

IV - Aktivni direktorijum

SADRŽAJ

4.1 Uvod u Aktivni direktorijum

4.2 Osobine Aktivnog direktorijuma

4.3 Servisi Aktivnog direktorijuma

4.4 Komponente Aktivnog direktorijuma

4.5 Pojmovi vezani za Aktivni direktorijum
Globalni katalog, Repliciranje, Odnosi poverenja,
Grupne politike

4.1 Uvod u Aktivni direktorijum

- Prvi zadatak mreže je da obezbedi servis zajedničkih mrežnih resursa
- Drugi zadatak je obezbeđivanje sigurnosti podataka koji se čuvaju
- Da bi se to ostvarilo gotovo svaki MOS koristi dve osnovne tehnike:
 1. Provera autentičnosti - traži se korisničko ime i odgovarajuća lozinka.
 2. Autorizacija - pretražuje se lista sa kontrolama pristupa mrežnom resursu (*Access Control List*) i dodelju odgovarajuća prava za taj resurs
- Mreže se sastoje od mnogih uređaja: klijentskih računara, servera, štampača, uređaja za međusobno povezivanje računara kao i korisnika.
- Oni nemaju ista prava na mreži, tj. pristup mrežnim resursima nije isti
- Upravljanje ovakvim složenim mrežama predstavlja veliki problem
Alat koji omogućava kreiranje, modifikovanje ili brisanje korisničkih naloga kao i resursa mreže iz jedne tačke, poznat je pod nazivom Active Directory Users and Computers.
- Termin direktorijum odnosi se na kolekciju uskladištenih podataka o objektima, koji su na neki način međusobno povezani.
- On mora da upamti sve podatke koji su potrebni za korišćenje i upravljanje tim objektima na jednom mestu.

4.2 Osobine Aktivnog direktorijuma

- Servis direktorijuma predstavlja **alat administratora i mrežnih korisnika**
- Servis direktorijuma se razlikuje od direktorijuma po tome što je on istovremeno i **izvor podataka ali i mehanizam za upravljanje njima**

1. Upravljanje direktorijumima: Svaki OS, čak i onaj koji se odlikuje najminimalnijom bezbedošću, poseduje u sebi **jedan ili više fajlova**, koji zajedno čine bazu podataka poznatih korisničkih naloga (**SAM datoteka**)

- ✓ Centralizovana baza podataka aktivnog direktorijuma smeštena je na računarima koji se zovu **kontroleri domena** (**NTDS.DIT datoteka**)
- ✓ Ova datoteka je modifikovana baza *Access*-a, tako da Windows u sebi **sadrži jednu varijantu Access-ove mašine** za rad sa bazama podataka.
- ✓ **NTDS.DIT** predstavlja **modifikovanu bazu podataka**, koja je u osnovi kreirana pomoću iste tehnologije kao i Microsoft Access i sadrži u sebi znatno **širi spektar različitih informacija o korisnicima**, nego što je to ikada bio slučaj sa SAM fajlovima.
- ✓ Informacije iz NTDS.DIT fajla i program koji upravlja ovim fajlom nazivaju se jednim imenom **direktorijumski servis** (***directory service***).

4.2 Osobine Aktivnog direktorijuma

- 2. Centralizovano skladištenje podataka:** svi bitni podaci nalaze se u jednom distribuiranom skladištu podataka. Na taj način omogućen je jednostavan pristup informacijama sa bilo koje lokacije u mreži.

 - ✓ Poboljšava **raspoloživost i organizaciju podataka**, smanjuje mogućnost dupliranja podataka i omogućava jednostavan *back-up* tih podataka.
 - ✓ Kada neko pokuša da pristupi deljivoj datoteci, ili da odštampa neki dokument preko deljivog štampača, **AD će ga proveriti**
 - ✓ Kada se implementira u potpunosti, AD može da **uštedi mnogo posla oko administracije** i ostalih mrežnih funkcija.
- 3. Pronalaženje servera:** Danas se posao obavlja na principu **klijent-server**. Kada računar pristupa serveru datoteka on je njen klijent, dok je server server. AD **pojednostavljuje proces pronalaženja servera** tako da klijent treba da zatraži od AD imena kontrolera domena.
- 4. Upravljanje klijentskom konfiguracijom:** uvode se savremenije tehnologije za upravljanje klijentskim računarima, kao što su **mobilitet korisnika i otkaz diska**, koje nam omogućavaju da uz minimum administriranja i bez prekida rada klijenta podešavamo te parametre.

4.2 Osobine Aktivnog direktorijuma

- 5. Podesivost:** podrazumeva laku prilagodljivost i proširivost objekata u AD koji je organizovan u više sekcija u koje može da se smesti ogroman broj objekata, pa čak i do nekoliko miliona objekata po jednom domenu. Za ubrzanje rada koristi se tehnika **indeksiranja i repliciranja**.
- 6. Fleksibilna provera autentičnosti:** Provera autentičnosti i davanje ovlašćenja korisnicima, obezbeđuje zaštitu podataka i minimizuje prepreke izlaska na Internet i nesmetanog rada na njemu. AD podržava nekoliko protokola za proveru autentičnosti kao što su: **Kerberos, SSL (Secure Socket Layer), TLS (Transport Layer Security)**.
- 7. Bezbedonosna integracija:** Sistem bezbednosti Windows Server-a direktno je zavisan od bezbednosti AD. Kontrola pristupa može biti definisana za svaki objekat u direktorijumu, ali može biti i definisana i za svako svojstvo objekta pojedinačno. Bezbedonosna politika primenjuje se na lokalnom nivou, na nivou lokacije, domena ili organizacione jedinice.
- 8. Delegirana administracija:** Hijerarhijska struktura AD-a omogućava dodeljivanje administratorskih prava po segmentima mreže, tako da se administratorski zadaci mogu izvršavati samo za taj specifični segment.

