UNIVERZITET „ *Džemal Bijedić* “
***F**akultet **I**nformacijskih **T**ehnologija*
M O S T A R

ACTIVE DIRECTORY NA WINDOWS 2003 SERVERU

(seminarski rad iz predmeta Server Operativni Sistemi)

Mostar, februar 2007. godine

Student:
Trkić Amer/1509
II godina

SADRŽAJ

1. Uvod

Od pojave Windowsa 2000 Active Directory (aktivni imenik) postao je jedna od najzanimljivijih tehnologija za mreže velikih organizacija.

Sedamdesetih godina svi računarski resursi koji su vam trebali ili koje ste mogli da koristite, nalazili su se na računaru ili na terminalu s kojeg ste se prijavljivali na taj računar.
Osamdesetih godina, pojava lokalnih mreža PC računara dovela je do toga da mnoge datoteke budu razmještene na razne mašine, do kojih su vodile fiksne putanje. Korisnici lokalne mreže djelili su te datoteke i resurse a elektronska pošta im je omogućavala komunikaciju.
Krajem dvadesetih godina, došlo je do velikih promjena jer je postalo moguće da se i podacima i resursima pristupa na bilo kom serveru u bilo kojoj mreži na bilo kom mjestu, a da pri tome korisnik opšte ne treba da zna gdje se određeni server nalazi. Poslje 2003 godine, bilo kojoj datoteci na bilo kojem serveru korisnici su mogli pristupati ne samo preko računara nego i preko PDA, mobilnog telefona i brojnih bežićnih uređaja.

Postoji više raznih registara i baza podataka koji aplikacijama i korisnicima pružaju usluge kakve se očekuju od jednog Active Directory-a. Međutim niti jedan od njih nije ni u kom pogledu povezan sa ostalima, niti zasnovan na dijeljenju resursa, niti distribuiran.

Active Directory je univerzalno distribuirano spremište podataka kroz koje se na standardiziran način može pristupati svim mrežnim objektima, kao što su konfiguracije aplikacija, usluge, računala, korisnici i procesi, i to širom cijele lokalne mreže ili šire mreže ciji je ona dio.

To nam omogućava logićka struktura imenika.

2. Zadatak Aciteve Directory-a

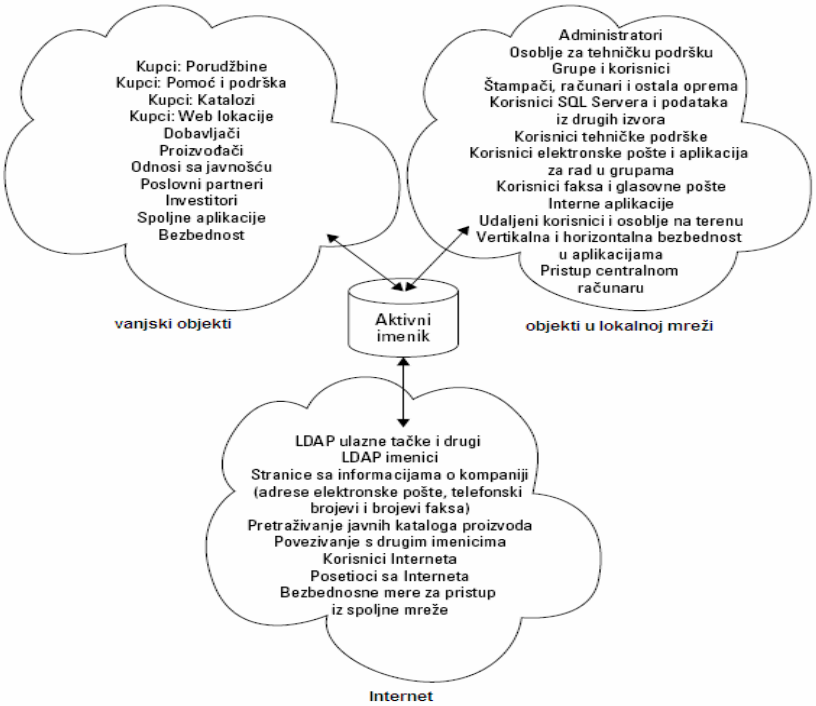
Active Directory sadrži podatke. U njegovom najjednostavnijem obliku, možemo ga usporediti s gigantskim telefonskim imenikom koji omogućava korisniku da pomoću imena i prezimena pronađe određeni telefonski broj.
U svijetu informacijskih tehnologija Active Directory je mnogo više od telefonskog imenika. On je regulator prometa u mrežnom svijetu jedne kompanije.

Active directory možemo opisati kao integrirani skup rješenja za distribuciju podataka, organizaciju resursa, sigurnost i administraiciju mreže. Oslanja se na Domain name system (DNS) za lociranje resursa i određivanje prostora imena domena (namespace).

Active Directory koristi Lagani protokol za pristup imeniku-directory-u (LDAP – Lightweight directory access protocol) koji omogućava i povezivanje sa drugim tipovima mreža. Active Directory omogućava centraliziranu administraciju tj. sa jednog računara je moguće kontrolirati sve resurse mreže (korisničke račune, mrežne konekcije, računala, štampaće idr.) gdje god se oni nalazili.

Jednokratna prijava i distribuirani sigurnosni parametri

Do pojave Active Directory-a, kretanje mrežnim svijetom neke kompanije (LAN – Local Area Network) j bilo prilično kompliciranо. U Windows NT mreži, u stvari u svakoj mreži, resurse nije moguće lako i jednostavno distribuirati.



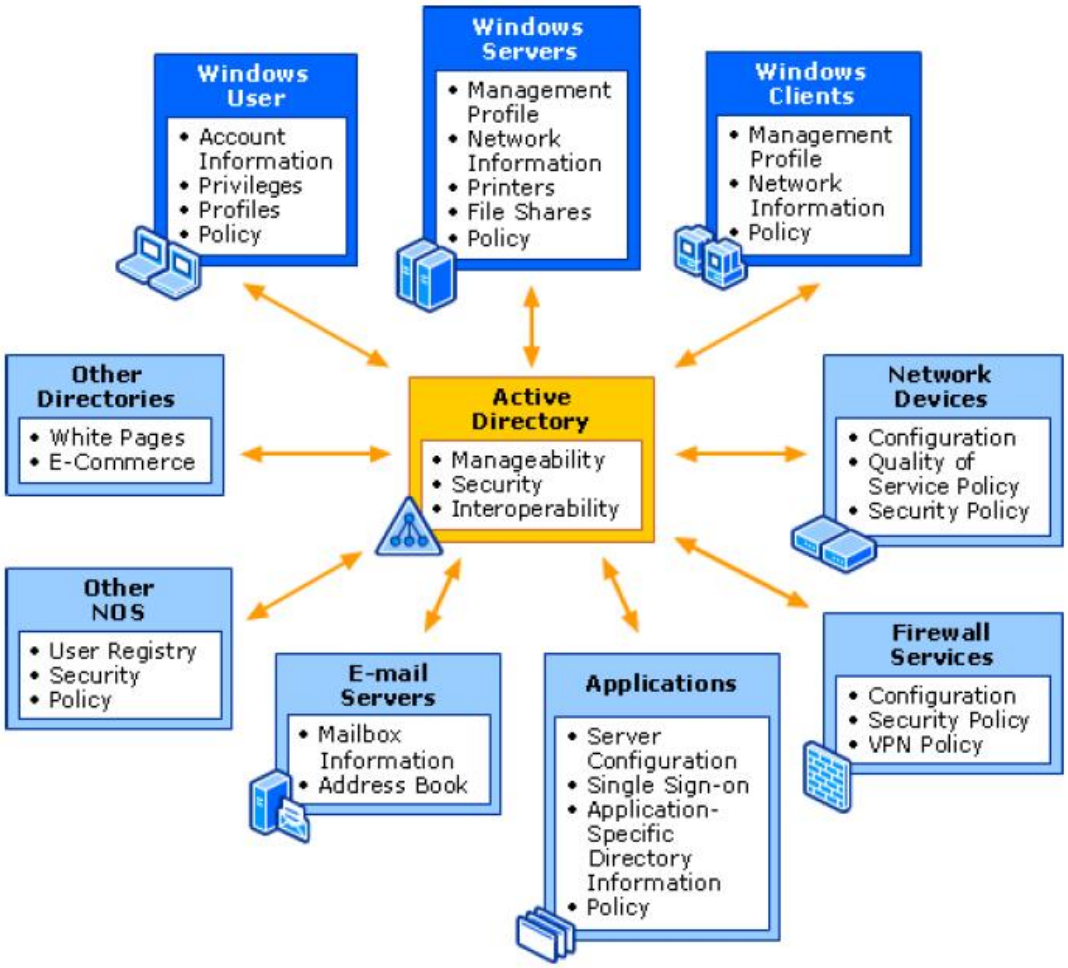
Slika 1. Aktivni imenik kao centralni sistem za identifikaciju korisnika

Mogućnost međuoperativnosti i prilagođavanja potrebama korisnika mnogobrojnih NT servisa, štampača, dijeljenih resursa, uređaja, datoteka, baza znanja i funkcionalnosti, značajno se smanjuje kada mrežne komponente i objekti nemaju sposobnost dijeljenja informacija sa drugim.

