Fakultet elektrotehnike i računarstva
Podatkovni višemedijski prijenos i računalne mreže

SEMINARSKI RAD

Directory Services

DARIO BOŠNJAK

SADRŽAJ

1. UVOD

Svijet danas, promatrajući ga iz informatičke perspektive, postaje sve više povezan pa se javlja potreba da informacije budu dostupne u bilo koje vrijeme sa bilo kojeg mjesta i pomoću bilo kojeg uređaja. Većina današnjih javnih ustanova, tvrtki, korporacija, banaka te bilo kojih drugih organizacija ima izgrađenu računalnu mrežnu infrastrukturu. Ta je mrežna infrastruktura kod velikih korporacija, univerziteta i sličnih glomaznih ustanova veoma razgranata i kompleksna i često redundantna. Svaka mreža barata sa određenim relevantim informacijama koje su brojnije kako mreža ekspandira. Te su informacije, koje primjerice opisuju različite korisnike, aplikacije , datoteke, printere i ostale resurse dostupne iz mreže, često pohranjene u više specijaliziranih baza podataka. Kako raste broj različitih mreža i aplikacija tako raste i broj tih specijaliziranih baza (direktorija) što na koncu rezultira stvaranjem informacijskih "otoka" koje je teško kontrolirati i kojima je teško upravljati. Kada bi se sve ove informacije mogle održavati, kontrolirati te njima upravljati na konzistentan i kontroliran način, tada bi one predstavljale "žarišnu točku" za integriranje distribuirane okoline u konzistentan i cjelovit sustav.

Obilježja računalnih sustava današnjice :

- Veliki broj resursa
- Distribuiranost resursa
- Različitost resursa
- Konstantan porast u broju i veličini
- Višestruki izvori nepovezanih resursa
- Dostupnost 24*7
- Zajamčena sigurnost
- Proširivost
- Low-cost administracija
- Aplikacijski specifični direktoriji

Vidimo da održavanje ovakvih sustava može predstavljati vrlo zahtjevnu, kompleksnu i mukotrpnu zadaću. Stoga su stručnjaci nastojali pronaći rješenje koje bi olakšalo posao mrežnim administratorima ali i rješenje koje bi poboljšalo i unaprijedilo neke bitne komponente (primjerice sigurnost) ovakvih sustava.
Rješenje stručnjaci vide u postojanju jednog centralnog mjesta na kojemu su pohranjene sve relevantne informacije i sa kojeg se može upravljati i nadgledati cjelokupni sustav. Riječ je dakako o direktoriju i direktorijskim uslugama.

2. Osnovni koncepti Directory service-a

U ovom poglavlju biti će govora o osnovnim konceptima direktorijskih servisa i teoretskim temeljima na kojima su izgrađene sve dostupne implementacije direktorijskih servisa. Konkretno će biti opisani X.500 i LDAP standardi na kojima se temelji svaki direktorij, a direktorij čini jezgru svakog directory service-a.

2.1 Direktorij opće namjene – X.500

Priča o direktorijima započinje opisom X.500 standarda. X.500 je direktorijski (Directory service standard) standard kojeg su zajedno donijeli ISO i ITU organizacije. Prilikom donošenja standarda, organizacije bile su vođene idejom stvaranja globalno distribuiranog sustava koji bi pružao homogeni pristup informacijama .
X.500 standard daje sljedeću karakterizaciju direktorija : "Direktorij je kolekcija otvorenih sustava koji međusobno kooperiraju kako bi čuvali logičku bazu informacija o skupovima objekata iz stvarnog svijeta".

Standard opisuje i sljedeće karakteristike direktorijskog sustava :

- Direktoriji su organizirani na objektno-orijentiran i hijerarhijski način. Informacije o objektima iz stvarnog svijeta pohranjene su u zapisu koji predstavlja taj objekt u direktoriju. Kako bi predstavili odnose između objekata na koje se odnose, zapisi su organizirani u stablastu strukturu.
- Direktorijski sustav pruža zajedničku shemu koja opisuje što se može/mora pohraniti u zapisu objekta.
- Direktorijski sustav opisuje standardni protokol za pristupanje direktoriju
- Direktorijski sustav nudi sigurnosni model.

X.500 standard se temelji na klijent/server modelu te u toj komunikaciji koristi OSI protokolni slog. U toj arhitekturi klijent šalje poslužitelju zahtjeve i od njega prima poruke definirane Directory Access Protocol (DAP) protokolom.

X.500 ima dosta nedostataka koji su mu onemogućile široku rasprostranjenost. Prije svega standard je bio previše kompleksan i stoga suviše težak za implementirati. Kako DAP protokol koristi kompletan OSI protokolni stog, sustav je bio iznimno zahtjevan što se tiče resursa, čak i u manjim okolinama.

2.2 Lightweight directory access protocol (LDAP)

LDAP je osmišljen kao "laganija" (lightweight) varijanta DAP protokola koji je korišten u X.500 direktorijima. On je trebao unijeti neka poboljšanja u DAP protokol među kojima je jedno od važnijih to da LDAP radi na TCP/IP protokolnom stogu za razliku od DAP-a koji koristi OSI model. LDAP također pojednostavljuje neke X.500 operacije i izbacuje neke egzotične feature-e.

Prva je verzija LDAP protokola definirana u X.500 Lightweight Access Protocol (RFC 1487) dokumentu kojeg je zamjenio Lightweight Directory Access Protocol (RFC 1777) dokument. Trenutna verzija protokola nosi ime LDAPv3 i opisana je u RFC 2251.

LDAP definira komunikacijski protokol između direktorijskog klijenta i direktorijskog poslužitelja ali ne definira programsko sučelje za klijenta (iako LDAP Application Programming Interface (rfc 1823) definira C API za pristup direktoriju korištenjem LDAP-a). LDAP dakle definira prijenos i format poruka koje koristi klijent da bi pristupio podacima u X.500 kompatibilnom direktoriju. Iako ljudi često govore o LDAP direktorijima, LDAP ne definira direktorijski servis već samo protokol.

