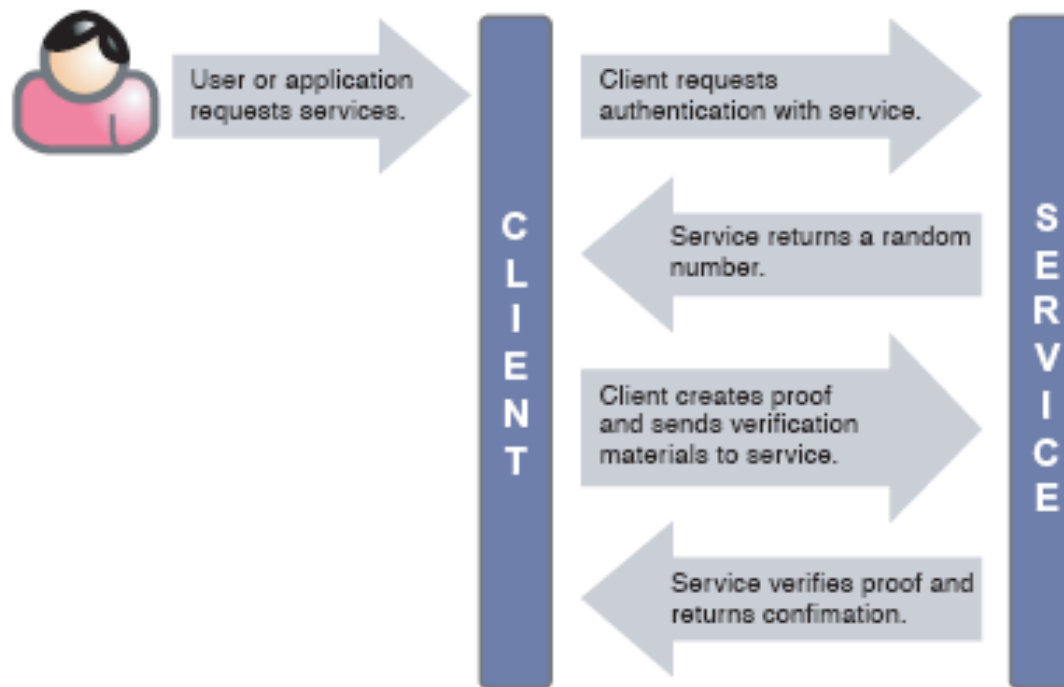
Charakterystyka typów obiektów klasy Container

Container Object	Can Exist In	Can Contain	Example
Country	[Root]	Organization	US
		Alias	FR
Organization	[Root]	Organizational Unit	Novell
	Country	All leaf objects	UCLA
Organizational Unit	Organization	Organizational Unit	Marketing
	Organizational Unit	All leaf objects	Engineering

Hierarchiczna struktura drzewa eDirectory



Rola usług eDirectory



Wpływ struktury drzewa eDirectory na dostęp do zasobów sieciowych

Największy wpływ na dostęp do zasobów sieciowych ma wielokontenerowe drzewo eDirectory, ponieważ:

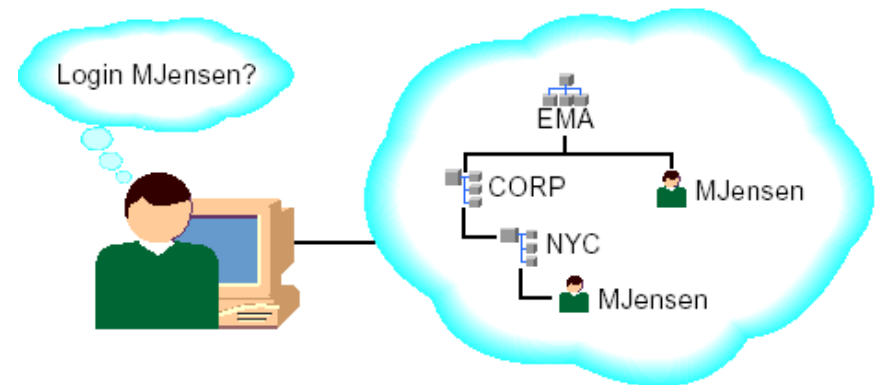
- Obiekty nie znajdują się w jednym kontenerze;
- Aby znaleźć obiekt, usługi eDirectory nie przeszukują całego drzewa eDirectory.