4.2 Osobine Aktivnog direktorijuma

9. Integracija sa sistemom domena (DNS) - servis DNS (*Domain Network System*) omogućava razrešavanje imena klijentima. Postupkom razrešavanja imena korisnici mogu da pristupe serverima na osnovu njihovih imena, umesto da koriste IP adrese koje se po pravilu teško pamte. **AD** koristi DNS konvencije da bi stvorio hijerarhisku strukturu koja obezbeđuje poznat, uređen i podesiv pogled na mrežne odnose.

10. Administriranje na bazi politike: omogućava nam da unapred definišemo dozvoljene akcije i parametre za korisnike i računare na nekoj određenoj lokaciji, domenu ili organizacionoj jedinici. Upravljanje na osnovu te politike pojednostavljuje zadatke kao što su ažuriranje operativnog sistema, instaliranje aplikacija, kao i zadatke koji se odnose na korisničke profile i blokade datih objekata.

11. Replikacije podataka: tehnika repliciranja predstavlja automatsko ažuriranje podataka na dva ili više objekta u mreži. To znači da u jednoj mreži možemo da imamo dva ili više kontrolera domena, svaki sa svojim AD, koji zahvaljujući tehnici repliciranja stalno međusobno razmenjuju informacije i na taj način u svakom trenutku imaju ažurne podatke.

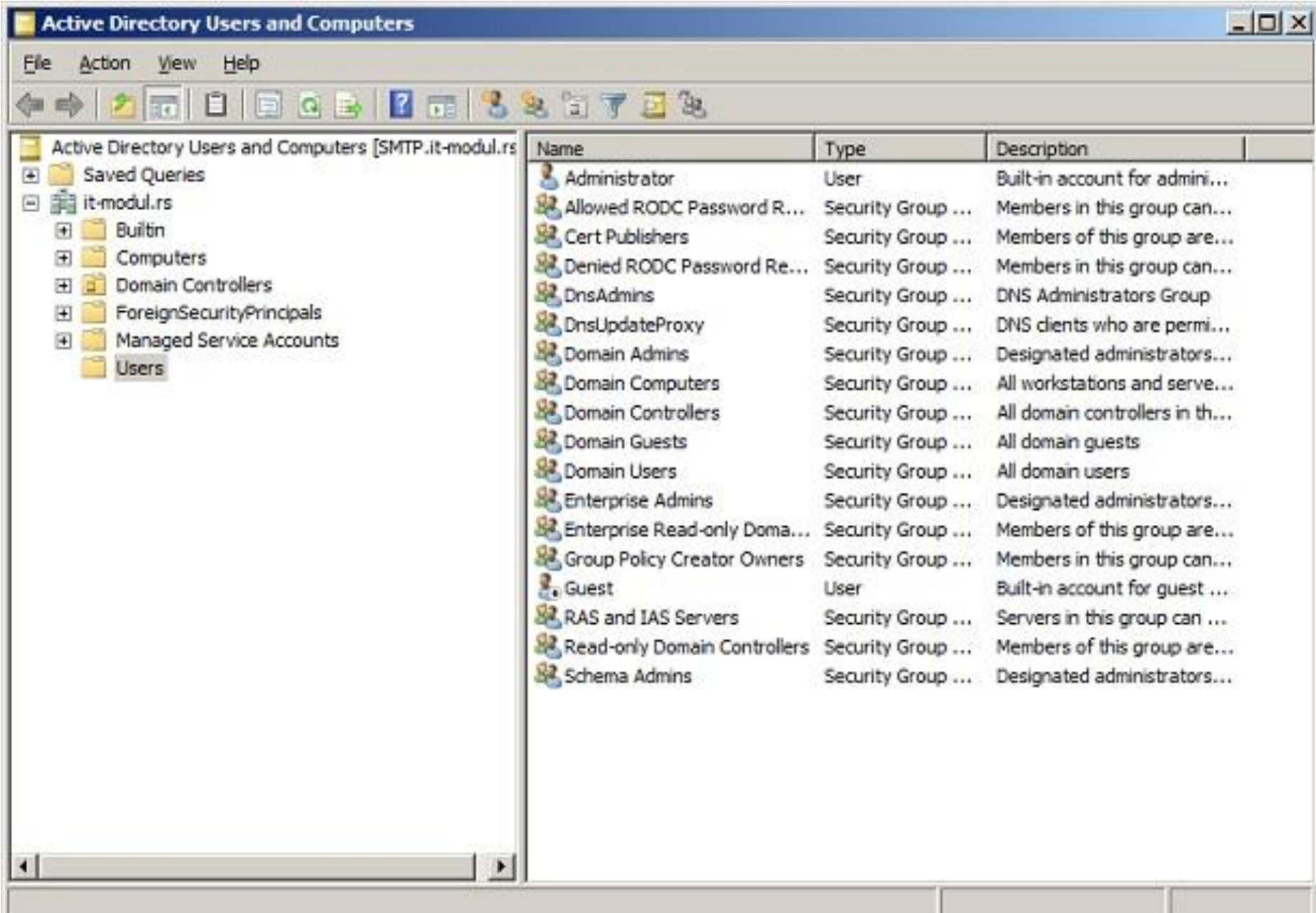
4.2 Osobine Aktivnog direktorijuma

12. Primena standardnog interfejsa: veliki deo proizvođača softvera nisu voljni da pišu programe koji zavise od slabo dokumentovanog sigurnosnog interfejsa, zato što se plaše da kada se pojavi naredna verzija OS u kojoj će se promeniti programski interfejs, oni ostaju na cedilu. Zbog toga je *Microsoft* izabrao da postavi jedan **industrijski standardni interfejs u svoj AD**, pod imenom **LDAP** (*Lightweight Directory Access Protocol*) koji je omogućio da se naprave alati za kreiranje strukture AD, domena, stabla, šume, organizacione jedinice, korisničkih naloga i dr.