LDAP je evolvirao iz uloge u kojoj je predstavljao "laganiju" protokolnu varijantu za pristup X.500 direktorijima u protokol koji je posve neovisan o X.500 direktorijima i koji se koristi za pristup isključivo "LDAP direktorijima" (direktorijima koji implementiraju LDAP protokol).

2.3 LDAP modeli

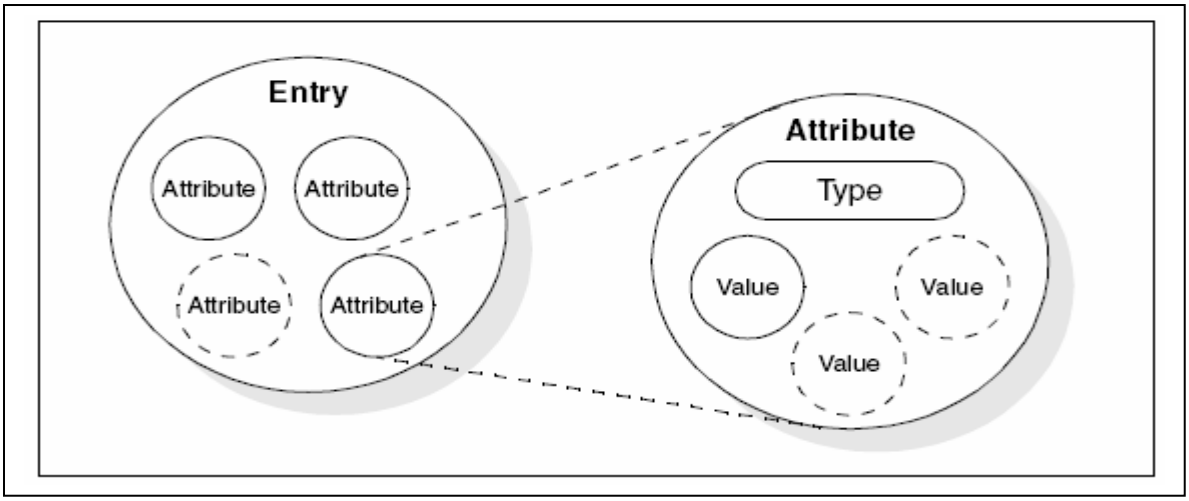
Temeljna definicija direktorija je ta da on predstavlja kolekciju informacija o objektima koja je organizirana na određen način, dakle neka vrsta specijalizirane baze podataka. Direktorijski sustav čine i usluge koje ove informacije čine dostupne i korisne administratorima, korisnicima, mrežnim servisima i aplikacijama. Pojedini su direktorijski sustavi integrirani sa operativnim sustavom, dok su drugi aplikacije poput e-mail direktorija.

Svaki aspekt direktorijskog sustava određen je pripadajućim modelom. Postoje 4 modela na kojima se temelji LDAP direktorij :

- Informacijski model
- Model imenovanja
- Funkcionalni model
- Sigurnosni model

2.3.1 Informacijski model

Direktoriji sadrže informacije o objektima iz stvarnog života. Informacije koje opisuju pojedini objekt su pohranjene u jednom **zapisu** (engl. **entry**). Zapis predstavlja osnovnu građevnu jedinicu direktorija. On je skup tzv. *name-value* parova koje zovemo **atributi**. Atributi mogu imati samo jednu vrijednost – *single-valued* ili pak više vrijednosti – *multi-valued* atributi.
Objekti u stvarnom životu pokazuju određenu sličnost pa kažemo da su pojedinog tipa. Princip grupiranja objekata unutar direktorija ostvaren je upotrebom **objektnih razreda** (engl. **object classes**). Objektni razred opisuje koje sve atribute objekt može (*optional* atributi) i mora (*mandatory* atributi) imati.
Postoji mogućnost nasljeđivanja razreda iz postojećih razreda. Podrazredi tako sadrže sve atribute nadrazreda te uz to mogu definirati i neke svoje atribute. Ovaj nam mehanizam omogućava izgradnju hijerarhije objektnih razreda.



Slika 1. zapis sa pripadajućim attribute-value parovima

Postoje tri tipa razreda: *abstraktni*, *strukturalni* i *pomoćn*i (engl. auxiliary). Abstraktni se objektni razredi koriste kao predlošci za izvođenje ostalih razreda te za formiranje viših nivoa hijerarhije objektnih razreda. Nije moguće instancirati objekt iz ovakvog razreda.

Strukturalni objektni razredi pak predstavljaju pravi "blueprint" pojedinog objekta. Jedino je iz ovakvih razreda moguće instancirati objekte.

Ponekad se pojavi potreba za pohranom dodatnih informacija koje nisu usko povezane sa strukturom objekta ili koje ne vrijede za sve objekte nekog razreda.Ove se dodatne informacije mogu čuvati u atributima kojim upravljaju pomoćni objektni razredi.Sa pomoćnim razredima možemo odrediti koje atribute mora imati podskup zapisa koji pripadaju istom strukturalnom razredu.