Dlatego, aby znaleźć właściwy obiekt, usługi eDirectory potrzebują precyzyjnych informacji - określenia bieżącego kontekstu.

Każda nazwa obiektu identyfikuje precyzyjnie obiekt i jego położenie w drzewie eDirectory.

Podając nazwę obiektu można użyć:

- Nazwy pełnej;
- Nazwy względnej.



Nazwy z typami (object name attributes)

W nazwie z typami stosuje się skróty atrybutów w celu odróżnienia w nazwie obiektu typów kontenerów od typów obiektów klasy Leaf.

Podawanie typów atrybutów pomaga unikać problemów, które mogą powstać w wypadku stosowania naw bez typów.

Typy atrybutów:

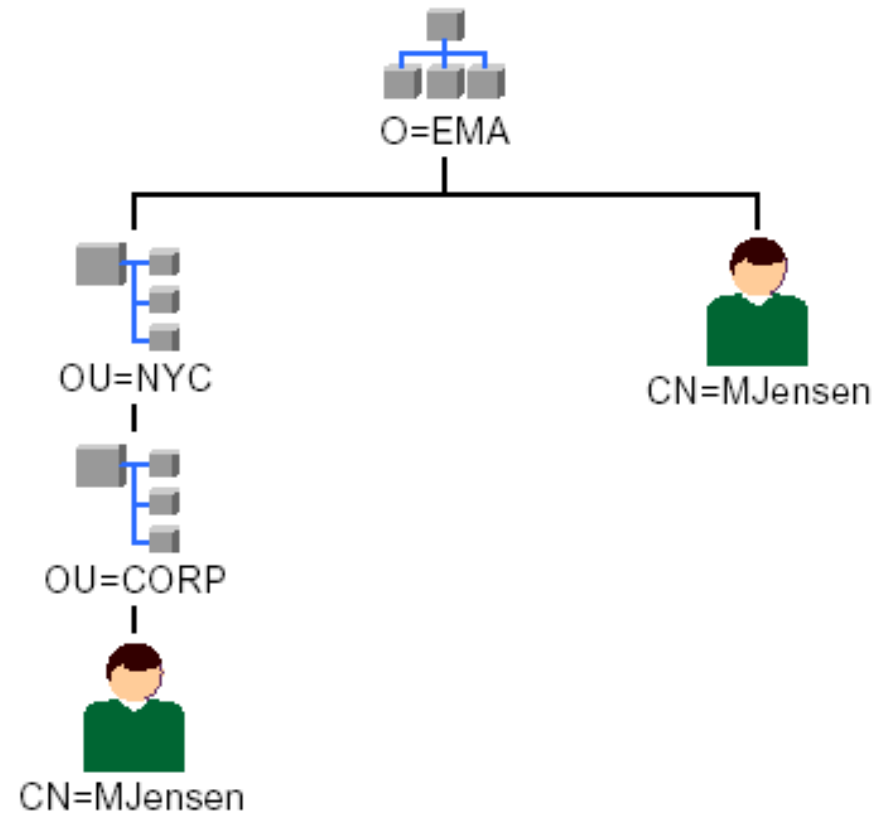
- Występują przed obiektem, który identyfikują;
- Odróżniają różne typy kontenerów od typów obiektów klasy Leaf.

Attribute Types	Description	Example
C	Country	C=IR (IRELAND)
O	Organization Name	O=EMA
OU	Organizational Unit Name	OU=CORP
CN	Common Name	CN=JMcKee (includes all leaf objects)

Nazwa zwykła (common name)

Nazwa zwykła (Common Name -CN) obiektu klasy Leaf jest nazwą umieszczoną obok tego obiektu w drzewie eDirectory.

Nazwa zwykła jest nazwą względną.



Kontekst (context)

Kontekst określa pozycję obiektu w drzewie eDirectory. Jest listą obiektów klasy Container prowadzącą od danego obiektu do obiektu klasy [Root]. (Zlokalizowanie obiektu poprzez kontekst odpowiada wskazaniu pliku za pomocą ścieżki dostępu.)

