# Deo 1
# Učite individualnim tempom

# 1 Uvod u servis Active Directory

Servis Active Directory omogućava upravljanje resursima mreže iz jedne tačke, tako što dozvoljava lako dodavanje, uklanjanje i premeštanje korisnika i resursa. U ovom poglavlju se upoznajete sa konceptima servisa Active Directory i zadacima administriranja prolaženjem kroz postupke koji su neophodni za planiranje infrastrukture servisa Active Directory.

**Napomena** U ovoj knjizi se izrazi „familija Windows Server 2003" i „Windows Server 2003" odnose na grupu od četiri proizvoda: Microsoft Windows Server 2003, Standard Edition; Microsoft Windows Server 2003, Enterprise Edition; Microsoft Windows Server 2003, Datacenter Edition; i Microsoft Windows Server 2003, Web Edition. Međutim, Windows Server 2003, Web Edition samo delimično podržava upotrebu servisa Active Directory. Windows Server 2003, Web Edition može biti server član u mreži koju omogućava Active Directory, ali se ne može koristiti kao Active Directory kontroler domena.

## Zašto je važno ovo poglavlje?

Ovo poglavlje vas uvodi u Active Directory. Dok budete čitali lekcije u ovom poglavlju, imajte na umu da će koncepti koje ovde srećete biti detaljnije istraženi u kasnijim poglavljima, dok budete učili kako da primenite i administrirate Windows Server 2003 Active Directory.

**Lekcije u ovom poglavlju:**



## Pre nego što počnete

Da biste savladali ovo poglavlje, morate poznavati osnovne koncepte administriranja koji se koriste u Microsoft Windowsu NT ili Microsoft Windowsu 2000.

# Lekcija 1: Pregled servisa Active Directory

Active Directory omogućava metodu za dizajniranje strukture direktorijuma koja zadovoljava potrebe vaše organizacije. U ovoj lekciji se upoznajete sa konceptom servisa direktorijuma, upotrebom objekata i funkcijama svake od komponenti servisa Active Directory.

**Po završetku ove lekcije, moći ćete da:**

- objasnite funkciju servisa direktorijuma;
- objasnite svrhu servisa Active Directory;
- objasnite svrhu šeme u servisu Active Directory;
- identifikujete komponente servisa Active Directory;
- opišete funkciju komponenti servisa Active Directory;
- objasnite svrhu globalnog kataloga u servisu Active Directory.

**Vreme predviđeno za lekciju: 30 minuta**

## Razumevanje servisa direktorijuma

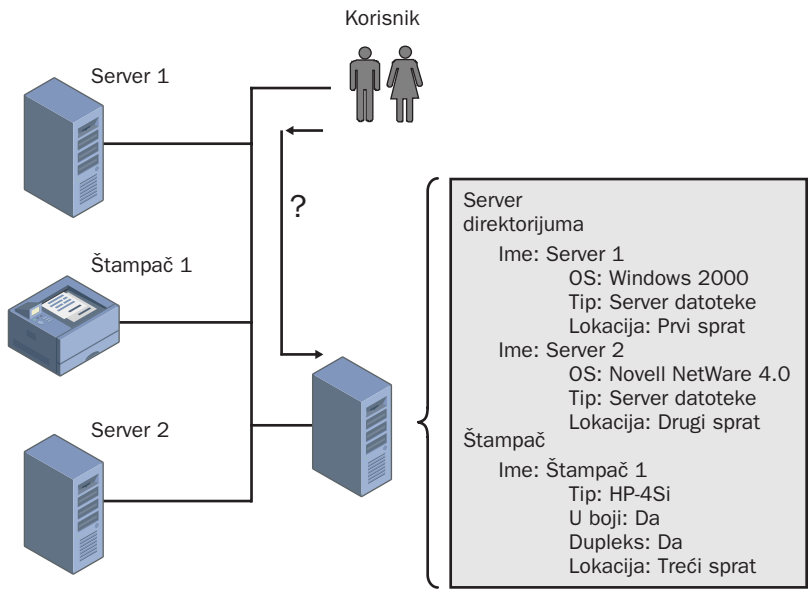
*Direktorijum* je kolekcija uskladištenih podataka o objektima koji su na neki način međusobno povezani. Na primer, adresar elektronskih adresa skladišti imena korisnika ili entiteta i njihove adrese elektronske pošte. Spisak elektronskog adresara može sadržavati i poštansku adresu ili druge podatke o korisniku ili entitetu.

U distribuiranom računarskom sistemu ili javnoj računarskoj mreži, kao što je Internet, ima mnogo objekata uskladištenih u direktorijumu, kao što su serveri datoteka, štampači, serveri faksova, aplikacije, baze podataka i korisnici. Korisnicima se mora omogućiti da te objekte nađu i upotrebe. Administratorima mora omogućiti da upravljaju korišćenjem tih objekata. *Servis direktorijuma* uskladištava sve informacije koje su potrebne za korišćenje i upravljanje tim objektima na jednoj centralnoj lokaciji, što pojednostavljuje proces pronalaženja i rukovanja ovim resursima. Servis direktorijuma se razlikuje od direktorijuma po tome što je istovremeno i izvor podataka i mehanizam koji te podatke stavlja na raspolaganje korisnicima.

Servis direktorijuma funkcioniše kao glavna centrala mrežnog operativnog sistema. On je centralna vlast koja upravlja identitetima i uređuje odnose između distribuiranih resursa i tako im omogućava da rade zajedno. Budući da servis direktorijuma obezbeđuje ove fundamentalne funkcije operativnog sistema, mora biti tesno povezan sa mehanizmima upravljanja i bezbednošću operativnog sistema, da bi obezbedio integritet i privatnost mreže. On, takođe, igra ključnu ulogu u sposobnosti organizacije da definiše i održava infrastrukturu mreže, obavlja administriranje sistema i kontroliše ukupno korisničko iskustvo sa informacionim sistemima kompanije.

## Zašto je potreban servis direktorijuma?

Servis direktorijuma je sredstvo za organizovanje i pojednostavljivanje pristupa resursima mrežnog računarskog sistema. Korisnici i administratori možda ne znaju tačan naziv objekata koji su im potrebni. Međutim, možda znaju jednu ili više karakteristika objekata o kojima se radi. Kao što je prikazano na slici 1-1, oni mogu da upotrebe servis direktorijuma da bi zatražili spisak objekata u kojima se poznate karakteristike pojavljuju. Na primer, „Nađi sve kolor štampače na trećem spratu" postavlja upit direktorijumu da nađe sve objekte kolor štampača koji su povezani sa karakteristikom „treći sprat" (ili možda sa karakteristikom lokacije koja je postavljena na „treći sprat"). Servis direktorijuma omogućava da se pronađe objekat na osnovu jedne njegove karakteristike ili više njih.




**Slika 1-1** Korišćenje servisa direktorijuma

Servis direktorijuma je istovremeno i alatka administratora i alatka krajnjeg korisnika. Kada mreža raste, treba upravljati sve većim brojem objekata i tada servis direktorijuma postaje neophodan.

## Servis direktorijuma Windows Servera 2003

*Active Directory* je servis direktorijuma koji je uključen u familiju Windows Server 2003. Active Directory je direktorijum koji uskladištava informacije o mrežnim resursima i sve servise koji te informacije čine dostupnim i korisnim. Servis Active Directory postoji i u Windowsu 2000.

## Odlike servisa Active Directory

Active Directory u familiji Windows Server 2003 je značajno poboljšanje u odnosu na prosti domenski model kakav ima Windows NT. Active Directory je integrisan u familiju Windows Server 2003 i nudi sledeće funkcije:

- **Centralizovano skladište podataka** Svi podaci u servisu Active Directory nalaze se u jednom, distribuiranom skladištu podataka, čime je omogućen lak pristup informacijama sa bilo koje lokacije. Jedno distribuirano skladište podataka zahteva manje administriranja i dupliranja i poboljšava raspoloživost i organizaciju podataka.
- **Prilagodljivost** Active Directory omogućava prilagođavanje direktorijuma kako bi se zadovoljili poslovni i mrežni zahtevi preko konfigurisanja domena i stabala i smeštanja kontrolera domena. Active Directory dozvoljava milione objekata po domenu, a za ubrzavanje rada koristi tehnologiju indeksiranja i napredne tehnike repliciranja.
- **Proširivost** Struktura baze podataka servisa Active Directory (šema) može se proširiti tako da dozvoli prilagođene tipove informacija.
- **Upravljivost** Za razliku od prostog domenskog modela kakav koristi Windows NT, Active Directory je zasnovan na hijerarhijskim organizacionim strukturama. To administratoru olakšava kontrolu nad ovlašćenjima i drugim bezbednosnim parametrima, a korisnicima pronalaženje mrežnih resursa kao što su datoteke i štampači.
- **Integrisanje sa sistemom imena domena (DNS)** Active Directory koristi DNS, standardni internetski servis koji prevodi lako čitljiva imena matičnih računara u numeričke IP adrese. Iako su zasebni i različito implementirani za različite svrhe, Active Directory i DNS imaju istu hijerarhijsku strukturu. Klijenti servisa Active Directory koriste DNS za lociranje kontrolera domena. Pri upotrebi DNS servisa Windows Servera 2003, primarne DNS zone mogu biti uskladištene u servisu Active Directory, što omogućava repliciranje na druge kontrolere domena servisa Active Directory.
- **Upravljanje klijentskom konfiguracijom** Active Directory nudi nove tehnologije za upravljanje parametrima klijentske konfiguracije, kao što su mobilnost korisnika i otkaz diska, uz minimum administriranja i prekida u radu za korisnika.
- **Administriranje na bazi politike** U servisu Active Directory politike se koriste za definisanje dozvoljenih akcija i parametara za korisnike i računare na datoj lokaciji, datom domenu ili datoj organizacionoj jedinici. Upravljanje na osnovu politike pojednostavljuje zadatke kao što su ažuriranje operativnog sistema, instaliranje aplikacija, kao i zadatke koji se odnose na korisničke profile i blokade stonog sistema.
- **Replikacija podataka** Active Directory koristi tehnologiju repliciranja sa više glavnih primeraka, koja obezbeđuje raspoloživost informacija, otpor-

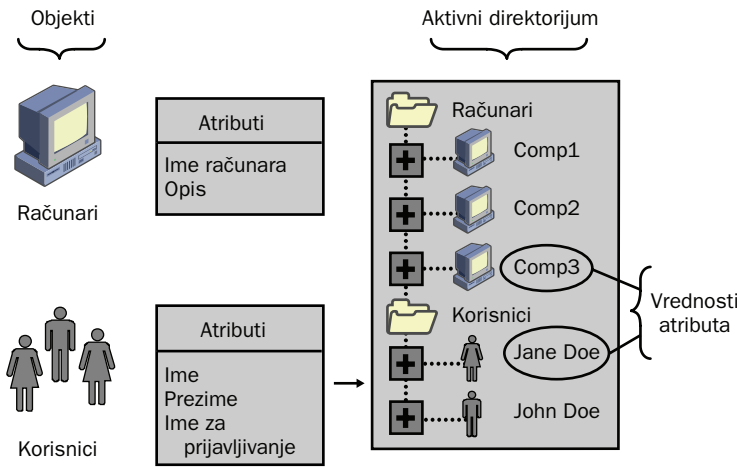
nost na greške, usklađivanje opterećenja i druga poboljšanja performansi. Repliciranje sa više glavnih primeraka omogućava ažuriranje direktorijuma na svakom kontroleru domena i repliciranje izmena direktorijuma na druge kontrolere domena. Budući da se koriste više kontrolera domena, replikacija se nastavlja čak i ako neki kontroler domena prestane da radi.