U mreži starog tipa gotovo je nemoguće da se svaki korisnik ne prijavljuje barem tri puta – na Windows NT domenu, na e-mail aplikaciju i web preglednik. O prijavama na korisničke aplikacije ne možemo ni govoriti jer su različite u raznim firmama.

To zahtjeva od korisnika da pamte na desetine korisničkih imena i šifri i tačno moraju znati gdje se koji resurs nalazi na mreži.

Active directory donosi rješenje u obliku neke vrste identifikacijske kartice. Korisnik se u sustav prijavljuje samo jedanput, i dalje se Active Directory brine o tome da mu otvara ili zatvara vrata prema resursima na mreži.



Slika 2. Prikaz povezanosti centralnog imenika sa cjelokupnim Informacijskim sistemom jedne kompanije

San o jednokratnom prijavljivanju na pretvoren je u stvarnost pomoću usluga Active Directory-a i podrške Windows servera 2003.

Ova usluga se zove jednokratno prijavljivanje (SSO – Single Sign-On). SSO je postao gotovo standard u zajednici kompanija koje podržavaju protokol Kreberos; među njima su Microsoft, Apple, Sun i Novell.

Kada se putem protokola Kerberos korisnik pravilno identificira, sve ostale usluge koje protokol Kerberos podržava mogu ga prihvatiti i omogućiti mu daljnji pristup. Kerberos to ćini tako što koristi „ulaznice" (end. tickets) tj. identifikacijske kartice, koje dodjeljuje usluga imenika.

Upravljanje izmjenama unutar sistema

Tehnologija Active Directory olakšava upravljanje pokretnim korisnicima, korporacijskim mrežama i računalima sa kojih ti korisnici uspostavljaju veze s mrežama. Kroz Active

Directory sistem administratori su dobili mogućnost upravljanja svim mrežnim atributima pojedinog korisnika te grupiranje korisnika po određenim atributima.

Group Policy, usluga Windows servera 2003 koja omogućava kontrolu i upravljanje izmjenama u sistemu, čuva sve podatke o korisnicima i računarima u Active Direcotry-u.

Također, administrativne funkcije i odgovornosti se mogu raspodjeliti na više cjelina radi lakšeg administriranja. Usluga distribuiranog imenika omogućava sistem administratorima da administriranje korisnika i mrežnih resursa raspodjele po organizavijskim cjelinama.

Budući da se Active Directory može tako podijeliti da potpuno preslika organizacijsku strukturu poduzeća, moguća je i raspodjela administrativnih poslova po dijelovima te strukture tako da se obavljanje rutinskog dijela administriranja resursima nekog dijela organizacije može delegirati na nekoga ko logićki tamo pripada.

Distribuirano upravljanje sistemom

Tehnologija Active Directory omogućava da administrativne funkcije i odgovornost raspodjelite na više cjelina. Tako ih možete organizovati i unutar mreže ili domena radi lakšeg administriranja. Usluga distribuiranog imenika omogućava vam da administriranje korisnika i mrežnih resursa raspodjelite širom organizacije. Na starijim NT sistemima mogli ste da definišete korisnike i grupe sa administratorskim pravima, ali je bilo gotovo nemoguće da od tih administratora sakrijete druge mrežne resurse.
Pošto aktivni imenik moće da bude izdjeljen tako da potpuno preslikava organizacionu strukturu preduzeća, moguća je i raspodela administrativnih poslova po djelovima te strukture. Drugim rjećima, logićno je da nekoga ko radi u odreođenom odjeljenju zadužite za obavljanje rutinskog djela upravljanja resursima tog odjeljenja.

Upravljanje aplikacijama

Tehnologija Active Directory olakšava razvijanje i distribuciju aplikacija. Projektantima aplikacija pružena su doljedna, otvorena i međuoperativna sučelja i API funkcije na osnovu kojih mogu pisati programski kod koji čuva podatke o aplikacijama, procesima i uslugama, u okruženju sa distribuiranim informacijama i rukuje tim podacima.

Omogućeno im je da pišu aplikacije i da ih zajedno s trajnim podacima smještaju u „devidljiva" skladišta koristeći za to otvorena sučelja.
U tom slučaju Active Directory služi kao spremište podataka specifičnih za aplikacije, a naročito za software koji je namjenjen podršci grupnom radu. Na taj način te vrste informacija su dostupne iz bilo kojeg dijela mreže, uključujući tu cijeli internet, pa čak i Internet (zahvaljujući tehnologiji .NET Framework).

Projektantima je omogućeno da napišu metode koje aplikaciju instaliraju na određeni mrežni imenik radi početnog podešavanja, a zatim i održavanja tijekom životnog vijeka aplikacije.
Bez potrebe da se bave unutrašnjim mehanizmom koji omogućava rad samog imenika omogućeno je da se informacijski ili konfiguracijski objekt napravi, inicijalizira i koristi bez obaveze da projektant brine o tome gdje će korisnik taj objekat instalirati ili odakle će ga pozvati. Objekt koji je napravljen uvijek je dostupan aplikaiciji, ma gdje ga mi premjestili.
Aplikacija može u svakom trenutku dobiti informacije o stanju na nivou cijele organizacije, a korisnike možemo grupirati po po pravima korištenja usluga ili pristupa određenim podacima, što se sve regulira pomoću objekata Active Directory.
Na primjer, aplikacija može prikazivati podatke o tome ko je sve trenutno prijavljen i radi na sistemu, koje se datoteke sistema za upravljanje bazama podataka (SQL Server ili Oracle) koriste i što sve korisnici trenutno rade. Korisnici se ne moraju ponovo prijavljivati samo zato da bi koristili aplikaciju.

Kada pokrenu aplikaciju, sistem provjerava da li ih je Active Directory identificirao, utvrđuje s kojeg računala pristupaju sistemu i koja su njihova prava pristupa. Na osnovi tih informacija, grafičko korisničko sučelje aplikacije popunjavamo isljučivo podacima koje korisnik smije vidjeti ili korisititi.

Svrha korištenja Active Directory domena je postizanje sljedećih ciljeva kod administriranja mreže:

Stvaranje administrativnih cjelina – Domena definira jednu administrativnu cjelinu. Sigurnosne politike (security policies) i ostale postavke (account policies i group policies) ne prelaze granice jedne domene. Domene nisu u potpunosti izolirane jedna od druge i ne predstavljaju sigurnosne cjeline. Samo šuma (forest) stvara sigurnosnu cjelinu.

Repliciranje informacija – Domena predstavlja Windows direktorijsku particiju. Ove direktorijske particije su jedinice repliciranja (replication). Svaka domena sadrži informacije samo o objektima koji se u njoj nalaze.

Promjenjivanje grupne politike (group policy) – Domena predstvalja jednu od više mogućih opsega grupne politike (group policy se može primjeniti i na organizacijske jedinice ili site-ove).

Određivanje administrativnih oblasti (delegate administrative authority) – Cilj je precizno određivanje područja ovlasti pojedinih administratora. Tako primjerice područje ovlasti pojedinih administratora. Tako primjerice područje ovlasti može biti organizacijska jedinica ili pak cijela domena. Obzirom da je domena administrativna granica, administrativne dozvole za jednu domenu su ograničene samo na tu domenu.

Kada se Active Directory podešava za korištenje na nivou cijele organizacije, prvi zadatak je izrada korijenske domene, odnosno onoga što se u terminologiji aktivnog imenika zove objekat korijenske domene (eng. Root domain object). Praksa je pokazala da je dobro zbog prepoznatljivosti kompanije da ta korijenska domena bude ujedno i Internet korijenska domena kompanije. Ta korjenska domena postaje prvi kontejnerski objekt napravljen u lancu objekata koji trebaju predstavljati strukturu domena lokalne mreže u Active Directory-u. „Ispod" te domene rade rade se dodatni kontejnerski objekti koji predstavljaju organizacijske jedinice kompanije.

2. Razlozi uvođenja Active Directory servisa

Razlozi uvođenja Active Directory servisa su: poboljšanje servisa, group policy managment console, jednostavnost prelaska na novi sustav.

Pobljšanje servisa

Servis Active Directory značajno pojednostavljuje administriranje složenih mrežnih imenika i korisnicima olakšava lociranje resursa čak i u najvećim mrežama. Ovaj imenički servis je skalabilan, izgrađen od samih temelja primjenom standardnih internetskih tehnologija i potpuno integriran na razini operacijskog sustava u poslužitelje Windows 2003 generacije. U novim verzijama, ovaj servis donosi i nove značajke uključujući koncepciju povjerenja između različitih stabala domena, sposobnost preimenovanja domena te sposobnost deaktiviranja atributa i klasa u schemama kako bi se njihove definicije mogle mijenjati.

Group Policy Managment Console

Administratori mogu koristiti grupna pravila za definiranje postavki i dopuštenih radnji za korisnike i računare. Za razliku od lokalnih pravila, organizacije mogu koristiti grupna pravila, za uspostavljanje pravila koja će se primjenjivati širom određenog mjesta, domene ili organizacijske jedinice u sistemu Active Directory-a. Upravljenje temeljeno na pravilima pojednostavljuje zadatke, kao što su operacija ažuriranja sistema, instalacija aplikacije, korisnički računi i blokiranje stolnih sistema. Group Policy Managment Console (GPMC) omogućuje nove okvire za upravljanje grupnim pravilima. Uz pomoć GPMC grupna pravila postaju mnogo jednostavnija za upotrenu, a to je prednost koja će mnogim kompanijama omogućiti bolju upotrenu sistema Active Directory te iskorištavanje moćnih upravljačkih postavki.