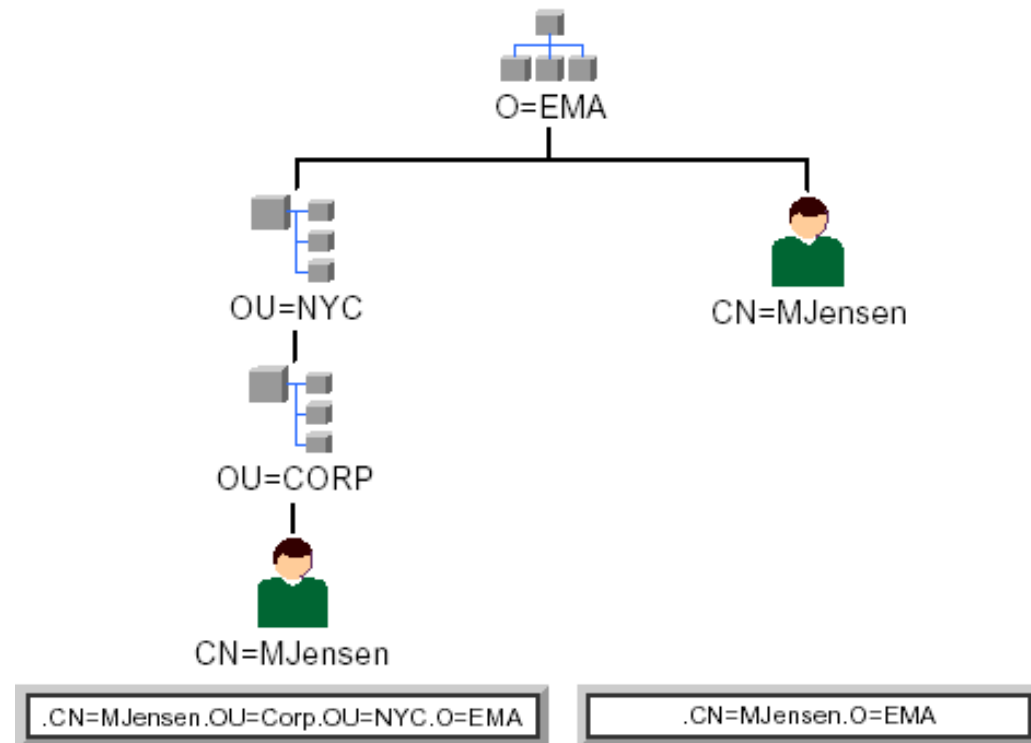
W drzewie eDirectory nie mogą występować w tym samym kontenerze dwa obiekty klasy Leaf mające identyczną nazwę. Drzewo eDirectory może jednak zawierać dwa takie obiekty o jednakowych nazwach, o ile obiekty te mieszczą się w **różnych kontenerach**.

Nazwa pełna (distinguished name)

Nazwa pełna obiektu jest połączeniem jego nazwy zwykłej i kontekstu.

Nazwa pełna zaczyna się od kropki. Obiekty występujące w nazwie są oddzielone kropkami, odgrywającymi taką samą rolę, jak odwrotne ukośniki używane w ścieżkach dostępu w systemie DOS. Kropka nie może występować na końcu nazwy pełnej.

Obiekt jest jednoznacznie identyfikowany przez nazwę pełną. Dwa obiekty nie mogą mieć takiej samej nazwy pełnej.



Kontekst bieżący (current context)

Kontekst bieżący to inaczej bieżąca pozycja użytkownika w drzewie eDirectory:

- Ma wpływ na to, ile zwykłych nazw obiektów trzeba podać w poleceniu, aby uzyskać dostęp do zasobu;
- Identyfikuje (w oprogramowaniu klienta Novella) domyślny kontener eDirectory przypisany do stacji roboczej bieżącego użytkownika;
- Pozwala użytkownikowi odwoływać się do obiektu występującego w kontekście bieżącym tego użytkownika za pomocą nazwy zwykłej obiektu, ponieważ kontekst bieżący użytkownika i kontekst obiektu są takie same.