13. Rad sa drugim servisima direktorijuma: Rad AD zasniva se na standardnim protokolima za pristupanje direktorijumima kao što su **LDAP** i **NSPI** (*Name Service Provider Interface*). LDAP je standardni protokol kod servisa direktorijuma a NSPI predstavlja **protokol koji se koristi kod Microsoft Exchange Servera**.

14. Potpisan i šifrovan LDAP saobraćaj: ova opcija **obezbeđuje verodostojnost podataka koji se šalju na mrežu**. Potpisan i šifrovan LDAP saobraćaj podrazumeva da paketi podataka stižu od poznatog izvora i da nisu neovlašćeno menjani.

4.2 Osobine Aktivnog direktorijuma



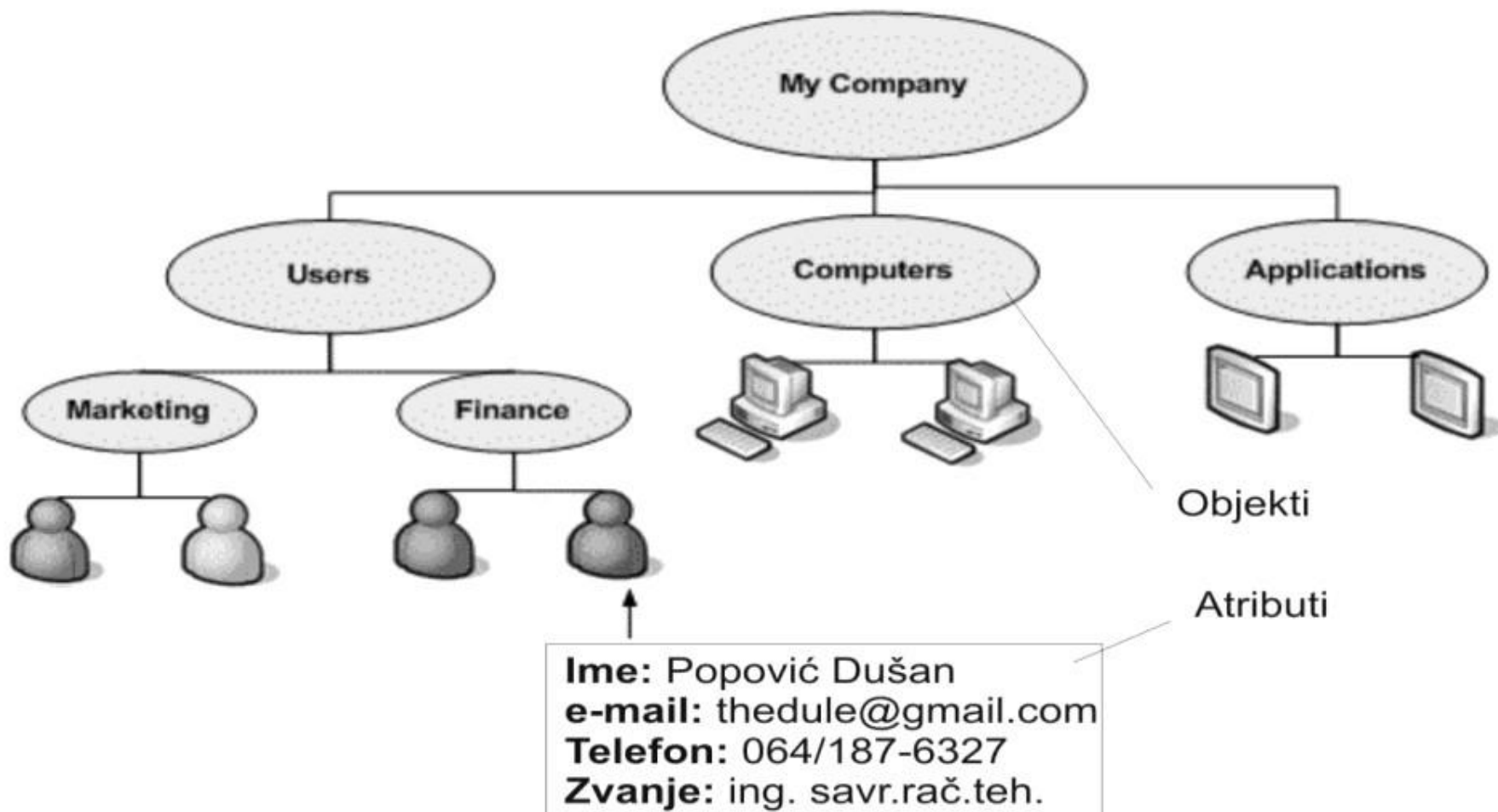
The screenshot displays the 'Active Directory Users and Computers' console window. The left pane shows a tree view of the directory structure, with 'Users' selected under the 'it-modul.rs' domain. The right pane shows a list of users and groups with columns for Name, Type, and Description.

Name	Type	Description
Administrator	User	Built-in account for admini...
Allowed RODC Password R...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Re...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Doma...	Security Group ...	Members of this group are...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...

4.3 Servisi Aktivnog direktorijuma

- Resursi čiji se podaci nalaze u AD predstavljaju se kao **objekti-objects**
- Objekat je jasno označen skup atributa koji predstavlja mrežni resurs.
- **Atributi** objekta su osobine objekata u direktorijumu. Na primer, u attribute korisničkog naloga mogu da spadaju ime i prezime korisnika, odeljenje kome pripada i njegova e-mail adresa.
- Svi objekti u AD-u mogu se organizovati u **klase**, koje predstavljaju logičke grupe objekata. Primeri klasa objekata su one koje predstavljaju korisničke naloge, grupe, računare, domene ili organizacione jedinice.
- **Šema Aktivnog direktorijuma** je lista definicija koje određuju vrstu objekta i tipova podataka o tim objektima, koji se smeštaju u AD.
- Same definicije su smeštene kao objekti, tako da AD može da upravlja objektima šeme istim operacijama upravljanja kao i sa objektima
- Postoje dve vrste definicija u šemi: **atributi** i **klase**.
- **Atributi** se definišu odvojeno od klasa i svaki atribut definisan je samo jednom i može se koristiti u više klasa.
- **Klase**, koje se takođe nazivaju klase objekata, opisuju koje je objekte moguće kreirati u AD i svaka klasa predstavlja kolekciju atributa.