Jednostavnost prelaska na novi sistem

Jedna od primarnih mogućnosti tehnologije Active Directory jest uklapanje sa starijim verzijama Windowsa NT. Većina kompanija neće preko noći prebaciti cjelokupno poslovanje na Windows Server 2003, već će ga neko vrijeme koristiti u paralelnom radu s Windows 2000 i NT.

Uobičajeno je da kompanije postave jedan Active Directory upravljač domene (domain controler), ili više njih, kao novi primarni kontroler domene (Primary Domain Controler, PDC), postojećih Windows NT domena. U mješovitim okruženjima (Server 2003, NT i Windows 2000), NT sistemi, radne stanice i klijenti prepoznaju Active Directory kao PDC poslužitelje. Korisnici, aplikacije i usluge neće niti primjetiti da se identifikacija obavlja u aktivnom imeniku, što omogućava NT domenama da nastave rad i ne znajući šta se zapravo dogodilo.

Tehnologija Active Directory omogućava ovakvu kombinaciju tako što u potpunosti emulira Windows NT 3.51 i NT 4.0 upravljače domene. U mješovitim okruženjima, upravljač Windows 2000 domene ponaša se kao Windows NT 4.0 upravljač domene. Čak će i aplikacije i usluge (uključujući i one od drugih proizvođaća) napisane na Win32 API nastaviti rad bez izmjena i u okruženju Active Directory.

3. Active Directory VS Registry

Vidjeli smo zbog čega su nam potrebne usluge Active Directory-a i odakle one potiću, gde se tu uklapa registar? U doba nastanka Windowsa 95 i Windowsa NT, Microsoft je poboljšao spremišta podataka o aplikacijama koje rade na Windows platformi tako što je dodao registar (registarsku bazu podataka). To je bilo veliko olakšanje poslje zbrke sa inicijalizacionim i konfiguracionim datotekama, nebezbjednim tekstualnim datotekama kojima je svako mogao da pristupa. Prvenstvena namjena registra je da stabilizuje operativni sistem kao spremište za podatke, koji služe za upravljanje podacima i konfigurisanje aplikacija i računara.

Kada bi korisnici Windowsa 3.11 greškom izbrisali .ini datoteku neke aplikacije, ona je bivala uništena (ako nije postojala rezervna kopija .ini datoteke). Primjena registra je to značajno promjenila. Danas ga neki od najvećih proizvođaća softvera još uvjek ne koriste.
Registar je postao i dom onoga što poznajemo pod imenom bezbjednosni upravljać nalozima (engl. Security Account Manager, SAM). Ta baza podataka upravlja svim bezbjednosnim parametrima pristupa mrežnim resursima.

Postoji sličnost između registra i aktivnog imenika. Na primjer, registar je:

- također baza podataka, ponešto šifrovana i složena, ali ipak baza podataka;
- otvoren i pristupačan, osim onog djela koji pripada SAM-u;
- softverski sistem koji može da se programira;

- struktura koja može da se replicira (od jednog originala), čime se obezbjeđuje osnova za distribuiran sistem;
- sistem hijerarhijskih struktura, koji sadrži zapise s podacima o konfiguraciji.

Sličnosti se ovde uglavnom i završavaju. Poređenje registra sa aktivnim imenikom je otprilike što i poređenje ribarskog čamca i nosača aviona. Aktivni imenik je potpuno drugačiji. Naravno, ništa vas ne sprečava da konfiguracione podatke i dalje čuvate u registru, koji ćete ionako koristiti na samostalnoj radnoj stanici ili na serveru, čak i na upravljanju domena.

Suštinsku razliku čini to što je aktivni imenik:
- distribuirana baza s više glavnih primjeraka (imenici u mreži ravnopravnih članova ažuriraju jedan drugog gotovo u realnom vremenu, ukoliko zanemarimo trajanje same operacije ažuriranja);
- sagrađen na osnovu otvorenih Internet standarda;
- objektno orjentisan;
- međuoperativan (gotovo srastao) sa DNS-om;
- sposoban da obradi zahtjev svakog mrežnog klijenta koji koristi TCP/IP;
- sposoban da se širi do gigantskih razmera.

Nažalost, danas mnoge aplikacije još uvjek čuvaju konfiguracione podatke u običnim tekstualnim datotekama, gotovo potpuno zanemarujući registar. Ukoliko zanemarite i registar i aktivni imenik, vaša aplikacija će vjerovatno biti nekompatibilna s Windowsom 2003 u funkcionalnom pogledu i neće moći da dobije uvjerenje o kompatibilnosti s Microsoftovim operativnim sistemima.

Svrha aktivnog imenika nije da zamjeni registar, koji još uvjek ima važnu ulogu u Windows Serveru 2003. Aktivni imenik u registar smješta neke konfiguracione podatke. Microsoft je poćeo da radi na imeniku, odnosno na sistemu za distribuirano skladištenje podataka, možda čak i uporedo s razvijanjem registra.

Od samog početka, u Microsoftu su smatrali da će aktivni imenik biti uspješan proizvod samo ako bude zasnovan na otvorenim standardima i međuoperativan sa Internetom. Drugim rjećima, svaki IP (LDAP) klijent moći će da pristupa aktivnom imeniku, a način tog pristupa neće zavisiti od operativnog sistema (pod kojim je aktivni imenik realizovan), slično IIS-u, FTP-u i drugim Internet uslugama.

- Aktivni imenik podržava DNS i LDAP i sarađuje s njima. Oba su modelovana prema standardu X.500, naroćito u djelu koji se tiće strukture i organizacije.
- Tehnologija Active Directory podržava otvorene i međuoperativne standarde, naročito u pogledu danas široko prihvaćenih konvencija za dodjelu imena.
- Tehnologija Active Directory se dobro uklapa u Internet zahvaljujući Microsoftovom potpunom prihvatanju i bezrezervnoj podršci protokolu TCP/IP. Svi ostali protokoli koje Microsoft podžava ponuođeni su prvenstveno radi očuvanja kompatibilnosti sa starijim verzijama NT-a, s drugim operativnim sistemima, sa starijim protokolima za prenos, kao što su SNA i DLC, i s NetBEUI klijentima.
- Tehnologija Active Directory nudi bogat skup interfejsa za jezike C/C++, Java, VB, .NET Framework i jezike za pisanje skriptova, što omogućava potpuno programiranje objekata aktivnog imenika.
- Tehnologija Active Directory je zasnovana na operativnom sistemu Windows NT (koji je još uvjek jezgro Windows Servera 2003 i Windowsa 2000), pa je tako kompatibilna sa starijim verzijama Windowsa NT.
- Aktivni imenik je potpuno distribuirana arhitektura koja omogučava administratoru da podatak upiše jednom i da ga potom sa iste tačke pristupa ažurira na bilo kom mestu u mreži.
- Aktivni imenik je veoma prilagodljiv i može sam sebe da replicira. Možete ga realizovati na jednom računaru ili u veoma maloj lokalnoj mreži, a zatim ga proširiti tako da zadovolji potrebe čak i najvećeg preduzeća na svetu. Ako resursi i

prihvatanje na tržištu budu dovoljni i kada se odreođene zapreke (a ima ih nekoliko) otklone, ova tehnologija će najverovatnije uskoro postati veoma popularna.

- Strukturni model aktivnog imenika može da se proširuje, što omogućava gotovo neograničenu evoluciju njegove šeme. U tom pogledu, tehnologija Active Directory mora da bude usaglašena sa specifikacijom X.500 koja propisuje da je za proširenje šeme neophodno da svaka nova klasa bude registrovana kod organizacije koja upravlja standardom X.500. Usklaođenost sa standardom obezbjeđuje se registrovanjem identifikatora objekta (Object Identifier, OID) kod odgovarajuće organizacije. U SAD to je Američki nacionalni institut za standarde (American National Standards Institute, ANSI).

U aktivnom imeniku usvojeni su trenutno najpopularniji modeli šema za dodjeljivanje imena. Primjenjen je koncept proširivog imenskog prostora (engl. namespace), koji je uklopljen u operativni sistem, mreže i aplikacije. Kompanije koje koriste tehnologiju Active Directory mogu da primjenjuju više različitih šema za dodjeljivanje imena, koje istovremeno postoje na njihovom heterogenom softveru i hardveru.

4. Elementi aktivnog direktorija

Aktivni imenik je veoma složen proizvod koji će svakako postati još složeniji i napredniji u budućim verzijama. U jezgru proizvoda nalazi se nekoliko elemenata koji su sastavni djelovi svakog sistema za usluge imenika, pa prema tome i aktivnog imenika.