- **Fleksibilna, bezbedna provera autentičnosti i ovlašćivanje** Provera autentičnosti i ovlašćivanje servisu Active Directory obezbeđuje zaštitu podataka i minimizuje prepreke obavljanju posla preko Interneta. Active Directory podržava viš protokola za proveru autentičnosti, kao što su Kerberos verzija 5, Secure Socket Layer (SSL) verzija 3 i Transport Layer Security (TLS) koji koristi certifikate X.509, verzija 3. Osim toga, Active Directory koristi bezbednosne grupe koje se prostiru preko više domena.
- **Bezbednosna integracija** Active Directory je integrisan sa bezbednošću Windows Servera 2003. Kontrola pristupanja može biti definisana za svaki objekat u direktorijumu i posebno za svako svojstvo objekta. Bezbednosna politika može biti primenjena lokalno ili na određenu lokaciju, domen ili organizacionu jedinicu.
- **Direktorijumski omogućene aplikacije i infrastruktura** Funkcije servisa Active Directory olakšavaju konfigurisanje i upravljanje aplikacijama i drugim direktorijumski omogućenim mrežnim komponentama. Osim toga, Active Directory daje moćno razvojno okruženje preko interfejsa servisa Active Directory (ADSI).
- **Mogućnost rada sa drugim servisima direktorijuma** Active Directory je zasnovan na standardnim protokolima za pristupanje direktorijumima, uključujući verziju 3 *LDAP protokola* i *Name Service Provider Interface* (NSPI) i može da komunicira sa drugim servisima direktorijuma koji koriste ove protokole. Budući da je LDAP standardni protokol servisa direktorijuma, mogu se praviti programi koji koriste LDAP kako bi se podaci servisa Active Directory mogli razmenjivati sa drugim servisima direktorijuma koji takođe podržavaju LDAP. Active Directory podržava protokol NSPI, koji koriste klijenti Microsoft Exchange Servera 4 i 5.*x*, kako bi obezbedio kompatibilnost sa direktorijumom Exchange.
- **Potpisan i šifrovan LDAP saobraćaj** Podrazumeva se da alatke servisa Active Directory u Windows Serveru 2003 potpisuju i šifruju LDAP saobraćaj. Potpisivanje LDAP saobraćaja garantuje da paketi podataka stižu od poznatog izvora i da nisu neovlašćeno menjani.

**Videti takođe** Za čitaoce koji već poznaju svojstva servisa Active Directory za Windows 2000, detaljan spisak novih svojstava koja Active Directory ima u familiji Windows Server 2003 nalazi se u dodatku A.

## Objekti servisa Active Directory

Podaci uskladišteni u servisu Active Directory, kao što su informacije o korisnicima, štampačima, serverima, bazama podataka, grupama, računarima i bezbednosnim politikama, su organizovani u objekte. *Objekat* je jedinstveno imenovan komplet atributa koji predstavlja jedan mrežni resurs. Atributi objekta su karakteristike objekta u direktorijumu. Na primer, atributi objekta korisničkog naloga mogu obuhvatati korisnikovo lično ime, prezime i ime za prijavljivanje, a atributi objekta računarskog naloga mogu obuhvatati naziv i opis računara (videti sliku 1-2).



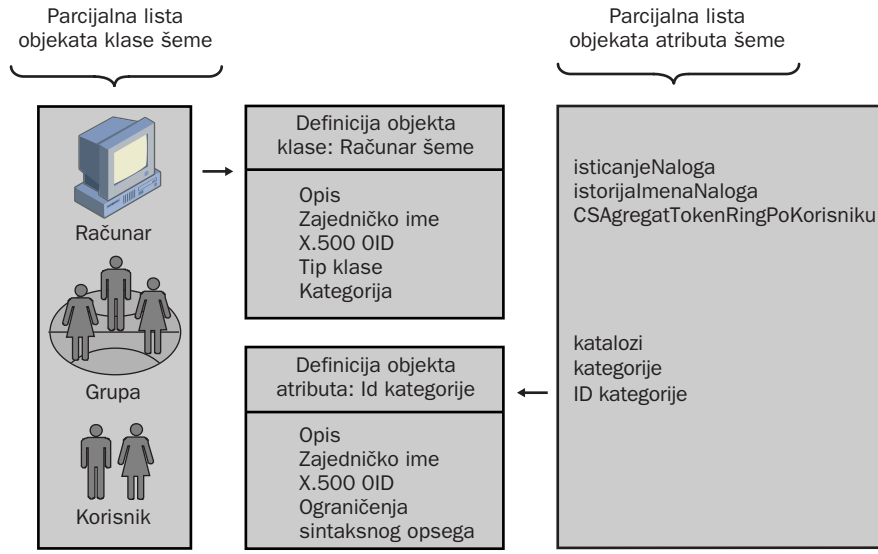

**Slika 1-2** Objekti i atributi servisa Active Directory

Neki objekti, poznati pod imenom *kontejneri*, mogu sadržavati druge objekte. Na primer, domen je objekat kontejner koji sadrži objekte kao što su korisnički i računarski nalozi. Na slici 1-2, omotnica Users je kontejner koji sadrži objekte korisničkih naloga.

### Šema Active Directory

Šema Active Directory definiše objekte koji mogu biti uskladišteni u servisu Active Directory. *Šema* je spisak definicija koje određuju vrste objekata i tipove informacija o tim objektima koji mogu biti uskladišteni u servisu Active Directory. Budući da su i same definicije u okviru šeme uskladištene kao objekti, njima se može upravljati na isti način kao i ostalim objektima u servisu Active Directory.

Šema je definisana pomoću dva tipa objekata: objekti klase (takođe poznati kao klase šeme) i objekti atributa (takođe poznati kao atributi šeme). Kao što je prikazano na slici 1-3, objekti klase i objekti atributa definisani su u zasebnim listama u okviru šeme. Objekti klase i objekti atributa nose zajedničko ime *objekti šeme* ili *metapodaci*.




**Slika 1-3** Objekti klase i objekti atributa u okviru šeme

*Objekti klase šeme* opisuju moguće objekte servisa Active Directory koji mogu biti stvoreni. Klasa šeme funkcioniše kao šablon za pravljenje novih objekata servisa Active Directory. Svaka klasa šeme je zbirka objekata atributa šeme. Kada napravite klasu šeme, atributi šeme uskladištavaju informacije koje opisuju objekat. Na primer, klasu User sačinjavaju mnogi atributi šeme, uključujući adresu mreže i matični direktorijum. Svaki objekat u servisu Active Directory je jedan primerak objekta klase šeme.

*Objekti atributa šeme* definišu objekte klase šeme sa kojima su povezani. Svaki atribut šeme definiše se samo jedanput, a može biti upotrebljen u mnogim klasama šeme. Na primer, atribut Description se koristi u mnogim klasama šeme, ali se definiše samo jedanput u šemi, čime se obezbeđuje doslednost.

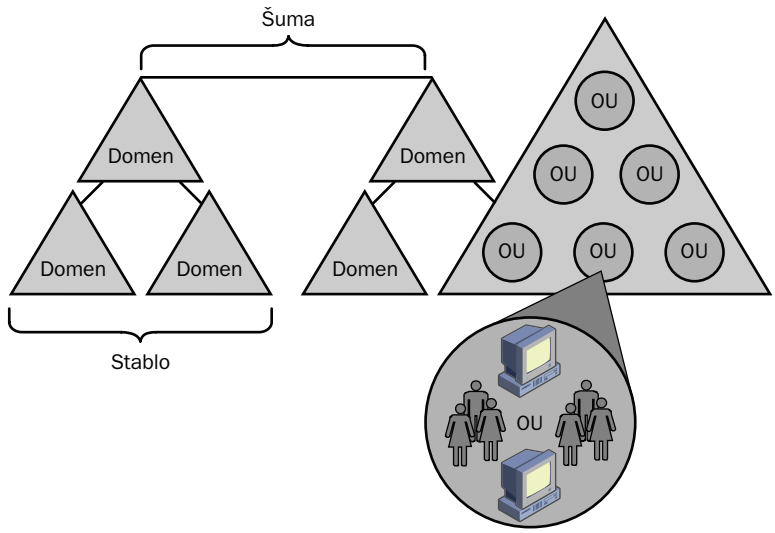
Skup osnovnih klasa šeme i atributa šeme isporučuje se uz Active Directory. Iskusni razvijaoci i administratori mreže mogu dinamički da prošire šemu definisanjem novih klasa i atributa za postojeće klase. Na primer, ako treba da obezbedite informacije o korisnicima koje nisu definisane u šemi, morate proširiti šemu za klasu User. Međutim, proširivanje šeme je napredna operacija koja može da ima ozbiljne posledice. Pošto šema ne može biti obrisana, nego samo deaktivirana i automatski se replicira, morate pažljivo uraditi plan i pripremu pre proširivanje šeme.

## Komponente servisa Active Directory

Razne komponente servisa Active Directory se koriste za izgradnju strukture direktorijuma koja zadovoljava potrebe vaše organizacije. Sledeće komponente servisa Active Directory predstavljaju logičke strukture u jednoj organizaciji: domeni, organizacione jedinice (OU), stabla i šume. Sledeće komponente servisa Active Directory predstavljaju fizičke strukture u jednoj organizaciji: lokacije (fizičke podmreže) i kontroleri domena. Active Directory u potpunosti razdvaja logičku od fizičke strukture.

### Logičke strukture

U servisu Active Directory organizujete resurse u logičku strukturu – strukturu koja odražava organizacioni model – pomoću domena, organizacionih jedinica, stabala i šuma. Logičko grupisanje resursa vam omogućava da lako nađete resurs po imenu, umesto da pamtite njegovu fizičku lokaciju. Budući da resurse grupišete logički, Active Directory čini fizičku strukturu mreže transparentnom za korisnike. Slika 1-4 ilustruje odnos između domena, organizacionih jedinica, stabala i šuma u servisu Active Directory.




**Slika 1-4** Odnos između domena, organizacionih jedinica, stabala i šuma u servisu Active Directory

**Domeni** Osnovna jedinica logičke strukture u servisu Active Directory je *domen*, koji može da uskladišti milione objekata. Objekti uskladišteni u domenu smatraju se vitalnim za mrežu. To su stavke koje su potrebne članovima umrežene zajednice za obavljanje poslova: štampači, dokumenti, adrese e-pošte, baze podataka, korisnici, distribuirane komponente i drugi resursi. Svi objekti mreže postoje u okviru domena, a svaki domen čuva informacije samo o objektima koji se u njemu nalaze. Active Directory je sačinjen od jednog

domena ili više njih. Domen može da se prostire šire od jedne fizičke lokacije. Domeni dele sledeće karakteristike:

- Svi objekti mreže postoje u okviru domena, a svaki domen čuva informacije samo o objektima koji se u njemu nalaze.
- Domen je bezbednosna granica. Pristup objektima u domenu rukovodi se listama za kontrolu pristupa (*access control list*, ACL) u kojima se nalaze dozvole za objekte. Te dozvole kontrolišu koji korisnici mogu pristupiti nekom objektu i koji tip pristupa mogu dobiti. U familiji Windows Server 2003 objekti obuhvataju datoteke, omotnice, deljenja, štampače i druge objekte servisa Active Directory. Nijedna od bezbednosnih politika i postavki – kao što su administrativna prava, bezbednosne politike i ACL-ovi – ne može se preneti iz jednog domena u drugi. Kao administrator domena, imate apsolutno pravo da podešavate politiku samo u okviru svog domena.