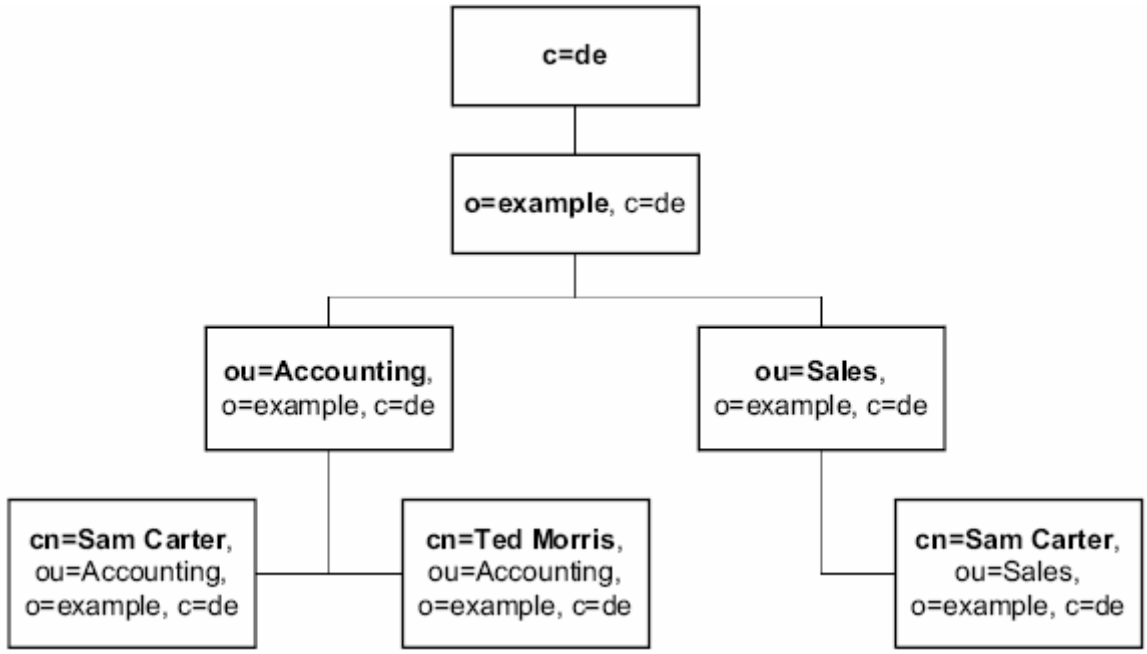
Postoji također jedan poseban strukturalni objektni razred koji se zove *alias*. Zapisi ovog tipa ne sadrže informacije o objektima već imaju funkciju placeholder-a koji pokazuje na druge zapise. Sa upotrebom aliasa moguće je pristupiti istim podacima pod različitim imenom.

Kolekcija sintaksnih pravila, tipova atributa i definicija objektnih razreda čini **shemu** (engl. **schema**). Ova meta informacija određuje šta se sve može pohraniti u direktoriju.

2.3.2 Model imenovanja

Model imenovanja određuje kako su zapisi organizirani i kako se mogu identificirati. Svi su zapisi unutar direktorija organizirani na hijerarhijski način te tako čine stablastu strukturu koja

se zove **Directory Information Tree** (**DIT**). Svi se zapisi unutar DIT-a mogu identificirati pomoću *jedinstvenog razlikovnog naziva* – **Distinguished Name** (**DN**). DN je dakle jedinstveno ime koje nedvosmisleno određuje konkretan zapis. DN je sastavljen od serije *relativnih razlikovnih zapisa* – **Relative Distinguished Names** (**RDN**). Svaki RDN unutar DN-a predstavlja dio DIT strukture polazeći od korijena stabla pa do tog direktorijskog zapisa.



2.3.3 Funkcionalni model

Funkcionalni model opisuje na koje se načine može pristupiti podacima smještenim u direktoriju. On opisuje operacije pomoću kojih korisnik putem programa koji se zove *Directory User Agent* (DUA) međudjeluje sa aplikacijom koja pruža direktorijske usluge – *Directory System Agent* (DSA).

Operacije se mogu razvrstati u tri kategorije :

- **Query** Uključuje operacije search i compare koje se koriste za dobavljanje informacija iz direktorija

- **Update** Uključuje operacije add, delete, modify i modify RDN koje ažuriraju informacije pohranjene u direktoriju
- **Authentification** Uključuje operacije bind, unbind i abandon koje služe za spajanje odnosno odspajanje sa LDAP servera

2.3.4 Sigurnosni model

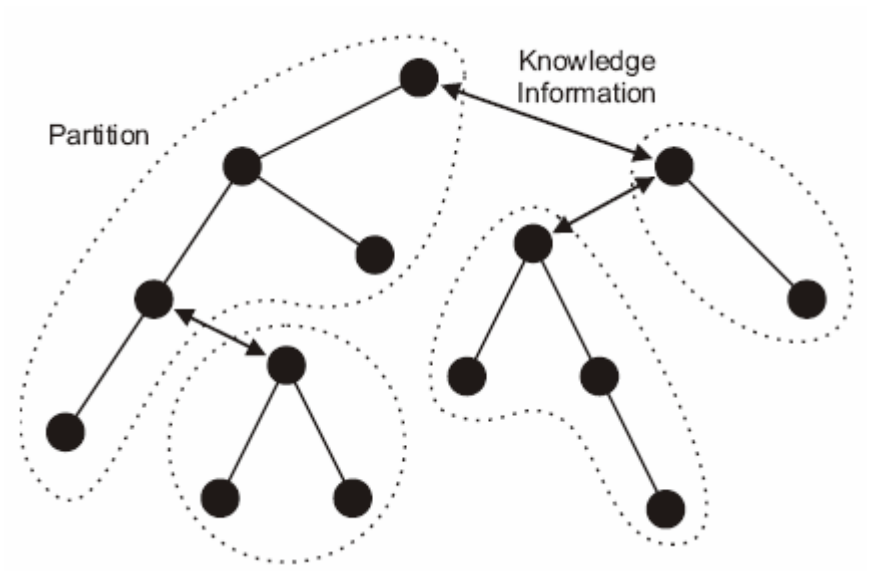
Sigurnost informacija unutar direktorija je od esencijalne važnosti. Iako postoje direktoriji namjenjeni javnom (bez potrebe za autentifikacijom i autorizacijom) pristupanju preko Interneta, kod većine ostalih direktorija postoje striktna pravila i ograničenja koja određuju tko je sve autoriziran pristupati određenim informacijama.
Stoga je jasno da moraju postojati adekvatni nivoi sigurnosti primjenjivi u direktoriju.