Imenski prostori i šeme imenovanja

U tehnologiji Active Directory koristi se nekoliko šema za dodjeljivanje imena, što omogućava aplikacijama i korisnicima da pristupaju aktivnom imeniku pomoću formata koje najbolje poznaju. Formate imena opisani su u sljedećim odjeljcima:

RFC822 imena
RFC822 je konvencija za dodjeljivanje imena na koju je većina među nama već navikla pri korištenju elektronske pošte ili krstarenju po Webu. Ova imena poznata su i kao glavna korisnička imena (User Principal Names, UPN): imekorisnika@imedomena. Primjer: 1509@fit.ba. Tehnologija Active Directory podržava RFC822 format imena za sve korisnike. Kad tražite broj lokala određene osobe u organizaciji (ako su ti brojevi javni), pogledajte u imeniku pod imekorisnika@imedomena.com (vaš softver će to prevesti u ispravan LDAP upit, kao što ćemo kasnije vidjeti). UPN je takođe ime ili šifra pod kojom se korisnik prijavljuje u domen Windows Servera 2003.
Korisnik Windowsa može sada da se prijavi u domen Windows Servera 2003 upisivanjem svoje identifikacione šifre i lozinke:

User: 1509@fit.ba
Password:*********

Domenu možete da dodjelite poseban UPN za prijavljivanje. Drugim rječima, možete napraviti domen koji ćete nazvati npr. MCITY, ali koji ćete podesiti tako da se korisnici u njega prijavljuju u obliku imekorisnika@imefirme.com, ćime ih ne primoravate da pamte više od svoje adrese elektronske pošte.

LDAP i X.500 imena
Imena koja se dodjeljuju po konvencijama LDAP i X.500, ponekad se zovu atributivna imena (engl. attributed names). Ime se sastoji od imena servera na kome se nalazi imenik (koji ćemo zvati domaćin imenika), imena korisnika, njegove organizacione jedinice itd. Na primer:

LDAP://nekildapserver.superfirma.com/cn=mikapetrovic,ou=racunovodstvo,
dc=superfirma,dc=com
Pomoću LDAP imena pretražujemo aktivne imenike.

Active Directory i Internet

Servere aktivnog imenika možete postaviti bilo gdje na Internetu ili unutar privatnog intraneta. To mogu da budu računari koji su istovremeno i Window Server 2003 upravljaći domena ili namjenski računari, koji služe isključivo kao serveri za LDAP imenike. Korisnici i klijenti tih servera neće primjetiti nikakvu razliku.

Da bi pribavio traženu informaciju, klijent treba samo da uspostavi vezu s najbližim Active Directory serverom. Ukoliko je server u istom domenu gdje i klijent, DNS server se svodi na Active Directory server u istoj podmreži kao klijent. Kada se Active Directory server nalazi u različitom domenu, onda se koristi kao server Internet imenika koji neće pružati usluge identifikacije korisnika. Više Active Directory servera mogu meođusobno da se povežu tako da pružaju globalnu uslugu imenika koja obuhvata cijeli kontinent.

Active Directory u jednokorisničkom režimu

Microsoftova namjera je da tehnologija Active Directory bude veoma prilagodljiva i da se širi brzinom koju resursi omogućavaju. Aktivni imenik se lako instalira i podešava na jednostavnom serveru. Isto važi kada se aktivni imenik instalira za rad u jednokorisnićkom režimu, a gotovo nimalo ne opterećuje sistem kada je u svom najjednostavnijem obliku. Drugim rječima, ako aktivni imenik treba da bude mali, može da bude mali, a kada treba da bude veliki, rašće zaprepašćujućom brzinom.

Tehnologiju Active Directory to čini savršenom čak i kada se koristi u najjednostavnijem obliku, kao spremište podataka s kojima radi određena aplikacija. Iako on ne može da zamjeni prave sisteme za upravljanje bazama podataka koji pružaju složenije usluge upravljanja podacima kao što su analize i pretraživanje podataka (ili upravljanje cjelokupnim podacima jedne firme), nije neuobičajeno da aplikacija projektovana za jednokorisnićki rad primjenjuje tehnologiju aktivnog imenika čime se olakšava naknadno proširivanje koje se tako svodi na jednostavnu operaciju dopune imenika. Aktivni imenik mož e da se instalira čak i na stonoj mašini koja radi na 133 MHz, sa 64 MB radne memorije. Takva konfiguracija se lako podešava i kao upravljač domena koji može da podrži poslovanje manje firme (Microsoft službeno ne preporučuje takvu konfiguraciju; trebalo bi da bude ograničena isključivo na poslove imenika s manjim brojem korisnika i računara).

Aktivni imenik može da se postavi tako da se širi do nevjerovatnih razmera. U ulozi spremišta podataka o objektima u domenu, "plafon" Windowsa NT 4.0. je oko 100.000 korisnika, dok aktivni imenik može da obuhvati milione – pa čak i cijeli Internet. Sve replike aktivnog imenika međusobno su sinhronizovane (što je već samo za sebe blagodet za administratora, kao što čemo uskoro videti). Sve kopije sistema aktivnih imenika jedne organizacije prosljeđuju izmjene jedna drugoj, slično naćinu na koji DNS serveri međusobno razmjenjuju podatke o domenima.

U praksi, NT domen postaje nestabilan kada ima približno 30.000 ili 40.000 naloga, pa mnoge velike kompanije uvode veći broj domena za resurse i naloge. Pošto aktivni imenik koriste i Windows 2000 i Windows Server 2003, među njima nema značajnije razlike kada se radi o mogučnostima proširenja.

Ključno za proširivost aktivnog imenika jeste stablo domena, odnosno hijerarhijska organizacija podataka koja, teorijski, može beskonaćno da se širi. Tehnologija Active Directory pruža jednostavnu metodu građenja obimnog stabla od dna prema vrhu. U aktivnom imeniku, svaki domen je jedna particija imenika. Domeni se zatim djele na organizacione jedinice, što administratorima omogućava da u model preslikaju fizićku strukturu organizacije ili odgovarajuće poslovne modele. Domen na početku može da sadrži veoma mali broj objekata i da kasnije naraste toliko da sadrži desetine miliona. To znaći da

objekte možete da definišete kao sliku strukture organizacije usitnjene do najnižeg nivoa detalja, bez ikakvog rizika da pretjerate s njihovim brojem, što je bio slučaj u Windowsu NT 4.0 i NetWareu 3.x i 4.x.

Jezgro Active Directory-a

Jezgro aktivnog imenika je lako dostupno samo zaluđenicima, za koje pojam sreće predstavlja red C++ koda. Uz aktivni imenik se ne isporučuju specijalne alatke, kao što je to slučaj sa MS Accessom, pomoću kojih biste mogli da vidite šta se nalazi unutar struktura ili na šta te strukture liče (nekoliko alatki iz kompleta Resource Kit to omogućavaju). Naredni odjeljci opisuju ključne komponente s namjerom da vam predoće unutrašnji mehanizam ove usluge.
Na fizičkom nivou, aktivni imenik je baza podataka i sistem za upravljanje bazom podataka – i to je sve. Podaci koje imenik sadrži mogu se pregledati i prikazivati u hijerarhijskom obliku. Baza podataka je skladište za podatke. To je softverska struktura koja omogućava skladištenje podataka, rad s njima i učitavanje svakom procesu koji im pristupa radi korišćenja sadržanih podataka. Ukoliko smatrate da ovo nije dobra definicija aktivnog imenika, primjenimo definiciju baze podataka (njenih pravila) na aktivni imenik:

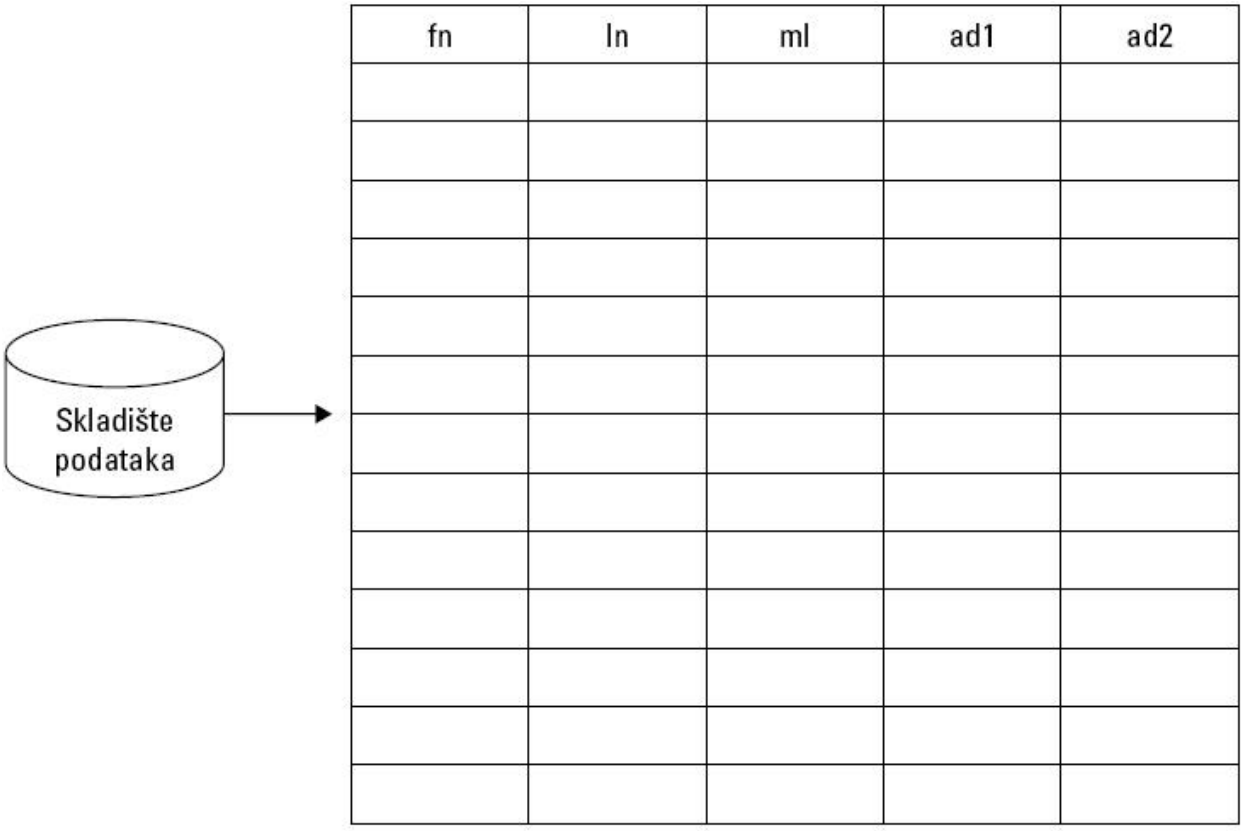
Baza podataka zadovoljava svoju definiciju kada ispunjava sljedeće uslove:

- Sadrži funkcionalne slojeve – u šta spada i šema baze podataka – koji definišu strukturu baze podataka, a to su načini na koje se podaci skladište, učitavaju i mjenjaju. U druge funkcionalne slojeve spada "mehanizam" čiji su zadaci ulazno/izlazne operacije, održavanje podataka, izvršavanje upita i obezbjeđivanje interfejsa ka spremištu podataka. To se često naziva mehanizam baze podataka.
- Podaci o određenom predmetu i njegova svojstva i atributi smješteni su u kontejnere koji se sastoje od zbirki zapisa, poznatih kao tabele (kao što je slućaj u relacionim bazama podataka) ili su u nekom drugom obliku (kao u objektnim bazama podataka).

Najjednostavnija definicija sistema za upravljanje bazama podataka jeste to da ga čine dvije komponente: softverska aplikacija povrh koje stoji korisnički interfejs, a koja upravlja podacima u bazi podataka, i sama baza podataka.
Sistem za upravljanje bazama podataka (DBMS) može da izdvoji tražene podatke (izvršavanjem upita), da ih formatira u zadati oblik, da ih prikaže korisniku i da ih odštampa ili prenese u razumljiv oblik. Savremeni sistemi za upravljanje bazama podataka, poput SQL Servera, svojim korisnicima stavljaju na raspolaganje tehnologiju koja omogućava tumačenje ili analiziranje podataka, za razliku od jednostavne kvantifikacije.

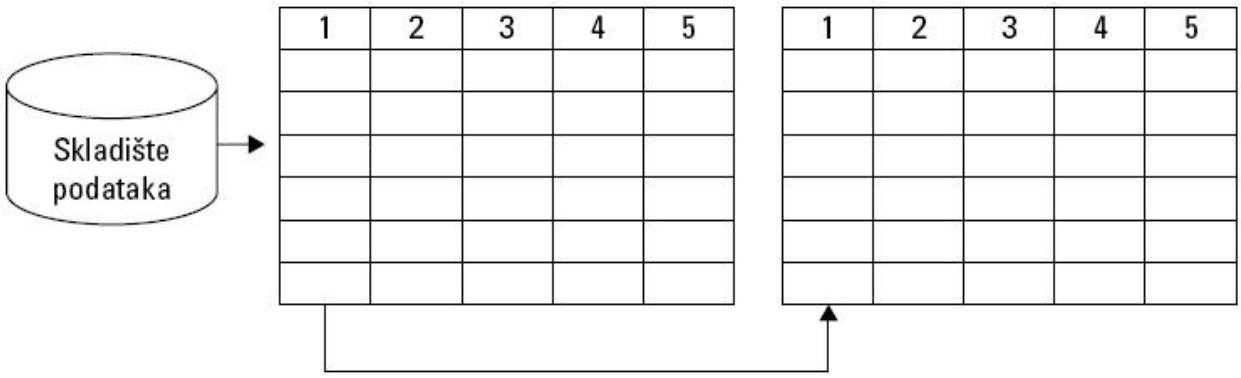
Korisnici baza podataka i sistema za upravljanje njima mogu da budu i ljudska bića i mašine. Mašine i računari koriste softver koji skladišti i učitava podatke, jer je to sredstvo pomoću koga svaki proces može da pristupi uskladištenom podatku. Uskladištene podatke može (i treba) da djeli više korisnika, bez obzira na to da li se radi o ljudima ili o uređajima koje su ljudi napravili.

Na primer, inžinjer može u bazu podataka da upiše određene podatke, na osnovu kojih robot obavlja određene standardizovane poslove. Aktivni imenik jeste sve prethodno opisano još i više od toga. Međutim, vjerovatno ga nećete koristiti da biste u bazi pronašli zapise o osobama koje predstavljaju poslovni rizik za vašu firmu, jer to nije svrha usluge imenika. Pošto pitanje da li je aktivni imenik relaciona ili objektna baza podataka može da nas odvede prilično daleko u diskusiji, nećemo se time baviti. Naša analiza tehnologije Active Directory pomoći će vam da sami dođete do zaključka. Relacionu bazu podataka čine tabele; svaka od njih sadrži kolone (zbirke) istovrsnih informacija koje su predmet našeg zanimanja, npr. kolonu ili zbirku imena.
Podaci koji čine svaku pojedinu stavku smještaju se po hronološkom redu, na primjer, peto ime po redu u zbirci (koloni) fn (engl. first name, ime) može biti David.
Na slici 3 prikazana je kolona imena.



Slika 3. Kolona u relacionoj bazi sadrži zapise koji su članovi zbirki ili grupa

Relaciona baza podataka može da sadrži više tabela. Moguće je i da "stvari" iz jedne tabele budu povezane sa "stvarima" u drugoj tabeli, ne samo sticajem okolnosti, već i namjerno, jer je tako baza podataka projektovana. U relacionoj bazi podataka možete da pristupate svojstvima određene "stvari" i podacima koje ona predstavlja tako što referencirate njeno mjesto u zbirci, kao u primeru na slici 4.



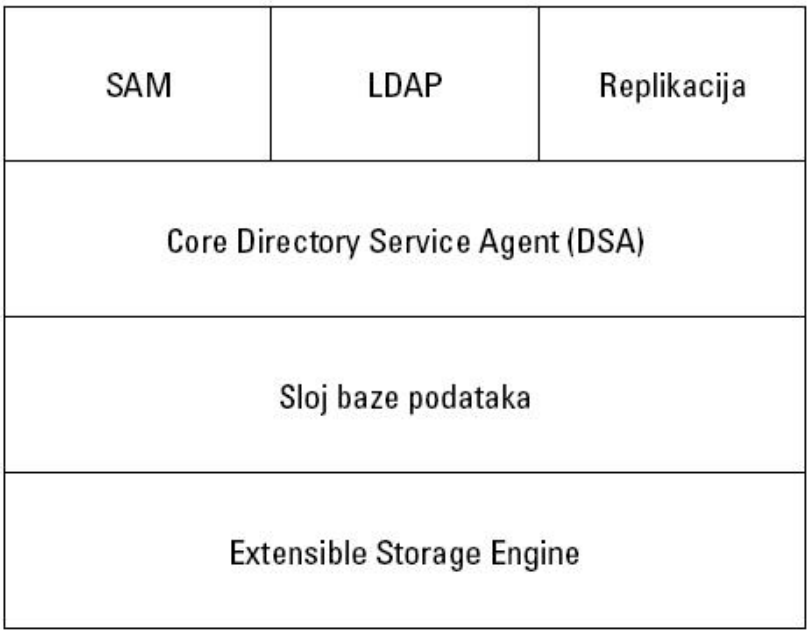
Slika 4. Dvije kolone relacione baze podataka sadrže međusobno povezane zapise

Objektna baza podataka se nešto teže definiše, prvenstveno zato što su mnogi oblici objektnih baza podataka evoluirali iz relacionih baza podataka. Važnije osobine jedne baze podataka koja podržava određeni objektni model jesu načini na koje korisnici pristupaju njenim podacima i logičkoj šemi na kojoj se ona zasniva; manje je važan način na koji je to omogućeno i tehnologija koja je primjenjena. Objektnu bazu podataka možemo opisati i kao bazu podataka koja je usklađena sa objektnim modelom, za razliku od relacione baze podataka. Ne znamo tačno kako radi aktivni imenik, pošto je jezgro sistema zatvorena tehnologija čiji je vlasnik Microsoft. Znamo da se podaci čuvaju u strukturama koje liće na

kolone (stupce) i redove. U tehnologiji Active Directory, Microsoft koristi isti mehanizam baze podataka (Jet) kao u Exchange Serveru. To znaći da imamo posla s bliskim rođakom Microsoftovog Accessa.

Struktura baze podataka aktivnog imenika

Realizacija aktivnog imenika je sistem koji se sastoji od više komponenata ili slojeva: agenta usluge imenika (CoreDirectory Service Agent, DSA), sloja baze podataka (Database Layer, DB) i proširivog mehanizma za skladištenje podataka (Extensible Storage Engine, ESE). Iznad tih slojeva nalazi se interfejs koji obuhvata funkciju replikacije, bezbednosni upravljač nalozima sličan SAM-u u Windowsu NT 4.0 (Security Account Manager, SAM), LDAP interfejs i skup API funkcija (ADSI). LDAP interfejs, kao što ćete kasnije vidjeti, obezbjeđuje pristup LDAP klijentima. LDAP podržavaju sva 32-bitna okruženja na stonim računarima i na radnim stanicama, a ugrađen je i u Outlook. U aktivnom imeniku, SAM obezbjeđuje bezbjednosni interfejs koji koristetehnologije za kontrolu pristupa podacima (slika 5).