*Funkcionalni nivo domena* (poznat kao *režim domena* u Windowsu 2000) obezbeđuje način omogućavanja funkcionalnosti servisa Active Directory u celom domenu, unutar mrežnog okruženja. Na raspolaganju su četiri funkcionalna nivoa domena: mešani Windows 2000 (podrazumevani), početni Windows 2000, privremeni Windows Server 2003 i Windows Server 2003. Funkcionalni nivo mešani Windows 2000 omogućava da kontroler domena Windows Server 2003 komunicira sa kontrolerima domena u okviru istog domena koji rade pod Windowsom NT 4, Windowsom 2000 ili familijom Windows Server 2003. Funkcionalni nivo početni Windows 2000 omogućava da kontroler domena Windows Server 2003 komunicira sa kontrolerima domena u okviru istog domena koji rade pod Windowsom 2000 ili Windows Serverom 2003. Funkcionalni nivo privremeni Windows Server 2003 omogućava kontroleru domena Windows Server 2003 da komunicira sa kontrolerima domena u okviru istog domena koji rade pod Windowsom NT 4 ili Windows Serverom 2003. Funkcionalni nivo Windows Server 2003 omogućava kontroleru domena Windows Server 2003 da komunicira samo sa kontrolerima domena u okviru istog domena koji rade pod Windows Serverom 2003. Funkcionalni nivo domena možete podići samo ako kontroleri domena u okviru domena rade pod odgovarajućom verzijom Windowsa. Detalje o podizanju funkcionalnih nivoa domena možete pročitati u poglavlju 3.

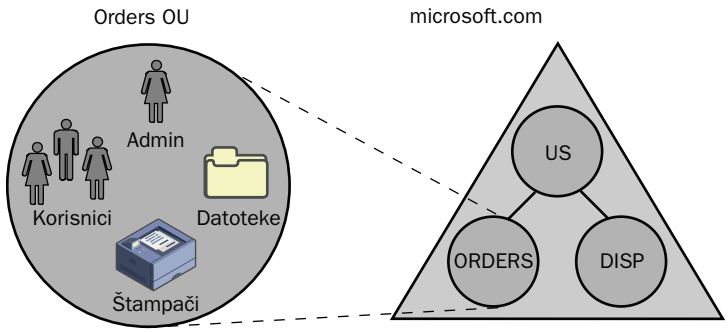
Kao administrator, morate napraviti strukturu domena koja će odražavati organizaciju vaše kompanije. Pročitajte lekciju 3, kako biste naučili osnove dizajna domena. Detalje o pravljenju domena možete pročitati u poglavlju 4.

**Organizacione jedinice** Organizaciona jedinica (*organizational unit*, OU) je kontejner koji se koristi za organizovanje objekata unutar domena u logičku administrativnu grupu. Organizacione jedinice obezbeđuju sredstva za rukovanje zadacima administriranja, kao što je administriranje korisnika i resursa, budući da su najmanje jedinice kojima možete delegirati administrativna ovlašćenja. Organizaciona jedinica može da sadrži objekte kao što su korisnički nalozi, grupe, računari, štampači, aplikacije, deljene datoteke i druge OU iz istog

domena. Hijerarhija OU unutar jednog domena je nezavisna od hijerarhijske strukture OU-a drugih domena – svaki domen može da primeni sopstvenu hijerarhiju organizacionih jedinica. Dodavanjem OU-a drugim OU-ima, odnosno *ugnežđavanjem*, možete omogućiti hijerarhijsku administrativnu kontrolu.

Kao administrator, morate napraviti strukturu OU tako da odražava organizaciju vaše kompanije. Videti lekciju 3, kako biste naučili osnove dizajna OU. Videti poglavlje 6, kako biste razumeli implementiranje strukture OU.

Na slici 1-5, domen *microsoft.com* preslikava organizaciju transportnog preduzeća i sadrži tri OU koje se zovu: US, Orders i Disp, pri čemu su Orders i Disp ugnežđene u organizacionu jedinicu US. U letnjim mesecima, broj preuzetih transportnih naloga se povećava, pa je rukovodstvo zatražilo dodavanje podadministratora za odeljenje Orders. Podadministrator mora imati samo dozvolu za pravljenje korisničkih naloga i obezbeđivanje pristupa korisnika datotekama i zajedničkim štampačima odeljenja Orders. Umesto pravljenja novog domena, taj zahtev se može ispuniti dodeljivanjem odgovarajućih dozvola podadministratoru u okviru OU Orders.

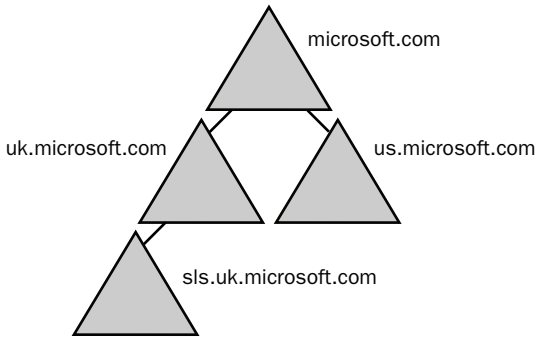



**Slika 1-5** Korišćenje OU za rukovanje zadacima administriranja

Ako podadministrator kasnije bude morao da pravi korisničke naloge u organizacionim jedinicama US, Orders i Disp, mogli biste mu odobriti odgovarajuće dozvole posebno u okviru svake OU. Međutim, budući da su OU Orders i Disp ugnežđene u OU US, efikasniji način bi bio da se dozvole odobre jedanput u OU US, a zatim da ih OU Orders i Disp naslede. Podrazumeva se da svi podređeni objekti (OU Orders i Disp) unutar servisa Active Directory nasleđuju dozvole od nadređenih objekata (OU US). Davanje dozvola na višem nivou i korišćenje svojstva nasleđivanja može da smanji zadatke administriranja.

**Stabla** *Stablo* je grupa ili hijerarhijsko uređenje jednog domena ili više domena Windows Servera 2003 koja se pravi dodavanjem podređenih domena postojećem nadređenom domenu. Domeni u stablu dele susedni prostor imena i hijerarhijsku strukturu imenovanja. Prostori imena su detaljno obrađeni u sledećoj lekciji. Prema DNS standardima, ime podređenog domena je relativno ime koje čini ime tog podređenog domena kome je dodato ime

nadređenog domena. Na slici 1-6, *microsoft.com* je nadređeni domen, a *us.microsoft.com* i *uk.microsoft.com* su njemu podređeni domeni. Podređeni domen domena *uk.microsoft.com* je *sls.uk.microsoft.com*. Pravljenjem hijerarhije domena u stablu možete zadržati bezbednost i omogućiti administriranje u okviru OU ili u okviru jednog domena u stablu. Struktura stabla olakšava pravljenje organizacionih izmena.



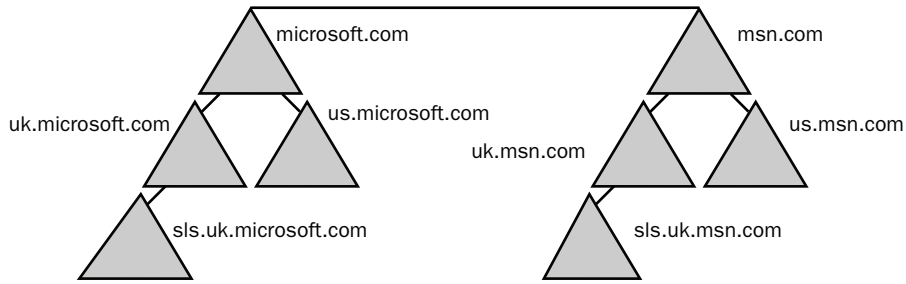

**Slika 1-6** Stablo domena

Kao administrator, morate napraviti strukturu stabla koja će odražavati organizaciju vaše kompanije. Videti lekciju 3, koja sadrži osnove dizajniranja stabala. Detalje o pravljenju stabala možete pročitati u poglavlju 4.

**Šume** *Šuma* je grupa ili hijerarhijsko uređenje jednog odvojenog i potpuno nezavisnog stabala domena ili više njih. Kao takve, šume imaju sledeće karakteristike:

- Svi domeni u šumi dele zajedničku šemu.
- Svi domeni u šumi dele zajednički globalni katalog.
- Svi domeni u šumi su povezani implicitnim dvosmernim tranzitivnim odnosima poverenja.
- Stabla u šumi imaju različite strukture imenovanja, u skladu sa svojim domenima.
- Domeni u šumi rade nezavisno, ali šuma omogućava komunikaciju unutar cele organizacije.

Na slici 1-7, stabla *microsoft.com* i *msn.com* čine šumu. Prostor imena je susedni samo unutar svakog stabla.




**Slika 1-7** Šuma stabala

*Funkcionalni nivo šume* omogućava funkcionalnosti servisa Active Directory u celoj šumi unutar mrežnog okruženja. Na raspolaganju su tri funkcionalna nivoa šume: Windows 2000 (podrazumevani), privremeni Windows Server 2003 i Windows Server 2003. Funkcionalni nivo Windows 2000 omogućava da kontroler domena Windows Server 2003 komunicira sa kontrolerima domena u okviru istog domena koji rade pod Windowsom NT4, Windowsom 2000 ili Windows Serverom 2003. Funkcionalni nivo privremeni Windows Server 2003 omogućava kontroleru domena Windows Server 2003 da komunicira sa kontrolerima domena u okviru istog domena koji rade pod Windowsom NT4 ili Windows Serverom 2003. Funkcionalni nivo Windows Server 2003 omogućava kontroleru domena Windows Server 2003 da komunicira samo sa kontrolerima domena u okviru istog domena koji rade pod Windows Serverom 2003. Funkcionalni nivo šume možete podići samo ako kontroleri domena u okviru šume rade pod odgovarajućom verzijom Windowsa. Detalje o podizanju funkcionalnih nivoa šuma možete pročitati u poglavlju 3.