Sigurnost direktorija podrazumjeva :

- **Autentifikaciju** Korisnik koji traži uslugu mora direktoriju dokazati svoj identitet
- **Kontrola pristupa** Direktorijski server poslužuje podacima samo korisnike koje imaju dozvolu pristupa odnosno koji su autorizirani.
- **Integritet** Podaci moraju biti pouzdano pohranjeni i transportirani tako da se može detektirati bilo kakva njihova promjena.

2.4 Particioniranje direktorija

Zbog hijerarhijske strukture direktorija, direktorijski sustav je pogodan da bude implementiran kao distribuirani sustav. Da bi se ovo postiglo DIT mora biti "particioniran" (podijeljen) na manja područja od kojih svako područje predstavlja povezano podstablo (engl. subtree) koje se ne poklapa sa drugim particijama. Slika 2. nam pokazuje ovaj pristup. Odvojeni poslužitelj bi upravljao svakom ovakvom particijom. U direktoriju također mogu biti pohranjene veze između particija koje zovemo *knowledge information.*



Slika 3. Particioniranje DIT-a i knowlege informacije

Ako klijent uputi zahtjev za zapisima koji se ne nalaze u particiji kojom upravlja određeni poslužitelj, poslužitelj ima dvije opcije na raspolaganju. Prva je da zatraži informacije od odgovornog poslužitelja umjesto klijenta. Ovaj mehanizam se zove ulančavanje (chaining). Druga opcija je da uputi (engl. refer) klijenta prema odgovornom poslužitelju. Klijentov je dakle zadatak da prati taj referral do novog poslužitelja te da primi podatke o traženom zapisu.

2.5 Dostupnost direktorijskog sustava

Direktorijski je sustav kritična komponenta u mrežnom okruženju. Ako dođe do pada tog sustava, umrežena se klijentska računala neće moći podići, korisnici se neće moći logirati, e-mail poruke će ostati neposlane itd.

Konstantnu je dostupnost moguće postići tako da direktorijski sustav bude distribuiran na više računala. Točnije, korištenjem jednog ili više backup poslužitelja koji će pružati uslugu u slučaju kvara primarnog poslužitelja. Podaci se repliciraju između takvih poslužitelja. Repliciranjem podataka eliminira se tzv. jedinstvena točka kvara (engl. single point of failure) i za hardverske i za softverske kvarove.

Također je neophodno implementirati mehanizam koji će obavljati redirekciju klijenata u slučaju pada određenog poslužitelja, jer klijenti nisu u mogućnosti sami locirati backup poslužitelj. Ovaj mehanizam se može implementirati "ručno", polu-automatski koristeći DNS sklopku (engl. DNS switch over) ili automatski koristeći load-balancing tehnologiju

(upotrebom routera koji je posebno dizajniran). Takav router prosljeđuje klijentske zahtjeve na jedan od poslužitelja prema određenim promjenjivim kriterijima.

Većina današnjih direktorija replicira podatke sa jedinstvenog "master" poslužiteljja na ostale njemu podređene poslužitelje. Ovakva replikacije nosi sa sobom neke nedostatke. Prije svega ovaj tip replikacije predstavlja jedinstvenu točku kvara jer ako je master poslužitelj u kvaru ažuriranje direktorija nije moguće provesti. Zatim vjerojatnost je da je fizička udaljenost između mastera i klijenata koji obavljaju update relativno velika što usporava sustav. I na koncu replikacija je manje efikasna jer se obavlja sa jedinstvene lokacije.
Kod "multimaster" replikacije klijenti mogu ažurirati direktorij preko svakog domenskog poslužitelja. Dakle ne postoje primarni i sekundarni poslužitelji već su svi poslužitelji ravnopravni. Ovakav scenarij uklanja single point of failure jer je ažuriranje moguće na drugom poslužitelju.
LDAP protokol sam po sebi ne poznaje i ne definira replikaciju. Općenito LDAP klijenti dobiju listu poslužitelja koje će koristiti kod svojih upita i oni će pokušati pristupiti tim serverima onim redoslijedom kako je navedeno u njihovim konfiguracijskim datotekama sve dotle dok i ne uspiju.

2.6 Sigurnost direktorijskog sustava

U mrežnim računalnim okolinama sigurnost igra vrlo važnu ulogu. Kako je direktorijski sustav također jedna vrsta mrežne okoline sigurnost će i u tom sustavu biti vrlo važan čimbenik.
U mrežnm se okolinama podaci često šalju preko "nesigurnih" kanala te postoji potreba da se ti povjerljivi podaci zaštite tijekom prijenosa. Također postoji i potreba provjere identiteta entiteta koji učestuju u razmjeni podatka preko mreže.
Ovdje ćemo se pozabaviti sa četiri poopćena sigurnosna aspekta :

- Autentifikacija
- Integritet informacija
- Tajnost ili povjerljivost informacija

- Autorizacija

Autentifikacija je proces provjere identiteta nekog entiteta (korisnika,racunala,programa). Taj nam proces osigurava da je entitet upravo onaj za kojeg se i predstavlja. Autentifikacija je uvjet da tri temeljna zahtjeva za sigurnost podataka: povjerljivost, ispravnost i dostupnost mogu biti ispravno primjenjena.

Autorizacija je proces u kojem neki entitet nastoji dokazati ili potvrditi drugom entitetu da je ovlašten pristupiti određenom resursu.
Autorizacija je beskorisna bez pravilne autentifikacije ali u kombinaciji sa autentifikacijom je vrlo korisna jer omogućava daljnja ograničenja korisniku, i osigurava sigurnost sustava i njegovih podataka.
Autorizacija se često temelji na **Access Control List (ACL)** listama. ACL je lista autorizacija koja se može pridružiti objektima i atributima unutar direktorija. ACL također određuje kakvu vrstu pristupa ima pojedini korisnik read,write,search ili modify)
Korištenjem ACL-ova administratori mogu ograničiti pristup različitim dijelovima direktorija ili specifičnim zapisima.