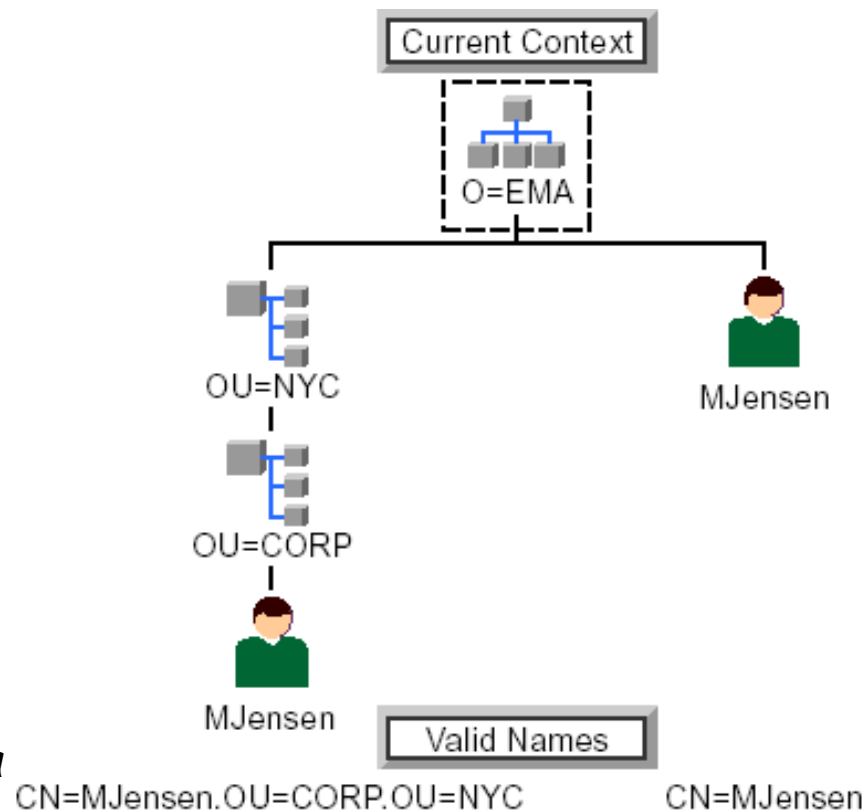
Kontekst bieżący jest też zwany *kontekstem nazwy*.

Nazwa względna (relative distinguished name)

- Jest listą obiektów tworzących ścieżkę prowadzącą od nazywanego obiektu do kontekstu bieżącego;
- Nie zaczyna się od kropki;
- Obiekty wymieniane w nazwie są oddzielone kropkami;
- Nazwa może kończyć się kropką.

Kiedy jest używana nazwa względna, eDirectory musi z niej utworzyć nazwę pełną. Następuje to przez połączenie nazwy względnej z kontekstem bieżącym:

Nazwa względna + Kontekst bieżący = Nazwa pełna



Name Submitted	Current Context	Resulting Distinguished Name
CN=MJensen	O=EMA	.CN=MJensen.O=EMA
CN=MJensen	OU=CORP.OU=NYC.O=EMA	.CN=MJensen.OU=CORP.OU=NYC.O=EMA

Kropki końcowe

Każda kropka końcowa nakazuje usługom eDirectory usunięcie nazwy jednego obiektu z początku kontekstu bieżącego.

Każda kropka dodana do podawanej nazwy względnej powoduje usunięcie kolejnego obiektu z początku bieżącego kontekstu. Kropki końcowe spełniają to analogiczną funkcję, jak kropki używane w poleceniu CD w systemie DOS.

Kropki końcowe mają zastosowanie tylko przy nazwach względnych.

Przykładowo, jeśli bieżący kontekst stacji roboczej to:

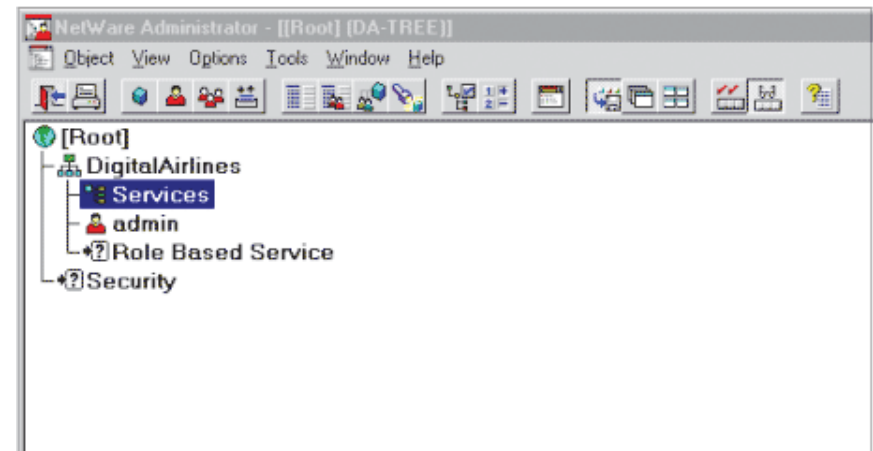
`marketing.London.Company`, a chcemy uzyskać dostęp do obiektu `jjones` w kontekście `London.Company`, wystarczy użyć następującego łańcucha: „`jjones.`”. eDirectory wykrywa końcową kropkę oraz usuwa składnik „`marketing`” z domyślnego kontekstu przed dopisanie nowego kontekstu. W ten sposób kontekst będzie poprawnie odczytany jako: „`jjones.London.Company`”.