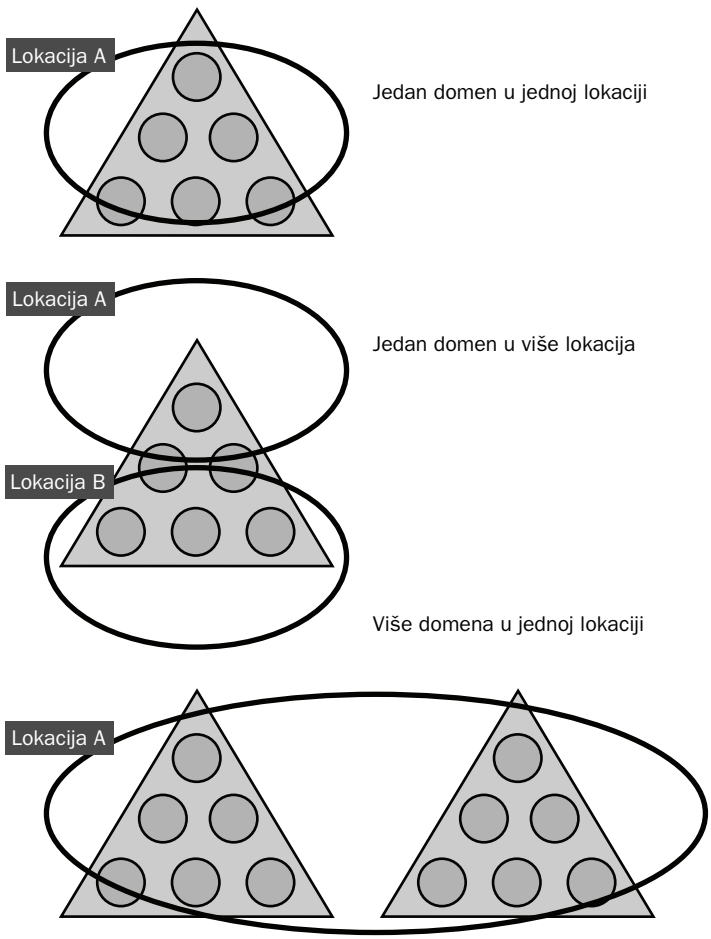
Kao administrator, morate napraviti strukturu šume koja će odražavati organizaciju vaše kompanije. Pročitajte lekciju 3 kako biste naučili osnove dizajniranja šume. Detalje o pravljenju šuma možete pročitati u poglavlju 4.

## Fizičke strukture

Fizičke komponente servisa Active Directory su lokacije i kontroleri domena. Kao administrator, vi koristite ove komponente za razvijanje strukture direktorijuma koja odražava fizičku strukturu vaše organizacije.

**Lokacije** *Lokacija* je kombinacija jedne IP podmreže, ili više njih, povezanih visokopouzdanom i brzom vezom u cilju lokalizovanja što je moguće više mrežnog saobraćaja. Lokacija obično ima iste granice kao lokalna računarska mreža (LAN). Kada grupišete podmreže u mreži, treba da kombinujete samo podmreže koje imaju brze, jeftine i pouzdane mrežne veze između sebe. Pod „brzom" mrežnom vezom se podrazumeva protok od najmanje 512 kilobita u sekundi (Kbps). Raspoloživi propusni opseg (prosečna vrednost propusnog opsega koji je na raspolaganju nakon što se obradi uobičajeni mrežni saobraćaj) od više od 128 Kbps dovoljan je za jednu lokaciju.

Kod servisa Active Directory, lokacije nisu deo prostora imena. Kada pretražujete logički prostor imena, vidite računare i korisnike grupisane u domene i organizacione jedinice, a ne lokacije. Lokacije sadrže samo objekte računara i veza koji se koriste za konfigurisanje replikacije između lokacija. Kao što je prikazano na slici 1-8, jedan domen se može prostirati na jednoj geografskoj lokaciji ili na više njih, a jedna lokacija može sadržati korisničke naloge i računare koji pripadaju različitim domenima.




**Slika 1-8** Odnos između struktura lokacije i domena

Kao administrator, morate napraviti strukturu lokacije koja će odražavati organizaciju vaše kompanije. Pročitajte lekciju 3 kako biste naučili osnove dizajna lokacije. Detalje o konfigurisanju lokacija možete pročitati u poglavlju 5.

**Kontroleri domena** *Kontroler domena* je računar pod Windows Serverom 2003 na kome je smeštena replika direktorijuma domena (baza podataka lokalnog domena). Budući da domen može da sadrži jedan kontroler domena ili više njih, svaki kontroler domena u domenu ima potpunu repliku dela direktorijuma koji mu pripada. Kontroler domena može da servisira samo jedan domen. Kontroler domena takođe proverava autentičnost korisničkih pokušaja prijavljivanja i održava bezbednosnu politiku za domen.

Sledeći spisak opisuje funkcije kontrolera domena:

- Svaki kontroler domena sadrži potpunu kopiju svih informacija servisa Active Directory za taj domen, upravlja izmenama tih informacija i replicira te izmene na druge kontrolere domena u istom domenu.
- Kontroleri domena u jednom domenu automatski repliciraju direktorijumske informacije svakog objekta u domenu svim ostalim objektima. Kada izvršite neku akciju koja uzrokuje ažuriranje servisa Active Directory, vi u stvari pravite izmenu na jednom od kontrolera domena. Zatim taj kontroler domena replicira izmenu svim drugim kontrolerima domena unutar domena. Replikaciju saobraćaja između kontrolera domena u mreži možete kontrolisati određivanjem učestalosti repliciranja i količine podataka koju svaki kontroler domena replicira odjedanput.
- Kontroleri domena odmah repliciraju neke važne izmene, kao što je onemogućavanje korisničkog naloga.
- Active Directory koristi repliciranje sa više glavnih primeraka, u kome ni jedan kontroler domena nije glavni kontroler domena. Svi kontroleri domena unutar domena su ravnopravni, i svaki kontroler domena sadrži kopiju baze podataka direktorijuma u koju je takođe moguće upisivati. Kontroleri domena mogu držati različite informacije neko vreme, dok se izmene servisa Active Directory ne sinhronizuju u svim kontrolerima domena.
- Iako Active Directory podržava repliciranje sa više mastera, neke izmene nije zgodno vršiti na taj način. Izvođenje repliciranja sa jednim glavnim primerkom može biti zadato jednom kontroleru domena, ili nekolicini njih, (operacije kojima nije dozvoljeno da se dešavaju na različitim mestima u mreži istovremeno). *Glavne uloge za operaciju* (engl. *operations master role*) su posebne uloge date jednom kontroleru domena, ili nekolicini njih, u istom domenu za izvršavanje repliciranja sa jednim glavnim primerkom.
- Kontroleri domena detektuju kolizije koje mogu nastati kada jedan kontroler domena izmeni neki atribut pre no što se izmena tog atributa u potpunosti reprodukuje na drugi kontroler domena. Kolizije se detektuju poređenjem svojstva broja verzije svakog atributa, koji se posebno dodeljuje atributu pri inicijalizaciji nakon pravljenja atributa. Active Directory razrešava koliziju repliciranjem izmenjenog atributa sa višim brojem verzije svojstva.

- Postojanje više od jednog kontrolera domena u domenu obezbeđuje otpornost na greške. Ako je jedan kontroler domena oflajn, drugi kontroler domena može da obezbedi sve potrebne funkcije, kao što je beleženje izmena u Active Directory.
- Kontroleri domena upravljaju svim aspektima korisničkih interakcija u domenu, kao što je lociranje objekata servisa Active Directory i potvrđivanje korisničkih pokušaja prijavljivanja.

Kao administrator, morate postaviti kontrolere domena na lokacije tako da odražavaju fizičku strukturu vaše organizacije i optimiziraju repliciranje i proveru autentičnosti. Videti lekciju 3 koja sadrži osnove smeštanja kontrolera domena. Detalje o stvaranju kontrolera domena pročitajte u poglavlju 2.

## Servisi kataloga – globalni katalog

Active Directory omogućava korisnicima i administratorima da pronađu objekte kao što su datoteke, štampači ili korisnici unutar svog domena. Međutim, pronalaženje objekata izvan domena i širom preduzeća zahteva mehanizam koji domenima omogućava da funkcionišu kao jedna celina. Servis kataloga sadrži izabrane informacije o svakom objektu u svim domenima u direktorijumu, što je korisno pri pretraživanju širom preduzeća. Globalni katalog je servis kataloga koji je omogućen od strane servisa Active Directory.

*Globalni katalog* je centralno skladište informacija o objektima u stablu ili šumi. Podrazumeva se da se globalni katalog stvara automatski na inicijalnom kontroleru domena u prvom domenu u šumi. Kontroler domena koji čuva kopiju globalnog kataloga zove se *server globalnog kataloga*. Bilo koji kontroler domena u šumi može biti postavljen kao server globalnog kataloga. Active Directory koristi repliciranje sa više glavnih primeraka za repliciranje informacija globalnog kataloga između servera globalnog kataloga u različitim domenima. On uskladištava kompletnu repliku svih atributa objekata u direktorijumu za svoj matični domen, a delimičnu repliku svih atributa objekata sadržanih u direktorijumu za svaki domen u šumi. Delimična replika uskladištava atribute koji se najčešće koriste pri pretraživanju (na primer, ime i prezime korisnika, ime za prijavljivanje, itd.). Pri definisanju u šemi Active Directory, atributi su ili označeni ili neoznačeni za repliciranje u globalnom katalogu. Atributi objekata repliciranih u globalnom katalogu nasleđuju iste dozvole koje imaju u izvornim domenima, čime se obezbeđuje bezbednost podataka u globalnom katalogu.

### Funkcije globalnog kataloga

Globalni katalog vrši ove dve ključne funkcije:

- Omogućava korisniku da se prijavi na mrežu tako što će pri iniciranju procesa prijavljivanja kontroleru domena dati informacije o članstvu u univerzalnoj grupi.
- Omogućava pronalaženje informacija direktorijuma nezavisno od toga koji domen u šumi sadrži tražene podatke.

Kada se korisnik prijavljuje na mrežu, globalni katalog daje informacije o članstvu u univerzalnoj grupi za njegov nalog kontroleru domena koji obrađuje informacije o prijavljivanju korisnika. Ako postoji samo jedan kontroler domena u domenu, na njemu se nalazi server globalnog kataloga. Ako ima više kontrolera domena u mreži, jedan od njih je konfigurisan da čuva globalni katalog. Ako globalni katalog nije na raspolaganju kada korisnik inicira proces prijavljivanja na mrežu, korisnik će moći da se prijavi samo na lokalni računar, osim ako je lokacija posebno konfigurisana da kešira podatke pretraživanja o članstvu u univerzalnoj grupi pri obradi pokušaja prijavljivanja korisnika.

**Savet** Ako je korisnik član grupe Domain Admins, moći će da se prijavi na mrežu čak i kada globalni katalog nije na raspolaganju.

Globalni katalog je napravljen tako da odgovara na programske i korisničke upite o objektima bilo gde u stablu domena ili šumi, maksimalnom brzinom i sa minimumom mrežnog saobraćaja. Budući da jedan globalni katalog sadrži informacije o svim objektima u svim domenima u šumi, upit o objektu koji se ne nalazi u lokalnom domenu može biti rešen od strane servera globalnog kataloga u domenu u kome je upit zadat. Na taj način, pronalaženje informacija u direktorijumu ne izaziva nepotreban saobraćaj upita preko granica domena.