4.3 Atributi i objekti Aktivnog direktorijuma



4.4 Komponente Aktivnog direktorijuma

- Da bi uspešno izgradio strukturu direktorijuma koji će zadovoljiti potrebe jedne organizacije AD koristi različite komponente.
- Vrste primenjenih komponentata zavise od toga da li se radi o logičkoj ili fizičkoj strukturi organizacije koja je kod AD potpuno razdvojena
- Logička struktura jedne organizacije predstavljena je: domenima, organizacionim jedinicama, stablima i šumama.
- Fizička struktura organizacije predstavljena sa: sajtovima (fizičkim pod mrežama) i kontrolerima domena.

1. **Logička struktura:** U AD resursi se organizuju u logičku strukturu koja predstavlja logičku strukturu same organizacije.

- ✓ Logičko grupisanje resursa omogućava pronalaženje resursa na osnovu njegovog imena, a ne na osnovu njegove fizičke lokacije.
- ✓ Logička struktura AD je fleksibilna i daje nam mogućnost projektovanja hijerarhije, unutar samih AD, koja je razumljiva i korisnicima i administratorima.
- ✓ Logičko grupisanje objekata omogućava nam da grupišemo objekte na osnovu njihove logičke pripadnosti a ne na osnovu fizičke lokacije.

4.4 Logička struktura - Domen

- Jedan od najvažnijih koncepata u teoriji i praksi Microsoftovih mreža jeste pojam domena (*domain*).

Domen predstavlja grupu servera i radnih stanica, koje su se složile oko centralizovanog čuvanja naziva i lozinki za korisničke i računarske naloge, u jednoj deljenoj (shared) bazi podataka.

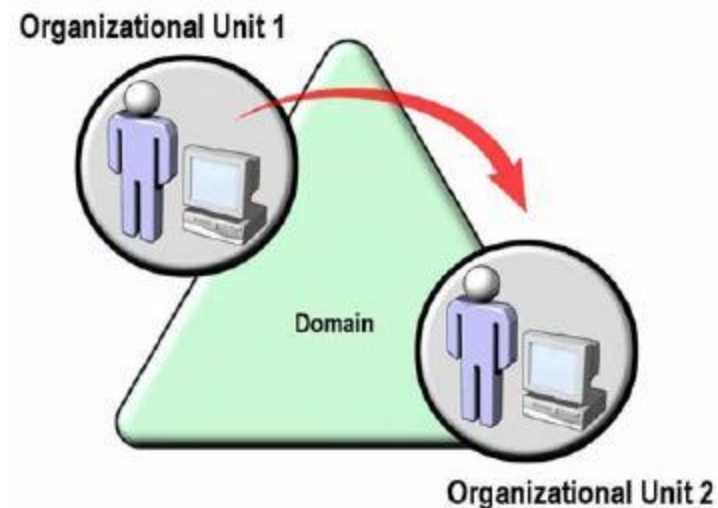
- Domen u stvari predstavlja srž logičke strukture AD u okviru koga možemo smestiti milione različitih objekata koji predstavljaju resurse koji su neophodni za pravilno i bezbedno funkcionisanje mreže.
- AD može imati jedan ili više domena.
- Jedan domen može sadržati više fizičkih lokacija.
- Grupisanje objekata u jedan ili više domena omogućava da mreža odslikava realnu strukturu organizacije.
- Domen je i skup sigurnosnih principa kao što su korisnički i računarski nalozi ali i drugih, poput dozvola za deljive štampače, foldere.
- Objekti na domenu su definisani od strane administratora i koriste zajedničku bazu podataka i jedinstveno ime.

4.4 Zadaci Domena

- Svi objekti mreže postoje unutar domena
- Oni pružaju mogućnost upotrebe grupe serverskih računara, koji igraju ulogu „servera za proveru autentičnosti“ ili „prijavnih servera“
- Na domenima se čuva i neprekidno ažurira indeks svih objekata na domenu, sa mogućnošću efikasnog pretraživanja, čime je korisnicima znatno olakšano pretraživanje željenih resursa na mreži.
- Omogućavaju kreiranje korisničkih naloga sa različitim ovlašćenjima
- Domeni se dalje mogu deliti na subdomene, koji se još nazivaju organizacionim jedinicama (*organization units* – OU).
- Domen predstavlja granicu bezbednosti jer se na njemu čuva jedna centralna lista korisnika i pripadajućih lozinki.
- **Liste za kontrolu pristupa** (*Acces Control List, ACL*) kontrolišu pristup objektima domena jer sadrže odgovarajuće dozvole za pristup
- Sve bezbednosne politike i parametri, kao administrativna prava i liste za kontrolu pristupa, ne mogu da prelaze iz jednog domena u drugi
- Administrator domena ima apsolutna prava da formira politiku samo u okviru tog domena.