3. Active Directory

U prošlom smo poglavlju opisali neka osnovna načela i principe direktorija, modele na kojima je zasnovan i standarde koji bi se trebali poštivati.
U ovom će poglavlju kako sam naslov kaže biti opisan Active Directory, komercijalna implementacija direktorijskog sustava koja čini temelj mrežnih Microsoftovih operativnih sustava (Windows 2000 i Windows 2003).
Namjena ovog poglavlja je da temeljito analiziramo način na koji je Microsoft izgradio svoju implementaciju direktorija, kako su teoretske koncepte realizirali u praksi, koje su sve vlastite tehnologije upotrijebili, da li su se do kraja pridržavali propisanih standarda i kako su sve te relativno neovisne komponente integrirali u jednu konzistentnu cjelinu.

3.1 Uloge i karakteristike Active Directory-a

Active Directory ima više uloga: od one da predstavlja kičmu distribuirane sigurnosti unutar operativnog sustava, do mehanizma koji pruža okosnicu za publiciranje mrežnih servisa. Active Directory pruža centralni servis koji administratorima omogućava da organiziraju mrežne resurse i da osiguraju intranet i Internet mrežni pristup.U mrežnoj ingrastrukturi koja se temelji na zadavanju politika (engl. policy-based network infrastructure), Active Directory dodatno služi kao "skladište" politika, mjesto gdje se one definiraju, održavaju i povezuju sa objektima.

Tvorci Active Directory-a iznose sljedeće njegove karakteristike koje smatraju njegovim prednostima:

- **Integracija sa DNS-om.** Active Directory koristi Domain Name System kao lokacijski servis
- **Fleksibilni upiti**. Postoji određen broj standardnih Windows alata pomoću kojih je vrlo jednostavno pronaći bilo koji objekt (na temelji nekih kriterija) koji se nalazi u mreži

- **Mogućnost proširivanja**. Active Directory je proširiv u smislu da administratori jednostavno mogu dodati nove razreda objekata u shemu kao i dodati nove atribute postojećim objektima azredima.
- **Policy-based administracija**. Grupnu politiku (engl. group policy) čine konfiguracijske postavke koje se primjenjuju na korisnike ili računala. Sve grupne postavke se nalaze u *Group Policy objektima* (GPO) i oni se mogu primjeniti na domene, site-ove i organizacijske jedinice
- **Replikacija informacija**. Active Directory koristi multimaster replikacij, koja vam dozvoljava da ažurirate direktorij na bilo kojem domeskom kontroleru.
- **Sigurnost informacija**. Menadžment korisničkih autentifikacija kao i kontrola pristupa (engl. access control) su potpuno ugrađeni u Active Directory i predstavljaju ključne sigurnosne mogućnosti .
- **Interoperabilnost**. Obzirom da je Active Directory izgrađen na standardnim protokolima za pristup direktoriju kao što je LDAP, on može međudjelovati sa drugim direktorijskim servisima koji također podržavaju ovaj protokol. Postoje i nekoliko API-a koji developerima omogućavaju pristup ovim protokolima

3.2 Logička organizacija Active Directory-a

Logička struktura Active Directory je izgrađena oko koncepta domena. Domena predstavlja logičko grupiranje računala, korisnika i ostalih resursa zbog administrativnih i sigurnosnih razloga.

Active Directory domena je izgrađena od sljedećih komponenata :

- hijerarhijska struktura objekata i kontejnera (container objects) temeljena na X.500 standardu (odnosno LDAP-u)
- DNS servis kao jedinstveni identifikator odnosno servis za lociranje
- sigurnosni servis kojim se autentificira svaki pristup određenom resursu putem korisničkog naloga (user account) unutar domene ili putem "trust" odnosa sa drugim domenama

- jedna ili više politika (policy) koje određuju prava korisnika i računala unutar te domene

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 podataka**. Domena predstavlja Windows direktorijsku particiju.Ove direktorijske particije su jedinice repliciranja (replication).Svaka domena sadrži informacije samo o objektima koji se u njoj nalaze.
- **Primjenjivanje grupne politike(group policy)**. Domena predstavlja jednu od više mogućih opsega grupne politike (group policy se može primjeniti i na organizacijske jedinice ili site-ove).
- **Određivanje administrativnih ovlasti (delegate administrative authority).** Cilj je da se precizno odrede područja 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.

3.2.1 Domenska stabla i šume

Windows 2000 & 20003 domene su organizirane u domenska stabla (*domain tree*) koja postoje unutar pojedine šume (forest). Kada instalirate Active Directory na prvi domain kontroler ujedno ste kreirali novu Active Directory šumu (forest), novo domensko stablo (domain tree) i korijensku domenu (root domain). Ako kasnije kreirate nove domene onda se one kreiraju ispod korjenske domene.

Domenska stabla

Domensko stablo možete zamisliti kao strukturu u kojoj se sve domene izvode iz korijenske domene. Ova struktura je u biti skup domena koje su međusobno hijerarhijski

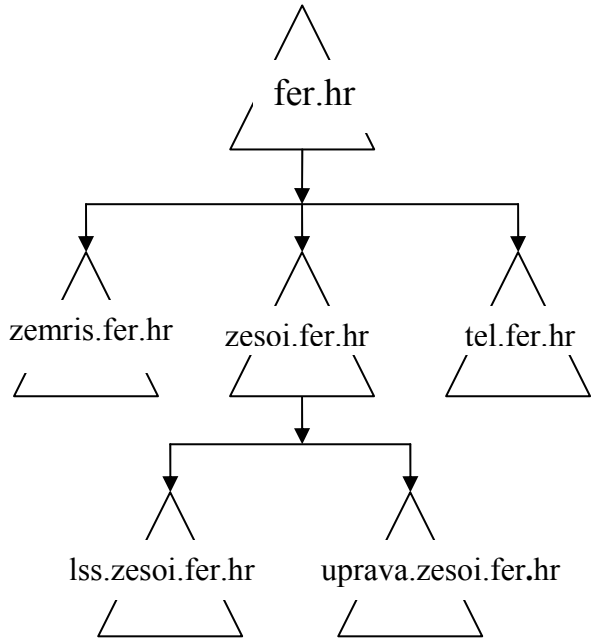
povezane i sve koriste jednu kontinuiranu shemu imenovanja odnosno koriste zajednički prostor imena.