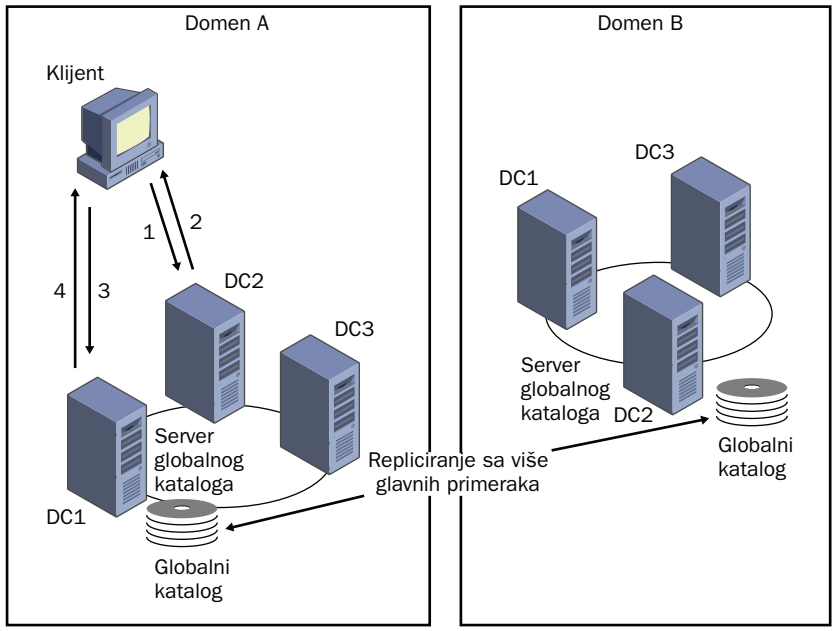
### Proces obrade upita

*Upit* je poseban zahtev koji korisnik šalje globalnom katalogu kako bi pribavio, menjao ili obrisao podatke servisa Active Directory. Sledeći koraci, ilustrovani na slici 1-9, opisuju proces obrade upita:

1. Klijent šalje upit svom DNS serveru o lokaciji servera globalnog kataloga.
2. DNS server traži lokaciju servera globalnog kataloga i kao odgovor vraća IP adresu kontrolera domena koji je konfigurisan kao server globalnog kataloga.
3. Klijent šalje upit za IP adresom kontrolera domena postavljenog kao server globalnog kataloga. Upit se šalje na port 3268 kontrolera domena; standardni upiti servisa Active Directory šalju se na port 389.
4. Server globalnog kataloga obrađuje upit. Ako globalni katalog sadrži atribut objekta koji se traži, server globalnog kataloga daje odgovor klijentu. Ako globalni katalog ne sadrži atribut objekta koji se traži, upit se šalje servisu Active Directory.

Bilo koji kontroler domena u šumi možete konfigurisati kao server globalnog kataloga, ili odrediti dodatne kontrolere domena za tu svrhu. Kada razmišljate koje kontrolere domena da odredite kao servere globalnog kataloga, odlučujte na osnovu sposobnosti strukture mreže da rukuje repliciranjem i saobraćajem upita.

Kao administrator, morate smestiti servere globalnog kataloga na lokacije kako biste obezbedili brze odgovore na upite korisnika, kao i redundantnost. Videti lekciju 3, koja obrađuje osnove dizajniranja smeštanja servera globalnog kataloga. Detalje o konfigurisanju servera globalnog kataloga pročitajte u poglavlju 5.




**Slika 1-9** Proces pravljenja upita

## Obnavljanje lekcije

Pitanja koja slede imaju za cilj da ponove ključne informacije koje su prezentirane u ovoj lekciji. Ako ne umete da odgovorite na neko pitanje, ponovo proučite lekciju, a zatim, ponovo pokušajte da odgovorite na to pitanje. Odgovori na pitanja mogu se naći u odeljku „Pitanja i odgovori" na kraju ovog poglavlja.

1. Kako se servis direktorijuma razlikuje od direktorijuma?

   _____

   _____

2. Na koji način je servis Active Directory prilagodljiv?

   _____

   _____

3. Šta je repliciranje sa više mastera?

_____

_____

4. Imenujte komponente servisa Active Directory koje se koriste za predstavljanje logičke strukture organizacije.

_____

_____

5. Imenujte fizičke komponente servisa Active Directory.

_____

_____

6. Šta je funkcija globalnog kataloga?

_____

_____

## Pregled lekcije

- Servis direktorijuma uskladištava sve podatke koji su potrebni za upotrebu i upravljanje sistemskim objektima na jednoj centralnoj lokaciji, što pojednostavljuje proces pronalaženja i upravljanja ovim resursima.
- Podaci uskladišteni u servisu Active Directory su organizovani u objekte, koji imaju atribute. Šema Active Directory definiše objekte koji se mogu uskladištiti u servisu Active Directory. Klase šeme i atributi šeme definišu šemu Active Directory.
- Logičke strukture organizacije predstavljene su sledećim komponentama servisa Active Directory: domeni, organizacione jedinice, stabla i šume.
- Fizičke komponente servisa Active Directory su lokacije i kontroleri domena.
- Globalni katalog je centralno skladište informacija o objektima u stablu ili šumi.

# Lekcija 2: Razumevanje koncepata servisa Active Directory i administrativnih zadataka

U familiji Windows Server 2003 i servisu Active Directory ima nekoliko novih koncepata i izmena u odnosu na koncepte iz Windowsa NT. Ovi koncepti uključuju repliciranje, odnose poverenja, upravljanje izmenama i konfiguracijama, grupne politike, DNS i imenovanje objekata. Važno je da razumete značenje koje ovi koncepti imaju u servisu Active Directory. Osim toga, treba da se upoznate sa zadacima administriranja servisa Active Directory, koji odgovaraju pojedinim poglavljima ovog paketa za obuku.

**Po završetku ove lekcije, moći ćete da:**

- objasnite repliciranje servisa Active Directory;
- objasnite bezbednosne odnose između domena u stablu (poverenja);
- objasnite komponente upravljanja promenama i konfigurisanjem;
- objasnite svrhu i funkciju grupne politike;
- opišete kako Active Directory koristi DNS;
- opišete kako se objekti imenuju u servisu Active Directory;
- opišete zadatke koji su potrebni za administriranje servisa Active Directory.

**Vreme predviđeno za lekciju: 20 minuta**

## Repliciranje

Korisnicima i servisima mora biti omogućeno pristupanje informacijama direktorijuma u svako doba sa svakog računara u stablu domena ili šumi. *Repliciranje* obezbeđuje da se izmene jednog kontrolera domena reflektuju na sve kontrolere domena u okviru domena. Informacije direktorijuma se repliciraju na kontrolerima domena kako unutar, tako i između lokacija.

### Koje informacije se repliciraju

Informacije uskladištene u direktorijumu (u datoteci Ntds.dit) su logički podeljene u četiri kategorije. Svaka od ovih kategorija informacija naziva se *particijom direktorijuma*. Particija direktorijuma se takođe naziva i *kontekst imenovanja*. Ove particije direktorijuma su jedinice repliciranja. Direktorijum sadrži sledeće particije:

- **Particija šeme** Ova particija definiše objekte koji se mogu napraviti u direktorijumu i atribute koje ti objekti mogu imati. Ovi podaci su zajednički za sve domene u šumi i repliciraju se na svim kontrolerima domena u šumi.
- **Particija konfiguracije** Ova particija opisuje logičku strukturu postavljanja, uključujući podatke kao što su struktura domena ili topologija repliciranja. Ovi podaci su zajednički za sve domene u šumi i repliciraju se na svim kontrolerima domena u šumi.

- **Particija domena** Ova particija opisuje sve objekte u jednom domenu. Ovi podaci pripadaju samo jednom domenu i ne repliciraju se drugim domenima. Međutim, podaci se repliciraju na svaki kontroler domena unutar tog domena.
- **Particija direktorijuma za aplikacije** Ova particija čuva dinamičke podatke koji se odnose na pojedinačne aplikacije u servisu Active Directory bez značajnog uticaja na performanse mreže tako što vam omogućava da kontrolišete područje repliciranja i smeštanje kopija. Particija direktorijuma za aplikacije može da sadrži bilo koji tip objekata osim principala bezbednosti (korisnici, grupe i računari). Podaci mogu biti eksplicitno preusmereni na kontrolere domena koje administrator odredi u okviru šume kako bi se izbegao nepotreban saobraćaj usled repliciranja, ili se može odrediti da se replicira sve na svim kontrolerima domena na isti način kao u particijama šeme, konfiguracije i domena.

Kontroler domena uskladištava i replicira:

- Podatke particije šeme za šumu.
- Podatke particije konfiguracije za sve domene u šumi.
- Podatke particije domena (sve objekte i svojstva direktorijuma) za svoj domen. Ovi podaci se repliciraju na dodatne kontrolere domena u domenu. U cilju nalaženja informacija, delimična kopija koja sadrži često korišćene atribute svih objekata u domenu replicira se u globalni katalog.

Globalni katalog uskladištava i replicira:

- Podatke particije šeme za šumu.
- Podatke particije konfiguracije za sve domene u šumi.
- Delimičnu repliku koja sadrži često korišćene atribute za sve objekte direktorijuma u šumi (repliciranje samo između servera globalnog kataloga).
- Potpunu repliku koja sadrži sve atribute svih objekata direktorijuma u domenu u kome je smešten globalni katalog.

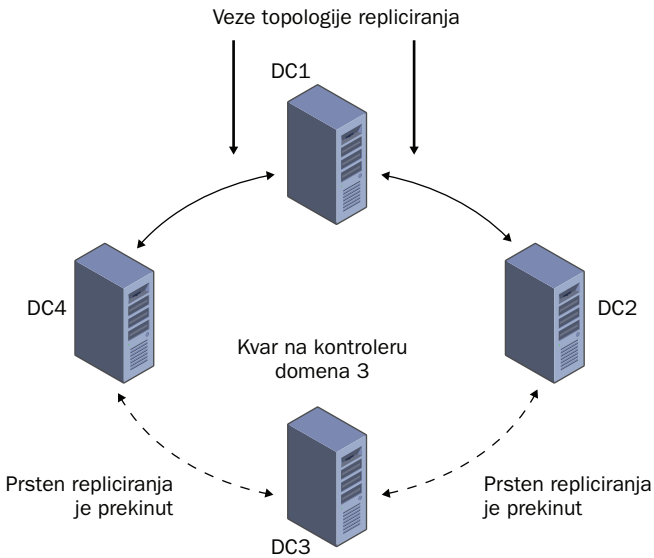
**Oprez** Proširenjima šeme u globalnom katalogu treba pristupati pažljivo. Proširenja šeme mogu imati katastrofalne efekte na velikim mrežama zato što se proširenja ne mogu obrisati (već samo onemogućiti) i zato što se stvara velika količina mrežnog saobraćaja, jer se proširenja sinhronizuju širom šume.

## Kako se informacije repliciraju

Active Directory replicira informacije na dva načina: *intrasajt* (unutar lokacije) i *intersajt* (između lokacija). Potreba za aktuelnim informacijama u direktorijumu balansirana je ograničenjima koja nameće raspoloživi propusni opseg mreže.

**Intrasajt repliciranje** Unutar lokacije, servis Windows Servera 2003 poznat kao *kontroler konzistentnosti znanja* (*knowledge consistency checker,* KCC) automatski generiše topologiju za repliciranje između kontrolera domena u istom domenu pomoću prstenaste strukture. KCC je ugrađeni proces koji se izvršava na svim kontrolerima domena. Topologija definiše putanju za ažuriranje direktorijuma koja teče od jednog do drugog kontrolera domena sve dok svi kontroleri domena na lokaciji ne prime ažurirane podatke direktorijuma. KCC odlučuje koji serveri su najpogodniji za međusobno repliciranje i određuje neke kontrolere domena kao partnere za repliciranje na bazi povezivosti, istorijata uspešnih replikacija i podudarnosti potpunih ili delimičnih replika. Kontroleri domena mogu imati više od jednog partnera za repliciranje. Zatim, KCC gradi objekte konekcije koji predstavljaju konekcije za repliciranje između partnera za repliciranje.