4.4 Logička struktura – Organizaciona jedinica

- Predstavlja jednu vrstu skladišta – kontejner, koju koristimo da bi smo organizovali objekte u okviru domena.
- Organizaciona jedinica može sadržati objekte kao što su korisnički nalozi, grupe, računari, aplikacije, deljene datoteke, aplikacije i druge organizacione jedinice iz istog domena.
- U jednom domenu hijerarhija organizacionih jedinica je potpuno nezavisna tj. ne zavisi od hijerarhije u drugom domenu.
- Organizaciona jedinica omogućava administratoru mreže da se prema većem skupu objekata odnosi kao prema jednom.
- U AD podrazumeva je opcija da svi podređeni objekti nasleđuju dozvole od svojih nadređenih objekata.
- Administrator samo jednom dodelom dozvola na višem nivou, rešava dodelu istih dozvola svim podređenim objektima.



4.4 Logička struktura - Stablo (*Tree*)

- Predstavlja način za grupisanje jednog ili više domena.
 - Grupisanje se vrši tako što jedan ili više domena dodajemo na postojeći nadređeni domen.
 - Svi domeni u stablu dele jedinstven prostor imena i strukturu imena.
 - Hijerahija domena u stablu omogućava nam da povećamo bezbednost domena i da svo administriranje svedemo na jednu OJ ili domen
 - Sa druge strane ovakva organizacija omogućava nam fleksibilnost u organizaciji mrežne strukture jer se lako prilagođava svim promenama.
- Generalno gledano sva stabla imaju neke zajedničke osobine i to:*

1. Imena podređenih domena u stablu sadrže imena nadređenih domena. To se uklapa sa standardom koji je definisao DNS.
2. Svim domenima unutar jednog stabla pripada zajednička šema koja predstavlja formalnu definiciju svih tipova objekata koje se smeštaju u servis Aktivnog direktorijuma.
3. U okviru stabla postoji zajednički **globalni katalog** koji predstavlja centralno skladište svih objekata koji pripadaju tom stablu.
4. Svi domeni iz tog stabla mogu nesmetano da pristupe tom skladištu.

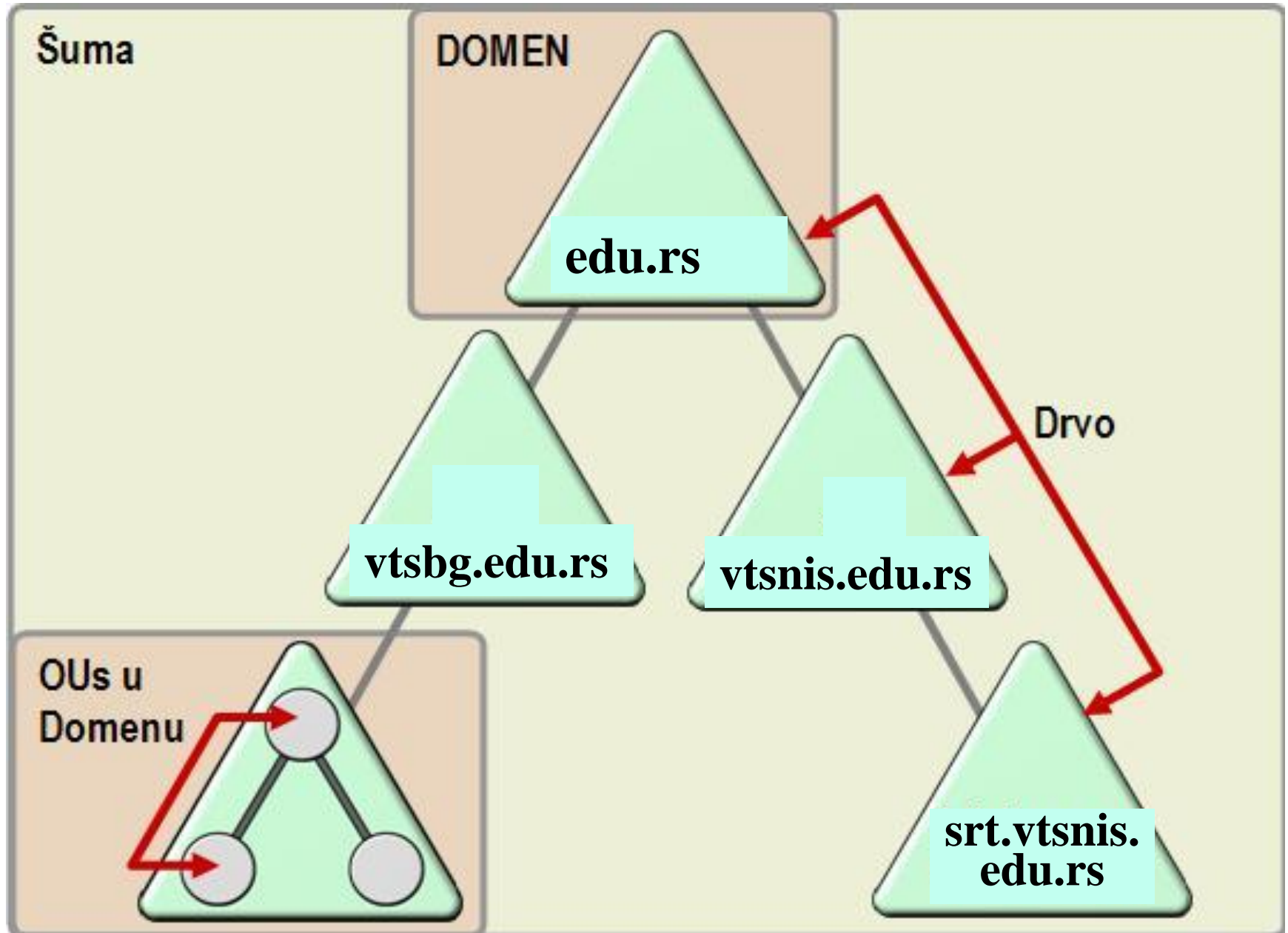
4.4 Logička struktura - Šuma (*Forest*)

➤ Predstavlja grupu ili hijerahijsko uređenje jednog ili više potpuno nezavisnih stabala.