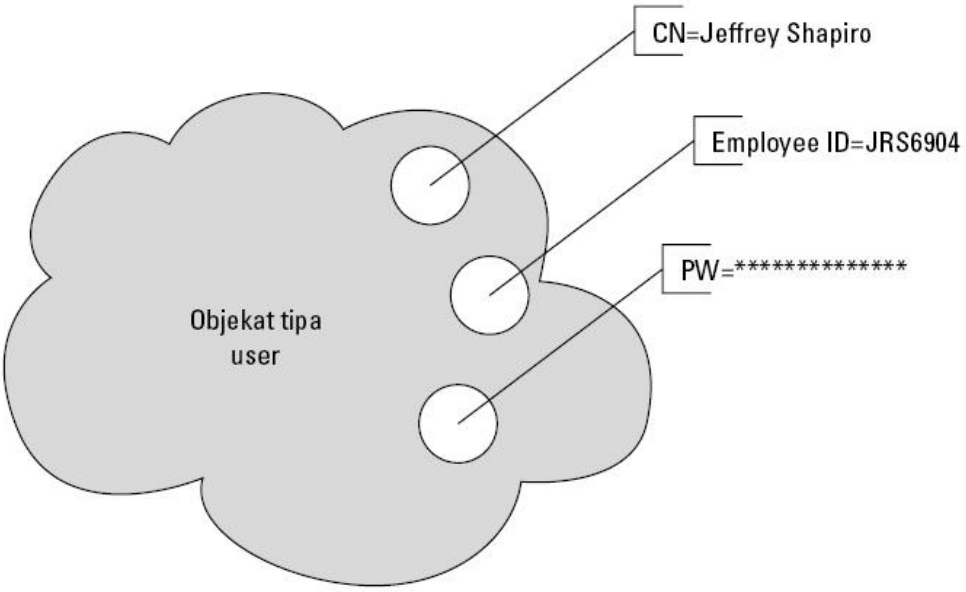
Slika 5. Aktivni imenik se sastoji od tri funkcionalne komponente, iznad kojih su postavljene komponente koje omogućavaju pristup podacima i njihovu replikaciju, i bezbednosna komponenta SAM.

Komponenta ESE (najniža na slici) radi s dvije tabele: jedna je tabela za podatke, a druga za veze između njih. ESE bazu podataka, čija je svrha da čuva podatke o strukturi imenika, klijenti ne vide i nemaju pristup u nju. Baza podataka samog aktivnog imenika, NTDS.DIT, sadrži sljedeće tabele kojima klijenti pristupaju posredno ili neposredno:

- Tabela šeme baze podataka (engl. schema table): Šema baze podataka određuje vrste objekata koji se mogu umetnuti u aktivni imenik, veze koje postoje između njih i obavezne i neobavezne atribute tih objekata. Važno je napomenuti da je šema proširiva, što znaći da može obuhvatiti i nove namjenske objekte koji nastaju tokom rada raznih aplikacija i usluga.
- Tabela veza (engl. link table): Sadrži podatke o vezama koje postoje između objekata u bazi podataka.
- Tabela podataka (engl. data table): Najvažnija struktura u sistemu baza podataka aktivnog imenika, jer se u njoj čuvaju svi podaci o objektima u imeniku ili njihovi atributi. Ona sadrži sve obavezne i neobavezne podatke koji čine objekte; npr. imena i prezimena korisnika, njihova korisnička imena, lozinke, grupe i podatke o pojedinim aplikacijama.

Objekti aktivnog imenika

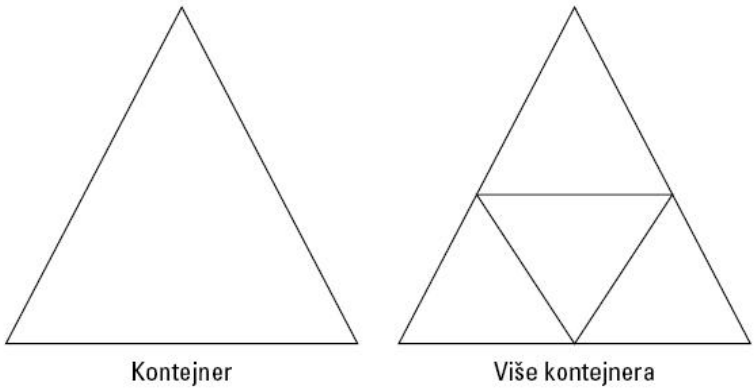
Kada bismo aktivni imenik uporedili s loncem u kome se kuha jelo, onda bi objekti bili sastojci tog jela. Bez objekata, aktivni imenik bio bi samo prazna posuda. Kada instalirate aktivni imenik, već na samom početku sistem u njega smješta nekoliko korisničkih objekata kojima možete odmah da pristupate.



Slika 6. Objekat koji u aktivnom imeniku predtavlja korisnika i njegova tri atributa

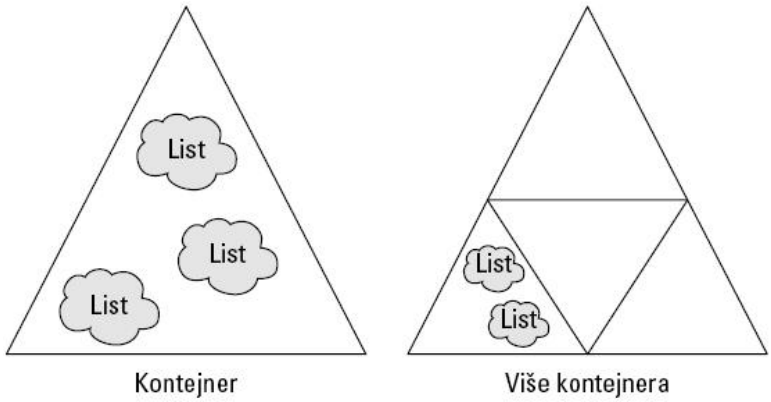
Neki od tih objekata predstavljaju korisničke naloge, kao što je Administrator, bez kojih ne biste mogli da se prijavite i obavite provjeru svog identiteta u aktivnom imeniku. Objekti imaju atribute ili svojstva, s podacima o resursima koje predstavljaju. Na primer: objekat koji predstavlja korisnika Windowsove mreže sadrži podatke (atribute) o imenu, prezimenu i korisničkom imenu za prijavljivanje. Na slici 6 prikazan je objektno orijentisani oblik objekta, koji u aktivnom imeniku predstavlja korisnika.
(Stvarna struktura podataka ima oblik tabele s kolonama ili poljima.)

Jedan aktivni imenik može da sadrži veliki broj različitih objekata. Neki od njih sadrže podatke koji se mogu direktno koristiti, a neki su samo kontejneri za druge objekte. Moglo bi se reći da je cjeli aktivni imenik jedan veliki objekat, koji sadrži kontejnerske objekte, u kojima se nalaze drugi objekti, koji i sami sadrže druge objekte, kao što je ilustrovano na slici z. Kontejnerski objekat (engl. Container object), smo nacrtali u obliku trougla, jer je to popularan simbol za spremište; on sadrži druge kontejnerske objekte. Ugnježđivanje objekata može da se nastavi dok se ne dođe do objekta koji se nalazi na poziciji lista, što znaći da on ne može da bude kontejner.



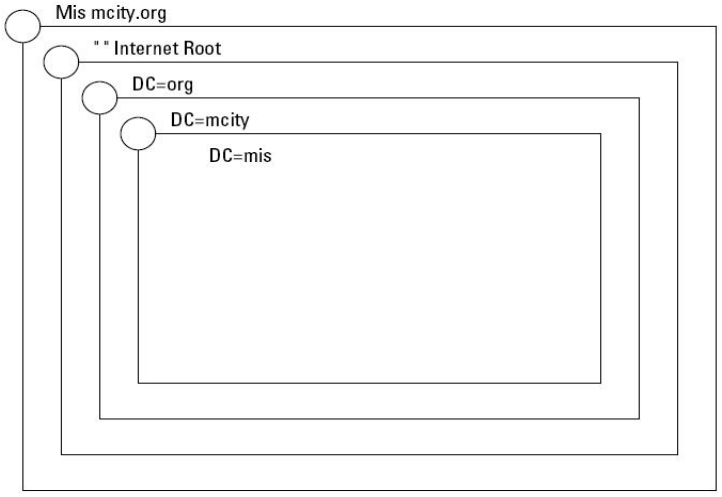
Slika 7. Kontejnerski objekat sadrži druge objekte, koji i sami mogu da sadrže objekte

Objekti koji nisu kontejneri, npr. objekat User (predstavlja korisnika), poznati su kao listovi, ili krajnji čvorovi (slika 8). Kada objekat tipa list (engl. leaf object) dodate u kontejner, to je posljednji nivo ugnježdavanja.



Slika 8. Objekat na mjestu lista (ili krajnjeg čvora) ne sadrži druge objekte.