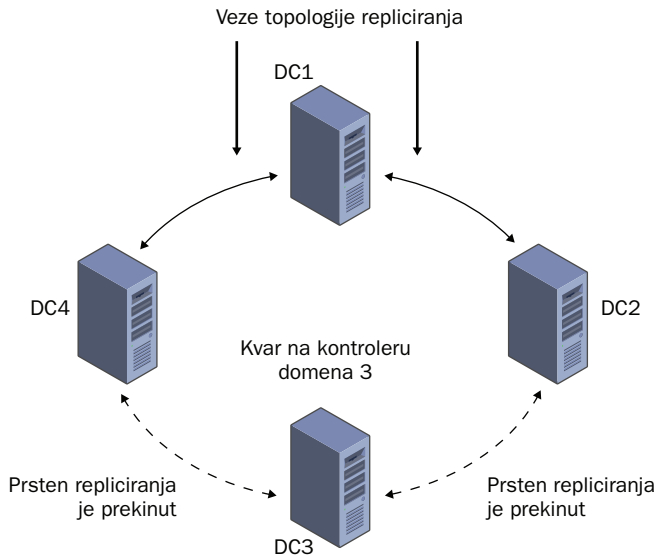
Prstenasta struktura obezbeđuje postojanje najmanje dve putanje repliciranja od jednog kontrolera domena do drugog; ako jedan kontroler domena privremeno ne radi, repliciranje se ipak nastavlja na svim drugim kontrolerima domena, kao što je prikazano na slici 1-10.




**Slika 1-10** Intrasajt topologija repliciranja

KCC analizira topologiju repliciranja unutar lokacije svakih 15 minuta kako bi potvrdio da i dalje funkcioniše. Ako dodate ili uklonite kontroler domena iz mreže ili sa lokacije, KCC ponovo konfiguriše topologiju tako da odražava novo stanje.

Kada se lokaciji doda više od sedam kontrolera domena, KCC pravi dodatne objekte konekcije preko prstenaste strukture tako da, ako se pojavi promena na nekom kontroleru domena, replikacijski partneri budu u mogućnosti da obezbede da nijedan kontroler domena ne bude više od tri skoka replikacije udaljen od drugoga, kao što je prikazano na slici 1-11. Ove konekcije za optimiziranje prave se slučajnim redosledom i ne moraju biti napravljene na svakom kontroleru domena.

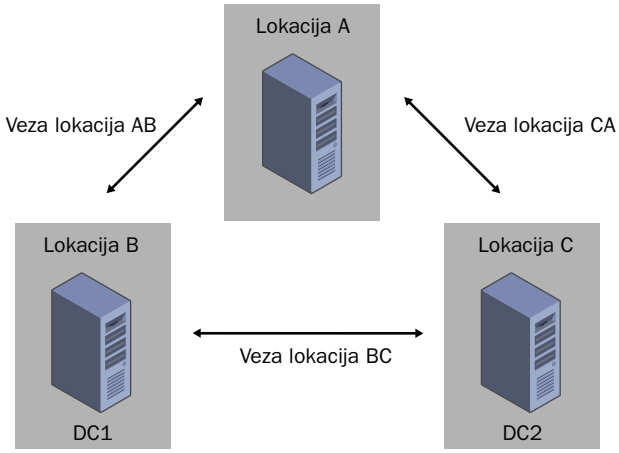



**Slika 1-11** Maksimalno tri skoka replikacije između kontrolera domena, zahvaljujući tome što je KCC dodao objekte konekcije.

**Intersajt repliciranje** Da biste obezbedili repliciranje između lokacija, morate ih manuelno povezati pravljenjem veza lokacija. Veze lokacija predstavljaju mrežne veze i omogućavaju repliciranje. Jedan kontroler KCC po lokaciji generiše sve veze između lokacija. Active Directory koristi informacije o povezanosti mreže za generisanje objekata konekcije koji omogućavaju efikasno repliciranje i otpornost na greške, kao što je prikazano na slici 1-12.

Vi obezbeđujete informacije o transportu repliciranja, ceni veze lokacija, vremenu u kome je veza na raspolaganju i koliko često bi vezu trebalo koristiti. Active Directory koristi te informacije za određivanje koja veza lokacija se koristi za repliciranje informacija. Prilagođavanje rasporeda repliciranja kako bi se repliciranje događalo u zadato vreme, na primer u vreme slabog mrežnog saobraćaja, čini replikaciju efikasnijom.

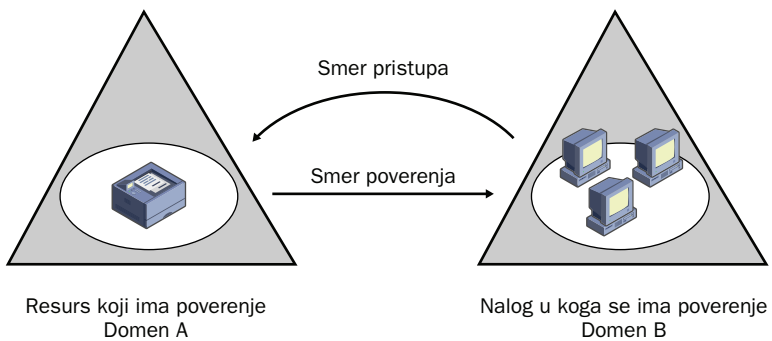
Kao administrator, morate konfigurisati lokacije i replikaciju kako biste obezbedili da najažurnije informacije budu korisnicima na raspolaganju. Repliciranje i konfiguracija veze lokacija detaljnije su obrađeni u poglavlju 5.




**Slika 1-12** Topologija intersajt repliciranja

## Odnosi poverenja

Odnos *poverenja* je veza između dva domena u kojoj domen koji ima poverenje priznaje proveru autentičnosti prijavljivanja iz domena u koji ima poverenje, kao što je prikazano na slici 1-13. Provera autentičnosti korisnika i aplikacija vrši se u familiji Windows Servera 2003 pomoću jednog protokola poverenja, ili pomoću dva: Kerberos verzija 5 ili NT LAN Manager (NTLM). Protokol Kerberos verzija 5 je podrazumevani protokol za računare na kojima se izvršava Windows Server 2003. Ako bilo koji računar koji učestvuje u transakciji ne podržava Kerberos verziju 5, koristi se protokol NTLM. Odnos poverenja je dozvoljen i sa svakim područjem MIT Kerberos verzije 5. Odnos poverenja čine dva domena – domen koji ima poverenje i domen u koga se ima poverenje.




**Slika 1-13** Domeni koji poklanjaju i imaju poverenje povezani jednosmernim poverenjem

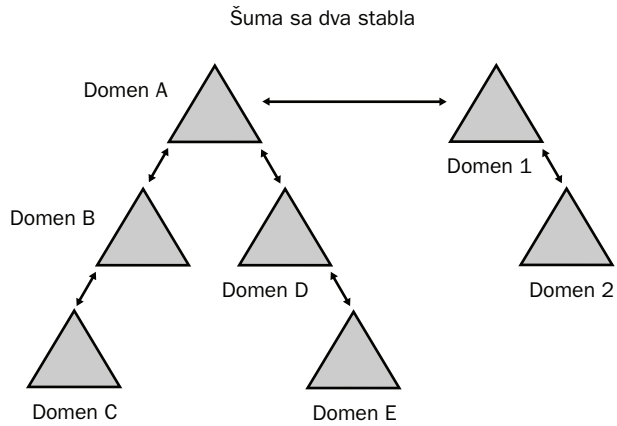
Poverenja imaju sledeće karakteristike:

- **Metod pravljenja** Poverenja se mogu praviti manuelno (eksplicitno) ili automatski (implicitno). Ne mogu se sva poverenja napraviti na oba načina.
- **Tranzitivnost** Poverenja mogu biti nevezana za domene koji su u odnosu poverenja (tranzitivna) ili vezana za njih (netranzitivna). Na primer, tranzitivno poverenje znači da ako domen A ima poverenje u domen B, i domen B ima poverenje u domen C, onda domen A ima poverenje u domen C. Slično tome, netranzitivno poverenje znači da ako domen A ima poverenje u domen B, a domen B ima poverenje u domen C, nema odnosa poverenja između domena A i C.
- **Smer** Poverenja mogu biti jednosmerna ili dvosmerna. Jednosmerno poverenje je jednostruki odnos poverenja u kome domen A ima poverenje u domen B, kao što je prikazano na slici 1-13. Jednosmerni odnos može biti netranzitivan ili tranzitivan zavisno od tipa poverenja koje se pravi. U dvosmernom poverenju, domen A ima poverenje u domen B i domen B ima poverenje u domen A. To znači da zahtevi za proveru autentičnosti mogu da se prenose između dva domena u oba smera.

U familiji Windows Server 2003, Active Directory podržava sledeće oblike odnosa poverenja:

- **Poverenje na nivou korena stabala** *Poverenje na nivou korena stabala* (engl. *tree-root trust*) pravi se implicitno kada šumi dodate nov osnovni domen stabla. Na primer, na slici 1-14 napravljeno je poverenje na nivou korena stabala između domena A i domena 1 kada je domen 1, novi koreni domen stabla, dodat šumi. Poverenje se pravi između domena koji ste napravili (novog koren stabla) i postojećeg osnovnog domena šume. Poverenje na nivou korena stabala može se uspostaviti samo između korenova dva stabla u istoj šumi. Poverenje je tranzitivno i dvosmerno.
- **Poverenje roditelj-dete** *Poverenje roditelj-dete* (engl. *parent-child trust*) se implicitno zasniva kada napravite nov podređeni domen u stablu. Na primer, na slici 1-14, ustanovljeno je poverenje nadređenog i podređenog domena između domena 1 i domena 2 kada je domen 2, novi podređeni domen, dodat stablu. Instalacioni proces servisa Active Directory automatski pravi odnos poverenja između novog domena i domena koji mu neposredno prethodi u hijerarhiji prostora imena (na primer, *uk.microsoft.com* je napravljen kao podređen domenu *microsoft.com*). Kao rezultat toga, za domen koji se priključuje stablu odmah se ustanovljavaju odnosi poverenja sa svakim domenom u stablu. Ovi odnosi poverenja stavljaju sve objekte u domenima stabla na raspolaganje svim drugim domenima u stablu. Poverenje je tranzitivno i dvosmerno.
- **Prečica poverenja** *Prečica poverenja* (engl. *shortcut trust*) mora biti eksplicitno napravljena od strane administratora sistema između dva domena u šumi. Ovo poverenje se koristi za poboljšanje vremena potrebnog za prijavljivanje korisnika, koje može biti predugo kada su dva domena

međusobno logički udaljena u hijerarhiji šume ili stabla. Poverenje je tranzitivno, a može biti jednosmerno ili dvosmerno.