Kao primjer jednog domenskog stabla zamisliti ćemo slijedeći slučaj.

Recimo da posjedujemo tvrtku koja se zove *Mycorp.*Prva domena koju smo kreirali (koja je ujedno i korjenska domena) zove se *mycorp.com.*Recimo da u tvrtki imamo sljedeće odjele : Finance,Marketing i Sales, te svaki od njih želi svoju vlastitu domenu.U tu svrhu kreiramo sljedeće nove domene : *finance.mycorp.com* , *mktg.mycorp.com* i *sales.mycorp.com.*

Domensko stablo koje odgovara prethodno definiranoj organizaciji prikazano je na slici 4.

Svako domensko stablo je nazvano po imenu koje je dodijeljeno korijenu stabla.Iz tog razloga se naše domensko stablo zove *mycorp.com* stablo.



Slika 5. domensko stablo FER-a

Domena koja se prva kreira je korijenska domena prvog stabla. Sve dodatne domene unutar istog stabla su "child" domene.

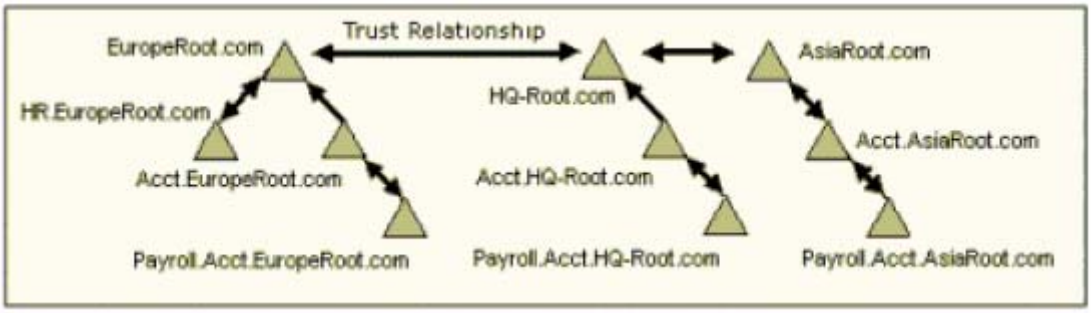
Šuma (Forest)

Šuma unutar Active Directory-a predstavlja distribuiranu bazu podataka,tj. bazu podataka koja je sastavljena od više djelomičnih baza podataka koje su raspoređene na više računala.Svi domenski kontroleri unutar šume pored domenske baze podataka čuvaju i kopiju konfiguracijskih i shematskih kontejnera (Configuration and Schema containers). Domenska baza podataka je dio *forest* baze podataka.

Druga definicija šume je da je šuma jednostavno kolekcija jednog ili više domenskih stabala.Unutar šume se dakle mogu kreriati više domenskih stabala

Višestruka domenska stabla unutar jedne šume ne dijele zajednički prostor imena.Iako stabla

ne dijele isti imenski prostor, šuma ima jednu korijensku domenu – *forest root domain.* Ta domena je po definiciji prva domena koja je kreirana unutar šume.



Slika 6. Šuma sa tri domenska stabla.Vidljivo je da ne postoji zajednički prostor imena

Korjenska domena svakog domenskog stabla uspostavlja tranzitivne trust odnose sa forest root domenom. Na slici 7. forest root domena je HQ-Root.com
Sve domene unutar svih domenskih stabala unutar jedne šume imaju sljedeća svojstva:

• imaju tranzitivne trust odnose sa drugim domenama unutar istog domenskog stabla
• imaju tranzitivne trust odnose sa drugim domenskim stablima unutar šume
• dijele zajedničke konfiguracijske informacije
• dijele zajedničku shemu
• dijele zajednički globalni katalog(GC)

3.3 Fizička organizacija Active Directory-a

3.3.1 SITE

Active Directory upotrijebljava termin SITE koji označava kolekcije subnetova koji koegzistiraju zajedno u LAN-u, odnosno fizičku mrežu na određenoj lokaciji sa dobrom povezanošću između svih dijelova te mreže. AD koristi site-ove za definiranje granica replikacije po fizičkoj mreži.AD replikacija je veoma učinkovita jer se repliciraju samo

promjenjeni atributi.Postoji također i tzv. link-value replikacija. Ona se koriste kod multi-value atrributa te se kod njih replicira samo promjenjnena vrijednost umjesto da se mijenjaju sve vrijednosti tog atributa.

Jedan od glavnih razloga upotrebe site-ova je da klijenti mogu naći njima najbliži DC. Iz ovog razloga informacija o subnetu mora biti povezana zajedno sa site-ovima. Klijenti koriste svoju IP adresu da bi odredili kojjem Active Directory subnetu pripadaju kao i kojem site-u. Informacija o site-u se upotrebljava za otkrivanje najbližeg DC-a.
Jednom kada kreirate site, Active Directory procces koji se zove Knowledge Consistency Checker automatski kreira i dinamički upravlja replikacijskim rasporedom te isto tako kreira skup intra site replikacijskih linkova između DC-ova unutar site-a.