Aktivni imenik podsjeća na veliku lutku "babušku". Na slici 9 prikazan je popularan dvodimenzionalan oblik predstavljanja principa kontejnera. Nama koji se bavimo informacionim tehnologijama i administriranjem Windows mreža, razumljivija je metafora stabla sa objektima, o čemu će uskoro biti riječi. Kada koristimo aktivni imenik, često govorimo i o klasama objekata. Klasa objekta (u ovom kontekstu) manje je klasa u smislu u kome se koristi u objektno orijentisanim tehnologijama – prije svega je kolektivno ime za vrstu i namjenu srodnih objekata organizovanih u grupe. Klase objekata mogu da budu korisnički nalozi, računari, mreže i druge grupe srodnih objekata; u stvari, to može biti svaka vrsta objekta koju tehnologija Active Directory trenutno podržava.



Slika 9. Kada spojimo tačke koje predstavljaju identifikacionu šifru svakog okvira, dobiñćmo hijerarhijski organizovanu zbirku okvira.

Klasu objekata, ili jednostavno klasu, zamišljamo i kao definiciju određenog objekta koji možemo da napravimo i koristimo unutar imenika. Pravila za sadržaj (engl. content rules) određuju šta sve mogu da budu atributi jednog objekta. Klasama su pridružena i dodatna pravila kojima se zadaje koje klase objekata mogu biti roditelji, koje djeca, a koje i jedno i drugo
.
Već smo napomenuli da je šema aktivnog imenika proširiva. To znači da programeri mogu da pišu kôd, iz koga korištenjem API funkcija mogu da stvaraju svoje objekte i upravljaju njima. Time se projektantima aplikacija omogućava da u aktivne imenike upisuju podatke o konfiguracijama i stanjima aplikacija.

Registar je i dalje dobro mjesto za čuvanje podataka o aplikacijama, naročito onima koje se odnose na hardver, ali aktivni imenik nudi mogućnosti kao što su replikacija, prosljeđivanje i bogatiji izbor vrsta objekata, npr. objekte tipa korisnik (User) na koje aplikacija može da djeluje i koji međusobno sarađuju.

Šema Active Directory-a

Šema (engl. schema) alfa je i omega aktivnog imenika. Kada u njemu pravite novi objekat, morate da poštujete pravila zadata u šemi imenika. Drugim rječima, morate da zadate vrijednosti svih obaveznih atributa za određenu vrstu objekta, inače nećete moći da ga napravite. Šema imenika propisuje tipove podataka, pravila sintakse, način imenovanja objekata i druge parametre. Kao što smo ranije napomenuli, šema aktivnog imenika je smještena u vlastitoj tabeli i može dinamički da se širi. To znači da program može da je dopunjava novim namenskim klasama i da definiše pravila po kojima će šema upravlaati tim klasama. Pošto to uradi, aplikacija može odmah da koristi dopunjenu šemu.

Pri proširenju ili izmjeni šeme, morate poštovati pravila programiranja i administriranja imenika. Pošto je i sama šema sastavni dio imenika, to znači da je ona, kao i aktivni imenik, usluga koja je dostupna širom organizacije. Glavnoj šemi najprije moramo pristupiti na propisan način, da bi se izmjene koje potom u njoj napravimo replikacijom prenjele u eventualne kopije.

Struktura aktivnog imenika

Do određenog objekta u aktivnom imeniku stižemo tako što sljedimo hijerarhijsku putanju koja se dobija tumačenjem imena objekta. Putanja sadrži sve kontejnerske objekte kroz koje treba da pređemo da bismo stigli do krajnjeg čvora. Na prvi pogled može biti neshvatljivo da, s jedne strane, govorimo o kontejnerima, dok, s druge strane, pričamo kako treba da pređete dug i krivudav put da biste stigli do imena objekta koji predstavlja list ili krajnji čvor na stablu. Proučite dijagram na slici 9; on pokazuje sistem okvira koji sadrže manje okvire itd. Ako spojite gornje leve uglove okvira, pomoliće se hijerarhijska putanja o kojoj govorimo.

U terminologiji aktivnog imenika, puna putanja, sastavljena od imena spojenih uglova i imena samog objekta, zove se jedinstveno ime (engl. distinguished name, DN). Ime samog objekta, koje se nalazi na kraju lanca, zove se relativno jedinstveno ime (engl. relative distinguished name, RDN); u ovom primjeru to je "mis". Kažemo da je kombinacija pune putanje do objekta i samog imena objekta jedinstvena, pošto nijedan drugi objekat ne može da ima isto DN ime objekta. Drugim riječima, objekat je jedinstven. Namena ovog mehanizma za imenovanje i pronalaženje objekta jeste da omogući LDAP klijentu da što brže pronađe traženi objekat i da iz njega učita podatke.

Relativno jedinstveno ime (RDN) objekta je ime samog objekta. To je jedan od atributa objekta. RDN ime ne mora uvek da bude jedinstveno (iako jeste jedinstveno unutar

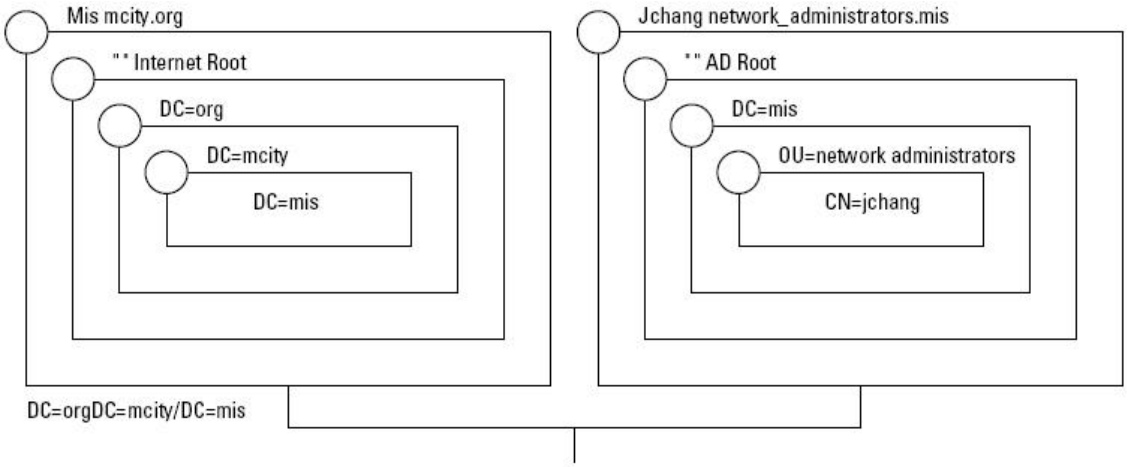
kontejnera aktivnog imenika u koji je objekat smješten), jer isto takvo ime može da postoji na kraju neke druge DN putanje u istom aktivnom imeniku. Na slici 10 prikazano je da dva objekta mogu imati isto RDN ime, ali na određenom nivou lanca sličnost prestaje, ako ne na drugom mjestu, svakako na nivou korjenskog ili roditeljskog čvora. Kada pretražujemo aktivni imenik (šaljemo mu upit), sasvim prirodno počinjemo od korjena DN putanje objekta i sljedimo putanju do krajnjeg čvora. U LDAP protokolu krećemo od RDN-a i učitavamo djelove imena sve do korjena putanje. Na ovaj način u upitu rekonstruišemo cjelo DN ime, na primer:

cn=okvir1,koren=,kontejner5=,kontejner6=,kontejner7=,kontejner8=..

Možda ćete lakše razumjeti princip pretraživanja ako u ovoj fazi napišete DN na parčetu papira. Kao vježbu, sastavite upit za korisnika čije je ime jchang. Da biste stigli do imena jchang, treba da počnete od cn imena objekta, što je jchang, zatim da pređete na kancelarija=232, sprat=3, zgrada=maocetung, grad=peking. LDAP kreće od dna i nastavlja ka vrhu. Ne pokušavajte da osmislite ulaznu tačku u aktivni imenik, već uvek počnite od objekta i sljedite putanju dok ne dođete do korjenskog objekta.

Konvencije za imenovanje objekata

Svaki segment DN putanje predstavlja atribut nekog objekta izražen u obliku tip_atributa=vrednost. Za ime samog objekta (RDN) kažemo da je kanonsko (engl. canonical) ili osnovno (engl. common), što se u LDAP žargonu izražava u obliku cn=. Kada se radi o objektu tipa korisnik, osnovno (kanonsko) ime prima oblik cn=jchang. RDN svakog objekta se čuva u aktivnom imeniku, a svaka referenca na njega sadrži i referencu na njegove roditelje. Sljedeći reference duž lanca, možemo da sastavimo DN putanju. Na taj način LDAP pretražuje imenik. Ovaj način imenovanja objekata veoma je sličan DNS mehanizmu (slika 10).



Slika 10. Hijerarhija domena na ljevoj strani predstavlja DNS sistem imenovanja koji se koristi na Internetu. Hijerarhija domena na desnoj strani predstavlja sistem imenovanja koji se koristi u aktivnom imeniku.

Pošto sada znate kako djeluje mehanizam imenovanja u aktivnom imeniku, treba da znate i to da Windows ne zahtjeva od običnih korisnika da sami obavljaju prethodno opisane operacije svaki put kada pristupaju određenom objektu. Korisnički interfejs obavlja cjeli posao i skriva sintaksu od vas. Međutim, zadavanje tih atributa je neophodno kada programirate koristeći API (ADSI) funkcije za rad sa aktivnim imenikom, ili direktno koristite LDAP, jezike za pisanje skriptova ili alatke za pretraživanje i rad sa aktivnim imenicima na napredniji način, koji standardne alatke ne omogućavaju.
Active Directory podržava i LDAP v2 i LDAP v3 stilove imenovanja objekata, koji su usklađeni sa Internet dokumentima RFC 1779 i 2247 o stilovima imenovanja.