**Slika 1-14** Struktura domena prikazuje poverenja osnova stabala i nadređenog i podređenog domena.

- **Spoljni odnos poverenja** *Spoljni odnos poverenja* (engl. *external trust*) administrator sistema mora eksplicitno da napravi između domena Windows Server 2003 koji se nalaze u različitim šumama, ili između domena Windows Server 2003 i domena čiji kontroleri domena rade pod Windowsom NT 4 ili ranijim verzijama. Ovo poverenje se može koristiti kada korisnicima treba pristup resursima smeštenim u Windows NT 4 domenu ili u domenu smeštenom u zasebnoj šumi koji se ne mogu povezati poverenjem šume. Poverenje je netranzitivno, a može biti jednosmerno ili dvosmerno.
- **Odnos poverenje šume** *Odnos poverenja šume* (engl. *forest trust*) administrator sistema mora eksplicitno da napravi između dva osnovna domena šume. Ovo poverenje omogućava svim domenima u jednoj šumi da imaju tranzitivno poverenje u sve domene u drugoj šumi. Poverenje šume nije tranzitivno na tri ili više šuma. Na primer, šuma A ima poverenje u šumu B, a šuma B ima poverenje u šumu C. Nema odnosa poverenja između šume A i šume C. Poverenje je tranzitivno samo između dve šume, a može biti jednosmerno ili dvosmerno. Poverenja šume su na raspolaganju samo kada je šuma na funkcionalnom nivou Windows Server 2003.
- **Poverenja u području** *Poverenje u području* (engl. *realm trust*) administrator sistema mora eksplicitno da napravi između područja van Windows Kerberosa i domena Windows Server 2003. Ovo poverenje obezbeđuje kompatibilnost između domena Windows Server 2003 i svakog područja upotrebljenog u primenama verzije 5 Kerberosa. Poverenje može biti tranzitivno ili netranzitivno i jednosmerno ili dvosmerno.

Kao administrator, morate planirati odnose poverenja kako biste korisnicima dali pristup resursima koji su im potrebni. Detalje o planiranju odnosa poverenja pročitajte u poglavlju 4.

## Upravljanje promenama i konfigurisanjem

Upravljanje promenama i konfigurisanjem je skup funkcija Windows Servera 2003 koje pojednostavljuju zadatke upravljanja kao što su:

- Upravljanje konfiguracijom radne površine svakog korisnika.
- Upravljanje načinom primene i instaliranja softvera na personalnim računarima kako bi se obezbedilo da korisnici imaju softver koji im je potreban za obavljanje posla.
- Instaliranje inicijalnog operativnog sistema na nov računar.
- Zamenjivanje računara.

Upravljanje promenama i konfigurisanjem uključuje funkcije upravljanja korisničkim podacima, instaliranje i održavanje softvera, upravljanje korisničkim parametrima i upravljanje računarskim parametrima, koje su poznate pod zajedničkim imenom tehnologije upravljanja IntelliMirror. Upravljanje promenama i konfigurisanjem takođe uključuje tehnologije instaliranja udaljenog operativnog sistema (OS).

### Odlike upravljanja promenama i konfigurisanjem

Tehnologije upravljanja IntelliMirror mogu se ovako opisati:

- **Upravljanje korisničkim podacima** Podaci i dokumenti prate korisnike kako bi mogli da pristupe podacima potrebnim za obavljanje posla. Tehnologije koje se koriste uključuju Active Directory, grupnu politiku, oflajn datoteke, upravljača sinhronizacije, kvote diska i putujuće korisničke profile.
- **Instaliranje i održavanje softvera** Softver prati korisnike kako bi mogli imati softver koji im treba za obavljanje posla. Tehnologije koje se koriste uključuju Active Directory, grupnu politiku, Windows Installer i Add/Remove Programs iz kontrolnog panela.
- **Upravljanje korisničkim parametrima** Korisnički parametri prate korisnike tako da mogu da vide raspored radne površine kakav su postavili. Tehnologije koje se koriste uključuju Active Directory i putujuće korisničke profile.
- **Upravljanje računarskim parametrima** Administratori mogu da definišu kako su računari prilagođeni i ograničeni na mreži. Tehnologije koje se koriste uključuju korisničke i računarske naloge servisa Active Directory i grupnu politiku.
- **Usluge udaljenog instaliranja** Administratori mogu da omoguće udaljeno instaliranje Microsoft Windowsa XP; Windows Servera 2003, Standard Edition; Windows Servera 2003, Enterprise Edition; Microsoft Windowsa 2000 Professional; Microsoft Windows 2000 Servera; i Windows 2000 Advanced Servera na novim ili zamenjenim računarima bez predinstaliranja ili tehničke podrške na licu mesta. Tehnologije koje se koriste uključuju Active Directory, grupnu politiku i usluge udaljenog instaliranja.

*IntelliMirror* je skup funkcija Windowsa 2000 koje pomažu pri upravljanju korisničkim i računarskim informacijama, podešavanjima i aplikacijama. Kada

se IntelliMirror koristi i na serveru i na klijentu, korisnički podaci, aplikacije i parametri prate korisnika kada pređe na drugi računar. IntelliMirror koristi Active Directory i grupnu politiku za upravljanje radnim površinama korisnika na osnovu njihovih poslovnih uloga, pripadnosti grupama i lokacijama. Možete konfigurisati radne površine tako da zadovolje zahteve novog korisnika svaki put kada se korisnik prijavi na mrežu.

## Grupne politike

*Grupne politike* su zbirke korisničkih i računarskih parametara konfiguracije koji se mogu povezati sa računarima, lokacijama, domenima i organizacionim jedinicama da bi odredili ponašanje radne površine korisnika. Na primer, korišćenjem grupnih politika možete postaviti koji programi će korisniku biti na raspolaganju, koji programi će se pojaviti na radnoj površini i opcije menija Start.

Da biste napravili određenu konfiguraciju radne površine za konkretnu grupu korisnika, napravićete objekte grupne politike (*Group Policy Object*, GPO). GPO je zbirka podešavanja grupne politike. Svaki računar koji radi pod Windows Serverom 2003 ima jedan lokalni GPO, a povrh toga može biti podložan raznim nelokalnim GPO-ima (baziranim na servisu Active Directory). Nelokalni GPO-i preklapaju lokalne. Nelokalni GPO-i su povezani sa objektima servisa Active Directory (lokacijama, domenima ili organizacionim jedinicama). Nelokalni GPO-i mogu biti primenjeni ili na korisnike (nezavisno od toga na kom računaru su prijavljeni) ili računare (nezavisno od toga ko je na njima prijavljen). U skladu sa svojstvima nasleđivanja u servisu Active Directory, nelokalni GPO-i se primenjuju hijerarhijski od najmanje restriktivne grupe (lokacije) do najrestriktivnije grupe (OU), i kumulativni su.

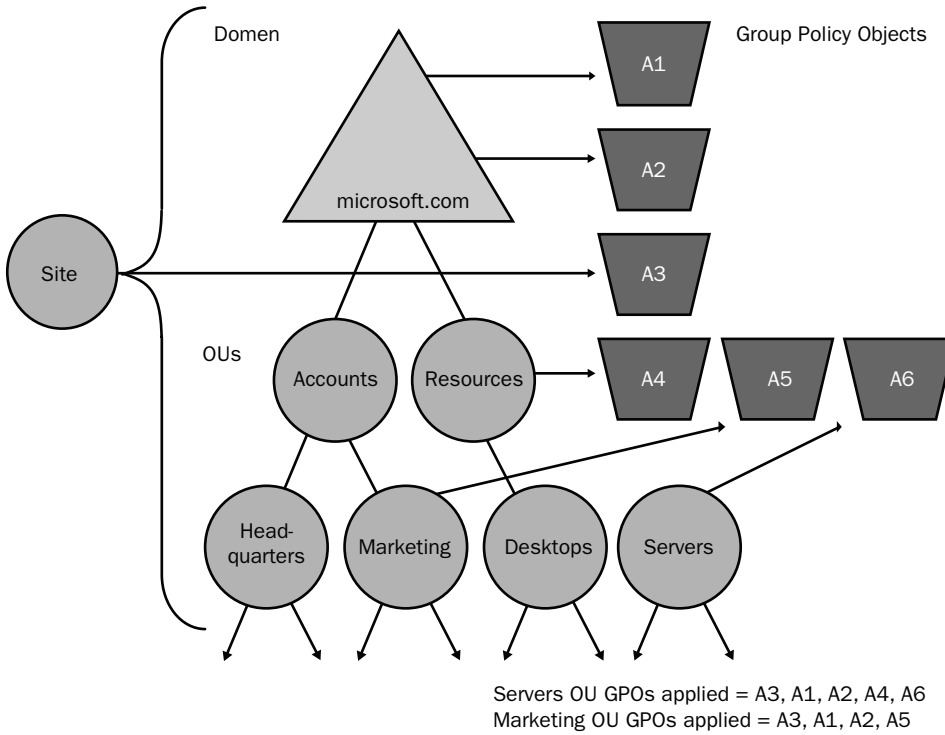
### Kako se GPO-i primenjuju

Budući da se nelokalni GPO-i primenjuju hijerarhijski, korisnikova ili računarova konfiguracija je rezultat GPO-a povezanih sa njihovom lokacijom, domenom i OU. GPO-i se primenjuju sledećim redosledom:

1. **Lokalni GPO** Svaki server pod Windows Serverom 2003 ima tačno jedan GPO koji je lokalno uskladišten.
2. **GPO-i povezani sa lokacijama** GPO-i koji su povezani sa lokacijom su sledeći na redu za primenjivanje. Primenjivanje GPO-a je sinhrono; administrator određuje redosled GPO-a povezanih sa lokacijom.
3. **GPO-i povezani sa domenima** GPO-i koji su povezani sa više domena primenjuju se sinhrono; administrator određuje redosled GPO-a povezanih sa domenom.
4. **GPO-i povezani sa OU** Prvo se primenjuju GPO-i povezani sa organizacionom jedinicom koja je najviša u hijerarhiji servisa Active Directory, zatim GPO-i koji su povezani sa podređenom OU, i tako dalje. Na kraju se primenjuju GPO-i povezani sa OU koja sadrži korisnika ili računar. Na nivou svake

OU u hijerarhiji servisa Active Directory može biti povezan jedan, više ili nijedan GPO. Ako je nekoliko grupnih politika povezano sa nekom OU, one se primenjuju sinhrono, redosledom koji odredi administrator.

Slika 1-15 prikazuje kako se grupna politika primenjuje na primeru organizacionih jedinica Marketing i Servers.




**Slika 1-15** Kako se primenjuje grupna politika

Podrazumevani redosled procesiranja parametara grupne politike može biti izmenjen uvođenjem izuzetaka ako je računar član radne grupe ili ako se za neki GPO pozovu parametri No Override, Block Policy Inheritance ili Loopback.

*Čarobnjak Resultant Set of Policy (RSoP)* olakšava primenjivanje politike i rešavanje problema. Čarobnjak RSoP je mašina za upite koja radi u dva režima: režim evidentiranja i režim planiranja. U režimu evidentiranja, čarobnjak ispituje postojeće politike i aplikacije povezane sa određenim korisnikom ili računarom, a zatim daje rezultate upita. U režimu planiranja, čarobnjak postavlja pitanja o planiranoj primeni politike, a zatim, izveštava o rezultatima upita.

Kao administrator, morate biti u stanju da administrirate grupnu politiku kako biste korisnicima obezbedili pristup resursima koji su im potrebni. Detalje o administriranju grupne politike naći ćete u poglavljima 10, 11 i 12.

## DNS

*DNS* je servis koji se koristi u TCP/IP mrežama, kao što je Internet, za lociranje računara i usluga pomoću lako čitljivih imena. DNS obezbeđuje metod imenovanja računara i mrežnih usluga pomoću hijerarhije domena. Kada korisnik unese lako čitljivo DNS ime u aplikaciju, DNS servisi mogu da razreše to ime u niz drugih informacija koje su sa njim povezane, kao što je IP adresa. Na primer, većini korisnika koji žele da lociraju računar na mreži lako je da zapamte i nauče ime kao što je *example.microsoft.com*. Međutim, računari komuniciraju preko mreže pomoću numeričkih adresa. DNS obezbeđuje način da se lako čitljivo ime računara ili usluge mapira u formi njegove numeričke adrese. Ako ste koristili pretraživač Weba, koristili ste DNS.