Site-ovi pružaju sljedeće usluge :

- Klijenti mogu tražiti usluge domenskog kontrolera koji je unutar istog site-a.
- Active Directory pokušava minimizirati replikacijsko kašnjenje za replikaciju unutar istog site-a - *intra-site replication*
- Active Directory nastoji minimizirati potrošnju bandwidth za intra-site replikaciju
- Site-ovi omogućuju planiranja rasporeda replikacije

Važno je uočiti da su site-ovi neovisni o domenama. Site-ovi predstavljaju fizičku strukturu mreže dok domene predstavljaju logičku strukturu neke organizacije.Logička i fizička struktura su neovisne jedna o drugoj što ima sljedeće posljedice:

- ne postoji veza između site-ova domenskih prostora imena
- ne postoji ovisnost fizičke mrežne strukture neke organizacije i domenske strukture iste.
- Active Directory omogućava da više domena budu u istom site-u odnosno da jedna domena bude u više site-ova

3.3.2 Global Catalog

Global Catalog (GC) je vrlo važan dio Active Directory –a jer se upotrebljava prilikom akcija pretraživanja na područje jedne šume (forest-wide searches). Kao što samo ime implicira GC je katalog svih objekata unutar jedne šume zajedno sa podskupom atributa za svaki objekt. U šumama sa više domena upit (query) se prvo upućuje GC-u da bi se locirali objekti koji nas zanimaju. Ako se želi pristupiti svim atributima tog objekta konkretniji upit se postavlja domenskom kontroleru koji je odgovoran za domenu unutar koje se nalazi traženi objekt, jer GC sadrži samo određeni podskup svih atributa.
Po defaultu Global catalog se kreira automatski na inicijalnom domain kontroleru u win2000 šumi, i svaka šuma mora imati najmanje jedan gloabal catalog.

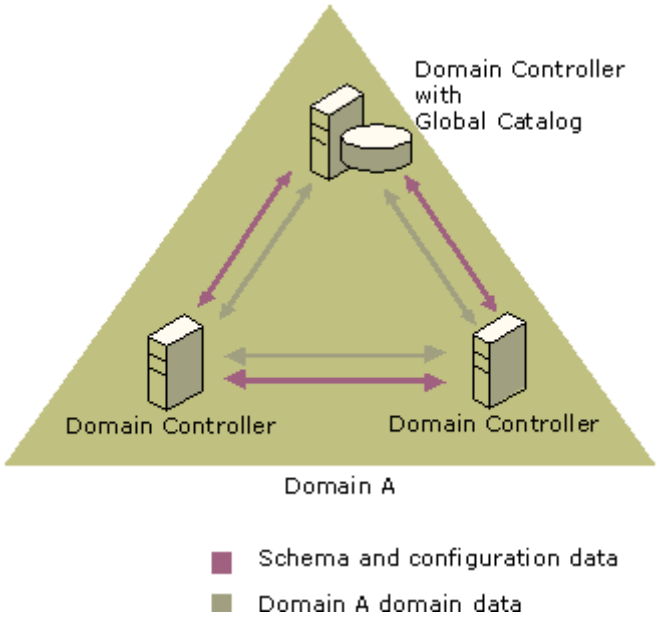
Global catalog ima dvije ključne uloge – logiranje i postavljanje upita (logon and querying):

- **Logon**. Global catalog omogućava logiranje Active Directory klijenata tako što pruža *Universal group membership information* za korisnički nalog šaljući zahtjev za logiranje domenskom kontroleru. Ne samo da svaki korisnik već i svaki objekt koji se nastoji autentificirati u Active Directory-u mora proći kroz global catalog, **uključujući svaki kompjuter koji se podiže (boot up**).
  Ako global catalog nije dostupan kada korisnik započne sa network logon procesom, onda se taj korisnik može logirati samo na localni kompjuter a ne i na mrežu. Jedini izuzetak od ovog su korisnici koji pripadaju grupi domain administratora.

- **Querying.**U šumi koja ima mnogo domena, GC omogućava da klijenti obavljaju pretraživanje(search) preko svih domena .GC omogućava da su direktorijske strukture unutar jedne šume transparentne krajnim korisnicima koji traže informacije.Većina Active Directory prometa su upiti- korisnici,administatori i programi traže informacije o direktorijskim objektima (directory objects).Upiti se javljaju mnogo češće nego updateovi unutar direktorija.

3.3.3 Multimaster uloge

Neki poslužitelji također mogu imati i ulogu koju nazivamo *flexible single master operation (FSMO)* uloga.Da bi objasnili FSMO ulogu moramo prvo objasniti što je to *umnožavanje* (**replication**).Umnožavanje je proces slanja ažuriranih informacija drugim domenskim kontrolerima.Windows koristi tzv. *multimaster* umnažanje.Obzirom da ne postoji neki primarni domenski kontroler, promjena Active Directory baze podataka se može dogoditi na bilo kojem kontroleru te je zadaće tog kontrolera da obavijesti sve ostale kontrolere da je došlo do promjene.Kako svaki Active Directory poslužitelj sadrži kopiju te baze ovaj proces je vrlo važan kako bi svaki poslužitelj imamo istu kopiju baze.



Problem je taj da su neke promjene baze podataka kompliciranije i i javljaju se problemi prilikom procesa umnažanja.Iz ovog razloga se pojedinim poslužiteljima daju *FSMO* uloge.To znači da samo ti kontroleri mogu primiti te problematične promjene baze podataka i samo oni mogu obavljati određene funkcije.

Postoji pet različitih FSMO uloga koje obuhvaćaju iznimke prilikom umnažanja (replication exceptions)

- **Schema master**
  samo jedan kontroler unutar jedne šume može imati ovu ulogu. Samo računalo koje ima ovu ulogu može ažurirati Active Directory shemu.

- **Domain Naming Master**

  ovu ulogu ima samo jedan kontroler unutar šume (forest).Domain Naming master kontrolira dodavanje i uklanjanje domena unutar šume.