Sve šume imaju sledeće zajedničke karakteristike:

1. Sva stabla u šumi imaju zajedničku šemu.
 2. Stabla u šumi imaju različite strukture imena koje su u skladu sa njihovim domenima.
 3. Svi domeni u šumi imaju jedan zajednički **globalni katalog**.
 4. Domeni u šumi dejstvuju nezavisno, ali postojanje šume omogućava komunikaciju kroz celu organizaciju.
 5. Između domena i stabala domena postoji implicitni dvosmerni odnos poverenja.
- ❑ Na primer: Iako stabla *vtsnis.edu.yu* i *vets.edu.yu* formiraju jednu šumu, prostor imena je jedinstven samo u okviru svakog stabla u šumi.

4.4 Logička struktura - šema



4.4 Fizička struktura – Lokacija (Site)

Predstavlja kombinaciju jedne ili više podmreža, na bazi IP komunikacije, a koje su povezane visoko pouzdanom i brzom vezom u cilju lokalizovanja što je moguće više mrežnog saobraćaja.

- Granice lokacije obično se poklapaju sa granicama LAN-a.
- Kada grupišemo podmreže u lokaciju, potrebno je voditi računa da to budu samo one koje imaju brze, jeftine i pouzdane međusobne veze.
- Postižemo dve veoma korisne stvari: prvo, smanjuje se saobraćaj za replikaciju i drugo, koristimo informacije o cenama puta, koje nam omogućavaju da pronađemo koja je najbolja ruta za replikacioni saobraćaj, uz najmanju cenu.
- U AD lokacije nisu deo prostora imena.
- Kada se pretražuje logički prostor imena, vide se računari i korisnici koji su grupisani u domene i organizacione jedinice, ali ne i lokacije.
- Lokacije sadrže samo objekte računare i objekte veze koji se koriste da bi se konfigurisala replikacija između lokacija.
- Jedna lokacija može da obuhvati korisničke naloge i računare koji su iz različitih domena.

4.4 Fizička struktura – Kontroler domena

- Predstavlja računar na kome se izvršava Windows Server OS i na kome je smeštena replika AD (baza podataka lokalnog domena).
- Kako jedan domen može da ima jedan ili više kontrolera domena, svi kontroleri domena unutar domena imaju kompletnu repliku AD
- Kontroler domena može da održava samo jedan domen i zadužen je za njegovu bezbedonosnu politiku.

Kontroler domena ima sledeće funkcije:

- ✓ Svaki kontroler domena sadrži potpunu kopiju svih podataka AD.
- ✓ Kontroleri domena unutar jednog domena automatski repliciraju sve promene koje mogu da se dogode nad objektima koje oni kontrolišu.
- ✓ Replikacioni saobraćaj između kontrolera domena može da se kontroliše tako što će se odrediti koliko često će se replikacija obavljati
- ✓ Kontroleri domena vrše trenutnu replikaciju kada se vrši ažuriranje nekih važnih podataka, na primer onemogućavanje korisničkog naloga.
- ✓ Svi kontroleri domena u domenu su ravnopravni, ne postoji glavni
- ✓ Više kontrolera domena u domenu daje veću otpornost na greške.
- ✓ Kontroleri domena upravljaju svim aspektima interakcije korisnika