Zarządzanie obiektami eDirectory

- NetWare Administrator,
- ConsoleOne,
- Novell iMonitor,
- Novell iManager.

NetWare Administrator

• **NetWare Administrator** - (SYS:\PUBLIC\WIN32\NWADMIN32.EXE) umożliwia on m.in. tworzenie i kasowanie obiektów w eDirectory, przesuwanie i zmiany nazwy, przypisywanie praw w strukturze drzewa katalogu i systemie plików, konfigurowanie usług drukowania oraz zarządzanie licencjami.

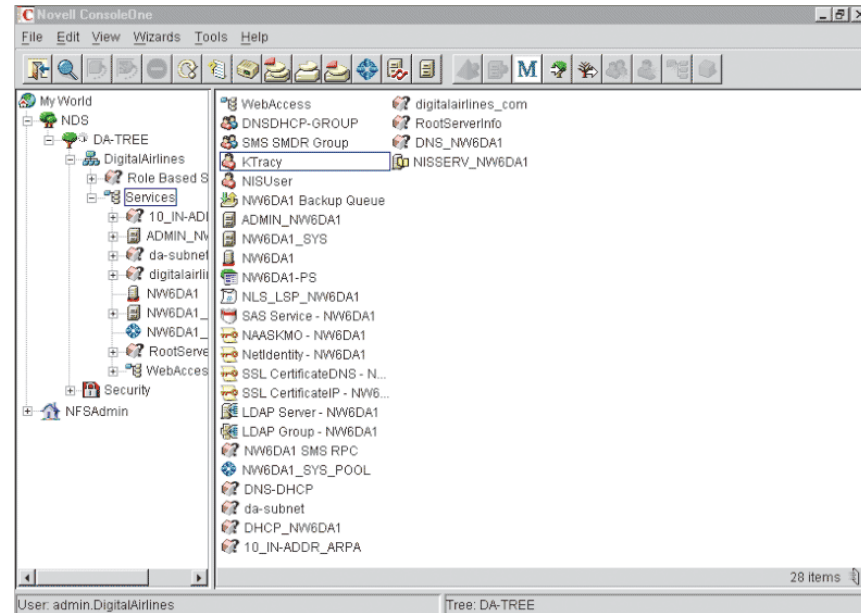


ConsoleOne

• **ConsoleOne** - graficzne narzędzie napisane w języku Java - ConsoleOne (SYS:\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE). Przy jego użyciu można wykonać następujące operacje:

- przeglądanie dużych kontenerów NDS, zawierających nawet miliony obiektów,
- wyszukiwanie obiektów z użyciem filtrów,
- konfiguracja usług LDAP,
- administracja wszystkimi obiektami eDirectory,
- rozszerzanie schematu eDirectory,
- administracja systemem plików na poszczególnych wolumenach.

Dzięki dodatkowym modułom (snap-in) możliwe jest administrowanie usługami NetWare - możliwości takiej nie oferuje NetWare Administrator.