Active Directory koristi DNS kao servis za imenovanje i lociranje domena. DNS ima sledeće prednosti:

- DNS imena su lako čitljiva, što znači da ih je lakše zapamtiti nego IP adrese.
- DNS imena su postojanija nego IP adrese. IP adresa nekog servera može da se menja, ali ime servera ostaje isto.
- DNS omogućava korisnicima da se povežu sa lokalnim serverima pomoću istih konvencija za imenovanje koje koristi i Internet.

**Videti takođe** Da biste saznali više o DNS-u, pokrenite mašinu za pretraživanje na Internetu i uradite pretraživanje na RFC 1034 i RFC 1035. Zahtevi za komentarom (RFC) su zvanični dokumenti IETF-a (*Internet Engineering Task Force*) u kojima su detaljno opisane nove internetske specifikacije ili protokoli. RFC 1034 nosi ime „Domain Names – Concepts and Facilities", a RFC 1035 „Domain Name – Implementation and Specification."

## Imenovanje objekata

Budući da je Active Directory servis direktorijuma koji podržava LDAP, klijenti mreže koriste LDAP za zadavanje upita bazi podataka Active Directory. Svaki objekat u servisu Active Directory identifikuje se po imenu, a LDAP standardi određuju kako će objekti biti imenovani. Active Directory koristi niz konvencija za imenovanje objekata: karakteristična imena, relativna karakteristična imena, globalno jedinstvene identifikatore i glavna korisnička imena.

**Videti takođe** Da biste saznali više o LDAP-u, pokrenite mašinu za pretraživanje na Internetu i uradite pretraživanje na RFC 1779, RFC 2247 i RFC 2251. RFC 1779 nosi naziv „A String Representation of Distinguished Names," RFC 2247 „Using Domains in LDAP/X.500 Distinguished Names," a RFC 2251 „Lightweight Directory Access Protocol (v3)."

### Karakteristično ime

Svaki objekat u servisu Active Directory ima *karakteristično ime (distinguished name,* DN*)* koje jedinstveno identifikuje objekat i sadrži informaciju koja je dovoljna za uzimanje objekta iz direktorijuma. DN uključuje ime domena koji sadrži objekat, kao i kompletnu putanju kroz hijerarhiju kontejnera do objekta. Na primer, sledeći DN identifikuje korisnički objekat Scott Cooper u domenu *microsoft.com*:

```
CN=Scott Cooper,OU=Promotions,OU=Marketing,DC=Microsoft,DC=Com
```

U DN-u se koriste tri LDAP skraćenice, CN, OU i DC, za atribut imenovanja. CN navodi obično ime objekta, OU ime organizacione jedinice, a DC ime komponente domena. DN mora biti jedinstven, jer Active Directory ne dozvoljava duplikate DN-a.

### Relativno karakteristično ime

Active Directory podržava upite po atributima, tako da objekat možete locirati čak i ako je tačno DN ime nepoznato ili promenjeno. *Relativno karakteristično ime (relative distinguished name,* RDN*)* objekta je deo imena koje je atribut samog objekta. U prethodnom primeru, RDN za korisnički objekat Scott Cooper je Scott Cooper. RDN nadređenog objekta je Promotions.

**Napomena** Active Directory ne prikazuje LDAP skraćenice za atribute imenovanja CN (obično ime), OU (organizaciona jedinica) i DC (komponenta domena). Te skraćenice su ovde prikazane samo kao ilustracija načina na koji LDAP prepoznaje delove karakterističnog imena. Većina alatki servisa Active Directory prikazuje imena objekata u kanoničkoj formi, koja navodi RDN od osnove, a DNS ime domena nadole.

### Globalno jedinstveni identifikator

*Globalno jedinstveni identifikator (globally unique identifier,* GUID*)* je 128-bitni heksadecimalni broj koji je garantovano jedinstven unutar preduzeća. GUID brojevi se dodeljuju objektima pri njihovom pravljenju. GUID se nikada ne menja, čak ni kada premestite ili preimenujete objekat. Aplikacije mogu da uskladište GUID nekog objekta i da ga koriste za uzimanje tog objekta bez obzira na njegovo aktuelno DN ime.

U Windowsu NT svaki resurs domena bio je povezan sa bezbednosnim identifikatorom (SID) koji se generisao unutar domena. To znači da je SID bio garantovano jedinstven samo unutar domena. GUID je jedinstven u svim domenima, što znači da možete da premeštate objekte iz domena u domen, a da oni i dalje imaju jedinstveni identifikator.

### Glavno korisničko ime

Svaki korisnički nalog ima „prijateljsko" ime, poznato kao *glavno korisničko ime (user principal name,* UPN*)*. UPN se sastoji od imena korisničkog naloga (koje se ponekad naziva *korisničko ime za prijavljivanje*) i imena domena koje identifikuje domen u kome se korisnički nalog nalazi. Na primer, korisnički objekat Scott Cooper u stablu *microsoft.com* može imati UPN *ScottC@microsoft.com* (sastavljeno od punog ličnog imena i prvog slova prezimena).

## Administrativni zadaci servisa Active Directory

Administriranje servisa Active Directory Windows Servera 2003 uključuje kako konfigurisanje, tako i svakodnevne zadatke održavanja. Administrativni zadaci mogu biti grupisani u kategorije koje su opisane u tabeli 1-1. Te administrativne kategorije grubo odgovaraju poglavljima u ovom kompletu za obuku.

**Tabela 1-1 Administrativni zadaci servisa Active Directory**

| Administrativna kategorija | Konkretni zadaci |
|---|---|
| Planiranje dizajna infrastrukture servisa Active Directory | Oformiti dizajnerski tim. Analizirati poslovno i tehničko okruženje. Napraviti plan šume. Napraviti plan domena. Napraviti plan OU. Napraviti plan topologije lokacije. |
| Instaliranje i konfigurisanje servisa Active Directory | Prikupiti informacije pre instaliranja. Instalirati Active Directory. Verifikovati instalaciju Active Directory. Ukloniti Active Directory. Upotrebiti alatke za proveravanje ispravnosti instalacije servisa Active Directory. |
| Administriranje servisa Active Directory | Upotrebiti administrativne alatke Active Directory. Upotrebiti i prilagoditi Microsoftove upravljačke konzole (MMC). Napraviti rezervnu kopiju i obnoviti Active Directory. |
| Instaliranje i upravljanje domenima, stablima i šumama | Planirati i napraviti dodatne domene, stabla i šume. Preneti glavnu ulogu za operaciju. Preuzeti glavnu ulogu za operaciju. Planirati i primeniti odnose poverenja. |
| Konfigurisanje lokacija i upravljanje repliciranjem | Planirati, napraviti i konfigurisati lokacije. Konfigurisati intersajt repliciranje. Konfigurisati servere globalnog kataloga. Upotrebiti alatke za rukovanje, praćenje i proveravanje repliciranja. |
| Primenjivanje strukture OU | Planirati, napraviti i upravljati strukturom OU. |
| Administriranje korisničkih naloga | Napraviti korisničke naloge, korisničke profile i matične direktorijume. Održavati korisničke naloge. |
| Administriranje grupnih naloga | Planirati, napraviti i rukovati grupnim nalozima. |

**Tabela 1-1 Administrativni zadaci servisa Active Directory (nastavak)**

| Administrativna kategorija | Konkretni zadaci |
|---|---|
| Administriranje objekata servisa Active Directory | Locirati objekte servisa Active Directory. Publikovati resurse u servisu Active Directory. Kontrolisati pristup objektima Active Directory. Delegirati administrativnu kontrolu nad objektima Active Directory. Premestiti objekte Active Directory. Upotrebiti skriptovanje za rukovanje objektima Active Directory. |
| Primenjivanje grupne politike | Planirati i napraviti GPO-e. Povezati GPO-e sa lokacijama, domenima i organizacionim jedinicama. |
| Administriranje grupne politike | Upotrebiti čarobnjaka RsoP za proveravanje rezultata GPO-a. Preusmeriti specijalne omotnice sa grupnom politikom. Upotrebiti alate za upravljanje i proveravanje grupne politike. |
| Postavljanje softvera pomoću grupne politike | Staviti softver u pogon pomoću grupne politike. Pustiti noviju verziju softvera ili bezbednosnu zakrpu u rad pomoću grupne politike. Upotrebiti alatke za upravljanje i proveravanje aktiviranog softvera. |
| Administriranje bezbednosti servisa Active Directory | Primeniti politiku restrikcije softvera. Primeniti politiku praćenja za evidentiranje bezbednosnih događaja. Administrirati bezbednosni dnevnik i pregledati bezbednosne događaje. Rukovati bezbednosnim šablonima. Upotrebiti alatke za konfigurisanje i analizu bezbednosti za analiziranje bezbednosti sistema. |
| Upravljanje performansama servisa Active Directory | Upotrebiti alatke za praćenje performansi servisa Active Directory za praćenje performansi servisa Active Directory. Optimizovanje i proveravanje performansi servisa Active Directory. |

## Obnavljanje lekcije

Pitanja koja slede imaju za cilj da ponove ključne informacije koje su prezentirane u ovoj lekciji. Ako ne umete da odgovorite na neko pitanje, ponovo proučite lekciju, a zatim, pokušajte da odgovorite na to pitanje. Odgovori na pitanja mogu se naći u odeljku „Pitanja i odgovori” na kraju ovog poglavlja.

**1.** Navedite četiri particije direktorijuma u bazi podataka Active Directory.

_____

_____

2. Šta je funkcija KCC-a?

_____

_____

3. Navedite šest tipova odnosa poverenja koji se koriste u servisu Active Directory.

_____

_____

4. Šta je upravljanje promenama i konfigurisanjem? Šta je IntelliMirror?

_____

_____

5. Objasnite funkciju grupnih politika.

_____

_____

6. Definišite svako od sledećih imena: DN, RDN, GUID, UPN.

_____

_____

## Pregled lekcije

- Informacije skladištene u direktorijumu su logički particionirane u četiri jedinice repliciranja u sledećim participama: particija šeme, particija konfiguracije, particija domena i particija aplikacije.
- Active Directory replicira informacije na dva načina: intrasajt (unutar lokacije) i intersajt (između lokacija).
- Odnos poverenja je veza između dva domena, u kojoj domen koji ima poverenje priznaje proveru autentičnosti prijavljivanja iz domena u koji ima poverenje. Windows Server 2003 podržava sledeće odnose poverenja: poverenje na nivou korena stabala, poverenje roditelj-dete, prečice poverenja, spoljni odnos poverenja, poverenje šume i poverenje u području.
- Grupne politike su kolekcije korisničkih i računarskih parametara konfiguracije koji se mogu povezati sa računarima, lokacijama, domenima i organizacionim jedinicama da bi odredili ponašanje radne površine korisnika. GPO je kolekcija parametara grupne politike.
- DNS je servis koji koriste TCP/IP mreže, kao što je Internet, za lociranje računara i usluga pomoću lako čitljivih imena. Active Directory koristi DNS kao servis za imenovanje i lociranje domena.