Stil ima sljedeći oblik:

cn=common name (osnovno ime)
ou= organizational unit (organizaciona jedinica)
o=organizacija
c=country (država)

U aktivnom imeniku se umjesto c=country i o=organizacija koristi dc=domain component (komponenta koja predstavlja domen). Na primer:

cn=jchang,ou=marketing,dc=mcity,dc=org

Zarezi u DN putanji služe kao graničnici koji razdvajaju elemente putanje. LDAP funkcije analiziraju DN putanju i na osnovu graničnika izdvajaju njene djelove.

U notaciji s tačkom, to bismo napisali ovako:

jchang.marketing.mcity.org.

Jedan od algoritama LDAP-a prevodi LDAP imena u DNS format i obrnuto. U skladu s LDAP formatom imena, svaki LDAP klijent može da pretražuje aktivni imenik zadajući jednoobraznu adresu resursa (Uniform Resource Locator, URL) koji traži, kao u sljedećem primjeru:

LDAP://ldapserver.mcity.org/cn=jchang,ou=marketing,dc=mcity,dc=org

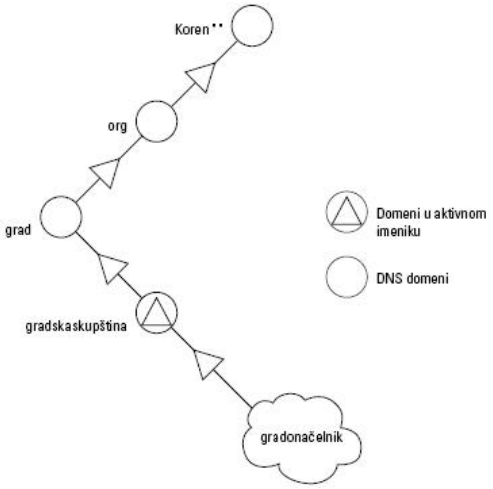
Objekti se u aktivni imenik smještaju i u njemu pronalaze na osnovu atributa koji sadrži jedinstveni globalni identifikator objekta (Globally Unique Identifier, GUID). Ime tog atributa je objectGUID. Zato identifikator objekta ostaje isti i kada objekat premještate ili mjenjate, pa čak i kada ga preimenujete. GUID je 128-bitni broj koji se objektu dodjeljuje kada ga napravite. Objekat ne može da postoji u aktivnom imeniku, a da mu nije dodjeljen GUID; to je jedan od obaveznih atributa, kome se vrijednost automatski dodjeljuje kada objekat nastane. Drugim rječima, objekat možete referencirati u aktivnom imeniku ili iz spoljnog programa koristeći njegov GUID. Stoga je objekat uvek dostupan dok postoji. Kuda god ga premjestili, on će i dalje biti dostupan. Pristup objektima u aktivnom imeniku kontroliše se pomoću SAM mehanizma za upravljanje pristupom i na osnovu lista za kontrolu pristupa (Access Control List, ACL). Drugim rječima, da biste određeni objekat izmjenili ili izbrisali, treba da dokažete da ste njegov vlasnik i da imate odgovarajuća prava na njega.

Objekti tipa domen

Kada aktivni imenik podešavate za korištenje na nivou cjele organizacije, vaš prvi zadatak je da napravite korjenski domen, odnosno ono što se u terminologiji aktivnog imenika zove objekat korjenskog domena (engl. root domain object). Ukoliko taj korejnski domen treba da bude i vaš Internet korjenski domen, trebalo bi da ga što prije registrujete u odgovarajućoj organizaciji za upravljanje domenima Interneta. (Jedna od takvih organizacija je Network Solutions, Inc.) Ukoliko ste već registrovali korkenski domen, možete da napravite objekat koji ga predstavlja u aktivnom imeniku i da ga povešete s DNS serverom koji preslikava to ime u adresu. Ako niste registrovali domen, možda nećete moći da mu date ime kompanije, pošto se nova imena domena registruju svakog sekunda tokom dana. Taj korjenski domen postaje prvi kontejnerski objekat napravljen u lancu objekata koji treba da predstavljaju strukturu domena vaše lokalne mreže u aktivnom imeniku. "Ispod" tog domena napravićete dodatne kontejnerske objekte koji predstavljaju organizacione jedinice vaše kompanije (o čemu će biti rjeći u nastavku). Na primer, mogli biste napraviti domen, nazvati ga mcity.org i registrovati u InterNIC-u. O pitanjima bezbjednosti govorićemo kasnije.

Zasad treba da znate samo to da su domeni koje pravite, u pogledu upravljanja njima i bezbjednosti, samostalne cjeline unutar vaše mreže, na isti način kao što su to bili domeni Windowsa NT 4.0 i starijih verzija.

Slika 11 predstavlja putaçnju, odozdo nagore, od korisnika do korjenskog domena. Kao što već znate, u aktivnom imeniku jedan objekat može da ima samo jedan roditeljski domen. Sasvim je moguće, čak i preporučljivo, da se ispod korjenskog domena prave poddomeni koji odslikavaju raspodjelu resursa, podjelu na sektore, politički i geografski različite segmente jedne firme, objekte u vlasništvu kompanije i drugo.



Slika 11. Objekat tipa korisnik (korisnički nalog) u lokalnom domenu jednog aktivnog imenika. U ovom primjeru postoji direktna veza između AD domena i DNS domena.

Domeni i kontrolisanje korisnika unutar mreže

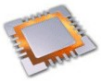
NT domen (ili domen Windowsove mreže) logička je grupa računara i uređaja koji su dostupni grupi ili grupama korisnika ili računara, bez obzira na mesto s kog se oni prijavljuju za rad. Domen je način grupisanja i kontrolisanja korisnika mreže, a definiše i granice bezbjednosnog okruženja u kome je računarima, korisnicima i operaterima obezbjeđena zaštita. Domeni Windows Servera 2003 imaju istu funkciju, što je objašnjeno u narednim poglavljima.

Ako ste novajlija u mrežama koje rade pod Windowsom, evo kratkog objašnjenja Windowsovog mrežnog domena: uporedite ga s radnom grupom. Kada je početkom devedesetih godina Microsoft ponudio Windows 3.11 i Windows for Workgroups, pružio je mogućnost da se računari međusobno povezuju kao ravnopravni članovi da bi svaki umreženi računar svoje resurse stavio na raspolaganje ostalim mašinama.

Za to je trebalo da prethodno izričito dozvolite pristup resursima svakog pojedinog računara unutar mreže. To je prilično zamoran posao u mreži koja obuhvata samo jednu kancelariju, jer se svaki računar ponaša kao samostalan server i tako treba njime i upravljati. Kada mreža počne da se širi, to postaje nepraktično, pa čak i gotovo nemoguće. S druge strane, domen je nastao zbog potrebe da se bezbjednost, prijavljivanje i pristup centralizuje na jedan "glavni" server, koji se zove primarni upravljać domena (Primary Domain Controller, PDC). Baza podataka SAM, koja je smeštena u registru, korisnicima je obezbjeđivala globalan pristup u centralnu bezbjednosnu bazu podataka, odakle su dobijali pristup svim resursima na svim računarima i uređajima priključenim u mrežu, kao što su štampači, ureođaji za pravljenje rezervnih kopija ili CD-R uređaji.

Liste za kontrolu pristupa

Kada se korisnik (čovjek ili usluga) prijavi u domen, mehanizam za identifikaciju i bezbjednost Windowsa NT odobrava mu pristup mreži i resursima koje ima pravo da koristi. To se postiže pomoću lista za kontrolu pristupa (Access Control Lists, ACL) i pristupnih žetona. Iskusni i vješti NT administratori će se podsjetiti kako se pristupa ACL listama i kako se mjenja njihov sadržaj. A ako vi ne znate kako se to radi, saznaćete kasnije. NT dodjeljuje korisniku i pristupni žeton (engl. access token), kojim se korisnik služi dok radi u mreži.



Pristupni žeton funkcioniše slično identifikacionoj kartici koju nosite kada ste na poslu. Kada je približte vratima ili nekom uređaju, ona se ili otvaraju ili vam uskraćuju prolaz. Obe vrste domena, Windows NT i Windows 2003, kontrolišu pristup pomoću ACL lista. U aktivnom imeniku, ACL liste (unutar imenika), napravćene na osnovu sadržaja baze podataka SAM, kontrolišu kome je i s kojim pravima dozvoljen pristup objektima. Sve usluge Windows Servera 2003 referenciraju se kao objekti. Ti objekti su smješteni u lokalnoj bazi podataka SAM, koja je u stvari grana registra, ili se korištenjem aktivnog imenika upravlja pomoću ACL liste. Svaka ACL lista sadrži podatke o dozvolama dodjeljenim korisnicima, s detaljnim opisom korisnika koji smije da pristupa određenom objektu i njegovih prava (npr. ima samo pravo čitanja ili pravo čitanja i pisanja). ACL liste su vezane za objekte u određenom domenu; one nisu privremeni objekti.