- **Relative ID (RID) Master**
  Upravlja distribucijom RID brojeva na druge kontrolere. Kada domenski kontroler generira novi *security ID* (SID) za novi korisnički- , računalni- ili grupni nalog (account) pritom koristi *domain security ID* i *RID* brojeve. RID master osigurava da ne postoje dva kontrolera koji imaju iste ili preklapajuće RID brojeve.Svaka domena unutar šume ima jednog RID mastera.

- **PDC Emulator**
  Koristi se ako unutar mreže postoje Windows NT klijenti

- **Infrastructure master**
  Ovu ulogu ima jedan kontroler unutar svake domene ažurira članove pojedinih grupa prema potrebi.
  Npr. ako se promjeni članstvo unutar određene grupe , Infrastructure master ažurira grupu.

3.4 Integracija Active Directory-a sa DNS-om

Integracija Active Directory-a sa DNS-o predstavlja jednu od glavnih karakteristika Win 2000 operativnog sustava. DNS domene i Active Directory domene koriste identična domenska imena za različite prostore imena (engl. namespace). Obzirom da ova dva servisa dijele identične domenske strukture, veoma je važno razumjeti da riječ o različitim prostorima imena.Svaki čuva različite podatke i stoga upravlja različitim objektima. DNS sadrži podatke o zonama i zapisima o resursima a Active Directory čuva podatke o domenaam i domenskim objektima.Svaka Win 2000 domena ima DNS ime, svako Win 2000 računalo ima također

svoje DNS ime. Stoga su domene i računala reprezentirana i kao Active Directory objekti i kao DNS čvorovi.

Active Directory je integriran sa DNS-om na sljedeći način :

- Active Directory domene i DNS domene dijele istu hijerarhijsku strukturu.Iako su zamišljeni za različite namjene, organizacijski DNS prostor imena i Active Directory domene imaju identičnu strukturu.
- DNS zone se mogu pohraniti u Active Directory-u. Primarne zone se mogu pohraniti u Active Directory-u zbog replikacije na druge domenske kontrolere te zbog pružanja poboljšane sigurnosti za DNS servis
- Active Directory klijenti koriste DNS za lociranjne domenskih kontrolera. Kako bi locirali domenski kontroler za odgovarajuću domenu, Active Directory klijenti ispituju svoj kofigurirani DNS server za specifični resursni zapis (engl. resource record).

SRV Resource Records i Dynamic Updates

Kako bi Active Directory pravilno funkcionirao , DNS serveri moraju podržavati tzv Service Location (SRV) resursne zapise.SRV zapisi mapiraju ime servisa sa imenom servera koji nudi taj servis. Active Directory klijenti i domenski kontroleri koriste SRV zapise kako bi saznali IP adresu domenskih kontrolera.
Uz navedene zahtjeve, Microsoft također preporuča da DNS serveri podržavaju DNS dinamičko ažuriranje (engl. dynamic update). Dinamičko ažuriranje definira protocol kojim se DNS server dinmački ažurira s novim ili promjenjenim vrijednostima. Bez ovog protokola,administratori be morali manualno konfigurirati zapise koje su kreirali domenski kontroleri i koje su pohranili DNS serveri. Iako postoje neki standardi za zaštitu dinamičkih updatova oni oš nisu raširenі u svojoj upotrebi a ni odviše funkcionalni tako da je misrosoft uveo vlastiti način zaštite a to je putem ACL-ova.naime moguće je postaviti ACL-ove na DNS objekte koji će sadržavati informacije o tome koji korisnici imaju pravo vršiti update.

Kako je Active Directory integriran sa DNS-om?

DNS podaci su integrirani u Active Directory što znači da je moguće pograniti informacije koje se nalaze unutar tzv. DNS zone datoteke u sam Active Directory i to kao hijerarhijsku strukturu. Integriranjem u Active Directory, DNS struktura se replicira na sve domenske kontrtolere unutar domene. Svaki DC čuva writable kopiju DNS podataka.DNS objekti koji se nalaze pohranjeni u Active Directory se mogu updateati na svakom DC-u koristeći LDAP operacije ili putem DDNS-a. Ovo znači da su svi domenski kontroleri primarni name serveri(znači mogu vršiti update zone). znači ovo je veliki napredak jer kod standardnog DNS modeela postoji samo jedan master poslužitelj i više slave poslužitelja (koji ne mogu vršiti update zone)
Također je upotrebom aplikacijskih particija moguće definirati na koje će se sve domenske kontrrolere replicirati DNS zon

4. Zaključak

Directory service već danas čini okosnicu mnogih računalnih mreža.
Za očekivati je da će u budućnosti i svi proizvođači operativnih sustava ugrađivati directory service u svoje proizvode te će on biti instaliran na svakom računalu. Obzirom da se računalne mreže neprestano šire i postaju kompleksnije u budućnosti će biti nemoguće zamisliti modernu računalnu mrežu bez directory service-a.
Ukratko : tehnologija sutrašnjice.

LITERATURA

1. **LDAP Implementation Cookbook**
Heinz Johner, Michel Melot, Harri Stranden, Permana Widhiasta
June 1999

2. **LDAPifying Applications**
Brad Marshall
http://quark.humbug.org.au/publications/ldap/ldap-apps.pdf

3**. Understanding LDAP**
Heinz Johner, Larry Brown, Franz-Stefan Hinner, Wolfgang Reis, Johan Westman
International Technical Support Organization
http://www.redbooks.ibm.com
June 1998

4**. Directory Services for Linux**
in comparison with Novell NDS
and Microsoft Active Directory
by
Norbert Klasen
RHEINISCH-WESTF ¨A LISCHE TECHNISCHE HOCHSCHULE
AACHEN, GERMANY
August 2001

5. **Evaluation of Distributed**
Authentication, Authorization and
Directory Services
Gombás Gábor
ELTE TTK, 2001.