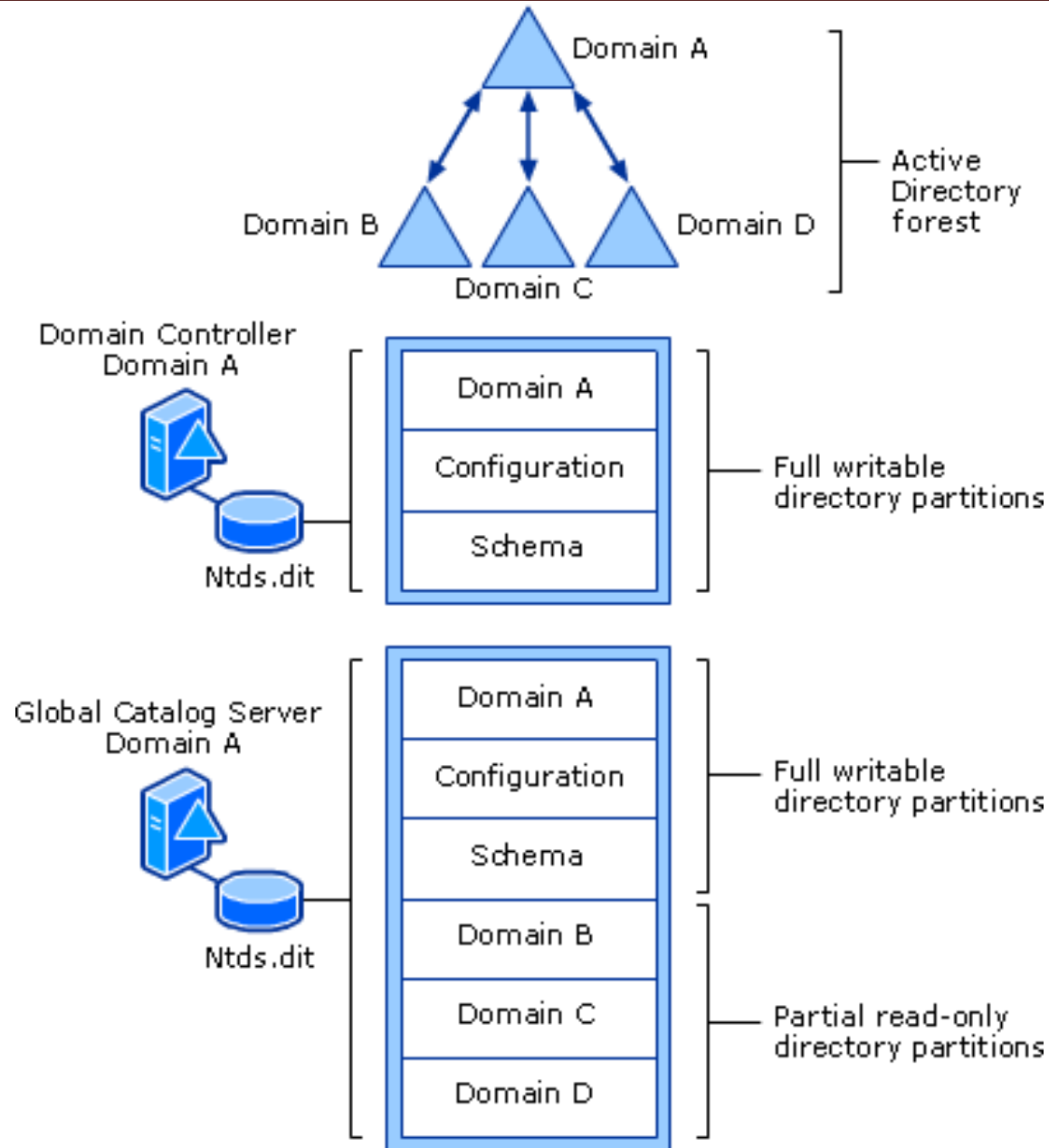
4.5 Globalni katalog

- Globalni katalog predstavlja centralno skladište informacija o objektima koji se nalaze u stablu ili šumi.
- Automatski se kreira na inicijalnom kontrol.domena u prvom domenu
- Kontroler domena koji čuva kopiju globalnog kataloga naziva se **server globalnog kataloga**.
- Na njemu je smeštena potpuna replika svih atributa objekata u direktorijumu njegovog matičnog domena i delimična replika svih atributa objekata sadržanih u direktorijumu svakog domena u šumi.

Dve osnovne funkcije koje treba da izvrši globalni katalog su:

1. da omogući korisniku da može da se prijavi na mrežu tako što će mu dati informaciju o članstvu u univerzalnim grupama.
 2. da omogući pronalaženje informacija direktorijuma nezavisno od toga koji domen u šumi sadrži tražene podatke.
- Globalni katalog treba da odgovara na upite korisnika ili programa o objektima koji su bilo gde na stablu ili šumi i to maksimalnom brzinom i uz najmanji mogući mrežni saobraćaj.
 - Svaki kontr.domena može da se konfigurise kao server global.kataloga

4.5 Globalni katalog



4.5 Repliciranje

- Sve informacije koje se nalaze u AD moraju svakog trenutka da budu dostupne svim korisnicima i servisima na tom domenu, stablu ili šumi.
- Kako u okviru ovih konfiguracija možemo imati više kontrolera domena, gde svaki kontroler nadgleda svoj deo oblasti, potrebno je obezbediti da se sve informacije budu dostupne svim korisnicima.
- Repliciranje upravo obezbeđuje da se sve izmene u okviru jednog kontrolera domena reflektuju na sve ostale kontrolere domena.
- Informacije direktorijuma se repliciraju na kontrolerima domena kako unutar, tako i između lokacija.
- Sve informacije koje se čuvaju u AD (*ntds.dit*) mogu se podeliti u četiri osnovne kategorije a svaka od tih kategorija informacija ima naziv *particija direktorijuma* ili *kontekst imenovanja*.
- Repliciranje se upravo vrši na osnovu ovih particija jer one predstavljaju osnovne jedinice na osnovu kojih se radi repliciranje.

4.5 Particije direktorijuma

1. Particija šeme: sadrži informacije o objektima koji se mogu napraviti u direktorijumu kao i njihove attribute i oni su zajednički za sve domene u šumi. Ova particija se replicira na svim kontrolerima domena u šumi.
2. Particija konfiguracije: podaci o logičkoj strukturi postavljanja, uključujući i podatke kao što su struktura domena ili topologija repliciranja nalaze se u ovoj particiji. I ovi podaci su zajednički za sve domene u šumi i repliciraju se na svim kontrolerima domena.
3. Particije domena: ova particija sadrži podatke o svim objektima u jednom domenu i ti podaci pripadaju samo jednom domenu pa se ne repliciraju na druge domene. Replikacija važi samo za sve kontrolere domena u okviru tog domena.
4. Particija direktorijuma za aplikacije: sadrži dinamičke podatke pojedinačnih aplikacija u AD. Na osnovu ovih podataka omogućeno nam je da kontrolišemo područje smeštanja kopija i proces repliciranja. U ovu particiju smeštaju se podaci za bilo koji tip objekta osim za one objekte koji se odnose na principe bezbednosti. Omogućeno je da se ovi podaci eksplicitno preusmere na kontrolere domena koje administrator odredi.

4.5 Repliciranje particija

Kontroler domena skladišti i replicira sledeće podatke:

*particije šeme za šumu,
particije konfiguracije za sve domene u šumi
particije domena za svoj domen.*

Globalni katalog skladišti i replicira sledeće podatke:

*particije šeme za šumu,
particije konfiguracije za sve domene u šumi,
delimičnu repliku koja sadrži često korišćene attribute za sve
objekte direktorijuma u šumi i
potpunu repliku koja sadrži sve attribute svih objekata
direktorijuma u domenu gde se nalazi globalni katalog.*

4.5 Odnosi poverenja

- Predstavlja vezu dva ili više domena koji veruju jedan drugom.
- To znači da ako je postavljena veza poverenja između domena, **provera autentičnosti prijavljivanja korisnika se vrši samo na jednom domenu.**
- Svi ostali domeni koji imaju poverenje **priznaju tu proveru** i korisnik može **nesmetano bez ponovne provere da radi sa resursima drugih domena**
- Provera autentičnosti korisnika i aplikacija vrši se putem jednog ili dva protokola poverenja: ***Kerberos*** ili ***NT LAN Manager*** (NTLM).
- Odnos poverenja čine **dva domena**: domen koji ima poverenje i domen u koga se ima poverenje.