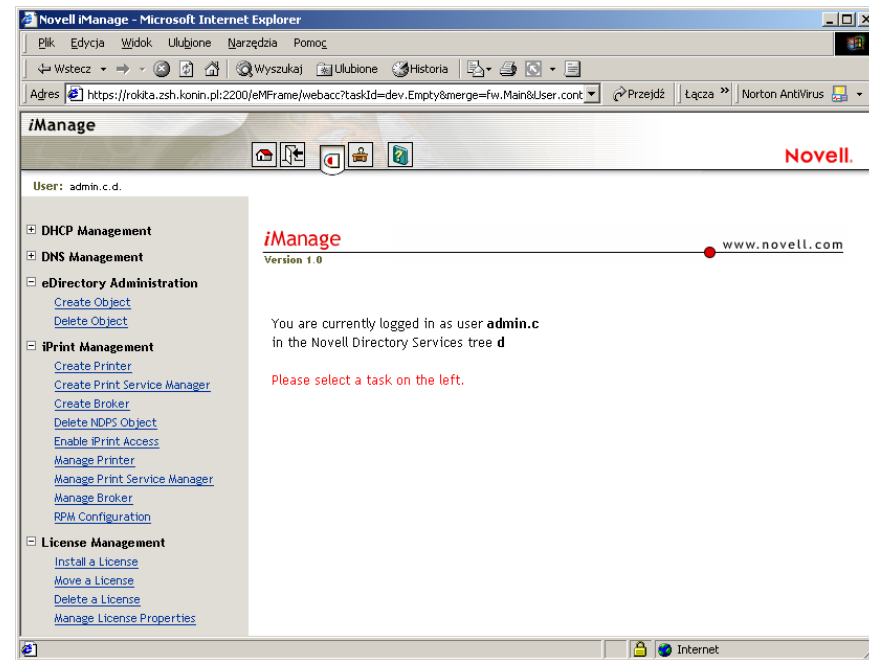


iManager

Novell iManage - ułatwia zarządzanie użytkownikami, organizowanie obiektów w kontenerach, tworzenie obiektów grup, kasowanie obiektów, przeglądanie oraz wyszukiwanie obiektów.

Dostęp do iManage z przeglądarki:

[https://\[nazwa_serwera_lub_IP\]:2200/eMFrame/iManage.html](https://[nazwa_serwera_lub_IP]:2200/eMFrame/iManage.html)

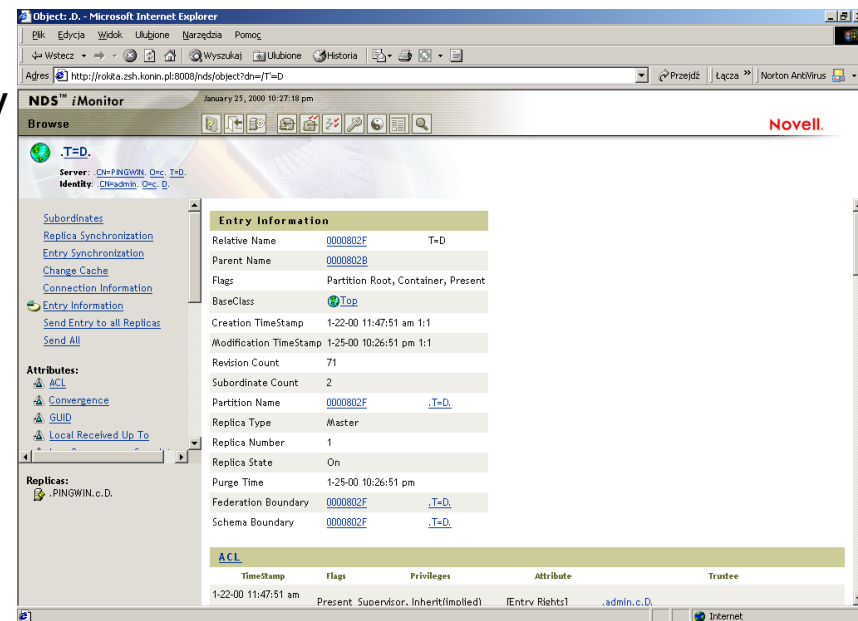


iMonitor

Novell iMonitor to narzędzie, które pozwala na monitorowanie usług katalogowych eDirectory z różnych systemów operacyjnych. Może zostać użyty do monitorowania NDS i eDirectory dla NetWare 4.11 i wyższych, Windows NT/2000, Linuksa, Solarisa i Tru64 UNIX.

Dostęp do Novell iMonitor poprzez przeglądarkę: http://adres_IP_serwera:port/nds

Novell iMonitor dostarcza alternatywnego dostępu do tradycyjnych narzędzi eDirectory, m.in. DSBROWSE, DSTRACE, DSDIAG oraz diagnostycznych elementów, np. DSREPAIR.



N