Možemo da definišemo neke opšte karakteristike poverenja i to:

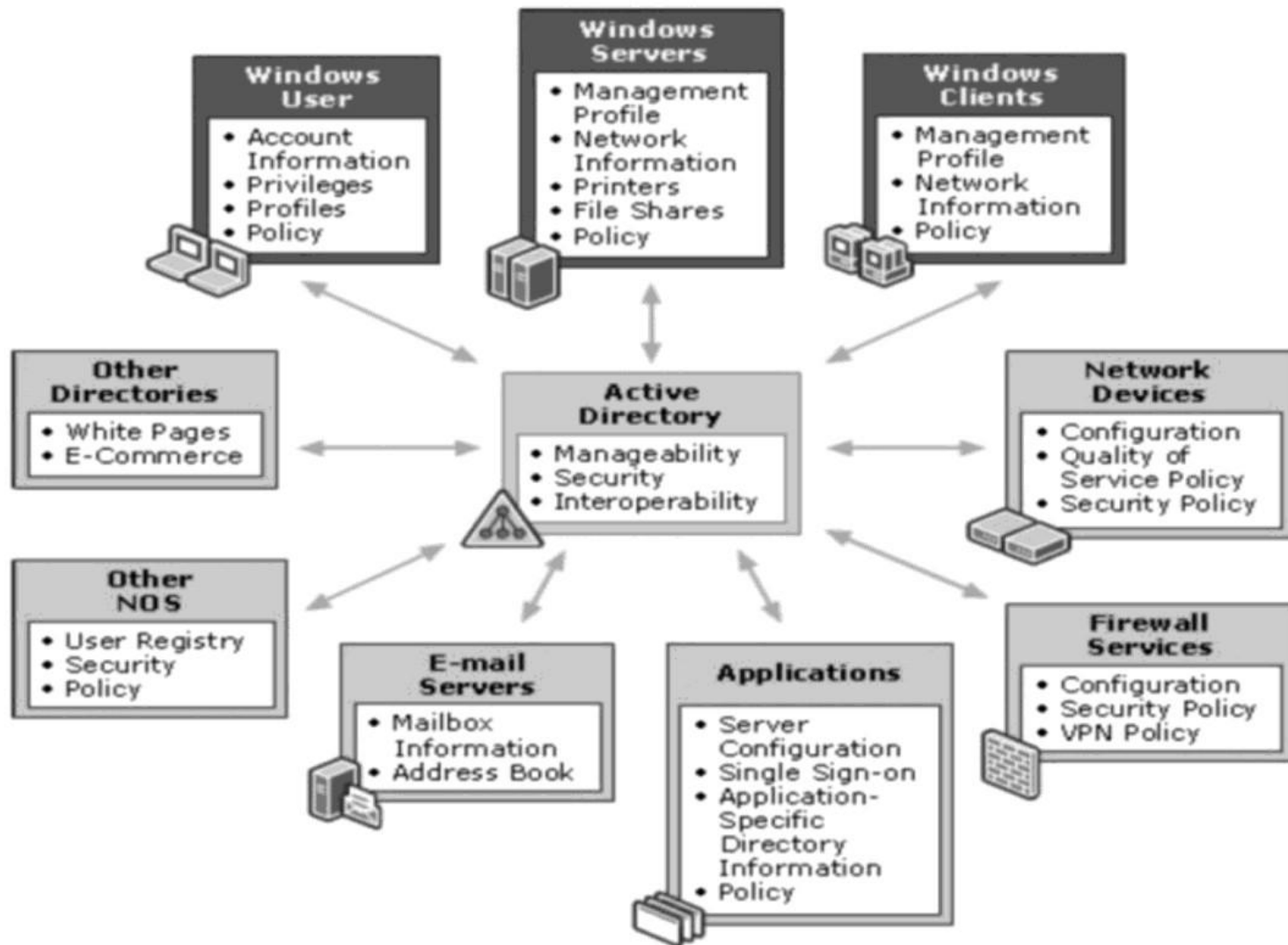
1. **Metod pravljenja**: postoje dva načina pravljenja poverenja i to **implicitno** (automatsko) i **eksplicitno** (ručno).
2. **Tranzitivnost**: poverenja mogu biti vezana za domene koji su **u odnosu** (netranzitivna) i **nevezana** (tranzitivna).
3. **Smer**: postoje **jednosmerna** i **dvosmerna** poverenja.

4.5 Grupne politike

Grupne politike predstavljaju zbirke korisničkih i računarskih parametara konfiguracije koji se mogu povezati sa računarima, lokacijama, domenima i organizacionim jedinicama da bi odredili ponašanje radne površine korisnika.

- Omogućava nam da se na više računara koji pripadaju jednoj grupi, odredi kako će izgledati radna površina, koji će programi biti na raspolaganju korisnicima kao i definisanje različitih drugih opcija.
- To se ostvaruje putem definisanja objekta grupne politike - **Group Policy Object** (GPO), koji će odrediti radnu površinu svake grupe
- Postoje dve vrste GPO i to lokalni i nelokalni.
- Lokalni GPO imaju svi računari koji rade pod Windows Server OS
- Nelokalni GPO povezani su sa objektima servisa AD: lokacijama, domenima ili organizacionim jedinicama.
- Nelokalni GPO mogu biti primenjeni na korisnike ili na računare.
- U skladu sa svojstvima nasleđivanja u servisu AD, nelokalni GPO se primenjuju hijerahijski od najmanje restriktivne grupe (lokacije) do najrestriktivnije grupe (organizacione jedinice)

Povezanost Aktivnog direktorijuma



Hvala na pažnji !!!



Pitanja

? ? ?